Aggiornare utilizzando ARL

Upgrade controllers

NetApp
February 10, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap-systems-upgrade/upgrade-arl/index.html on February 10, 2026. Always check docs.netapp.com for the latest.

Sommario

Aggiornare utilizzando ARL . . . 1
Inizia da qui: Scegli la tua procedura di aggiornamento ARL . . . 1
Utilizzare i comandi "sostituzione controller di sistema" con ONTAP 9.15,1 o versione successiva . . . 1
Aggiornare i modelli di controller nello stesso chassis . . . 1
Utilizzare i comandi "System controller REPLACE" con ONTAP 9.8 o versioni successive . . . 2
Utilizzare i comandi "System controller REPLACE" con ONTAP 9 9,7 . . . 3
Utilizzare i comandi ARL manuali . . . 3
Utilizzare i comandi "sostituzione controller di sistema" per aggiornare l'hardware del controller introdotto in ONTAP 9.15.1 e versioni successive . . . 4
Scopri di più sulla procedura di aggiornamento ARL . . . 4
Automatizzare il processo di aggiornamento del controller . . . 6
Decidere se utilizzare questa procedura di ricollocazione aggregata . . . 6
Strumenti e documentazione richiesti . . . 8
Linee guida per l'aggiornamento dei controller con ARL . . . 8
Scopri la sequenza di aggiornamento ARL . . . 9
Fase 1. Preparatevi per l'aggiornamento . . . 11
Fase 2. Spostare e dismettere il node1 . . . 16
Fase 3. Installazione e boot node3 . . . 20
Fase 4. Spostare e dismettere il node2 . . . 40
Fase 5. Installazione e boot node4 . . . 42
Fase 6. Completare l'aggiornamento . . . 63
Risolvere i problemi . . . 69
Riferimenti . . . 76
Utilizzare i comandi "System controller replace" per aggiornare i modelli di controller nello stesso chassis . . . 77
Scopri di più sulla procedura di aggiornamento ARL . . . 77
Decidere se utilizzare questa procedura di ricollocazione aggregata . . . 79
Strumenti e documentazione richiesti . . . 81
Linee guida per l'aggiornamento dei controller . . . 82
Scopri la sequenza di aggiornamento ARL . . . 82
Fase 1. Preparatevi per l'aggiornamento . . . 85
Fase 2. Spostare le risorse e dismettere il node1 . . . 90
Fase 3. Fare il boot node1 con i moduli di sistema sostitutivi . . . 113
Fase 4. Spostare le risorse e dismettere il node2 . . . 125
Fase 5. Installare i moduli di sistema sostitutivi sul nodo 2 . . . 128
Fase 6. Fare il boot node2 con i moduli di sistema sostitutivi . . . 139
Fase 7. Completare l'aggiornamento . . . 156
Risolvere i problemi . . . 163
Riferimenti . . . 169
Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller con ONTAP 9.8 o versione successiva . . . 171
Scopri di più sulla procedura di aggiornamento ARL . . . 171
Automatizzare il processo di aggiornamento del controller . . . 172
Decidere se utilizzare questa procedura di ricollocazione aggregata . . . 173

Strumenti e documentazione richiesti . . . 175
Linee guida per l'aggiornamento dei controller con ARL . . . 175
Verificare lo stato della configurazione MetroCluster . . . 177
Verificare la presenza di errori di configurazione MetroCluster . . . 178
Verificare lo switchover, la riparazione e lo switchback . . . 178
Scopri la sequenza di aggiornamento ARL . . . 178
Fase 1. Preparatevi per l'aggiornamento . . . 180
Fase 2. Spostare e dismettere il node1 . . . 186
Fase 3. Installazione e boot node3 . . . 189
Fase 4. Spostare e dismettere il node2 . . . 217
Fase 5. Installazione e boot node4 . . . 219
Fase 6. Completare l'aggiornamento . . . 248
Risolvere i problemi . . . 254
Riferimenti . . . 261
Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller che esegue ONTAP 9.5 a 9.7 . . . 263
Scopri di più sulla procedura di aggiornamento ARL . . . 263
Automatizzare il processo di aggiornamento del controller . . . 264
Decidere se utilizzare questa procedura di ricollocazione aggregata . . . 264
Strumenti e documentazione richiesti . . . 266
Linee guida per l'aggiornamento dei controller con ARL . . . 266
Verificare lo stato della configurazione MetroCluster . . . 268
Verificare la presenza di errori di configurazione MetroCluster . . . 269
Verificare lo switchover, la riparazione e lo switchback . . . 269
Scopri la sequenza di aggiornamento ARL . . . 269
Fase 1. Preparatevi per l'aggiornamento . . . 271
Fase 2. Spostare e dismettere il node1 . . . 276
Fase 3. Installazione e boot node3 . . . 281
Fase 4. Spostare e dismettere il node2 . . . 306
Fase 5. Installazione e boot node4 . . . 309
Fase 6. Completare l'aggiornamento . . . 334
Risolvere i problemi . . . 341
Riferimenti . . . 348
Aggiornare manualmente l'hardware del controller con ONTAP 9.8 o versione successiva . . . 350
Scopri di più sulla procedura di aggiornamento ARL . . . 350
Decidere se utilizzare questa procedura di ricollocazione aggregata . . . 351
Workflow di upgrade ARL . . . 352
Linee guida per l'aggiornamento dei controller con ARL . . . 355
Strumenti e documentazione richiesti . . . 358
Foglio di lavoro: Informazioni da raccogliere prima e durante l'aggiornamento del controller . . . 358
Fase 1. Preparatevi per l'aggiornamento . . . 360
Fase 2. Spostare e dismettere il node1 . . . 381
Fase 3. Installazione e boot node3 . . . 395
Fase 4. Registrare le informazioni e dismettere il node2 . . . 430
Fase 5. Installazione e boot node4 . . . 435

Fase 6. Completare l’aggiornamento . . . 462
Risolvere i problemi . . . 468
Riferimenti . . . 474
Aggiornare manualmente l’hardware del controller con ONTAP 9.7 o versione precedente . . . 477
Scopri di più sulla procedura di aggiornamento ARL . . . 477
Decidere se utilizzare questa procedura di ricollocazione aggregata . . . 478
Workflow di upgrade ARL . . . 478
Linee guida per l’aggiornamento dei controller con ARL . . . 481
Strumenti e documentazione richiesti . . . 484
Foglio di lavoro: Informazioni da raccogliere prima e durante l’aggiornamento del controller . . . 485
Riconfigurare il layout dello switch FC per ONTAP 9.1 o versione successiva . . . 487
Fase 1. Preparatevi per l’aggiornamento . . . 491
Fase 2. Spostare e dismettere il node1 . . . 512
Fase 3. Installazione e boot node3 . . . 527
Fase 4. Registrare le informazioni e dismettere il node2 . . . 562
Fase 5. Installazione e boot node4 . . . 567
Fase 6. Completare l’aggiornamento . . . 596
Risolvere i problemi . . . 602
Riferimenti . . . 609

Aggiornare utilizzando ARL

Inizia da qui: Scegli la tua procedura di aggiornamento ARL

Puoi aggiornare l'hardware dei controller senza interruzioni utilizzando il trasferimento degli aggregati (ARL). Per altri metodi per aggiornare l'hardware del controller, vedere "Eseguire l'upgrade spostando volumi o storage".

Con ARL, potrai eseguire l'upgrade dell'hardware del controller senza interruzioni su una coppia di nodi con ONTAP e migrando gli aggregati non root dai nodi originali ai nuovi nodi dello stesso cluster. I dati ospitati sui nodi che vengono aggiornati sono accessibili durante l'aggiornamento.

ARL sfrutta la configurazione ha per consentirti di spostare la proprietà degli aggregati non root da un nodo a un altro, se condividono lo storage all'interno dello stesso cluster.

Esistono diversi metodi ARL per aggiornare l'hardware del controller. Per selezionare la procedura appropriata, consultare le seguenti informazioni sui sistemi e sulle versioni ONTAP supportate per ciascuna opzione di aggiornamento ARL.

Utilizzare i comandi "sostituzione controller di sistema" con ONTAP 9.15,1 o versione successiva

Se lo scenario di aggiornamento è elencato nella seguente tabella dei sistemi supportati, andare a "Utilizzare i comandi "sostituzione controller di sistema" per aggiornare l'hardware del controller introdotto in ONTAP 9.15.1 e versioni successive" per avviare la procedura di aggiornamento.

Mostra i sistemi supportati

Controller esistente	Controller sostitutivo	Supportato a partire da ONTAP…
AFF A400	AFF A50	9.16.1
AFF A300	AFF A50	9.16.1
AFF A220, AFF A150	AFF A20	9.16.1
AFF C400	AFF C60, AFF C80	9.16.1
FAS8200, FAS8300, FAS9000	FAS70, FAS90, FAS50	9.15.1P3 per FAS70, FAS90 9.16.1P2 per FAS50
FAS8700	FAS70, FAS90	9.15.1P3
FAS9500	FAS90	9.15.1P3
AFF A300, AFF A400, AFF A700	AFF A70, AFF A90, AFF A1K	9.15.1
AFF A900	AFF A90, AFF A1K	9.15.1

Aggiornare i modelli di controller nello stesso chassis

Se lo scenario di aggiornamento è elencato nella seguente matrice dei sistemi supportati, andare a"Utilizzare i comandi "System controller replace" per aggiornare i modelli di controller nello stesso chassis" per avviare la

procedura di aggiornamento.

Mostra i sistemi supportati

Vecchio sistema	Sistema sostitutivo	Versioni di ONTAP supportate
AFF C250	AFF C30, AFF C60	9.16.1 e versioni successive
AFF A250	AFF A50, AFF A30	9.16.1 e versioni successive
AFF C800	AFF C80	9.16.1 e versioni successive
AFF A800	AFF A70 o AFF A90	9.15.1 e versioni successive
AFF A220 configurato come ASA (All SAN Array)	ASA A150	9.13.1P1 e successivi
AFF A220	AFF A150	9.10.1P15, 9.11.1P11, 9.12.1P5 e versioni successive
AFF A200	AFF A150	9.10.1P15, 9.11.1P11 e successivi **Nota**: AFF A200 non supporta le versioni ONTAP successive alla 9.11.1.
AFF C190	AFF A150	9.10.1P15, 9.11.1P11, 9.12.1P5 e versioni successive
FAS2620	FAS2820	9.11.1P7 o versioni successive delle patch (FAS2620) **Nota**: FAS2620 non supporta le versioni ONTAP successive alla 9.11.1. 9.13.1 e versioni successive (FAS2820)
FAS2720	FAS2820	9.13.1 e versioni successive
AFF A700 configurato come ASA	ASA A900	9.13.1P1 e successivi
AFF A700	AFF A900	9.10.1P10, 9.11.1P6 e versioni successive
FAS9000	FAS9500	9.10.1P10, 9.11.1P6 e versioni successive

Utilizzare i comandi "System controller REPLACE" con ONTAP 9.8 o versioni successive

Se lo scenario di aggiornamento è elencato nella seguente tabella dei sistemi supportati, andare a "Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller con ONTAP 9.8 o versione successiva" per avviare la procedura di aggiornamento.

Mostra i sistemi supportati

Vecchio controller	Controller sostitutivo
FAS8020, FAS8040, FAS8060, FAS8080	FAS8200, FAS8300, FAS8700, FAS9000
FAS8060, FAS8080	FAS9500
AFF8020, AFF8040, AFF8060, AFF8080	AFF A300, AFF A400, AFF A700, AFF A800
AFF8060, AFF8080	AFF A900
FAS8200	FAS8300, FAS8700, FAS9000, FAS9500
FAS8300, FAS8700, FAS9000	FAS9500
AFF A300	AFF A400, AFF A700, AFF A800, AFF A900
AFF A320	AFF A400
AFF A400, AFF A700	AFF A900

Utilizzare i comandi "System controller REPLACE" con ONTAP 9 9,7

Se lo scenario di aggiornamento è elencato nella seguente tabella dei sistemi supportati, andare a "Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller che esegue ONTAP 9.5 a 9.7" per avviare la procedura di aggiornamento.

Mostra i sistemi supportati

Vecchio controller	Controller sostitutivo
FAS8020, FAS8040, FAS8060, FAS8080	FAS8200, FAS8300, FAS8700, FAS9000
AFF8020, AFF8040, AFF8060, AFF8080	AFF A300, AFF A400, AFF A700, AFF A800
FAS8200	FAS8700, FAS9000, FAS8300
AFF A300	AFF A700, AFF A800, AFF A400

Utilizzare i comandi ARL manuali

Se lo scenario di aggiornamento non è supportato utilizzando "comandi di sistema", è possibile eseguire un aggiornamento ARL utilizzando i comandi manuali.

Mostra i sistemi supportati

ONTAP 9.8 o successivo

Gli aggiornamenti manuali ARL sono supportati per i seguenti sistemi che eseguono ONTAP 9.8 e versioni successive:

- Dal sistema FAS al sistema FAS
- Dal sistema AFF al sistema AFF

  È possibile eseguire l'aggiornamento a un sistema sostitutivo della stessa serie:

  - Dal sistema AFF A-Series al sistema AFF A-Series
  - Da sistema AFF C-Series a sistema AFF C-Series
- Dal sistema ASA al sistema ASA

  > Gli aggiornamenti ASA a un sistema sostitutivo ASA R2 non sono supportati. Per informazioni sulla migrazione dei dati da ASA a ASA R2, vedere "Abilitare l'accesso ai dati dagli host SAN al sistema di storage ASA R2".

  È possibile eseguire l'aggiornamento a un sistema sostitutivo della stessa serie:

  - Dal sistema ASA A-Series al sistema ASA A-Series
  - Da sistema ASA C-Series a sistema ASA C-Series

"Aggiornare manualmente l'hardware del controller con ONTAP 9.8 o versione successiva"

ONTAP 9.7 o precedente

Gli aggiornamenti manuali ARL sono supportati per i seguenti sistemi che eseguono ONTAP 9.7 e versioni precedenti:

- Dal sistema FAS al sistema FAS
- Dal sistema AFF al sistema AFF

"Aggiornare manualmente l'hardware del controller con ONTAP 9.7 o versione precedente"

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

Scopri di più sulla procedura di aggiornamento ARL

Esistono diversi metodi di rilocazione aggregata (ARL) per aggiornare l'hardware del controller. Questa procedura ARL descrive come aggiornare una coppia di controller HA nei sistemi di storage AFF e FAS introdotti in ONTAP 9.15.1 o versioni successive con nuovi controller, mantenendo i dati e i dischi esistenti.

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. Devi anche leggere e comprendere il "linee guida per l'aggiornamento dei controller con ARL" e il "Sequenza di 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 introdotto in ONTAP 9.15.1 o versioni successive, ONTAP converte l'efficienza dello storage dei volumi esistenti 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.
  - Per i sistemi AFF A20, AFF A30, AFF A50, AFF A70, AFF A90, AFF A1K, AFF C30, AFF C60 e AFF C80, ONTAP converte l'efficienza dello storage di tutti i volumi con thin provisioning esistenti, inclusi quelli che non utilizzano l'efficienza dello storage.
  - Per un sistema FAS70 e FAS90, ONTAP converte solo l'efficienza dello storage dei volumi con thin provisioning esistenti che hanno ottenuto l'efficienza dello storage prima dell'upgrade.

  "Scopri di più sull'efficienza dello storage".
- I sistemi AFF A20, AFF A50, AFF A70, AFF A90, AFF A1K, FAS70 e FAS90 condividono 100GbE porte di rete per le connessioni in cluster e ha. Questi sistemi possono supportare connessioni cluster 10GbE o 25GbE a switch cluster legacy; tuttavia, NetApp consiglia di eseguire l'aggiornamento a velocità cluster 100GbE quando gli switch 10GbE e 25GbE non sono più necessari. Per ulteriori informazioni, vedere i seguenti articoli della Knowledge base:
  - "Come configurare porte cluster 10G o 25g in una nuova configurazione cluster"
  - "Come convertire le porte del cluster 10G o 25g esistenti in porte del cluster 40G o 100g"

Il sistema AFF A20 condivide le porte di rete 10GbE GbE e 25GbE GbE per le connessioni cluster e ha. Queste sono le uniche connessioni cluster di porte di rete supportate da un sistema AFF A20.

Se non è possibile collegare e0a o e0b porte cluster sul nodo esistente alle porte cluster sul nuovo nodo, vedere "ID bug online di NetApp CONTAP-166978".

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 questa procedura di ricollocazione aggregata

Esistono diversi metodi di rilocazione aggregata (ARL) per l'aggiornamento dell'hardware dei controller. Questa procedura ARL descrive come aggiornare una coppia di controller HA nei sistemi di storage AFF e FAS introdotti in ONTAP 9.15.1 o versioni successive con nuovi controller, mantenendo i dati e i dischi esistenti. Si tratta di una procedura complessa che dovrebbe essere utilizzata solo da amministratori ONTAP esperti.

Per aiutarti a decidere se questa procedura ARL è adatta all'aggiornamento hardware del tuo controller, dovresti esaminare tutte le seguenti circostanze per gli aggiornamenti supportati e non supportati.

Aggiornamenti supportati per questa procedura ARL

È possibile utilizzare questa procedura ARL per aggiornare una coppia di nodi nelle seguenti circostanze:

- Sul computer è in esecuzione 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 del volume.
- Si è esperti nell'amministrazione di ONTAP e si è soddisfatti dei rischi di lavorare in modalità privilegi diagnostici.
- La combinazione di aggiornamento hardware è elencata in matrice modello supportata .

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

Aggiornamenti non supportati per questa procedura ARL

Non è possibile utilizzare questa procedura ARL per aggiornare una coppia di nodi nelle seguenti circostanze:

- Si sta eseguendo uno dei seguenti aggiornamenti:

Controller esistente	Controller sostitutivo
AFF A250	AFF A50, AFF A30
AFF A800	AFF A70, AFF A90

Controller esistente	Controller sostitutivo
AFF C250	AFF C30, AFF C60
AFF C800	AFF C80

Per eseguire l'aggiornamento di un aggiornamento elencato nella tabella precedente, vedere il "Riferimenti"collegamento ai comandi *Use "System controller replace" (utilizza comandi di sostituzione del controller di sistema) per aggiornare i modelli di controller nello stesso chassis*.

- 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*.

Combinazioni di aggiornamento del sistema supportate

La tabella seguente mostra le combinazioni di aggiornamento del controller supportate tramite ARL per i sistemi AFF e FAS introdotti in ONTAP 9.15.1 o versioni successive. Se la combinazione di aggiornamento del controller non è elencata, contattare l'assistenza tecnica.

Controller esistente	Controller sostitutivo	Supportato a partire da ONTAP…
AFF A400	AFF A50 [2]	9.16.1
AFF A300	AFF A50 [2]	9.16.1
AFF A220, AFF A150	AFF A20 [2]	9.16.1 [1]
AFF C400	AFF C60, AFF C80	9.16.1
FAS8200, FAS8300, FAS9000	FAS70, FAS90, FAS50	9.15.1P3 per FAS70, FAS90 9.16.1P2 per FAS50
FAS8700	FAS70, FAS90	9.15.1P3
FAS9500	FAS90	9.15.1P3
AFF A300, AFF A400, AFF A700	AFF A70 [2] , AFF A90 [2], AFF A1K	9.15.1
AFF A900	AFF A90 [2], AFF A1K	9.15.1

[1] per eseguire l'aggiornamento a AFF A20, è necessario prima convertire un AFF A150 o AFF A220 in uno shelf DS224C sostituendo il modulo controller con un modulo IOM12. Vedere "Convertire un nodo originale in uno shelf di dischi".

[2] AFF A20, AFF A50, AFF A70 e AFF A90 sono sistemi integrati con due controller in una configurazione ha e dischi integrati in un unico chassis:

- Se si sta eseguendo l'aggiornamento a AFF A20, AFF A50, AFF A70 o AFF A90 con unità interne, è necessario rimuovere la proprietà di queste unità interne prima di eseguire l'aggiornamento. Dopo aver completato l'upgrade, puoi assegnare i dischi interni ai nodi AFF A20, AFF A50, AFF A70 o AFF A90 e utilizzarli per creare aggregati di dati. Non è necessario migrare aggregati root o di dati su dischi interni.
- Se si esegue l'aggiornamento a un AFF A20, AFF A50, AFF A70 o AFF A90 senza unità interne, non è necessario assegnare unità interne al termine dell'aggiornamento.

Scegli una procedura di aggiornamento hardware diversa

- "Esaminare i metodi ARL alternativi disponibili per l'aggiornamento dell'hardware del controller".
- 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*.

Informazioni correlate

Fare riferimento a "Riferimenti" per collegarsi alla *Documentazione 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, vedere"Risolvere i problemi" per maggiori informazioni e possibili soluzioni.

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

Scopri la sequenza di 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 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	Descrizione
"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

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. Se mancano dei dischi, fare riferimento al "Riferimenti"collegamento alla gestione *disco e aggregato con la CLI*, alla gestione *logica dello storage con la CLI* e alla gestione *coppia ha* 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

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 <aggregate_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
```

Sposta gli aggregati falliti o sottoposti a veto sul nodo 2

Se uno qualsiasi degli aggregati non riesce a essere riposizionato o viene sottoposto a veto, è necessario riposizionarlo manualmente sul nodo 2 oppure, se necessario, ignorare i veti o i controlli di destinazione.

A proposito di questa attività

Il sistema interrompe l'operazione di ricollocazione 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 <aggregate_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 <aggregate_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 <aggregate_list> -ndo-controller-upgrade true -override-vetoes true -override-destination-checks true`

Ritirare il node1

Per ritirare node1, è necessario riprendere l'operazione automatizzata per disabilitare la coppia HA con node2 e arrestare correttamente node1. Più avanti nella procedura, si rimuove 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

Dopo aver ritirato node1, verificare che sia spento e non connesso alla rete. Lasciare il vecchio hardware del nodo 1 in questo stato finché non si completa l'aggiornamento sia del nodo 1 che del nodo 2. È quindi possibile disattivare il nodo 1 durante"Fase 6. Completare l'aggiornamento" .

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

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.

Non ignorare il ritardo; se non si lascia caricare la batteria, si potrebbe verificare una 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`

Se DHCP (Dynamic host Configuration Protocol) è…	Quindi…
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. Avviare il nodo nel menu di avvio:

```
boot_ontap menu
```

26. Quando node3 si ferma al menu di avvio, riassegnare i dischi di node1 a node3 eseguendo il seguente comando su node3:

```
boot_after_controller_replacement
```

Dopo un breve intervallo di tempo, viene richiesto di inserire il nome del nodo da sostituire. Se sono presenti dischi condivisi (chiamati anche Advanced Disk Partitioning (ADP) o dischi partizionati), viene richiesto di inserire il nome del nodo del partner ha.

Questi prompt potrebbero essere interrati nei messaggi della console. Se non si immette un nome di nodo o non si immette un nome corretto, viene richiesto di inserire nuovamente il nome.

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>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner 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      ""           000000000000000002000000000000a008a81976
   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 i LIF spostati oppure migrare e modificare manualmente i LIF del nodo 1 che non sono riusciti a trasferirsi automaticamente nel nodo 3.

Ripristinare e ripristinare i LIF spostati

a. Elencare eventuali LIF spostati:

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

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

```
cluster controller-replacement network displaced-interface
restore-home-node -node <node3_nodename> -vserver <vserver name>
-lif-name <lif_name>
```

Migrare e modificare manualmente i LIF

a. Migrare i LIF che non sono riusciti a trasferirsi automaticamente al nodo 3:

```
network interface migrate -vserver <vserver name> -lif <lif_name>
-destination-node <node3_nodename> -destination-port
<port_on_node3>
```

b. Modificare il nodo home e la porta home per i LIF migrati:

```
network interface modify -vserver <vserver_name> -lif
<data_lif_name> -home-node <node3_nodename> -home-port
<home_port>
```

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

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 <aggregate_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
```

Sposta gli aggregati falliti o sottoposti a veto sul nodo 3

Se uno qualsiasi degli aggregati non riesce a essere riposizionato o viene sottoposto a veto, è necessario riposizionarlo manualmente sul nodo 3 oppure, se necessario, ignorare i veti o i controlli di destinazione.

A proposito di questa attività

Il sistema interrompe l'operazione di ricollocazione 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 <node2> -destination <node3>
-aggregate-list <aggregate_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 node2 -destination node3 -aggregate-list <aggregate_list> -ndo-controller-upgrade true -override-vetoes true`
Ignorare i controlli di destinazione	Utilizzare il seguente comando: `storage aggregate relocation start -node node2 -destination node3 -aggregate-list <aggregate_list> -ndo-controller-upgrade true -override-vetoes true -override-destination-checks true`

Andare in pensione node2

Per dismettere node2, è necessario arrestare node2 correttamente e quindi rimuoverlo dal rack o dallo chassis.

Fasi

1. Riprendere l'operazione:

   ```
   system controller replace resume
   ```

   Il nodo si arresta automaticamente.

Al termine

Dopo aver ritirato node2, verificare che sia spento e non connesso alla rete. Lasciare il vecchio hardware del nodo 2 in questo stato finché non si completa l'aggiornamento sia del nodo 1 che del nodo 2. È quindi possibile disattivare node2 durante"Fase 6. Completare l'aggiornamento" .

Fase 5. Installazione e boot 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 l'avvio di rete del nodo 4 se la versione ONTAP sul nodo 4 è diversa dalla versione ONTAP sul nodo 2. Dopo aver installato node4, avviarlo dall'immagine ONTAP 9 memorizzata sul server web. È quindi possibile scaricare i file corretti sul dispositivo di supporto di avvio per i successivi avvii del sistema seguendo le istruzioni 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.

   Cablare le seguenti connessioni, utilizzando le istruzioni contenute nelle *Istruzioni di installazione e configurazione* per la piattaforma node4, il documento appropriato sullo scaffale dei dischi e la *gestione delle coppie HA*.

   Fare riferimento a"Riferimenti" per collegarsi alla *gestione delle coppie HA*.

   - 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.

   Non ignorare il ritardo; se non si lascia caricare la batteria, si potrebbe verificare una 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`

Se DHCP (Dynamic host Configuration Protocol) è…	Quindi…
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. Avviare il nodo nel menu di avvio:

```
boot_ontap menu
```

26. Quando node4 si ferma al menu di avvio, riassegnare i dischi di node2 a node4 eseguendo il seguente comando su node4:

```
boot_after_controller_replacement
```

Dopo un breve intervallo di tempo, viene richiesto di inserire il nome del nodo da sostituire. Se sono presenti dischi condivisi (chiamati anche Advanced Disk Partitioning (ADP) o dischi partizionati), viene richiesto di inserire il nome del nodo del partner ha.

Questi prompt potrebbero essere interrati nei messaggi della console. Se non si immette un nome di nodo o non si immette un nome corretto, viene richiesto di inserire nuovamente il nome.

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>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner 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 i LIF spostati oppure migrare e modificare manualmente i LIF del nodo 2 che non sono riusciti a trasferirsi automaticamente nel nodo 4.

Ripristinare e ripristinare i LIF spostati

a. Elencare eventuali LIF spostati:

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

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

```
cluster controller-replacement network displaced-interface
restore-home-node -node <node4_nodename> -vserver <vserver name>
-lif-name <lif_name>
```

Migrare e modificare manualmente i LIF

a. Migrare i LIF che non sono riusciti a trasferirsi automaticamente al nodo 4:

```
network interface migrate -vserver <vserver name> -lif <lif_name>
-destination-node <node4_nodename> -destination-port
<port_on_node4>
```

b. Modificare il nodo home e la porta home per i LIF migrati:

```
network interface modify -vserver <vserver_name> -lif
<data_lif_name> -home-node <node4_nodename> -home-port
<home_port>
```

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

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

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

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.
"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.
"Gestione delle coppie HA"	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.

Contenuto	Descrizione
"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.
"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.

Utilizzare i comandi "System controller replace" per aggiornare i modelli di controller nello stesso chassis

Scopri di più sulla procedura di aggiornamento ARL

Esistono diversi metodi di rilocazione aggregata (ARL) per aggiornare l'hardware del controller. Questa procedura descrive come aggiornare i controller di storage in una coppia HA convertendo il sistema esistente nel sistema sostitutivo, mantenendo lo chassis e i dischi del sistema esistenti.

ARL sfrutta la configurazione ha e la comunicazione di interconnessione del cluster. In questo modo, è possibile spostare la proprietà di aggregati non root da un nodo a un altro, se condividono lo storage all'interno dello stesso cluster.

Durante la procedura, l'hardware del controller originale viene aggiornato con l'hardware del controller sostitutivo, riallocando la proprietà degli aggregati non root. Oltre a migrare gli aggregati non root tra i vecchi nodi di controller. Dopo l'installazione dei nodi di sostituzione, è possibile migrare gli aggregati non root dai vecchi nodi di controller ai nodi di sostituzione. I dati ospitati sui nodi che si sta aggiornando sono accessibili durante la procedura di aggiornamento. Inoltre, è possibile migrare i dati LIF tra i nodi del cluster durante la migrazione.

L'hardware del controller che si sostituisce dipende dal tipo di modello di sistema esistente:

Se il tuo sistema esistente è…	**Quindi…**
AFF A250, AFF C250	Sostituire i due controller AFF A250 o AFF C250 con i nuovi controller e moduli i/O.
AFF A800, AFF C800	Sostituire i due controller AFF A800 o AFF C800 con i nuovi controller e moduli i/O.
AFF A220, AFF A200, AFF C190, FAS2620 o FAS2720	Scambiare il modulo controller su ciascun nodo del vecchio controller con il nuovo modulo.
AFF A700 o FAS9000	Scambiare il controller e i moduli NVRAM su ciascun nodo del vecchio controller con i nuovi moduli. **Nota**: Non è necessario spostare, scollegare o ricollegare le schede i/o, i cavi dati, gli shelf di dischi e i dischi.

I termini **node1** e **node2** sono utilizzati solo come riferimento ai nomi dei nodi in questo documento. Quando si segue la procedura, è necessario sostituire i nomi effettivi dei nodi.

Requisiti e limitazioni

Prima di iniziare la procedura di aggiornamento, è necessario considerare fattori importanti.

Prima di avviare la procedura di aggiornamento, è necessario leggere attentamente tutte le seguenti informazioni importanti.

- Questa procedura è complessa e presuppone che si disponga di competenze di amministrazione avanzate di ONTAP. Dovresti anche leggere e comprendere il "linee guida per l'aggiornamento dei controller" E "Sequenza di aggiornamento ARL" prima di iniziare l'aggiornamento.
- Questa procedura presuppone che l'hardware del controller sostitutivo sia nuovo e non sia stato utilizzato in un altro sistema. I passaggi necessari per preparare i controller usati con `wipeconfig` i comandi non sono inclusi in questa procedura. È necessario contattare il supporto tecnico se l'hardware del controller sostitutivo è stato utilizzato in precedenza come parte di un altro cluster ONTAP o come sistema standalone a nodo singolo.
- 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 ha nel cluster.
- Se si dispone di uno switch non supportato dalla versione di ONTAP e dal sistema sostitutivo a cui si sta eseguendo l'aggiornamento, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*.
- I sistemi AFF A250 e AFF C250 utilizzano porte 10/25 GbE integrate per l'interconnessione dei cluster. Per aggiornare i cluster switchless a due nodi di un sistema AFF A250 o AFF C250 a un sistema AFF A50, AFF A30, AFF C60 o AFF C30, è necessario utilizzare una scheda X60132A a 4 porte 10/25 GbE nello slot 1 su entrambi i nodi. Ciò fornisce l'interconnessione dei cluster per i LIF del cluster a una porta temporanea sulla piattaforma di destinazione.

- I sistemi AFF A30, AFF A50, AFF A70, AFF A90, AFF A1K, AFF C30, AFF C60, AFF C80, FAS70 e FAS90 condividono 100GbE porte di rete per le connessioni cluster e ha. Questi sistemi possono supportare connessioni cluster 10GbE o 25GbE a switch cluster legacy; tuttavia, NetApp consiglia di eseguire l'aggiornamento a velocità cluster 100GbE quando gli switch 10GbE e 25GbE non sono più necessari. Per ulteriori informazioni, vedere i seguenti articoli della Knowledge base:
  - "Come configurare porte cluster 10G o 25g in una nuova configurazione cluster"
  - "Come convertire le porte del cluster 10G o 25g esistenti in porte del cluster 40G o 100g"

  Se non puoi collegare e0a o e0b porte cluster sul nodo esistente alle porte cluster sul nuovo nodo, consulta le seguenti per ulteriori informazioni:
  - "ID bug online di NetApp CONTAP-166978"
  - "Bug online di NetApp ID 1127315"
- I sistemi ASA A900, AFF A900 e FAS9500 supportano solo l'alimentazione di linea alta (da 200V a 240V). Se il sistema AFF A700 o FAS9000 è alimentato a bassa tensione (da 100 V a 120 V), è necessario convertire l'alimentazione in ingresso del sistema AFF A700 o FAS9000 prima di utilizzare questa procedura.
- Se si esegue l'aggiornamento da un sistema esistente con tempi di inattività inclusi nel"matrice dei sistemi supportati" , è possibile aggiornare l'hardware del controller spostando lo storage o contattando l'assistenza tecnica. Fare riferimento a"Riferimenti" per collegarsi a *Aggiorna spostando volumi o storage*.

Automatizzare il processo di aggiornamento del controller

Questa procedura fornisce i passaggi per la procedura automatica, che utilizza l'assegnazione automatica del disco e i controlli di raggiungibilità delle porte di rete per semplificare l'esperienza di aggiornamento del controller.

Decidere se utilizzare questa procedura di ricollocazione aggregata

Esistono diversi metodi di rilocazione aggregata (ARL) per aggiornare l'hardware del controller. Questo articolo descrive come aggiornare i controller di storage in una coppia HA convertendo il sistema esistente nel sistema sostitutivo, mantenendo lo chassis e i dischi del sistema esistente. Questa complessa procedura dovrebbe essere utilizzata solo da amministratori ONTAP esperti.

Per aiutarti a decidere se questa procedura ARL è adatta all'aggiornamento hardware del tuo controller, dovresti esaminare tutte le seguenti circostanze per gli aggiornamenti supportati e non supportati.

Supportato per questo aggiornamento ARL

È possibile utilizzare questa procedura ARL nelle seguenti circostanze:

- L'aggiornamento del controller è elencato in matrice dei sistemi supportati .
- Con il rappresentante di vendita NetApp hai verificato di aver ricevuto l'hardware necessario per l'aggiornamento del controller:
  - Due controller AFF A90, AFF A70 o AFF C80 e tutti i moduli di i/O. Le lunghezze richieste di cavi 100GbE.
  - Due controller AFF A50, AFF A30, AFF C30 o AFF C60 e moduli i/o e i cavi richiesti

- Controller ASA A150, AFF A150 o FAS2820
- Moduli e parti ASA A900, AFF A900 o FAS9500 controller e NVRAM

- È in esecuzione la versione ONTAP minima per l'aggiornamento. Per ulteriori informazioni, fare riferimento alla combinazioni di aggiornamento del sistema supportate.
- Si è esperti nell'amministrazione di ONTAP e si è soddisfatti dei rischi di lavorare in modalità privilegi diagnostici.
- I sistemi eseguono ONTAP 9.15.1 o versione successiva e utilizzano switch Ethernet per la connessione allo storage Ethernet.

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

Non supportato per questo aggiornamento ARL

Non è possibile utilizzare questa procedura ARL nelle seguenti circostanze:

- Vuoi aggiungere i nuovi controller come nuova coppia ha al cluster e migrare i dati utilizzando gli spostamenti dei volumi.
- Si sta aggiornando una configurazione IP di MetroCluster.

  Per aggiornare una configurazione IP di MetroCluster, consultare "Riferimenti"il collegamento al contenuto *MetroCluster Upgrade and Expansion*.

Combinazioni di aggiornamento del sistema supportate

Nella tabella seguente viene mostrata la matrice dei sistemi supportati per eseguire un aggiornamento del controller convertendo il sistema esistente nel sistema sostitutivo, mantenendo lo chassis e i dischi del sistema esistente.

Questa procedura si applica rigorosamente alle seguenti configurazioni di aggiornamento. Non utilizzare questa procedura per eseguire un aggiornamento tra qualsiasi altra combinazione di sistema. Per tutti gli altri modelli di controller, fare riferimento al "Riferimenti"collegamento ai comandi *utilizzo dei comandi "sostituzione dei controller di sistema" per aggiornare l'hardware dei controller che eseguono ONTAP 9,8 o versioni successive* e *utilizzo del trasferimento degli aggregati per aggiornare manualmente l'hardware dei controller che esegue ONTAP 9,8 o versioni successive*.

Sistema esistente	Sistema sostitutivo	Versioni di ONTAP supportate
AFF C250 [1]	AFF C30, AFF C60	9.16.1
AFF A250 [1]	AFF A30, AFF A50	9.16.1
AFF C800 [1]	AFF C80	9.16.1
AFF A800 [1]	AFF A90 o AFF A70	9.15.1 e versioni successive
AFF A220 configurato come ASA (All SAN Array)	ASA A150	9.13.1P1 e successivi
AFF A220	AFF A150	9.10.1P15, 9.11.1P11, 9.12.1P5 e versioni successive

Sistema esistente	Sistema sostitutivo	Versioni di ONTAP supportate
AFF A200	AFF A150	9.10.1P15, 9.11.1P11 e successivi [2]
AFF C190	AFF A150	9.10.1P15, 9.11.1P11, 9.12.1P5 e versioni successive
FAS2620	FAS2820	9.11.1P7 o versioni successive delle patch (FAS2620) [2] 9.13.1 e versioni successive (FAS2820)
FAS2720	FAS2820	9.13.1 e versioni successive
AFF A700 configurato come ASA	ASA A900	9.13.1P1 e successivi
AFF A700	AFF A900	9.10.1P10, 9.11.1P6 e versioni successive
FAS9000	FAS9500	9.10.1P10, 9.11.1P6 e versioni successive

[1] quando si esegue l'upgrade a un sistema introdotto in ONTAP 9.15.1 o versione successiva, 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"

[2] I sistemi AFF A200 e FAS2620 non supportano le versioni ONTAP successive alla 9.11.1.

> NetApp consiglia vivamente, quando possibile, di disporre della stessa versione di ONTAP sui sistemi vecchi e sostitutivi.
>
> Le versioni minime di ONTAP riportate nella tabella precedente sono obbligatorie. Queste versioni di ONTAP dispongono della versione del firmware del processore di servizio o del BMC (Baseboard Management Controller) necessaria per supportare la combinazione di tipi di controller all'interno di uno chassis durante un aggiornamento.

Scegli una procedura di aggiornamento hardware diversa

- "Esaminare i metodi ARL alternativi disponibili per l'aggiornamento dell'hardware del controller".
- 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*.

Informazioni correlate

Fare riferimento a "Riferimenti" per collegarsi alla *Documentazione ONTAP 9*.

Strumenti e documentazione richiesti

Per eseguire l'aggiornamento, è necessario disporre di una cintura di messa a terra e consultare altri documenti durante il processo di aggiornamento.

Per un aggiornamento AFF A800 a un AFF A90 o AFF A70, verificare che i cavi 100GbE siano lunghi almeno un metro.

Fare riferimento a. "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

Per capire se è possibile utilizzare il trasferimento aggregato (ARL), mantenendo il vecchio chassis e i dischi del sistema, dipende dalla configurazione di aggiornamento del sistema e dalla versione di ONTAP.

Aggiornamenti supportati per ARL

Gli aggiornamenti dei controller sono supportati per alcune configurazioni di sistema. Fare riferimento al "combinazioni di aggiornamento del sistema supportate" per un elenco dei sistemi supportati e la versione minima di ONTAP.

Se è stato ricevuto un nuovo sistema AFF A30, AFF A50, AFF A70, AFF A90, AFF A150, AFF A900, AFF C30, AFF C60, AFF C80, FAS2820 o FAS9500 come sistema completo, incluso un nuovo chassis, fare riferimento al "Riferimenti"collegamento per i comandi _use "system controller replace" (utilizza sostituzione controller di sistema) per aggiornare l'hardware del controller che esegue ONTAP 9,8 o versioni successive.

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.

Switch Attached Clusters

Se si stanno aggiornando i nodi in un cluster collegato a uno switch del cluster, è necessario verificare che la marca, il modello, la versione del firmware, l'RCF e la versione di ONTAP in esecuzione sullo switch siano uguali a quelle in esecuzione sul controller sostitutivo dopo l'aggiornamento. Se necessario, è necessario eseguire l'aggiornamento dello switch prima di aggiornare i controller utilizzando ARL.

Per ulteriori informazioni, vedere "Connettersi a un cluster collegato allo switch".

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.

In caso di problemi, fare riferimento al "Risolvere i problemi" sezione alla fine della procedura per ulteriori informazioni e possibili soluzioni. Le informazioni sui guasti che possono verificarsi sono elencate in base alla fase della procedura nella "Sequenza di aggiornamento ARL" .

Se non trovi una soluzione al problema riscontrato, contatta l'assistenza tecnica.

Scopri la sequenza di 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	Fasi
"Fase 1: Preparazione per l'aggiornamento"	Durante la fase 1, verificare di disporre dell'hardware corretto per l'aggiornamento, eseguire i controlli preliminari e, se necessario, correggere la proprietà aggregata. Se si gestisce Storage Encryption utilizzando Onboard Key Manager, è necessario registrare alcune informazioni ed è possibile 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: Trasferire le risorse e dismettere il node1"	Durante la fase 2, è possibile spostare gli aggregati non root node1 e le LIF dei dati NAS da node1 a 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. È inoltre possibile preparare il netboot node1 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	Fasi
"Fase 3: Nodo di boot 1 con i moduli di sistema sostitutivi"	Durante la fase 3, si avvia node1 con i moduli di sistema aggiornati e si verifica l'installazione aggiornata node1. Se si utilizza NetApp Volume Encryption (NVE), viene ripristinata la configurazione del gestore delle chiavi. È inoltre possibile spostare gli aggregati non root node1 e le LIF dei dati NAS da node2 al node1 aggiornato e verificare che le LIF SAN esistano sul node1. Proprietà aggregata alla fine della fase 3: • Upgrade node1 è il proprietario di casa e l'attuale proprietario di node1 aggregati • Node2 è il proprietario domestico e proprietario corrente degli aggregati node2
"Fase 4: Trasferire le risorse e dismettere il node2"	Durante la fase 4, è possibile spostare aggregati non root e LIF dati NAS da node2 al node1 aggiornato e dismettere node2. Proprietà aggregata alla fine della fase 4: • Il node1 aggiornato è il proprietario della casa e l'attuale proprietario di aggregati che originariamente appartenevano al node1 • Upgrade node1 è l'attuale proprietario degli aggregati node2
"Fase 5: Installare i moduli di sistema sostitutivi sul nodo 2"	Durante la fase 5, si installano i nuovi moduli di sistema ricevuti per il node2 aggiornato e quindi il node2 di netboot. Proprietà aggregata alla fine della fase 5: • Il node1 aggiornato è il proprietario di casa e l'attuale proprietario degli aggregati che originariamente appartenevano al node1. • Il node2 aggiornato è il proprietario della casa e l'attuale proprietario di aggregati che originariamente appartenevano al node2.
"Fase 6: Punto di avvio2 con i moduli di sistema sostitutivi"	Durante la Fase 6, si avvia node2 con i moduli di sistema aggiornati e si verifica l'installazione di node2 aggiornata. Se si utilizza NVE, ripristinare la configurazione del gestore delle chiavi. Per gli aggiornamenti dei cluster collegati allo switch, è necessario verificare che il file di configurazione di riferimento dello switch del cluster (RCF) supporti le porte cluster/HA condivise. Si spostano inoltre gli aggregati non root del nodo 1 e i LIF dei dati NAS dal nodo 1 al nodo 2 aggiornato e si verifica che i LIF SAN siano presenti sul nodo 2.
"Fase 7: Completare l'aggiornamento"	Durante la fase 7, 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

Verificare l’hardware di aggiornamento

Prima di avviare l’aggiornamento, verificare di disporre dei moduli corretti per il sistema sostitutivo. In caso di componenti mancanti, contattare il supporto tecnico o il rappresentante commerciale NetApp per assistenza.

Se stai effettuando l’aggiornamento da …	Il sistema di sostituzione deve avere …
AFF A250, AFF C250	• Due moduli controller e nuovi moduli io • Una scheda X60132A a 4 porte 10/25GbE per configurazioni di aggiornamento senza switch a due nodi
AFF A800, AFF C800	Due moduli controller, due NVRAM e nuovi moduli io
• AFF A220 configurato come ASA • AFF A220, AFF A200, AFF C190 • FAS2620, FAS2720	Due moduli controller Se stai convertendo il sistema esistente in uno shelf di archiviazione in modo da poterlo collegare a un altro sistema, il sistema sostitutivo deve avere anche due moduli io.
• AFF A700 configurato come ASA • AFF A700 • FAS9000	Due controller e due moduli NVRAM

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. Elencare la versione del firmware del Service Processor (SP) o del Baseboard Management Controller (BMC) in esecuzione sul vecchio controller:

   ```
   service-processor show
   ```

   Verificare di disporre di una versione del firmware SP o BMC supportata:

Vecchio controller	SP o BMC	Versione minima del firmware
AFF A800	BMC	10,9
AFF A220	BMC	11,9P1
AFF A200	SP	5.11P1
AFF C190	BMC	11,9P1

Vecchio controller	SP o BMC	Versione minima del firmware
FAS2620	SP	5.11P1
FAS2720	BMC	11,9P1

2. Iniziare il processo di sostituzione del controller immettendo il seguente comando nella modalità avanzata dei privilegi della riga di comando ONTAP:

   ```
   set -privilege advanced

   system controller replace start -nodes node_names
   ```

   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 procedures.

   Do you want to continue? {y|n}: y
   ```

3. Selezionare `y`. Viene visualizzato il seguente output:

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

   Durante la fase di precheck, il sistema esegue il seguente elenco di controlli in background.

Eseguire un controllo preliminare	Descrizione
Verifica dello stato del cluster	Controlla tutti i nodi nel cluster per confermare che siano integri.
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.
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. Se mancano dei dischi, fare riferimento al "Riferimenti"collegamento alla gestione *disco e aggregato con la CLI*, alla gestione *logica dello storage con la CLI* e alla gestione *coppia ha* 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 AutoSupport non sono configurate, l'attività non riesce. È necessario attivare AutoSupport 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.

4. Una volta avviata l'operazione di sostituzione del controller e completate le verifiche preliminari, l'operazione viene interrotta, consentendo di raccogliere le informazioni di output necessarie in seguito nel processo di aggiornamento del controller.
5. Eseguire il seguente set di comandi come indicato dalla procedura di sostituzione del controller sulla console di sistema.

   Eseguire i comandi dalla porta seriale collegata a ciascun nodo, eseguire e salvare individualmente l'output dei 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`
   - `run -node local sysconfig -ac`
   - `run -node local aggr status -r`
   - `vol show -fields type`
   - `run local aggr options data_aggregate_name`
   - `vol show -fields type , space-guarantee`
   - `storage aggregate show -node local`
   - `volume show -node local`
   - `storage array config show -switch switch_name`
   - `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 Gestione chiavi integrata 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.

6. 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)

> Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha.
>
> È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

"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

Ogni nodo del cluster deve disporre di un proprio file di licenza NetApp (NLF).

Se non si dispone di un NLF, le funzionalità attualmente concesse in licenza nel cluster sono disponibili per il nuovo controller. Tuttavia, l'utilizzo di funzionalità senza licenza sul controller potrebbe non essere conforme al contratto di licenza, pertanto è necessario installare l'NLF per il nuovo controller al termine dell'aggiornamento.

Fare riferimento a. "Riferimenti" Per accedere al *sito di supporto NetApp* dove è possibile ottenere il proprio NLF. Gli NLFs sono disponibili nella sezione *My Support* sotto *licenze software*. Se il sito non dispone delle risorse di rete non disponibili, contattare il rappresentante commerciale NetApp.

Per informazioni dettagliate sulle licenze, fare riferimento a. "Riferimenti" Per collegarsi al *System Administration Reference*.

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 le risorse e dismettere il node1

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

Prima di poter sostituire il node1 con i moduli sostitutivi per l'aggiornamento del sistema, è necessario spostare gli aggregati non root e le LIF dei dati NAS da node1 a node2 prima di ripristinare le risorse node1 sul node1 in esecuzione sul sistema sostitutivo. Questo processo è in gran parte automatizzato; l'operazione viene interrotta per consentirti di controllarne lo stato.

Prima di iniziare

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

A proposito di questa attività

Le LIF remote gestiscono il traffico verso le LUN SAN durante la procedura di aggiornamento. Non è necessario spostare LE LIF SAN per lo stato del cluster o del servizio durante l'aggiornamento. È necessario verificare che i file LIF siano integri e posizionati sulle porte appropriate dopo aver portato il node1 online come sistema sostitutivo.

> 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 <aggregate_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`

Sposta gli aggregati falliti o sottoposti a veto sul nodo 2

Se uno qualsiasi degli aggregati non riesce a essere riposizionato o viene sottoposto a veto, è necessario riposizionarlo manualmente sul nodo 2 oppure, se necessario, ignorare i veti o i controlli di destinazione.

A proposito di questa attività

Il sistema interrompe l'operazione di ricollocazione 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 <aggregate_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 <aggregate_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 <aggregate_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 la coppia ha con node2 e spegnere il node1 correttamente.

Fasi

1. Riprendere l'operazione:

   ```
   system controller replace resume
   ```

2. Verificare che il node1 sia stato arrestato:

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

   Dopo che il node1 si è arrestato completamente, node1 dovrebbe essere al prompt LOADER>. Per visualizzare il prompt LOADER>, connettersi alla console seriale di node1.

Sostituire i moduli di sistema node1

Sostituire i moduli controller AFF A250 o AFF C250

In questa fase, il node1 è inattivo e tutti i dati sono serviti dal node2. È necessario rimuovere solo il modulo controller node1. In genere, il nodo 1 è il controller A, situato sul lato sinistro dello chassis quando si guardano i controller dal retro del sistema. L'etichetta del controller si trova sul telaio, direttamente sopra il modulo controller.

Non spegnere lo chassis perché node1 e node2 si trovano nello stesso chassis e sono collegati agli stessi alimentatori.

Rimuovere il modulo controller AFF A250 o AFF C250

Per rimuovere il modulo controller node1, rimuovere prima il dispositivo di gestione dei cavi, sbloccare i fermi di bloccaggio, quindi rimuovere il modulo controller dal telaio.

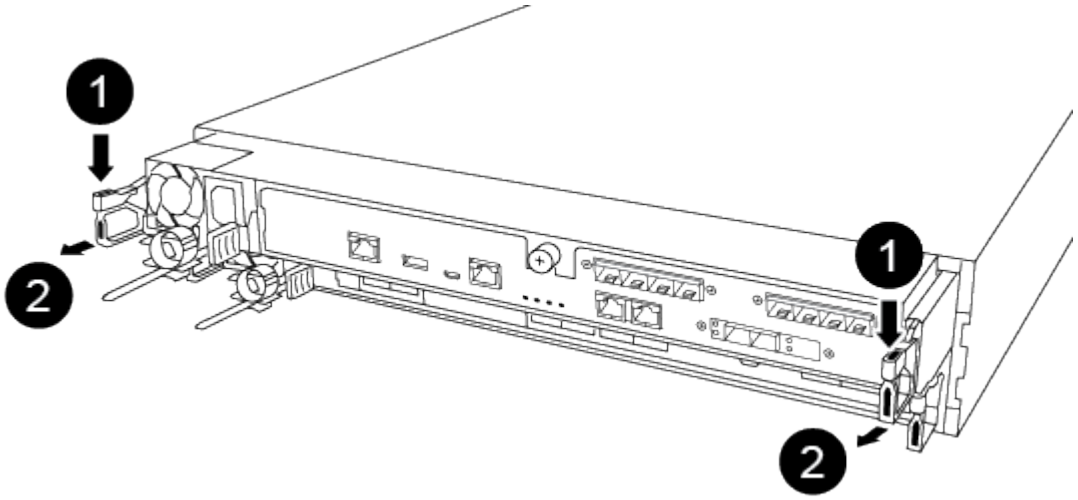
Prima di iniziare

Se non si è già collegati a terra, mettere a terra correttamente.

Fasi

1. Inserire l'indice nel meccanismo di blocco su entrambi i lati del modulo controller, premere la leva con il pollice ed estrarre delicatamente il controller dal telaio.

   In caso di difficoltà nella rimozione del modulo controller, posizionare le dita di riferimento attraverso i fori all'interno (incrociando le braccia).



1	Leva
2	Meccanismo di blocco

2. Andare sul retro del telaio.
3. Scollegare l'alimentazione del modulo controller node1 dalla fonte di alimentazione.
4. Rilasciare i fermi dei cavi di alimentazione, quindi scollegare i cavi dagli alimentatori per node1.

   I collegamenti di alimentazione per node1 e node2 si trovano l'uno sopra l'altro. Fare attenzione a scollegare solo i cavi per node1. Scollegare i cavi per node1 e node2 potrebbe causare un'interruzione dell'alimentazione di entrambi i nodi della coppia ha.

5. Allentare il gancio e la fascetta che fissano i cavi al dispositivo di gestione dei cavi, quindi scollegare i cavi di sistema e i moduli SFP e QSFP (se necessario) dal modulo controller, tenendo traccia della posizione in cui sono stati collegati i cavi.

   Lasciare i cavi nel dispositivo di gestione dei cavi in modo che quando si reinstalla il dispositivo di gestione dei cavi, i cavi siano organizzati.

6. Rimuovere il dispositivo di gestione dei cavi dal modulo controller e metterlo da parte.
7. Premere verso il basso entrambi i fermi di bloccaggio, quindi ruotare entrambi i fermi verso il basso contemporaneamente.

   Il modulo controller si sposta leggermente fuori dallo chassis.

8. Con entrambe le mani, afferrare i lati del modulo controller ed estrarlo delicatamente dallo chassis e posizionare il modulo su una superficie piana e stabile.

   Assicurarsi di sostenere il peso del modulo controller mentre lo si estrae dallo chassis.

Installare il modulo controller AFF A30, AFF A50, AFF C30 o AFF C60

Installare, cablare e collegare il modulo sostitutivo in node1.

Prima di iniziare

Verificare di avere una scheda X60132A a 4 porte 10/25 GbE nello slot 1 del nodo 1. La scheda X60132A è necessaria per l'interconnessione dei cluster nelle configurazioni di cluster switchless a due nodi durante l'aggiornamento.

Fasi

1. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.

   Non inserire completamente il modulo controller nel telaio fino a quando non viene richiesto di farlo più avanti nella procedura.

2. Collegare le porte di gestione e console al modulo controller node1.

   Poiché lo chassis è già ACCESO, node1 avvia l'inizializzazione del BIOS seguita da un'OPERAZIONE di AUTOBOOT non appena si inserisce il nuovo modulo controller. Per evitare questo problema, NetApp consiglia di collegare i cavi seriali e console prima di inserire il modulo controller.

3. Con la maniglia della camma in posizione aperta, spingere con decisione il modulo controller fino a quando non raggiunge la scheda intermedia e non è completamente inserito. Il dispositivo di chiusura si solleva quando il modulo controller è completamente inserito. Chiudere la maniglia della camma in posizione di blocco.

   Per evitare di danneggiare i connettori, non esercitare una forza eccessiva quando si fa scorrere il modulo controller nel telaio.

4. Collegare la console seriale non appena il modulo è inserito ed essere pronti per interrompere L'AUTOBOOT del node1.
5. Dopo aver interrotto L'AUTOBOOT, node1 si ferma al prompt DEL CARICATORE.

   Se non INTERROMPETE L'AUTOBOOT in tempo e node1 inizia l'avvio, attendete il prompt e premete Ctrl-C per entrare nel menu di avvio. Dopo che il nodo si è fermato al menu di avvio, utilizzare opzione `8` per riavviare il nodo e interrompere l'AUTOBOOT durante il riavvio.

6. Al prompt LOADER> di node1, impostare le variabili di ambiente predefinite:

```
set-defaults
```

7. Salvare le impostazioni predefinite delle variabili di ambiente:

```
saveenv
```

Sostituire i moduli controller AFF A800 o AFF C800

In questa fase, il node1 è inattivo e tutti i dati sono serviti dal node2. È necessario rimuovere solo il modulo controller node1. In genere, il nodo 1 è il controller A, situato sul lato sinistro dello chassis quando si guardano i controller dal retro del sistema. L'etichetta del controller si trova sul telaio, direttamente sopra il modulo controller.

Non spegnere lo chassis perché node1 e node2 si trovano nello stesso chassis e sono collegati agli stessi alimentatori.

Prima di iniziare

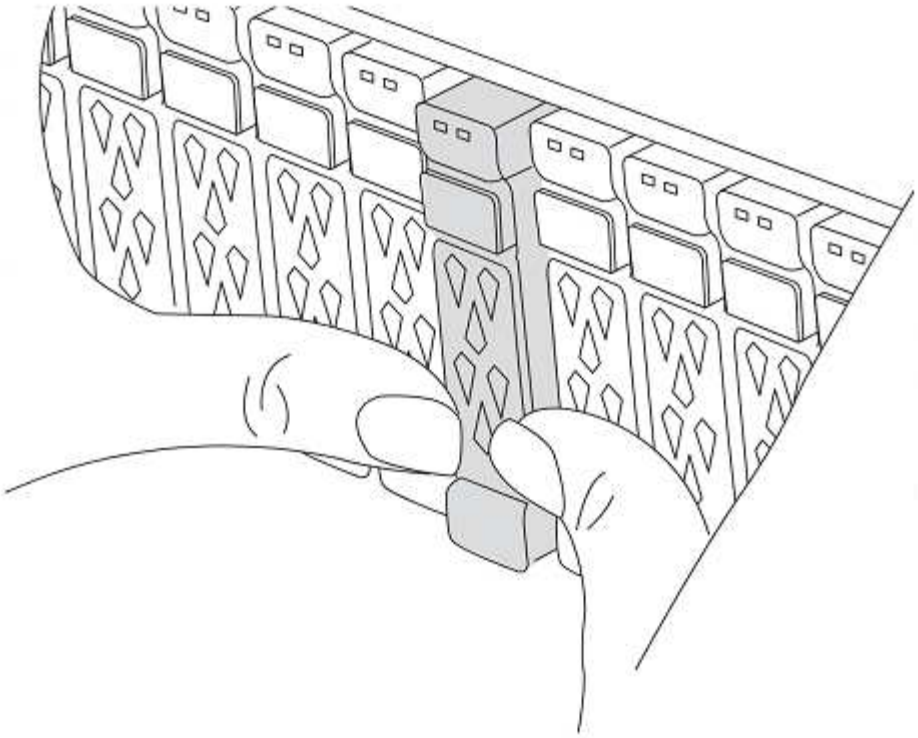
Se non si è già collegati a terra, mettere a terra correttamente.

Rimuovere il modulo controller AFF A800 o AFF C800

Rimuovere il dispositivo di gestione dei cavi dal modulo esistente e spostare leggermente il controller fuori dallo chassis.

Fasi

1. Preparazione per la rimozione del modulo controller:
   a. Sulla parte anteriore del telaio, utilizzare i pollici per spingere con decisione ogni unità negli alloggiamenti superiore e inferiore finché non si avverte un arresto sicuro. In questo modo si garantisce che le unità siano saldamente fissate al piano intermedio del telaio.

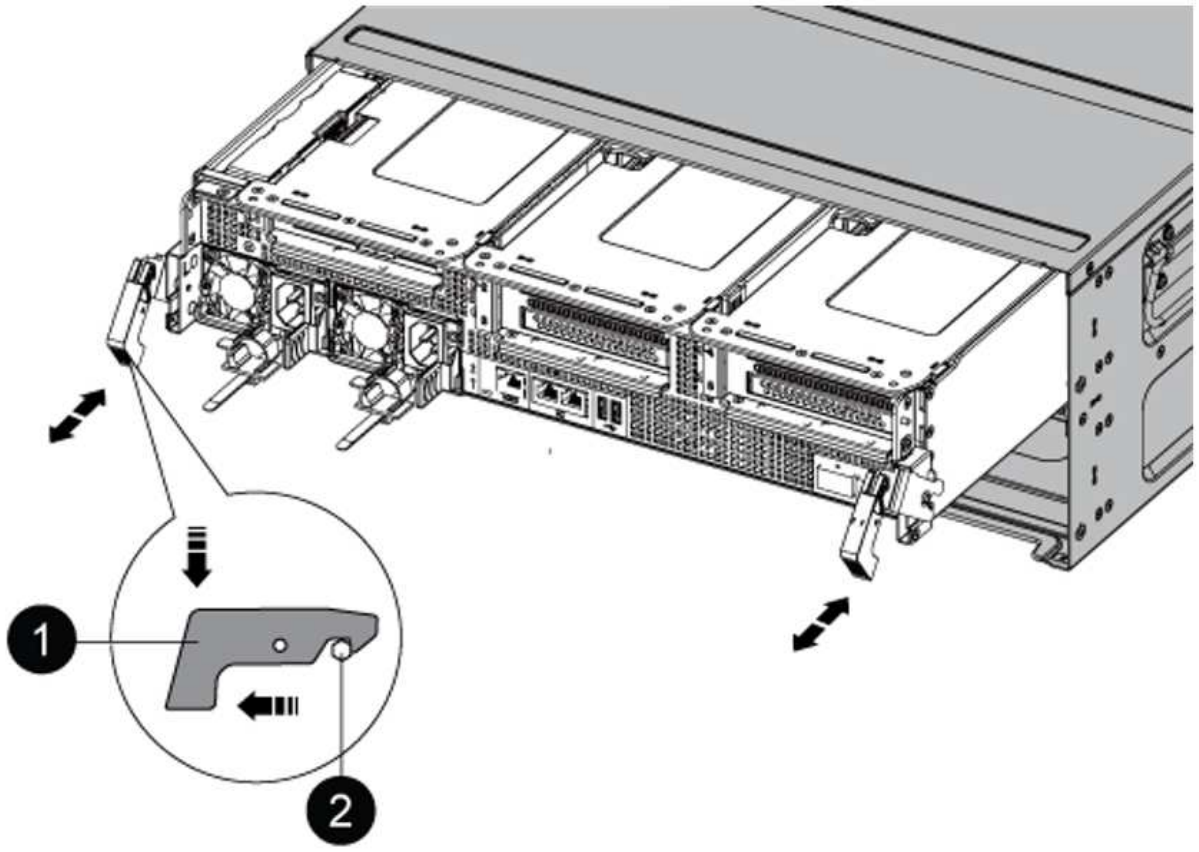


1. Scollegare gli alimentatori del modulo controller node1 dalla fonte di alimentazione.
2. Rilasciare i fermi dei cavi di alimentazione, quindi scollegare i cavi dagli alimentatori.
3. Allentare il gancio e la fascetta che fissano i cavi al dispositivo di gestione dei cavi, quindi scollegare i cavi di sistema e i moduli SFP e QSFP (se necessario) dal modulo controller, tenendo traccia della posizione in cui sono stati collegati i cavi.

   Lasciare i cavi nel dispositivo di gestione dei cavi in modo che quando si reinstalla il dispositivo di gestione dei cavi, i cavi siano organizzati.

4. Rimuovere il dispositivo di gestione dei cavi dal modulo controller e metterlo da parte.
5. Premere verso il basso entrambi i fermi di bloccaggio, quindi ruotare entrambi i fermi verso il basso contemporaneamente.

   Il modulo controller si sposta leggermente fuori dallo chassis.



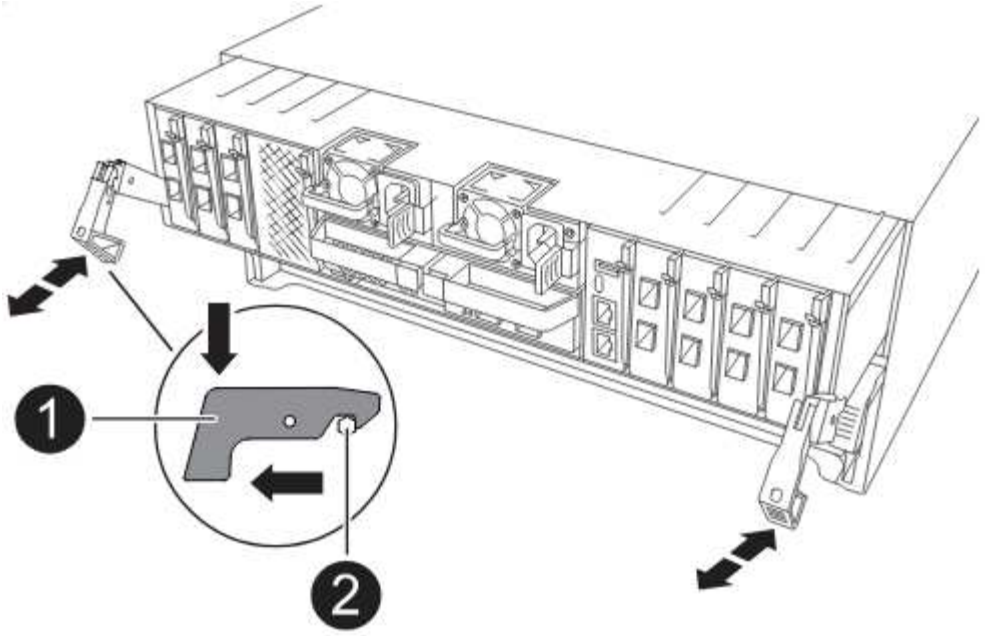
1	Fermo di bloccaggio
2	Perno di bloccaggio

Installare il modulo controller AFF A90, AFF A70 o AFF C80. Installare, cablare e collegare il modulo controller AFF A90, AFF A70 o AFF C80 in node1.

Fasi

1. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.

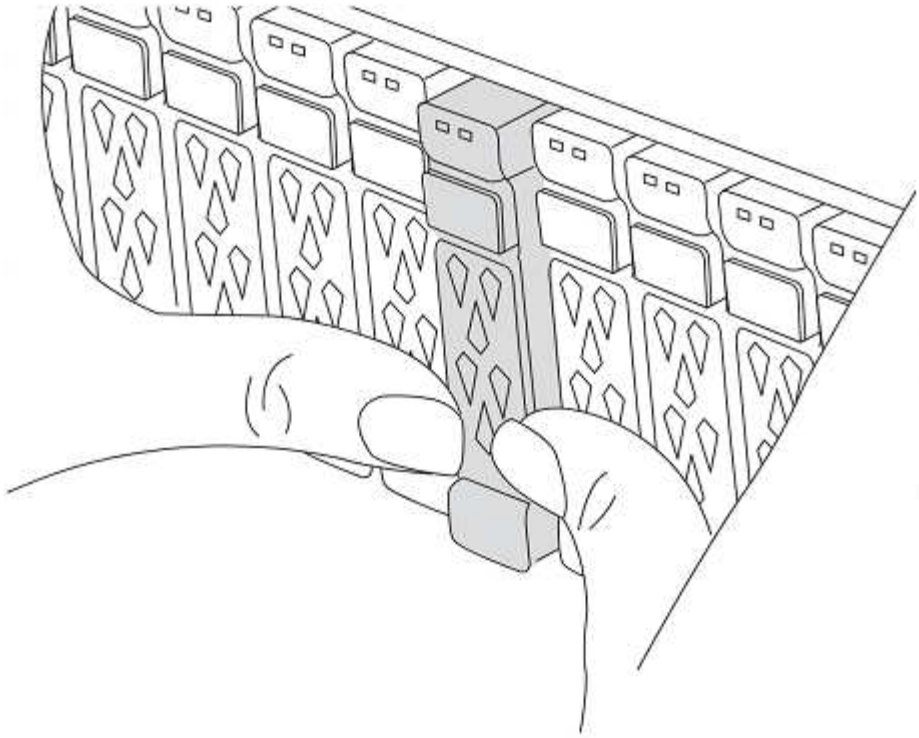
> Non inserire completamente il modulo controller nel telaio fino a quando non viene richiesto di farlo più avanti nella procedura.



2. Collegare le porte di gestione e console al modulo controller node1.

> Poiché lo chassis è già ACCESO, node1 avvia l'inizializzazione del BIOS seguita da un'OPERAZIONE di AUTOBOOT non appena si inserisce il nuovo modulo controller. Per evitare questo problema, NetApp consiglia di collegare i cavi seriali e console prima di inserire il modulo controller.

3. Sulla parte anteriore del telaio, utilizzare i pollici per spingere con decisione ogni unità negli alloggiamenti superiore e inferiore finché non si avverte un arresto sicuro. In questo modo si garantisce che le unità siano saldamente fissate al piano intermedio del telaio.



a. Andare sul retro del telaio.

4. Con la maniglia della camma in posizione aperta, spingere con decisione il modulo controller fino a quando non raggiunge la scheda intermedia e non è completamente inserito. Il dispositivo di chiusura si solleva quando il modulo controller è completamente inserito. Chiudere la maniglia della camma in posizione di blocco.

> Per evitare di danneggiare i connettori, non esercitare una forza eccessiva quando si fa scorrere il modulo controller nel telaio.

5. Collegare la console seriale non appena il modulo è inserito ed essere pronti per interrompere L'AUTOBOOT del node1.
6. Dopo aver interrotto L'AUTOBOOT, node1 si ferma al prompt DEL CARICATORE.

   Se non INTERROMPETE L'AUTOBOOT in tempo e node1 inizia l'avvio, attendete il prompt e premete Ctrl-C per entrare nel menu di avvio. Dopo che il nodo si è fermato al menu di avvio, utilizzare opzione `8` per riavviare il nodo e interrompere l'AUTOBOOT durante il riavvio.

7. Al prompt LOADER> di node1, impostare le variabili di ambiente predefinite:

   ```
   set-defaults
   ```

8. Salvare le impostazioni predefinite delle variabili di ambiente:

   ```
   saveenv
   ```

Sostituire il modulo controller AFF A220, AFF A200, AFF C190, FAS2620 o FAS2720

In questa fase, il node1 è inattivo e tutti i dati sono serviti dal node2. È necessario rimuovere solo il modulo controller node1. In genere, il nodo 1 è il controller A, situato sul

lato sinistro dello chassis quando si guardano i controller dal retro del sistema. L'etichetta del controller si trova sul telaio, direttamente sopra il modulo controller.

> Non spegnere lo chassis perché node1 e node2 si trovano nello stesso chassis e sono collegati agli stessi alimentatori.

Prima di iniziare

Se non si è già collegati a terra, mettere a terra correttamente.

Rimuovere il modulo controller AFF A220, AFF A200, AFF C190, FAS2620 o FAS2720

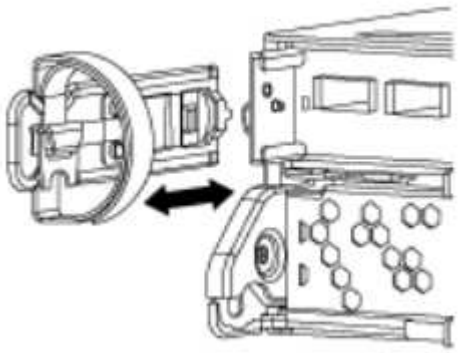
Per accedere ai componenti all'interno del controller, rimuovere il modulo controller dal sistema, quindi rimuovere il coperchio sul modulo controller.

Fasi

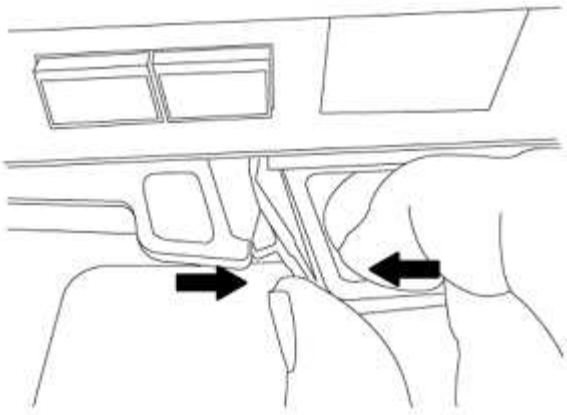
1. Allentare il gancio e la fascetta che fissano i cavi al dispositivo di gestione dei cavi, quindi scollegare i cavi di sistema e gli SFP (se necessario) dal modulo controller, tenendo traccia del punto in cui sono stati collegati i cavi.

   Lasciare i cavi nel dispositivo di gestione dei cavi in modo che quando si reinstalla il dispositivo di gestione dei cavi, i cavi siano organizzati.

2. Rimuovere e mettere da parte i dispositivi di gestione dei cavi dai lati sinistro e destro del modulo controller.



3. Premere il dispositivo di chiusura sulla maniglia della camma fino al rilascio, aprire completamente la maniglia della camma per rilasciare il modulo controller dalla scheda intermedia, quindi estrarre il modulo controller dallo chassis con due mani.



4. Capovolgere il modulo controller e posizionarlo su una superficie piana e stabile.

Installare il modulo controller ASA A150, AFF A150 o FAS2820

Installare, collegare e collegare il modulo controller ASA A150, AFF A150 o FAS2820 in node1.

Fasi

1. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.

   Non inserire completamente il modulo controller nel telaio fino a quando non viene richiesto di farlo più avanti nella procedura.

2. Collegare le porte di gestione e console al modulo controller node1.

   Poiché lo chassis è già ACCESO, node1 avvia l'inizializzazione del BIOS seguita da un'operazione di AUTOBOOT non appena è completamente inserito. Per interrompere l'avvio node1, prima di inserire completamente il modulo controller nello slot, si consiglia di collegare la console seriale e i cavi di gestione al modulo controller node1.

3. Con la maniglia della camma in posizione aperta, spingere con decisione il modulo controller fino a quando non raggiunge la scheda intermedia e non è completamente inserito. Il dispositivo di chiusura si solleva quando il modulo controller è completamente inserito. Chiudere la maniglia della camma in posizione di blocco.

   Per evitare di danneggiare i connettori, non esercitare una forza eccessiva quando si fa scorrere il modulo controller nel telaio.

4. Collegare la console seriale non appena il modulo è inserito ed essere pronti per interrompere L'AUTOBOOT del node1.
5. Dopo aver interrotto L'AUTOBOOT, node1 si ferma al prompt DEL CARICATORE. Se non INTERROMPETE L'AUTOBOOT in tempo e node1 inizia l'avvio, attendete il prompt e premete Ctrl-C per entrare nel menu di avvio. Dopo che il nodo si è fermato al menu di avvio, utilizzare opzione `8` per riavviare il nodo e interrompere l'AUTOBOOT durante il riavvio.
6. Al prompt LOADER> di node1, impostare le variabili di ambiente predefinite:

   ```
   set-defaults
   ```

7. Salvare le impostazioni predefinite delle variabili di ambiente:

```
saveenv
```

Sostituire il controller AFF A700 o FAS9000 e i moduli NVRAM

In questa fase, il node1 è inattivo e tutti i dati sono serviti dal node2. Rimuovere solo il modulo controller node1 e il modulo NVRAM node1. In genere, il nodo 1 è il controller A, situato sul lato sinistro dello chassis quando si guardano i controller dal retro del sistema. L'etichetta del controller si trova sul telaio, direttamente sopra il modulo controller.

> Non spegnere lo chassis perché node1 e node2 si trovano nello stesso chassis e sono collegati agli stessi alimentatori.

Prima di iniziare

Se non si è già collegati a terra, mettere a terra correttamente.

Rimuovere il modulo del controller AFF A700 o FAS9000

Scollegare e rimuovere il modulo controller AFF A700 o FAS9000 da node1.

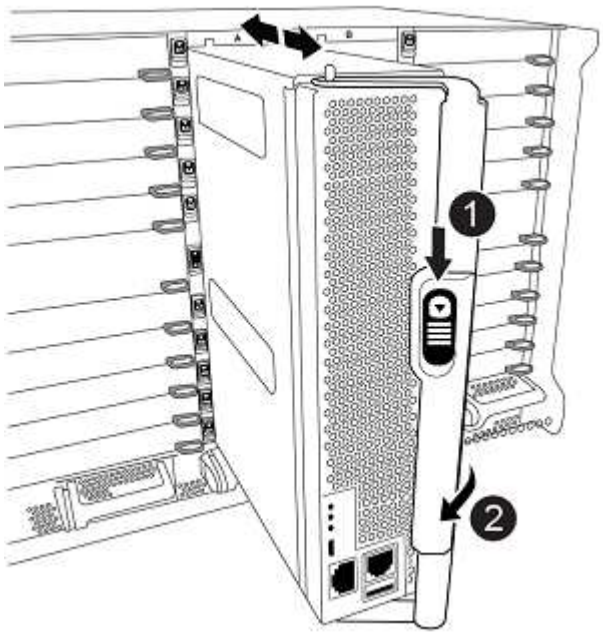
Fasi

1. Scollegare il cavo della console, se presente, e il cavo di gestione dal modulo controller node1.

> Quando si lavora sul node1, rimuovere solo i cavi console e e0M dal node1. Durante questa procedura, non rimuovere o sostituire altri cavi o collegamenti sul nodo 1 o sul nodo 2.

2. Sbloccare e rimuovere il modulo controller A dal telaio.

   a. Far scorrere il pulsante arancione sulla maniglia della camma verso il basso fino a sbloccarla.



1	Pulsante di rilascio della maniglia della camma
2	Maniglia CAM

a. Ruotare la maniglia della camma in modo da disimpegnare completamente il modulo controller dal telaio, quindi estrarre il modulo controller dal telaio.

   Assicurarsi di sostenere la parte inferiore del modulo controller mentre lo si sposta fuori dallo chassis.

Rimuovere il modulo NVRAM AFF A700 o FAS9000

Sbloccare e rimuovere il modulo NVRAM AFF A700 o FAS9000 da node1.

Il modulo NVRAM AFF A700 o FAS9000 si trova nello slot 6 e ha un'altezza doppia rispetto agli altri moduli del sistema.

Fasi

1. Sbloccare e rimuovere il modulo NVRAM dallo slot 6 del nodo 1.

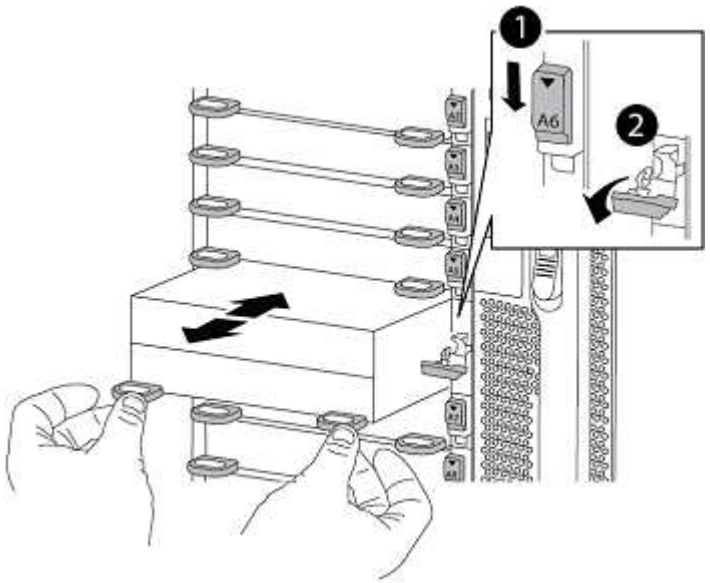
   a. Premere il tasto contrassegnato e numerato CAM.

      Il pulsante CAM si allontana dal telaio.

   b. Ruotare il fermo della camma verso il basso fino a portarlo in posizione orizzontale.

      Il modulo NVRAM si disinnesta dal telaio e si sposta di alcuni centimetri.

   c. Rimuovere il modulo NVRAM dallo chassis tirando le linguette di estrazione sui lati del lato anteriore del modulo.



1	Latch i/o Cam intestato e numerato
2	Fermo i/o completamente sbloccato

Installare ASA A900, AFF A900 o FAS9500 NVRAM e moduli controller

Installare, collegare e collegare i moduli controller e NVRAM ASA A900, AFF A900 o FAS9500 in node1.

Quando si esegue l'installazione, tenere presente quanto segue:

- Spostare tutti i moduli di riempimento vuoti negli slot 6-1 e 6-2 dal vecchio modulo NVRAM al nuovo modulo NVRAM.
- NON spostare il dispositivo di scarico dal modulo NVRAM AFF A700 al modulo NVRAM ASA A900 o AFF A900.
- Spostare tutti i moduli flash cache installati nel modulo NVRAM FAS9000 nel modulo NVRAM FAS9500.

Prima di iniziare

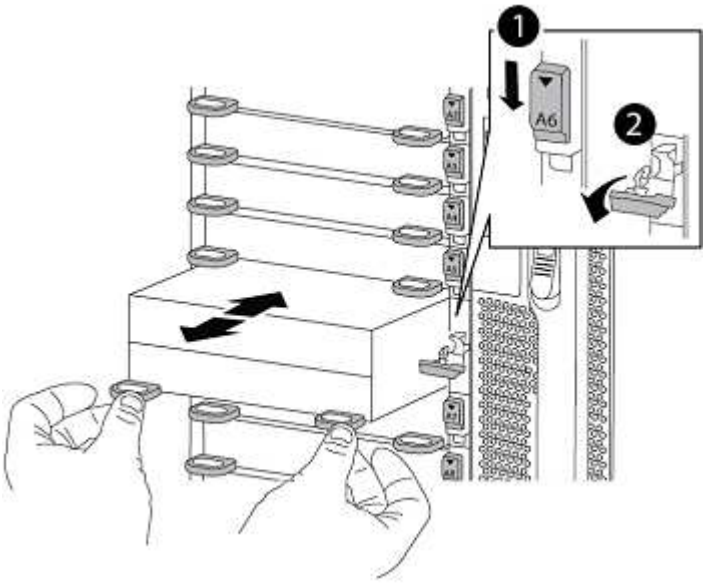
Se non si è già collegati a terra, mettere a terra correttamente.

Installare il modulo NVRAM ASA A900, AFF A900 o FAS9500

Installare il modulo NVRAM ASA A900, AFF A900 o FAS9500 nello slot 6 di node1.

Fasi

1. Allineare il modulo NVRAM ai bordi dell'apertura dello chassis nello slot 6.
2. Far scorrere delicatamente il modulo NVRAM nello slot fino a quando il dispositivo di chiusura della camma i/o con lettere e numeri inizia a innestarsi nel perno della camma i/o, quindi spingere il dispositivo di chiusura della camma i/o fino in fondo per bloccare il modulo NVRAM in posizione.



1	Latch i/o Cam intestato e numerato
2	Fermo i/o completamente sbloccato

Installare il modulo controller ASA A900, AFF A900 o FAS9500 su node1.

Utilizzare la seguente procedura per installare il modulo controller ASA A900, AFA A900 o FAS9500 in node1.

Fasi

1. Allineare l'estremità del modulo controller con l'apertura A nel telaio, quindi spingere delicatamente il modulo controller a metà corsa nel sistema.

   Non inserire completamente il modulo controller nel telaio fino a quando non viene richiesto di farlo più avanti nella procedura.

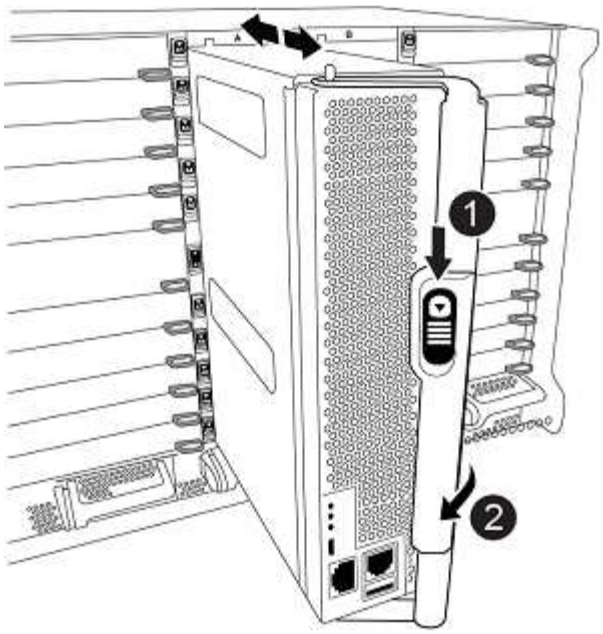
2. Collegare le porte di gestione e console al modulo controller node1.

   Poiché lo chassis è già ACCESO, node1 avvia l'inizializzazione del BIOS seguita da un'operazione di AUTOBOOT non appena è completamente inserito. Per interrompere l'avvio node1, prima di inserire completamente il modulo controller nello slot, si consiglia di collegare la console seriale e i cavi di gestione al modulo controller node1.

3. Spingere con decisione il modulo controller nello chassis fino a quando non raggiunge la scheda intermedia e non è completamente inserito.

   Il dispositivo di chiusura si solleva quando il modulo controller è completamente inserito.

   Per evitare di danneggiare i connettori, non esercitare una forza eccessiva quando si fa scorrere il modulo controller nel telaio.



1	Fermo di bloccaggio della maniglia della camma
2	Maniglia della camma in posizione sbloccata

4. Collegare la console seriale non appena il modulo è inserito ed essere pronti per interrompere L'AUTOBOOT del node1.
5. Dopo aver interrotto L'AUTOBOOT, node1 si ferma al prompt DEL CARICATORE. Se non INTERROMPETE L'AUTOBOOT in tempo e node1 inizia l'avvio, attendete il prompt e premete Ctrl-C per entrare nel menu di avvio. Dopo che il nodo si è fermato al menu di avvio, utilizzare opzione `8` per riavviare il nodo e interrompere l'AUTOBOOT durante il riavvio.
6. Al prompt LOADER> di node1, impostare le variabili di ambiente predefinite:

   ```
   set-defaults
   ```

7. Salvare le impostazioni predefinite delle variabili di ambiente:

   ```
   saveenv
   ```

Node1 NetBoot

Dopo aver scambiato i moduli di sistema sostitutivi corrispondenti, è necessario eseguire il netboot node1. Il termine netboot significa che si sta eseguendo l'avvio da un'immagine ONTAP memorizzata su un server remoto. Quando ci si prepara per il netboot, si aggiunge una copia dell'immagine di boot di ONTAP 9 su un server web a cui il sistema può accedere.

Non è possibile verificare la versione di ONTAP installata sul supporto di avvio del modulo controller sostitutivo, a meno che non sia installato in uno chassis e acceso. La versione ONTAP sul supporto di avvio

del sistema sostitutivo deve essere la stessa della versione ONTAP in esecuzione sul vecchio sistema che si sta aggiornando e sia l'immagine di avvio primaria che quella di backup sul supporto di avvio devono corrispondere. Per verificare la versione minima ONTAP supportata per l'aggiornamento, vedere"matrice dei sistemi supportati" .

È possibile configurare le immagini eseguendo un netboot seguito da `wipeconfig` dal menu di boot. Se il modulo controller è stato utilizzato in precedenza in un altro cluster, il `wipeconfig` il comando cancella qualsiasi configurazione residua sul supporto di avvio.

Per eseguire l'avvio da rete, è possibile utilizzare anche l'opzione di avvio USB. 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.
- Scaricare i file di sistema necessari per il sistema e la versione corretta di ONTAP dal *sito di supporto NetApp*. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp*.

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. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* e scaricare i file utilizzati per eseguire il netboot del sistema.
2. Scarica il software ONTAP appropriato dalla sezione di download del software del *sito di supporto NetApp* e memorizza 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.
4. L'elenco delle directory deve contenere `<ontap_version>_image.tgz`.
5. 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`

Se DHCP (Dynamic host Configuration Protocol) è…	Quindi…
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.

6. Eseguire il netboot al nodo 1:

   `netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`

   Non interrompere l'avvio.

7. (Solo aggiornamenti AFF A250 e AFF C250) quando node1 per il modulo controller sostitutivo è in fase di avvio, viene visualizzato il seguente messaggio di avviso perché la configurazione include node2 per il controller esistente:

   ```
   ****************************************************
   * WARNING: Partner is not of the same family/model. *
   * Mixing is only allowed when upgrading the system. *
   * The system will shut down in 24 hours.            *
   ****************************************************
   Do you want to continue (y/n):
   ```

   Risposta `y`.

   Questo avviso viene visualizzato per ogni avvio del sistema fino all'aggiornamento di node2. Questo è il comportamento previsto.

8. Attendere che il node1 in esecuzione sul modulo controller sostitutivo si avvii e visualizzi le opzioni del menu di avvio come mostrato di seguito:

```
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)?
```

9. 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`

   Questa nota si applica agli aggiornamenti software ONTAP senza interruzioni e non agli aggiornamenti del 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.

10. 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`

    Il `<path_to_the_web-accessible_directory>` dovrebbe portare alla posizione in cui è stato scaricato `<ontap_version>_image.tgz` poll Fase 2.

11. 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.

12. Cancellare qualsiasi configurazione precedente sul supporto di avvio.

a. Al prompt seguente, eseguire il comando `wipeconfig` comando e premere il tasto Invio:

```
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)? wipeconfig
```

b. Quando viene visualizzato il messaggio riportato di seguito, rispondere `yes`:

```
This will delete critical system configuration, including cluster
membership.
Warning: do not run this option on a HA node that has been taken
over.
Are you sure you want to continue?:
```

c. Il nodo viene riavviato per terminare `wipeconfig` e poi si ferma al menu di boot.

Attendi che il nodo si arresti nel menu di avvio dopo aver completato l'operazione `wipeconfig` operazione.

13. Selezionare l'opzione `5` per passare alla modalità di manutenzione dal menu di avvio. Risposta `yes` al prompt finché il nodo non si arresta in modalità di manutenzione e al prompt dei comandi `*>`.

14. 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
```

15. 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
```

16. Verificare `ha-config` impostazioni:

```
ha-config show
```

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

17. Arrestare il nodo 1:

```
halt
```

Node1 dovrebbe arrestarsi al prompt DEL CARICATORE.

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

```
date
```

19. Al nodo 1, controllare la data utilizzando il seguente comando al prompt dell'ambiente di boot:

```
show date
```

20. Se necessario, impostare la data sul node1:

```
set date mm/dd/yyyy
```

Impostare la data UTC corrispondente al nodo 1.

21. In node1, controllare l'ora utilizzando il seguente comando al prompt dell'ambiente di boot:

```
show time
```

22. Se necessario, impostare l'ora su node1:

```
set time hh:mm:ss
```

Impostare l'ora UTC corrispondente su node1.

23. Impostare l'ID del sistema partner su node1:

    `setenv partner-sysid node2_sysid`

    Per il node1, il `partner-sysid` deve essere quello del node2. È possibile ottenere l'ID di sistema node2 da `node show -node node2` output del comando su node2.

    a. Salvare le impostazioni:

       `saveenv`

24. Al nodo 1, al prompt DEL CARICATORE, verificare `partner-sysid` per il nodo 1:

    `printenv partner-sysid`

Fase 3. Fare il boot node1 con i moduli di sistema sostitutivi

Cavo node1 per cluster-ha e storage condivisi

Se stai eseguendo uno dei seguenti upgrade, devi connettere il cluster, l'ha, lo storage, i dati e le connessioni di gestione che erano stati precedentemente connessi al node1 sul sistema esistente al node1 appena installato sul sistema sostitutivo.

Sistema esistente	Sistema sostitutivo
AFF A250	AFF A30, AFF A50
AFF C250	AFF C30, AFF C60
AFF A800	AFF A70, AFF A90
AFF C800	AFF C80

Collegare le porte e0M e BMC

Se il sistema esistente dispone di una porta di gestione (e0M) e di una porta BMC, le porte e0M e BMC sono combinate e accessibili attraverso la porta "chiave inglese" sul sistema sostitutivo. Prima di eseguire la connessione al sistema sostitutivo, è necessario assicurarsi che le porte e0M e BMC siano connesse allo stesso switch e alla stessa subnet del sistema esistente.

Se…	Quindi…
Gli indirizzi IP e0M e BMC si trovano sulla stessa subnet IP	Collegare la porta e0M o BMC del sistema esistente alla porta "chiave" del sistema sostitutivo.
Gli indirizzi IP e0M e BMC si trovano su sottoreti diverse	1. Unire gli indirizzi IP e0M e BMC in un'unica subnet IP. 2. Collegare la porta e0M o BMC del sistema esistente alla porta "chiave" del sistema sostitutivo.

Connettersi a un cluster senza switch a due nodi

Le tabelle seguenti mostrano l'utilizzo delle porte dello switch per le configurazioni cluster senza switch a due nodi.

Tipo di porta	AFF A800, AFF C800	AFF A90	AFF A70, AFF C80
Cluster	e0a	e1a	e1a
Cluster	e1a	e7a (utilizzare e1b se non è presente e7a)	e1b
HA	e0b	Non connetterti	Non connetterti
HA	e1b	Non connetterti	Non connetterti
Porte di storage SAS (se presenti e utilizzate)	Qualsiasi porta disponibile	Qualsiasi porta disponibile	Qualsiasi porta disponibile
Porte di storage Ethernet per NS224 shelf	Qualsiasi porta disponibile	Fare riferimento alla mappatura della connettività dello storage Ethernet	Fare riferimento alla mappatura della connettività dello storage Ethernet

Porta	AFF A250, AFF C250	AFF A30, AFF C30, AFF C60	AFF A50
Cluster	e0c	e1a (utilizzare e1a per l'interconnessione temporanea del cluster)	e1a (utilizzare e1a per l'interconnessione temporanea del cluster)
Cluster	e0d	e1b (utilizzare e1b per l'interconnessione temporanea del cluster)	e1b (utilizzare e1b per l'interconnessione temporanea del cluster)
HA	Non richiesto	Le porte HA non sono necessarie per l'aggiornamento del nodo 1	Le porte HA non sono necessarie per l'aggiornamento del nodo 1
Porte di storage Ethernet	Qualsiasi porta disponibile	e3a, e3b	e3a, e3b
Porte di storage SAS	Qualsiasi porta disponibile	3a, 3b	3a, 3b

Connettersi a un cluster collegato allo switch

Per un cluster con collegamento a switch, verificare di soddisfare i seguenti requisiti per il nodo (sostitutivo) AFF A30, AFF A50, AFF A70, AFF A90, AFF C30, AFF C60 o AFF C80:

- Le porte cluster identiche sul nodo di sostituzione si trovano sullo stesso switch. Ad esempio, al termine dell'upgrade, collegare E1a su node1 e E1a su node2 a uno switch del cluster. Analogamente, la seconda porta cluster di entrambi i nodi deve essere collegata al secondo switch cluster. La connessione incrociata tra porte ha e cluster condivisi, in cui E1a di node1 è connesso allo switch e E1a di node2 è connesso allo switch, causa errori di comunicazione ha.
- Il nodo sostitutivo utilizza porte Ethernet ha-cluster condivise.
- Verificare che gli switch del cluster siano installati con un file di configurazione di riferimento (RCF) che supporti le porte condivise cluster-ha:

a. Rimuovere la configurazione esistente sullo switch:

Se il modello dello switch in uso è…	Vai a…
Cisco Nexus	Articolo della Knowledge base "Come cancellare la configurazione su uno switch Cisco Interconnect mantenendo la connettività remota"
Broadcom BES-53248	Articolo della Knowledge base "Come cancellare la configurazione su uno switch di interconnessione Broadcom mantenendo la connettività remota"

b. Configurare e verificare l'impostazione dello switch:

Se il modello dello switch in uso è…	Vai a…
Cisco Nexus 9336C-FX2	"Aggiornamento del file di configurazione di riferimento (RCF)"
Broadcom BES-53248	"Aggiornamento del file di configurazione di riferimento (RCF)"
NVIDIA SN2100	"Installare o aggiornare lo script RCF (Reference Configuration file)"

Se lo switch del cluster supporta solo velocità 10/25 GbE, è necessario utilizzare una scheda X60130A a 4 porte 10/25 GbE nello slot 1 o nello slot 2 del sistema sostitutivo per l'interconnessione del cluster.

Fare il boot node1 con i moduli di sistema sostitutivi

Il Nodo 1 con i moduli sostitutivi è ora pronto per l'avvio. I moduli sostitutivi supportati sono elencati in"matrice dei sistemi supportati" .

Quando si sostituiscono i moduli controller, spostare tutti i collegamenti dal vecchio al modulo controller sostitutivo.

Quando si sostituiscono i moduli controller e NVRAM, spostare solo la console e le connessioni di gestione.

Fasi

1. (Solo aggiornamento AFF A250, AFF C250, AFF A800 o AFF C800) al prompt di Loader, accedere alla modalità di manutenzione:

   ```
   boot_ontap maint
   ```

   a. Risposta `y` alla richiesta di conferma della piattaforma mista.

   b. Rispondere `yes` al prompt di conferma.

   c. Mostrare lo stato delle interfacce 100GbE:

   ```
   storage port show.
   ```

   Tutte le porte 100GbE collegate agli shelf NS224 o agli switch di storage devono riportare il rapporto come `storage` porte, come mostrato nell'output di esempio riportato di seguito.

```
*> storage port show
Port Type Mode    Speed(Gb/s) State    Status  VLAN ID
---- ---- ------- ----------- -------- ------- -------
e8a  ENET storage 100 Gb/s    enabled  online  30
e8b  ENET storage 100 Gb/s    enabled  online  30
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

a. Uscire dalla modalità di manutenzione:

```
halt
```

2. Se sono installate unità NetApp Storage Encryption (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`**

> Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha. È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

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".

3. Avviare il nodo nel menu di boot:

```
boot_ontap menu
```

4. Quando il nodo si ferma al menu di avvio, riassegnare i vecchi dischi node1 al node1 sostitutivo eseguendo il seguente comando su node1:

```
boot_after_controller_replacement
```

Dopo un breve intervallo di tempo, viene richiesto di inserire il nome del nodo da sostituire. Se sono presenti dischi condivisi (chiamati anche Advanced Disk Partitioning (ADP) o dischi partizionati), viene richiesto di inserire il nome del nodo del partner ha.

Questi prompt potrebbero essere interrati nei messaggi della console. Se non si immette un nome di nodo o non si immette un nome corretto, viene richiesto di inserire nuovamente il nome.

Se `[localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified encrypting drive` e, oppure `[localhost:diskown.errorDuringIO:error]: error 3 (disk failed) on disk` in caso di errori, attenersi alla seguente procedura:

a. Arrestare il nodo al prompt DEL CARICATORE.
b. Controllare e ripristinare i bootargs di codifica di archiviazione menzionati in Fase 2.
c. Al prompt del CARICATORE, avviare:

```
boot_ontap
```

È possibile utilizzare il seguente esempio come riferimento:

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>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner 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:
```

Gli ID di sistema mostrati nell'esempio precedente sono ID di esempio. Gli ID di sistema effettivi dei nodi che si stanno aggiornando saranno diversi.

Tra l'immissione dei nomi dei nodi al prompt e il prompt di accesso, il nodo viene riavviato alcune volte per ripristinare le variabili di ambiente, aggiornare il firmware sulle schede del sistema e per altri aggiornamenti del ONTAP.

Ripristinare la configurazione del gestore delle chiavi sul nodo aggiornato 1

Se si utilizza NetApp aggregate Encryption (NAE) o NetApp Volume Encryption (NVE) per crittografare i volumi sul sistema che si sta aggiornando, la configurazione della crittografia deve essere sincronizzata con i nuovi nodi. Se non si risincronizza il gestore delle chiavi, quando si trasferono gli aggregati node1 da node2 al node1 aggiornato utilizzando ARL, potrebbero verificarsi errori perché node1 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 node1:

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

2. Prima di spostare gli aggregati di dati, verificare che la chiave SVM-KEK sia ripristinata su "true" in node1:

   ```
   ::> security key-manager key query -node node1 -fields restored -key
   -type SVM-KEK
   ```

   Esempio

   ```
   ::> security key-manager key query -node node1 -fields restored -key
   -type SVM-KEK

   node     vserver   key-server   key-id
   restored
   -------- --------- -----------  ----------------------------------------
   --------
   node1    svm1      ""           000000000000000020000000000a008a81976
   true
                                   2190178f9350e071fbb90f00000000000000000
   ```

Sposta node1 aggregati non root e LIF dati NAS da node2 TB a node1 aggiornato

Dopo aver verificato la configurazione di rete sul nodo 1, è necessario spostare i LIF dei dati NAS di proprietà del nodo 1 dal nodo 2 al nodo 1 e confermare che i LIF SAN siano presenti sul nodo 1.

A proposito di questa attività

I LIF remoti gestiscono il traffico verso le LUN SAN durante la procedura di aggiornamento. Lo spostamento dei SAN LIF non è necessario per l'integrità del cluster o del servizio durante l'aggiornamento. I LIF SAN non vengono spostati a meno che non sia necessario mapparli su nuove porte.

Dopo aver portato online node1, è necessario verificare che i LIF siano integri e posizionati sulle porte corrette.

Fasi

1. 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

   Il sistema sospende l'operazione in questa fase del controllo di raggiungibilità della rete

2. Eseguire un controllo della raggiungibilità della rete:

   ```
   network port reachability show -node node1
   ```

   Verificare che tutte le porte connesse, inclusi il gruppo di interfacce e le porte VLAN, mostrino il loro stato come `OK`.

3. Per i seguenti upgrade, è necessario riassegnare le LIF SAN FCP.

Sistema esistente	Sistema sostitutivo
AFF A250	AFF A30, AFF A50
AFF C250	AFF C30, AFF C60
AFF A800	AFF A70, AFF A90
AFF C800	AFF C80

   Per tutti gli altri aggiornamenti del sistema, passare alla Fase 4.

a. Riassegna le LIF SAN FCP utilizzate per l'accesso ai dati FCP o FC-NVMe alle porte home corrette:

```
network interface show -vserver <vserver_hosting_fcp_lifs>
```

b. Per le LIF con il nodo corrente come node1 aggiornato e la porta corrente riporta "status oper" come "-" (poiché la porta esisteva sul nodo AFF A800 ma non esiste sul nodo AFF A90), modificare la porta corrente prima di poterla portare online.

Verificare che la connettività fisica sia stabilita alla porta di destinazione FC in cui è necessario spostare la LIF FC:

i. Impostare lo stato LIF su "DOWN" (giù):

```
network interface modify -vserver <vserver_name> -lif <lif_name>
-status-admin down
```

ii. Modifica la porta home della LIF:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -
home-node <node1> -home-port <FC_target_port>
```

iii. Impostare lo stato della LIF su "UP":

```
network interface modify -vserver <vserver> -lif <lif_name>  -status
-admin up
```

+
Ripetere i passaggi secondari a e b per ogni LIF FC SAN che viene home su node1.

4. riprendere l'operazione di rilocazione:

```
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 node1.

L'operazione di sostituzione del controller viene interrotta al termine del trasferimento delle risorse.

5. 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.

6. Se necessario, ripristinare e ripristinare i LIF spostati oppure migrare e modificare manualmente i LIF del nodo 1 che non sono riusciti a trasferirsi automaticamente nel nodo 1.

Ripristinare e ripristinare i LIF spostati

a. Elencare eventuali LIF spostati:

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

b. In caso di spostamento di LIF, ripristinare il nodo home al nodo node1:

```
cluster controller-replacement network displaced-interface
restore-home-node -node <node1_nodename> -vserver <vserver name>
-lif-name <lif_name>
```

Migrare e modificare manualmente i LIF

a. Migrare i LIF che non sono riusciti a trasferirsi automaticamente al nodo 1:

```
network interface migrate -vserver <vserver name> -lif <lif_name>
-destination-node <node1_nodename> -destination-port
<port_on_node1>
```

b. Modificare il nodo home e la porta home per i LIF migrati:

```
network interface modify -vserver <vserver_name> -lif
<data_lif_name> -home-node <node1_nodename> -home-port
<home_port>
```

7. 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 le risorse e dismettere il node2

Spostare aggregati non root e LIF dati NAS da node2 a node1

Prima di poter sostituire il node2 con il modulo di sistema sostitutivo, è necessario prima spostare gli aggregati non root di proprietà di node2 in node1.

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 al nuovo node1.

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 che tutti gli aggregati non root e le LIF di dati non SAN vengano migrati nel nuovo node1.

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 node1:

   ```
   storage aggregate show -node node1 -state online -root false
   ```

   L'esempio seguente mostra che gli aggregati non root sul nodo 1 sono online:

   ```
   cluster::> storage aggregate show -node node1 state online -root false

   Aggregate     Size        Available   Used%   State   #Vols  Nodes
   RAID     Status
   ----------    ---------   ---------   ------  -----   -----  ------
   -------  ------
   aggr_1        744.9GB     744.8GB     0%      online      5  node1
   raid_dp  normal
   aggr_2        825.0GB     825.0GB     0%      online      1  node1
   raid_dp  normal
   2 entries were displayed.
   ```

   Se gli aggregati sono andati offline o diventano estranei sul node1, portarli online utilizzando il seguente comando sul nuovo node1, una volta per ogni aggregato:

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

2. Verificare che tutti i volumi siano online sul nodo 1 utilizzando il seguente comando sul nodo 1 ed esaminandone l'output:

   ```
   volume show -node node1 -state offline
   ```

   Se alcuni volumi sono offline sul nodo 1, portarli online utilizzando il seguente comando sul nodo 1, 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
   nodename - status-admin up
   ```

4. Verificare che non vi siano dati LIF rimasti sul nodo 2 utilizzando il seguente comando ed esaminando l'output:

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

Sposta gli aggregati falliti o sottoposti a veto sul nodo 1

Se uno qualsiasi degli aggregati non riesce a essere riposizionato o viene sottoposto a veto, è necessario riposizionarlo manualmente sul nodo 1 oppure, se necessario, ignorare i veti o i controlli di destinazione.

A proposito di questa attività

Il sistema interrompe l'operazione di ricollocazione 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 <node2> -destination <node1>
   -aggregate-list <aggregate_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 node2 -destination node1 -aggregate-list <aggregate_list> -ndo-controller-upgrade true -override-vetoes true`
Ignorare i controlli di destinazione	Utilizzare il seguente comando: `storage aggregate relocation start -node node2 -destination node1 -aggregate-list <aggregate_list> -ndo-controller-upgrade true -override-vetoes true -override-destination-checks true`

Andare in pensione node2

Per dismettere node2, è necessario arrestare node2 correttamente e quindi rimuoverlo dal rack o dallo chassis.

Riprendere l'operazione di sostituzione del controller di sistema

Fasi

1. Riprendere l'operazione:

   ```
   system controller replace resume
   ```

   Il nodo si arresta automaticamente.

Rimuovere il modulo controller AFF A800 o AFF C800

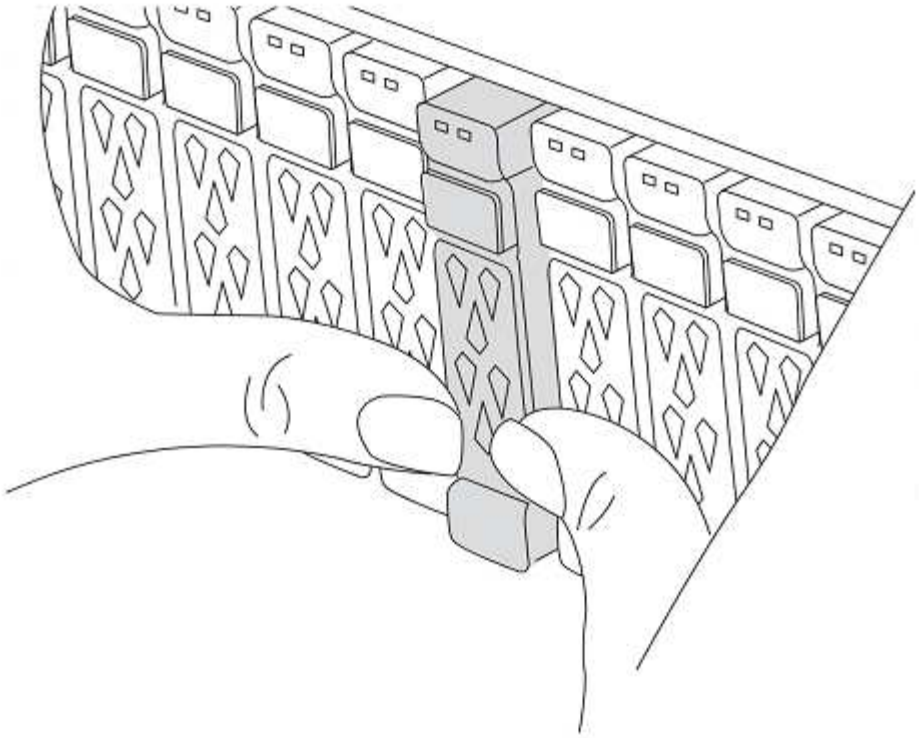
Rimuovere il dispositivo di gestione dei cavi dal modulo esistente e spostare leggermente il controller fuori dallo chassis.

Prima di iniziare

Se non si è già collegati a terra, mettere a terra correttamente.

Fasi

1. Preparazione per la rimozione del modulo controller:
   a. Sulla parte anteriore del telaio, utilizzare i pollici per spingere con decisione ogni unità negli alloggiamenti superiore e inferiore finché non si avverte un arresto sicuro. In questo modo si garantisce che le unità siano saldamente fissate al piano intermedio del telaio.



b. Andare sul retro del telaio.

2. Scollegare gli alimentatori del modulo controller node2 dalla sorgente.
3. Rilasciare i fermi dei cavi di alimentazione, quindi scollegare i cavi dagli alimentatori.
4. Allentare il gancio e la fascetta che fissano i cavi al dispositivo di gestione dei cavi, quindi scollegare i cavi di sistema e i moduli SFP e QSFP (se necessario) dal modulo controller, tenendo traccia della posizione in cui sono stati collegati i cavi.

   Lasciare i cavi nel dispositivo di gestione dei cavi in modo che quando si reinstalla il dispositivo di gestione dei cavi, i cavi siano organizzati.

5. Rimuovere il dispositivo di gestione dei cavi dal modulo controller e metterlo da parte.
6. Premere verso il basso entrambi i fermi di bloccaggio, quindi ruotare entrambi i fermi verso il basso contemporaneamente.

   Il modulo controller si sposta leggermente fuori dallo chassis.

Al termine

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

Fase 5. Installare i moduli di sistema sostitutivi sul nodo 2

Installare i moduli di sistema sostitutivi sul nodo 2

Installare il modulo AFF A30, AFF A50, AFF C30 o AFF C60 su node2

Installare il modulo controller sostitutivo ricevuto per l'aggiornamento su node2. Il Nodo 2 è il controller B, situato nella metà inferiore dello chassis se si guardano i controller dalla

parte posteriore del sistema.

Fasi

1. Posizionare il sistema di stoccaggio sulle guide al centro del cabinet o del rack per telecomunicazioni, quindi sostenere il sistema di archiviazione dal basso e farlo scorrere in posizione.

   Non inserire completamente il modulo controller nel telaio fino a quando non viene richiesto di farlo più avanti nella procedura.

2. Collegare le porte di gestione e console al modulo controller node2.

   Poiché lo chassis è già acceso, node2 avvia l'inizializzazione del BIOS seguita da AUTOBOOT non appena è completamente inserito. Per interrompere l'avvio del nodo 2, prima di inserire completamente il modulo controller nello slot, si consiglia di collegare i cavi della console seriale e di gestione al modulo controller del nodo 2.

3. Con la maniglia della camma in posizione aperta, spingere con decisione il modulo controller fino a quando non raggiunge la scheda intermedia e non è completamente inserito. Il dispositivo di chiusura si solleva quando il modulo controller è completamente inserito. Chiudere la maniglia della camma in posizione di blocco.

   Per evitare di danneggiare i connettori, non esercitare una forza eccessiva quando si fa scorrere il modulo controller nel telaio.

4. Collegare la console seriale non appena il modulo è inserito e prepararsi a interrompere l'AUTOBOOT del nodo 2.
5. Dopo aver interrotto L'AUTOBOOT, node2 si ferma al prompt DEL CARICATORE. Se non INTERROMPETE L'AUTOBOOT in tempo e node2 inizia l'avvio, attendete il prompt e premete Ctrl-C per entrare nel menu di avvio. Dopo che il nodo si è fermato al menu di avvio, utilizzare opzione `8` per riavviare il nodo e interrompere l'AUTOBOOT durante il riavvio.
6. Al prompt LOADER> di node2, impostare le variabili di ambiente predefinite:

   ```
   set-defaults
   ```

7. Salvare le impostazioni predefinite delle variabili di ambiente:

   ```
   saveenv
   ```

8. Per configurazioni switchless a due nodi, verificare di avere una scheda X60132A a 4 porte 10/25 GbE nello slot 1 del nodo 2. La scheda X60132A è necessaria per l'interconnessione del cluster durante l'aggiornamento.

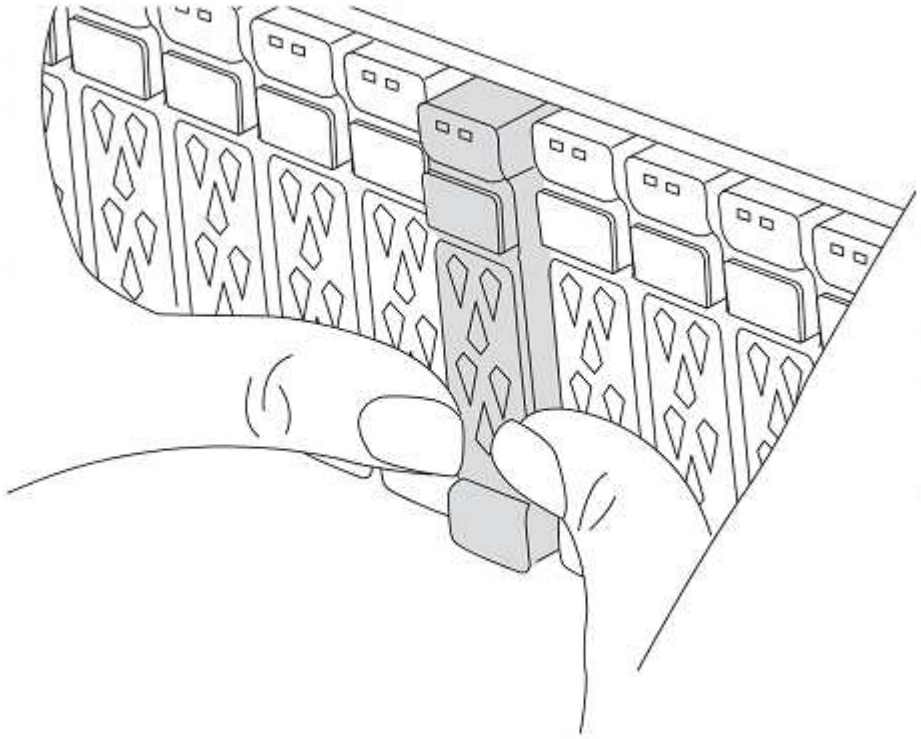
Installare il modulo AFF A90 o AFF A70 su node2

Installare il modulo controller AFF A90 o AFF A70 ricevuto per l'aggiornamento sul nodo 2. Il nodo 2 è il controller B situato nell'alloggiamento inferiore dello chassis, se si guardano i controller dalla parte posteriore del sistema.

Fasi

1. Sulla parte anteriore del telaio, utilizzare i pollici per spingere con decisione ogni unità negli alloggiamenti superiore e inferiore finché non si avverte un arresto sicuro. In questo modo si garantisce che le unità

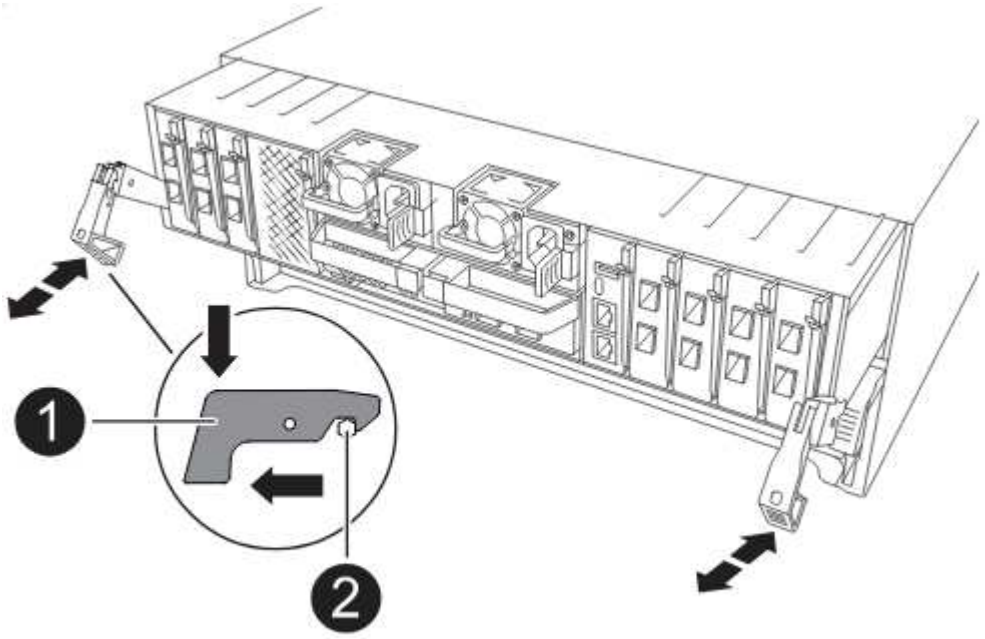
siano saldamente fissate al piano intermedio del telaio.



a. Andare sul retro del telaio.

2. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.

Non inserire completamente il modulo controller nel telaio fino a quando non viene richiesto di farlo più avanti nella procedura.



3. Collegare le porte di gestione e console al modulo controller node2.

> Poiché lo chassis è già acceso, node2 avvia l'inizializzazione del BIOS seguita da AUTOBOOT non appena è completamente inserito. Per interrompere l'avvio del nodo 2, prima di inserire completamente il modulo controller nello slot, si consiglia di collegare i cavi della console seriale e di gestione al modulo controller del nodo 2.

4. Con la maniglia della camma in posizione aperta, spingere con decisione il modulo controller fino a quando non raggiunge la scheda intermedia e non è completamente inserito. Il dispositivo di chiusura si solleva quando il modulo controller è completamente inserito. Chiudere la maniglia della camma in posizione di blocco.

> Per evitare di danneggiare i connettori, non esercitare una forza eccessiva quando si fa scorrere il modulo controller nel telaio.

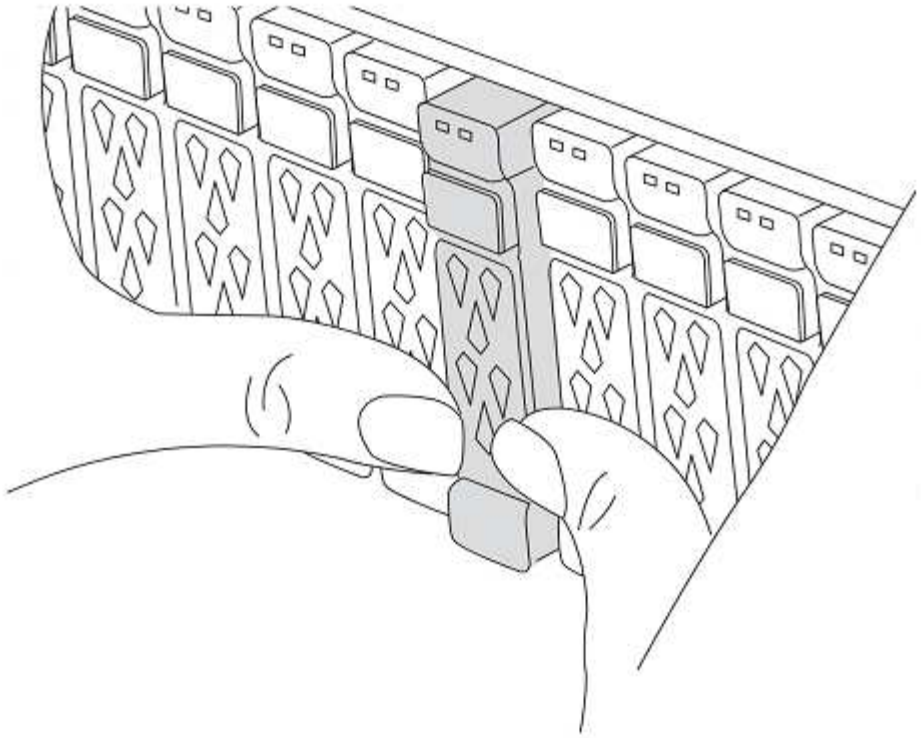
5. Collegare la console seriale non appena il modulo è inserito e prepararsi a interrompere l'AUTOBOOT del nodo 2.
6. Dopo aver interrotto L'AUTOBOOT, node2 si ferma al prompt DEL CARICATORE. Se non INTERROMPETE L'AUTOBOOT in tempo e node2 inizia l'avvio, attendete il prompt e premete Ctrl-C per entrare nel menu di avvio. Dopo che il nodo si è fermato al menu di avvio, utilizzare opzione `8` per riavviare il nodo e interrompere l'AUTOBOOT durante il riavvio.
7. Al prompt LOADER> di node2, impostare le variabili di ambiente predefinite:

   ```
   set-defaults
   ```

8. Salvare le impostazioni predefinite delle variabili di ambiente:

   ```
   saveenv
   ```

9. Sulla parte anteriore del telaio, utilizzare i pollici per spingere con decisione ogni unità negli alloggiamenti superiore e inferiore finché non si avverte un arresto sicuro. In questo modo si garantisce che le unità siano saldamente fissate al piano intermedio del telaio.



a. Andare sul retro del telaio.

Installare il modulo controller ASA A150, AFF A150 o FAS2820 su node2

Installare il modulo controller ASA A150, AFF A150 o FAS2820 ricevuto per l'aggiornamento su node2. Il nodo 2 è il controller B situato sul lato destro dello chassis guardando i controller dal retro del sistema.

Prima di iniziare

- Se non si è già collegati a terra, mettere a terra correttamente.
- Scollegare tutti i cavi, inclusi console, gestione, storage SAS e rete dati, dal controller da rimuovere.

Fasi

1. Allineare l'estremità del modulo controller con l'alloggiamento B dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.

   Il vano B si trova sul lato destro del telaio.

   Non inserire completamente il modulo controller nel telaio fino a quando non viene richiesto di farlo successivamente nella procedura.

2. Collegare le porte di gestione e console al modulo controller node2.

   Poiché lo chassis è già acceso, node2 inizia l'avvio non appena è completamente inserito. Per impedire l'avvio di node2, collegare i cavi della console e di gestione prima di inserire completamente il modulo controller.

3. Spingere con decisione il modulo controller nello chassis fino a quando non raggiunge la scheda

intermedia e non è completamente inserito.

Il dispositivo di chiusura si solleva quando il modulo controller è completamente inserito.

> Per evitare di danneggiare i connettori, non esercitare una forza eccessiva quando si fa scorrere il modulo controller nel telaio.

4. Collegare la console seriale non appena il modulo è inserito e prepararsi a interrompere l'AUTOBOOT del nodo 2.
5. Dopo aver interrotto L'AUTOBOOT, node2 si ferma al prompt DEL CARICATORE. Se non INTERROMPETE L'AUTOBOOT in tempo e node2 inizia l'avvio, attendete il prompt e premete Ctrl-C per entrare nel menu di avvio. Dopo che il nodo si è fermato al menu di avvio, utilizzare opzione `8` per riavviare il nodo e interrompere l'AUTOBOOT durante il riavvio.

Installare la NVRAM ASA A900, AFF A900 o FAS9500 e i moduli controller su node2

Installare la NVRAM ASA A900, AFF A900 o FAS9500 e i moduli controller ricevuti per l'aggiornamento su node2. Il nodo 2 è il controller B situato sul lato destro dello chassis guardando i controller dal retro del sistema.

Quando si esegue l'installazione, tenere presente quanto segue:

- Spostare tutti i moduli di riempimento vuoti negli slot 6-1 e 6-2 dal vecchio modulo NVRAM al nuovo modulo NVRAM.
- NON spostare il dispositivo di scarico dal modulo NVRAM AFF A700 al modulo NVRAM ASA A900 o AFF A900.
- Spostare tutti i moduli flash cache installati nel modulo NVRAM FAS9000 nel modulo NVRAM FAS9500.

Prima di iniziare

Se non si è già collegati a terra, mettere a terra correttamente.

Installare il modulo NVRAM ASA A900, AFF A900 o FAS9500

Installare il modulo NVRAM ASA A900, AFF A900 o FAS9500 nello slot 6 di node2.

Fasi

1. Allineare il modulo NVRAM ai bordi dell'apertura dello chassis nello slot 6.
2. Far scorrere delicatamente il modulo NVRAM nello slot fino a quando il dispositivo di chiusura della camma i/o con lettere e numeri inizia a innestarsi nel perno della camma i/o, quindi spingere il dispositivo di chiusura della camma i/o fino in fondo per bloccare il modulo NVRAM in posizione.

Installare il modulo controller ASA A900, AFF A900 o FAS9500 in node2

Installare, collegare e collegare il modulo controller ASA A900, AFF A900 o FAS9500 in node2.

Fasi

1. Allineare l'estremità del modulo controller con l'alloggiamento B dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.

> L'etichetta dell'alloggiamento si trova sul telaio direttamente sopra il modulo controller.

Non inserire completamente il modulo controller nel telaio fino a quando non viene richiesto di farlo successivamente nella procedura.

2. Collegare le porte di gestione e console al modulo controller node2.

Poiché lo chassis è già acceso, node2 inizia l'avvio non appena è completamente inserito. Per evitare l'avvio node2, si consiglia di collegare la console e i cavi di gestione al modulo controller node2 prima di inserire completamente il modulo controller nello slot.

3. Spingere con decisione il modulo controller nello chassis fino a quando non raggiunge la scheda intermedia e non è completamente inserito.

   Il dispositivo di chiusura si solleva quando il modulo controller è completamente inserito.

Per evitare di danneggiare i connettori, non esercitare una forza eccessiva quando si fa scorrere il modulo controller nel telaio.

4. Collegare la console seriale non appena il modulo è inserito e prepararsi a interrompere l'AUTOBOOT del nodo 2.
5. Dopo aver interrotto L'AUTOBOOT, node2 si ferma al prompt DEL CARICATORE. Se non INTERROMPETE L'AUTOBOOT in tempo e node2 inizia l'avvio, attendete il prompt e premete Ctrl-C per entrare nel menu di avvio. Dopo che il nodo si è fermato al menu di avvio, utilizzare opzione `8` per riavviare il nodo e interrompere l'AUTOBOOT durante il riavvio.
6. Al prompt LOADER> di node2, impostare le variabili di ambiente predefinite:

   ```
   set-defaults
   ```

7. Salvare le impostazioni predefinite delle variabili di ambiente:

   ```
   saveenv
   ```

Node2 NetBoot

Dopo aver scambiato i corrispondenti moduli di sistema node2 sostitutivi, potrebbe essere necessario eseguire il netboot. Il termine netboot significa 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.

Non è possibile verificare la versione di ONTAP installata sul supporto di avvio del modulo controller sostitutivo, a meno che non sia installato in uno chassis e acceso. La versione di ONTAP sul supporto di avvio del sistema sostitutivo deve essere la stessa della versione di ONTAP in esecuzione sul vecchio sistema che si sta aggiornando e le immagini di avvio primaria e di backup devono corrispondere. È possibile configurare le immagini eseguendo un netboot seguito da `wipeconfig` comando dal menu di avvio. Se il modulo controller è stato precedentemente utilizzato in un altro cluster, `wipeconfig` comando cancella ogni configurazione residua sul supporto di avvio.

Per eseguire l'avvio da rete, è possibile utilizzare anche l'opzione di avvio USB. 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.
- Scaricare i file di sistema necessari per il sistema e la versione corretta di ONTAP dal *sito di supporto NetApp*. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp*.

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. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* e scaricare i file utilizzati per eseguire il netboot del sistema.
2. Scarica il software ONTAP appropriato dalla sezione di download del software del sito di supporto NetApp e memorizza 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.
4. L'elenco delle directory deve contenere `<ontap_version>_image.tgz`.
5. 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 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.

6. Eseguire il netboot al nodo 2:

`netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`

Non interrompere l'avvio.

7. Attendere che il node2 ora in esecuzione sul modulo controller sostitutivo si avvii e visualizzare le opzioni del menu di avvio come mostrato nell'output seguente:

```
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)?
```

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`

   Questa nota si applica agli aggiornamenti software ONTAP senza interruzioni e non agli aggiornamenti del 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`

   Il `<path_to_the_web-accessible_directory>` dovrebbe portare alla posizione in cui è stato scaricato `<ontap_version>_image.tgz` poll Fase 2.

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. Cancellare qualsiasi configurazione precedente sul supporto di avvio.

    a. Al prompt seguente, eseguire il comando `wipeconfig` comando e premere il tasto Invio:

    ```
    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)? wipeconfig
    ```

    b. Quando viene visualizzato il messaggio riportato di seguito, rispondere `yes`:

    ```
    This will delete critical system configuration, including cluster
    membership.
    Warning: do not run this option on a HA node that has been taken
    over.
    Are you sure you want to continue?:
    ```

    c. Il nodo viene riavviato per terminare `wipeconfig` e poi si ferma al menu di boot.

Attendi che il nodo si arresti nel menu di avvio dopo aver completato l'operazione `wipeconfig` operazione.

12. Selezionare la modalità di manutenzione `5` dal menu di boot e premere `y` quando viene richiesto di continuare con l'avvio.
13. 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
    ```

14. 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`

15. Arrestare il nodo 2:

    `halt`

    Node2 dovrebbe arrestarsi al prompt LOADER>.

16. Al nodo 1, controllare la data, l'ora e il fuso orario del sistema:

    `date`

17. Al nodo 2, controllare la data utilizzando il seguente comando al prompt dell'ambiente di boot:

    `show date`

18. Se necessario, impostare la data sul node2:

    `set date` *`mm/dd/yyyy`*

    Impostare la data UTC corrispondente al nodo 2.

19. In node2, controllare l'ora utilizzando il seguente comando al prompt dell'ambiente di boot:

    `show time`

20. Se necessario, impostare l'ora su node2:

    `set time` *`hh:mm:ss`*

Impostare l'ora UTC corrispondente al nodo 2.

21. Impostare l'ID del sistema partner su node2:

    `setenv partner-sysid node1_sysid`

    Per il node2, il `partner-sysid` deve essere quello del node1 che si sta aggiornando.

    a. Salvare le impostazioni:

       `saveenv`

22. All'accensione del node2, al prompt DEL CARICATORE, verificare `partner-sysid` per il nodo 2:

    `printenv partner-sysid`

Fase 6. Fare il boot node2 con i moduli di sistema sostitutivi

Cavo node2 per cluster-ha e storage condivisi

Se si esegue uno dei seguenti aggiornamenti, è necessario connettere le connessioni cluster, HA, storage, dati e gestione precedentemente connesse al node2 sul sistema esistente al node2 appena installato sul sistema sostitutivo.

Sistema esistente	Sistema sostitutivo
AFF A250	AFF A30, AFF A50
AFF C250	AFF C30, AFF C60
AFF A800	AFF A70, AFF A90
AFF C800	AFF C80

Collegare le porte e0M e BMC

Se il sistema esistente dispone di una porta di gestione (e0M) e di una porta BMC, le porte e0M e BMC sono combinate e accessibili attraverso la porta "chiave inglese" sul sistema sostitutivo. Prima di eseguire la connessione al sistema sostitutivo, è necessario assicurarsi che le porte e0M e BMC siano connesse allo stesso switch e alla stessa subnet del sistema esistente.

Se…	Quindi…
Gli indirizzi IP e0M e BMC si trovano sulla stessa subnet IP	Collegare la porta e0M o BMC del sistema esistente alla porta "chiave" del sistema sostitutivo.
Gli indirizzi IP e0M e BMC si trovano su sottoreti diverse	1. Unire gli indirizzi IP e0M e BMC in un'unica subnet IP. 2. Collegare la porta e0M o BMC del sistema esistente alla porta "chiave" del sistema sostitutivo.

Connettersi a un cluster senza switch a due nodi

Le tabelle seguenti mostrano l'utilizzo delle porte dello switch per le configurazioni cluster senza switch a due nodi.

Tipo di porta	AFF A800, AFF C800	AFF A90	AFF A70, AFF C80
Cluster	e0a	e1a	e1a
Cluster	e1a	e7a (utilizzare e1b se non è presente e7a)	e1b
HA	e0b	Non connetterti	Non connetterti
HA	e1b	Non connetterti	Non connetterti
Porte di storage SAS (se presenti e utilizzate)	Qualsiasi porta disponibile	Qualsiasi porta disponibile	Qualsiasi porta disponibile
Porte di storage Ethernet per NS224 shelf	Qualsiasi porta disponibile	Fare riferimento alla mappatura della connettività dello storage Ethernet	Fare riferimento alla mappatura della connettività dello storage Ethernet

Tipo di porta	AFF A250, AFF C250	AFF A30, AFF C60	AFF A50
Cluster	e0c	e1a (utilizzare e1a per l'interconnessione temporanea del cluster)	e1a (utilizzare e1a per l'interconnessione temporanea del cluster)
Cluster	e0d	e1b (utilizzare e1b per l'interconnessione temporanea del cluster)	e1b (utilizzare e1b per l'interconnessione temporanea del cluster)
HA	La porta e0c HA è condivisa con la porta del cluster	e4a sul nodo 1 è collegato direttamente a e4a sul nodo 2 tramite un cavo da 100 GbE	e4a sul nodo 1 è collegato direttamente a e4a sul nodo 2 tramite un cavo da 100 GbE
HA	La porta e0d HA è condivisa con la porta del cluster	e2a sul nodo 1 è collegato direttamente a e2a sul nodo 2 tramite un cavo da 100 GbE. Se e2a non è presente o non supporta 100 GbE, collegare direttamente e4b sul nodo 1 a e4b sul nodo 2 tramite un cavo da 100 GbE.	e2a sul nodo 1 collegato direttamente a e2a sul nodo 2 tramite un cavo da 100 GbE. Se e2a non è presente o non supporta 100 GbE, collegare direttamente e4b sul nodo 1 a e4b sul nodo 2 tramite un cavo da 100 GbE.
Porta di archiviazione Ethernet	Qualsiasi porta disponibile	e3a, e3b	e3a, e3b
Porta di archiviazione SAS	Qualsiasi porta disponibile	3a, 3b	3a, 3b

Connettersi a un cluster collegato allo switch

Per un cluster con collegamento a switch, verificare di soddisfare i seguenti requisiti per il nodo (sostitutivo) AFF A30, AFF A50, AFF A70, AFF A90, AFF C30, AFF C60 o AFF C80:

- Le porte cluster identiche sul nodo di sostituzione si trovano sullo stesso switch. Ad esempio, al termine dell'upgrade, collegare E1a su node1 e E1a su node2 a uno switch del cluster. Analogamente, la seconda porta cluster di entrambi i nodi deve essere collegata al secondo switch cluster. La connessione incrociata tra porte ha e cluster condivisi, in cui E1a di node1 è connesso allo switch e E1a di node2 è connesso allo switch, causa errori di comunicazione ha.
- Il nodo sostitutivo utilizza porte Ethernet ha-cluster condivise.
- Verificare che gli switch del cluster siano installati con un file di configurazione di riferimento (RCF) che supporti le porte condivise cluster-ha:
  a. Rimuovere la configurazione esistente sullo switch:

Se il modello dello switch in uso è…	**Vai a…**
Cisco Nexus	Articolo della Knowledge base "Come cancellare la configurazione su uno switch Cisco Interconnect mantenendo la connettività remota"
Broadcom BES-53248	Articolo della Knowledge base "Come cancellare la configurazione su uno switch di interconnessione Broadcom mantenendo la connettività remota"

  b. Configurare e verificare l'impostazione dello switch:

Se il modello dello switch in uso è…	**Vai a…**
Cisco Nexus 9336C-FX2	"Aggiornamento del file di configurazione di riferimento (RCF)"
Broadcom BES-53248	"Aggiornamento del file di configurazione di riferimento (RCF)"
NVIDIA SN2100	"Installare o aggiornare lo script RCF (Reference Configuration file)"

Se lo switch del cluster supporta solo velocità 10/25 GbE, è necessario utilizzare una scheda X60130A a 4 porte 10/25 GbE nello slot 1 o nello slot 2 del sistema sostitutivo per l'interconnessione del cluster.

Fare il boot node2 con i moduli di sistema sostitutivi

Node2 con i moduli sostitutivi è ora pronto per l'avvio. I moduli sostitutivi supportati sono elencati in"matrice dei sistemi supportati" .

È possibile spostare la console e le connessioni di gestione solo quando si esegue l'aggiornamento scambiando i moduli di sistema.

Fasi

1. Se sono installate unità NetApp Storage Encryption (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**`

Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha. È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

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".

2. Avviare il nodo nel menu di boot:

```
boot_ontap menu
```

3. Quando il nodo si ferma al menu di avvio, riassegnare i vecchi dischi node2 al node2 sostitutivo eseguendo il seguente comando su node2:

```
boot_after_controller_replacement
```

Dopo un breve intervallo di tempo, viene richiesto di inserire il nome del nodo da sostituire. Se sono presenti dischi condivisi (chiamati anche Advanced Disk Partitioning (ADP) o dischi partizionati), viene richiesto di inserire il nome del nodo del partner ha.

Questi prompt potrebbero essere interrati nei messaggi della console. Se non si immette un nome di nodo o non si immette un nome corretto, viene richiesto di inserire nuovamente il nome.

Se `[localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified encrypting drive` e, oppure `[localhost:diskown.errorDuringIO:error]: error 3 (disk failed) on disk` in caso di errori, attenersi alla seguente procedura:

a. Arrestare il nodo al prompt DEL CARICATORE.
b. Controllare e ripristinare i bootargs di crittografia dello storage indicati nella Fase 1.
c. Al prompt del CARICATORE, avviare:

```
boot_ontap
```

È possibile utilizzare il seguente esempio come riferimento:

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>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner 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:
```

Gli ID di sistema mostrati nell'esempio precedente sono ID di esempio. Gli ID di sistema effettivi dei nodi che si stanno aggiornando saranno diversi.

Tra l'immissione dei nomi dei nodi al prompt e il prompt di accesso, il nodo viene riavviato alcune volte per ripristinare le variabili di ambiente, aggiornare il firmware sulle schede del sistema e per altri aggiornamenti del ONTAP.

Verificare l'installazione di node2

Verificare l'installazione del nodo 2 con i moduli di sistema sostitutivi. Poiché non sono state apportate modifiche alle porte fisiche, non è necessario mappare le porte fisiche dal vecchio nodo 2 al nodo sostituz.2.

A proposito di questa attività

Una volta avviato il nodo 1 con il modulo di sistema sostitutivo, verificare che sia installato correttamente. È necessario attendere che node2 si unisca al quorum e quindi riprendere l'operazione di sostituzione del controller.

A questo punto della procedura, l'operazione viene messa in pausa mentre il nodo 2 si unisce al quorum.

Fasi

1. Verificare che node2 si sia Unito al quorum:

   ```
   cluster show -node node2 -fields health
   ```

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

2. Questo passaggio si applica alle seguenti configurazioni di aggiornamento. Per tutti gli altri aggiornamenti di sistema, saltare questo passaggio e andare a Fase 3 :

   - Cluster switchless a due nodi
   - Passare dai sistemi AFF A250 o AFF C250 collegati a un sistema AFF A50, AFF A30, AFF C30 o AFF C60.

   Se node2 non si unisce automaticamente al quorum:

   a. Controllare lo spazio IP delle porte e1a ed e1b:

      ```
      network port show
      ```

   b. Se lo spazio IP non è "Cluster", modifica lo spazio IP in "Cluster" su e1a ed e1b:

      ```
      network port modify -node <node_name> -port <port> -ipspace Cluster
      ```

   c. Verificare che lo spazio IP delle porte e1a ed e1b sia "Cluster":

      ```
      network port show
      ```

d. Migrare i LIF del cluster node2 a e1a ed e1b:

```
network interface migrate -vserver Cluster -lif <cluster_lif1> -destination
-node <node2_name> -destination-port <port_name
```

3. Verifica che node2 e node1 facciano parte dello stesso cluster e che il cluster sia integro:

```
cluster show
```

4. Passare alla modalità avanzata dei privilegi:

```
set advanced
```

5. Questo passaggio si applica solo agli aggiornamenti di configurazione switchless a due nodi da un AFF A250 o AFF C250 a un AFF A50, AFF A30, AFF C60 o AFF C30. Per tutti gli altri aggiornamenti di sistema, saltare questo passaggio e andare a Fase 6 :

   Verificare che le porte e4a, e2a, e1a, e1b oppure le porte e4a, e4b, e1a, e1b siano le porte del cluster nel dominio di broadcast "Cluster".

   I sistemi AFF A50, AFF A30, AFF C30 e AFF C60 condividono porte cluster e HA. È possibile migrare in sicurezza tutti i LIF del cluster a e4a, e4b o e4a, e2a su node1 e node2:

   a. Elenca le porte domestiche e le porte correnti per tutti i LIF del cluster:

   ```
   network interface show -role Cluster -fields home-port,curr-port
   ```

   b. Su node1 e node2, migrare i LIF del cluster che utilizzano e1a come porta home su e4a:

   ```
   network interface migrate -vserver Cluster -lif <cluster_lif1> -destination
   -node <node> -destination-port e4a
   ```

   c. Su node1 e node2, modificare i cluster LIF migrati in sottofase b per utilizzare e4a come porta di casa:

   ```
   network interface modify -vserver Cluster -lif <cluster_lif> -home-port e4a
   ```

   d. Verificare che il cluster sia in quorum:

   ```
   cluster show
   ```

   e. Ripetere sottofase b e sottofase c per migrare e modificare il secondo cluster LIF su ciascun nodo in e2a o e4b:

   Se e2a è presente ed è una porta di rete 100GbE, questa è la seconda porta predefinita del cluster. Se e2a non è una porta di rete 100GbE, ONTAP utilizza e4b come seconda porta del cluster e HA.

   f. Rimuovere e1a ed e1b dal dominio di broadcast "Cluster":

   ```
   broadcast-domain remove-ports -broadcast-domain Cluster -ipspace Cluster
   -ports <node_name>:e1a
   ```

   g. Verificare che solo le porte del cluster e4a, e2a o e4a, e4b siano nel dominio di broadcast "Cluster"

   ```
   broadcast domain show
   ```

h. Rimuovere i collegamenti via cavo tra e1a node1 ed e1a node2 e tra e1b node1 ed e1b node2 per garantire che vengano utilizzate solo connessioni cluster-HA valide e che non vi sia alcuna connettività ridondante.

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

```
system controller replace show

system controller replace show-details
```

7. Riprendere l'operazione di sostituzione del controller:

```
system controller replace resume
```

8. L'operazione di sostituzione del controller viene interrotta per l'intervento con il seguente messaggio:

```
Cluster::*> system controller replace show
Node          Status                       Error-Action
------------  -------------------------
-----------------------------------
Node2         Paused-for-intervention      Follow the instructions given
in
                                           Step Details
Node1         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 node2*.

9. Con la sostituzione del controller in stato di pausa, passare a. Ripristinare la configurazione di rete sul nodo 2.

Ripristinare la configurazione di rete sul nodo 2

Dopo aver confermato che node2 è in quorum e può comunicare con node1, verificare che le VLAN, i gruppi di interfacce e i domini di broadcast di node1 siano visibili sul node2. Inoltre, verificare che tutte le porte di rete node2 siano configurate nei 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 al contenuto di *Network Management*.

Fasi

1. Elencare tutte le porte fisiche sul nodo aggiorno2:

   ```
   network port show -node node2
   ```

   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 2:

   ```
   network port reachability show -node node2
   ```

   L'output dovrebbe essere simile all'esempio seguente. I nomi delle porte e delle trasmissioni variano.

```
Cluster::> reachability show -node node1
  (network port reachability show)
Node      Port     Expected Reachability                Reachability
Status
--------- -------- ----------------------------------
---------------------
Node1
          a0a      Default:Default                      ok
          a0a-822  Default:822                          ok
          a0a-823  Default:823                          ok
          e0M      Default:Mgmt                         ok
          e1a      Cluster:Cluster                      ok
          e1b      -                                    no-reachability
          e2a      -                                    no-reachability
          e2b      -                                    no-reachability
          e3a      -                                    no-reachability
          e3b      -                                    no-reachability
          e7a      Cluster:Cluster                      ok
          e7b      -                                    no-reachability
          e9a      Default:Default                      ok
          e9a-822  Default:822                          ok
          e9a-823  Default:823                          ok
          e9b      Default:Default                      ok
          e9b-822  Default:822                          ok
          e9b-823  Default:823                          ok
          e9c      Default:Default                      ok
          e9d      Default:Default                      ok
20 entries were displayed.
```

Nell'esempio precedente, node2 si è avviato e si è Unito al quorum dopo la sostituzione del controller. Dispone di diverse porte che non sono raggiungibilità e che sono in attesa di una scansione di raggiungibilità.

4. riparare la raggiungibilità per ciascuna delle porte su node2 con uno stato di raggiungibilità diverso da `ok` utilizzando il seguente comando, nel seguente ordine:

`network port reachability repair -node` *`node_name`* `-port` *`port_name`*

a. Porte fisiche
b. Porte VLAN

L'output dovrebbe essere simile al seguente esempio:

```
Cluster ::> reachability repair -node node2 -port e9d
```

```
Warning: Repairing port "node2:e9d" 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 nell'esempio precedente, è previsto per le porte con uno stato di raggiungibilità che potrebbe essere diverso dallo stato di raggiungibilità del dominio di broadcast 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. 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.

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

   ```
   network port show
   ```

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

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

8. 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:

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

9. 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 2

Se si utilizza NetApp aggregate Encryption (NAE) o NetApp Volume Encryption (NVE) per crittografare i volumi sul sistema che si sta aggiornando, la configurazione della crittografia deve essere sincronizzata con i nuovi nodi. Se non si risincronizza il gestore delle chiavi, quando si trasferono gli aggregati node2 dal nodo aggiornato1 al nodo aggiornato2 utilizzando ARL, potrebbero verificarsi errori perché node2 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 node2:

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

2. Prima di spostare gli aggregati di dati, verificare che la chiave SVM-KEK sia ripristinata su "true" in node2:

   ```
   ::> security key-manager key query -node node2 -fields restored -key
   -type SVM-KEK
   ```

   Esempio

   ```
   ::> security key-manager key query -node node2 -fields restored -key
   -type SVM-KEK

   node     vserver   key-server   key-id
   restored
   -------- --------- -----------  ----------------------------------------
   --------
   node2    svm1      ""           000000000000000020000000000a008a81976
   true
                                   2190178f9350e071fbb90f00000000000000000
   ```

Verificare la configurazione RCF sugli switch del cluster

In questa fase della procedura di aggiornamento, tutti gli aggregati di dati dovrebbero trovarsi sul nodo 1. Se si sta aggiornando una configurazione con cluster collegati allo switch, è necessario verificare che il file di configurazione di riferimento dello switch del cluster (RCF) supporti le porte cluster/HA condivise per i nuovi controller.

Se si sta eseguendo l'aggiornamento a una configurazione cluster switchless a due nodi, è possibile saltare questa sezione e passare a"Riportare al nodo gli aggregati non root e le LIF dei dati NAS 2" .

Fasi

1. Passare alla modalità avanzata dei privilegi:

   ```
   set advanced
   ```

2. Controllare lo stato di "IC RDMA":

   ```
   ha interconnect status show
   ```

   Nell'output, la "Connessione IC RDMA" dovrebbe avere lo stato `Up` .

Se lo stato "IC RDMA Connection" è …	Quindi…
`Up`	Vai a"Riportare al nodo gli aggregati non root e le LIF dei dati NAS 2" .
`Down`	Vai aFase 3 .

3. Controllare le porte del cluster e commutare RCF.

   Per ulteriori informazioni, vedere "Connettersi a un cluster collegato allo switch".

4. Verificare che lo stato "IC RDMA Connection" sia cambiato in `Up` :

   ```
   ha interconnect status show
   ```

Cosa c'è dopo?

"Riportare al nodo gli aggregati non root e le LIF dei dati NAS 2"

Riportare al nodo gli aggregati non root e le LIF dei dati NAS 2

Dopo aver verificato la configurazione di rete sul nodo 2, è necessario spostare i LIF dei dati NAS di proprietà del nodo 2 dal nodo 1 al nodo 2 e confermare che i LIF SAN siano presenti sul nodo 2.

A proposito di questa attività

I LIF remoti gestiscono il traffico verso le LUN SAN durante la procedura di aggiornamento. Lo spostamento dei SAN LIF non è necessario per l'integrità del cluster o del servizio durante l'aggiornamento. I LIF SAN non vengono spostati a meno che non sia necessario mapparli su nuove porte.

Dopo aver portato online node2, è necessario verificare che i LIF siano integri e posizionati sulle porte corrette.

Fasi

1. 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

Il sistema sospende l'operazione in questa fase del controllo di raggiungibilità della rete

2. 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 in node2, che è ora in esecuzione sul controller sostitutivo.

L'operazione di sostituzione del controller viene interrotta al termine del trasferimento delle risorse.

3. 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.

4. Se necessario, ripristinare e ripristinare i LIF spostati oppure migrare e modificare manualmente i LIF del nodo 2 che non sono riusciti a trasferirsi automaticamente sul nodo 2.

Ripristinare e ripristinare i LIF spostati

a. Elencare eventuali LIF spostati:

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

b. In caso di spostamento di LIF, ripristinare il nodo home al nodo node2:

```
cluster controller-replacement network displaced-interface
restore-home-node -node <node2_nodename> -vserver <vserver name>
-lif-name <lif_name>
```

Migrare e modificare manualmente i LIF

a. Migrare i LIF che non sono riusciti a trasferirsi automaticamente al nodo 2:

```
network interface migrate -vserver <vserver name> -lif <lif_name>
-destination-node <node2_nodename> -destination-port
<port_on_node2>
```

b. Modificare il nodo home e la porta home per i LIF migrati:

```
network interface modify -vserver <vserver_name> -lif
<data_lif_name> -home-node <node2_nodename> -home-port
<home_port>
```

5. 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 7. Completare l’aggiornamento

Gestire l’autenticazione utilizzando i server KMIP

A partire da ONTAP 9.10.1, è possibile 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, verificare che la coppia ha sia attivata. Inoltre, è possibile verificare che node1 e node2 possano accedere reciprocamente allo storage e che nessuno dei due possieda le LIF dei dati appartenenti ad altri nodi del cluster. Inoltre, è possibile verificare che tutti gli aggregati di dati si trovino sui nodi principali corretti e che i volumi di entrambi i nodi siano online. Se uno dei nuovi nodi dispone di un adattatore di destinazione unificato, è necessario ripristinare le configurazioni delle porte e modificare l’utilizzo dell’adattatore.

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
----------  -----------     ------------  ------------------
node1       node2           true          Connected to node2
node2       node1           true          Connected to node1
```

3. Verificare che node1 e node2 appartengano allo stesso cluster utilizzando il seguente comando ed esaminando l'output:

   ```
   cluster show
   ```

4. Verificare che node1 e node2 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 node1 né node2 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 1 o node2 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 gli aggregati siano di proprietà dei rispettivi nodi principali.

   ```
   storage aggregate show -owner-name <node1>

   storage aggregate show -owner-name <node2>
   ```

7. Determinare se i volumi sono offline:

   ```
   volume show -node <node1> -state offline

   volume show -node <node2> -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 esaminandone l'output:

```
system license show
```

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

12. se nella configurazione vengono utilizzate unità con crittografia automatica ed è stato impostato `kmip.init.maxwait` variabile a. `off` (Ad esempio, in *Boot node2 with the replacement system modules*, "Fase 1"), 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: 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 node1 e node2, 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.

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 di gestione delle chiavi esterne. Riportare online quei volumi 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

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: Manuale riferimento pagina*.

Gli aggregati originalmente sul node1 sono di proprietà di node2 dopo il completamento dell'upgrade

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

A proposito di questa attività

Gli aggregati potrebbero non riuscire a riallocare correttamente, ovvero hanno node2 come nodo principale invece di node1, nelle seguenti circostanze:

- Durante la fase 3, quando gli aggregati vengono ricollocati dal nodo 2 al nodo 1.

  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 viene lasciato indietro al nodo 2.

- Dopo la fase 4, quando il node2 viene sostituito con i nuovi moduli di sistema.

  Quando node2 viene sostituito, aggr_node_1 verrà online con node1 come nodo home invece di node2.

È possibile risolvere il problema di proprietà errato dopo la fase 6, dopo aver attivato il failover dello storage,

completando la seguente procedura:

Fasi

1. Ottieni un elenco di aggregati:

   `storage aggregate show -nodes node2 -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 sul nodo 2:

   `storage aggregate relocation start -node node2 -aggr aggr_node_1 -destination node1`

   Non utilizzare il parametro -ndo-controller-upgrade durante questo trasferimento.

4. Verificare che node1 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 node1 come proprietario di casa possono essere ricollocati in node1 utilizzando lo stesso comando di rilocazione nella 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 serve ancora 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

Node1 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.

Node1 si blocca durante la prima fase di verifica con la coppia ha disattivata

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

Fasi

1. Far salire il node1.
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 node1. Node1 serve 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 node1.

Fasi

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

Node1 si blocca durante la prima fase di recupero delle risorse durante il trasferimento degli aggregati

Se node1 si blocca mentre node2 sta spostando gli aggregati in node1, l'attività continua dopo l'avvio di node1.

A proposito di questa attività

Node2 continua a servire gli aggregati rimanenti, ma gli aggregati che erano già stati ricollocati in node1 incontrano un'interruzione del client durante l'avvio di node1.

Fasi

1. Far salire il node1.
2. Continuare con l'aggiornamento del controller.

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

Node1 o node2 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

Node1 si blocca durante la seconda fase di rilascio delle risorse

Se node1 si blocca mentre node2 sta spostando gli aggregati, l'attività continua dopo l'avvio di node1.

A proposito di questa attività

Node2 continua a servire gli aggregati rimanenti, ma gli aggregati già ricollocati negli aggregati di node1 e node1 incontrano interruzioni del client durante l'avvio di node1.

Fasi

1. Far salire il node1.
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

Node1 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

Node1 si blocca durante la seconda fase di verifica

Se node1 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 nodo 1.

Fasi

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

Node2 si blocca durante la seconda fase di verifica

Se node2 si blocca durante questa fase, il takeover non si verifica. Node1 serve i dati degli aggregati.

A proposito di questa attività

Si verifica un'interruzione per gli aggregati non root che sono stati già ricollocati fino al riavvio di node2.

Fasi

1. Alzati il node2.
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

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.
"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.
"Gestione delle coppie HA"	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.
"Gestione MetroCluster e disaster recovery"	Descrive come eseguire le operazioni di switchover e switchback MetroCluster, sia nelle operazioni di manutenzione pianificate che in caso di disastro.

Contenuto	Descrizione
"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 9.0: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.0 supportati.
"Comandi di ONTAP 9.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.1 supportati.
"Comandi di ONTAP 9.2: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.2 supportati.
"Comandi di ONTAP 9.3: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.3 supportati.
"Comandi di ONTAP 9.4: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.4 supportati.
"Comandi di ONTAP 9.5: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.5 supportati.
"Comandi di ONTAP 9.6: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.6 supportati.
"Comandi di ONTAP 9.7: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.7 supportati.
"Comandi di ONTAP 9.8: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.8 supportati.
"Comandi di ONTAP 9.9.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.9.1 supportati.
"Comandi di ONTAP 9.10.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.10.1 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.

Contenuto	Descrizione
"Utilizzare i comandi "sostituzione controller di sistema" per aggiornare l'hardware del controller introdotto in ONTAP 9.15.1 e versioni successive"	Descrive le procedure di trasferimento degli aggregati necessarie per aggiornare senza interruzioni i controller introdotti in ONTAP 9.15.1 e versioni successive utilizzando i comandi "system controller replace".
"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.
"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.
"Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller che esegue ONTAP 9.5 a ONTAP 9.7"	Vengono descritte le procedure di riposizionamento degli aggregati necessarie per aggiornare senza interruzioni i controller che eseguono ONTAP 9.5 a ONTAP 9.7 utilizzando i comandi "system controller replace".
"Utilizzare il trasferimento di aggregati per aggiornare manualmente l'hardware del controller con ONTAP 9.7 o versione precedente"	Descrive le procedure di trasferimento degli aggregati necessarie per eseguire aggiornamenti manuali dei controller senza interruzioni con ONTAP 9.7 o versione precedente.

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.

Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller con ONTAP 9.8 o versione successiva

Scopri di più sulla procedura di aggiornamento ARL

Esistono diversi metodi di ricollocazione aggregata (ARL) per aggiornare l'hardware del controller. Questa procedura descrive come aggiornare l'hardware del controller utilizzando la ricollocazione aggregata (ARL) con "comandi di sostituzione del controller di sistema" su sistemi che eseguono ONTAP 9.8 o versioni successive.

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. Devi anche leggere e comprendere il "linee guida per l'aggiornamento dei controller con ARL" e il "Sequenza di 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 `wipeconfig` i comandi non sono inclusi in questa procedura. È necessario contattare il supporto tecnico se l'hardware del controller sostitutivo è stato utilizzato in precedenza, soprattutto se i controller eseguivano Data ONTAP in modalità 7.
- È possibile utilizzare ARL per eseguire un aggiornamento semplificato senza interruzioni del controller a un nuovo controller che esegue una versione ONTAP successiva rispetto alla versione in esecuzione sul cluster che si sta aggiornando. Le combinazioni della versione ONTAP per i controller vecchi e nuovi sono determinate dal modello di cadenza NDU della release software ONTAP. Ad esempio, se si dispone di un controller che esegue ONTAP 9.8 e si tratta dell'ultima versione supportata per tale controller, è possibile eseguire l'aggiornamento a un nuovo controller che esegue una versione di ONTAP successiva a ONTAP 9.8.

  Questa procedura di aggiornamento si applica principalmente agli scenari di aggiornamento in cui il modello di controller da sostituire non supporta le versioni successive di ONTAP e il nuovo controller non supporta le versioni precedenti di ONTAP.

- 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.
- Questa procedura si applica ai sistemi FAS e AFF .
- Questa procedura si applica ai sistemi che eseguono la configurazione NetApp MetroCluster a 4 nodi o superiore. Poiché i siti di configurazione MetroCluster possono trovarsi in due posizioni fisicamente diverse, l'aggiornamento automatizzato del controller deve essere eseguito singolarmente in ciascun sito MetroCluster per una coppia ha.
- Per i sistemi non MetroCluster, come i cluster ha, l'upgrade ARL è l'unica procedura supportata.
- Se si sta eseguendo l'aggiornamento da un sistema AFF A320, è possibile utilizzare i movimenti dei volumi per aggiornare l'hardware del controller o contattare il supporto tecnico. Fare riferimento a. "Riferimenti" Per collegarsi a *Upgrade spostando volumi o storage*.

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. Le versioni precedenti di

questo contenuto contenevano istruzioni per un processo di aggiornamento del controller senza interruzioni, che comprendeva passaggi interamente manuali. Questo contenuto fornisce i passaggi per la nuova procedura automatica che utilizza i controlli automatici di raggiungibilità delle porte di rete per semplificare ulteriormente l'esperienza di upgrade del controller.

Il processo manuale è stato lungo e complesso, ma in questa procedura semplificata è possibile implementare un aggiornamento del controller utilizzando il trasferimento degli aggregati, consentendo aggiornamenti più efficienti e senza interruzioni per le coppie ha. Le procedure manuali sono notevolmente inferiori, in particolare per quanto riguarda la convalida, la raccolta di informazioni e i controlli successivi.

Decidere se utilizzare questa procedura di ricollocazione aggregata

Esistono diversi metodi di ricollocazione aggregata (ARL) per aggiornare l'hardware del controller. Questa procedura descrive come aggiornare l'hardware del controller utilizzando la ricollocazione aggregata (ARL) con "comandi di sostituzione del controller di sistema" su sistemi che eseguono ONTAP 9.8 o versioni successive. Questa complessa procedura dovrebbe essere utilizzata solo da amministratori ONTAP esperti.

Per aiutarti a decidere se questa procedura ARL è adatta all'aggiornamento hardware del tuo controller, dovresti esaminare tutte le seguenti circostanze per gli aggiornamenti supportati:

- Sul computer è in esecuzione ONTAP 9,8 o versione successiva.
- Non vuoi aggiungere i nuovi controller come nuova coppia ha al cluster e migrare i dati utilizzando gli spostamenti dei volumi.
- Si è esperti nell'amministrazione di ONTAP e si è soddisfatti dei rischi di lavorare in modalità privilegi diagnostici.
- Durante l'upgrade di una configurazione MetroCluster, si tratta di una configurazione FC a quattro nodi o superiore che utilizza ONTAP 9,8 o versioni successive.

  Per aggiornare le configurazioni IP di MetroCluster, fare riferimento al "Riferimenti"collegamento *aggiornamento ed espansione MetroCluster*.

- Se si sta aggiornando un sistema scambiando i moduli del controller nello stesso chassis, come AFF A800 o AFF C800, NetApp consiglia vivamente di utilizzare la procedura di aggiornamento che"aggiorna i modelli di controller utilizzando ARL, mantenendo lo chassis e i dischi del sistema esistenti" . Questa procedura ARL include i passaggi che garantiscono che i dischi interni rimangano saldamente nello chassis quando si rimuovono e si installano i controller durante la procedura di aggiornamento.

  "Scopri le combinazioni di aggiornamento del sistema supportate utilizzando ARL, mantenendo lo chassis e i dischi del sistema esistenti".

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

Combinazioni di aggiornamento del sistema supportate

Nella tabella seguente viene mostrata la matrice dei sistemi supportati per eseguire un aggiornamento del controller utilizzando questa procedura ARL.

Vecchio controller	Controller sostitutivo
FAS8020[3], FAS8040[3], FAS8060, FAS8080	FAS8200, FAS8300, FAS8700, FAS9000
FAS8060[4], FAS8080[4]	FAS9500
AFF8020[3], AFF8040[3], AFF8060, AFF8080	AFF A300, AFF A400, AFF A700, AFF A800[1]
AFF8060[4], AFF8080[4]	AFF A900
FAS8200	FAS8300[2], FAS8700, FAS9000, FAS9500
FAS8300, FAS8700, FAS9000	FAS9500
AFF A300	AFF A400[2], AFF A700, AFF A800[1], AFF A900
AFF A320[4]	AFF A400
AFF A400, AFF A700	AFF A900

Se la combinazione del modello di aggiornamento del controller non è riportata nella tabella precedente, contattare il supporto tecnico.

[1]per i passaggi aggiuntivi necessari per i sistemi AFF A800, andare al passo che fa riferimento a A800 nella sezione "Riassegnare node1 dischi a node3, passaggio 9", o "Riassegnare node2 dischi a node4, passaggio 9".

[2]se stai eseguendo l'aggiornamento da un AFF A300 a un AFF A400 o da un FAS8200 a un sistema FAS8300 in una configurazione cluster senza switch a due nodi, devi scegliere le porte cluster temporanee per l'aggiornamento del controller. I sistemi AFF A400 e FAS8300 sono disponibili in due configurazioni, come bundle Ethernet in cui le porte della scheda mezzanine sono di tipo Ethernet e come bundle FC in cui le porte mezzanine sono di tipo FC.

- Per un sistema AFF A400 o FAS8300 con configurazione di tipo Ethernet, è possibile utilizzare una qualsiasi delle due porte mezzanine come porte cluster temporanee.
- Per un sistema AFF A400 o FAS8300 con configurazione di tipo FC, è necessario aggiungere una scheda di interfaccia di rete 10GbE a quattro porte (codice X1147A) per fornire porte cluster temporanee.
- Dopo aver completato un aggiornamento del controller utilizzando porte cluster temporanee, è possibile migrare senza interruzioni le LIF del cluster a e3a ed e3b, porte 100GbE su un sistema AFF A400 e porte e0c ed e0d, 100GbE su un sistema FAS8300.

[3]per gli aggiornamenti dei sistemi FAS8020, FAS8040, AFF8020 e AFF8040 ai controller sostitutivi di destinazione elencati nella tabella precedente, i controller sostitutivi devono eseguire la stessa versione ONTAP del vecchio controller. I sistemi FAS8020, FAS8040, AFF8020 e AFF8040 non supportano le versioni di ONTAP successive a ONTAP 9.8.

[4]la tabella seguente mostra le versioni minime e successive di ONTAP supportate per queste combinazioni di upgrade del controller.

Vecchio controller		Controller sostitutivo	
Sistema	Versione di ONTAP	Sistema	Versione di ONTAP
AFF A320	9.9.1 o versione successiva	AFF A400	9.9.1 o versione successiva
AFF8060	9.8P13 o patch successive	AFF A900	da 9.10.1 a 9.12.1

Vecchio controller		Controller sostitutivo	
AFF8080	9.8P10 o patch successive	AFF A900	da 9.10.1 a 9.12.1
FAS8060	9.8P13 o patch successive	FAS9500	Da 9.10.1P3 a 9.12.1
FAS8080	9.8P12 o patch successive	FAS9500	Da 9.10.1P3 a 9.12.1

Per le combinazioni di upgrade illustrate nella tabella precedente:

- Non è necessario utilizzare la stessa versione di ONTAP sui controller esistenti e sostitutivi. L'aggiornamento del software ONTAP viene eseguito con l'aggiornamento del controller.
- Durante l'aggiornamento, è necessario installare un controller sostitutivo con una versione di ONTAP e un livello di patch supportati.
- Non è possibile annullare o annullare un aggiornamento del controller dopo aver avviato la procedura e aver aggiornato il primo nodo.

Scegli una procedura di aggiornamento hardware diversa

- "Esaminare i metodi ARL alternativi disponibili per l'aggiornamento dell'hardware del controller".
- 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*.

Informazioni correlate

Fare riferimento a "Riferimenti" per collegarsi alla *Documentazione 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 che eseguono ONTAP 9.8 o versioni successive, è necessario disporre della piattaforma e della configurazione dei controller originali e sostitutivi.

Aggiornamenti supportati per ARL

Quando si aggiorna una coppia di nodi utilizzando questa procedura ARL per ONTAP 9.8 o versioni successive, è necessario verificare che ARL possa essere eseguito sui controller originali e su quelli sostitutivi.

È necessario controllare le dimensioni di tutti gli aggregati definiti e il numero di dischi supportati dal sistema originale. È quindi necessario confrontare le dimensioni e il numero di dischi aggregati supportati con le dimensioni e il numero di dischi aggregati supportati dal nuovo sistema. Fare riferimento a. "Riferimenti" Per collegarsi al *Hardware Universe* dove queste informazioni sono disponibili. 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.

È necessario verificare nelle regole di combinazione del cluster se i nuovi nodi possono diventare parte del cluster con i nodi esistenti quando il controller originale viene sostituito. Per ulteriori informazioni sulle regole di combinazione dei cluster, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*.

> Se si sta aggiornando un sistema che supporta dischi interni (ad esempio, un sistema FAS2700 o AFF A250) ma NON dispone di dischi interni, fare riferimento a. "Riferimenti" E utilizzare la procedura descritta nella sezione *aggregate Relocation to Manually Upgrade Controller hardware* content (trasferimento aggregato per aggiornare manualmente l'hardware del controller) corretta per la versione di ONTAP in uso.

Se si dispone di un sistema con più di due porte cluster per nodo, ad esempio un sistema FAS8080 o AFF8080, prima di avviare l'aggiornamento, è necessario migrare e riassegnare le LIF del cluster a due porte cluster per nodo. Se si esegue l'aggiornamento del controller con più di due porte cluster per nodo, le LIF del cluster potrebbero non essere presenti sul nuovo controller dopo l'aggiornamento.

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 è possibile eseguire i seguenti aggiornamenti:

- Ai 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.

- Ai controller entry-level con dischi interni, ad esempio FAS 2500.

  Se si desidera aggiornare i controller entry-level con dischi interni, fare riferimento a. "Riferimenti" Per collegarsi a *Upgrade spostando volumi o storage* e passare alla procedura *aggiornamento di una coppia di nodi che eseguono Clustered Data ONTAP spostando volumi*.

Configurazione MetroCluster FC

In una configurazione FC MetroCluster, è necessario sostituire i nodi del sito di disaster recovery/failover il prima possibile. La mancata corrispondenza nei modelli di controller all'interno di un MetroCluster non è supportata perché la mancata corrispondenza del modello di controller può causare la offline del mirroring del disaster recovery. Utilizzare il `-skip-metrocluster-check true` comando per ignorare i controlli MetroCluster quando si sostituiscono i nodi del secondo sito.

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.

In caso di problemi, fare riferimento al "Risolvere i problemi" sezione alla fine della procedura per ulteriori informazioni e possibili soluzioni. Le informazioni sui guasti che possono verificarsi sono elencate in base alla fase della procedura nella "Sequenza di aggiornamento ARL" .

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

Verificare lo stato della configurazione MetroCluster

Prima di avviare un aggiornamento su una configurazione Fabric MetroCluster, è necessario verificare lo stato della configurazione MetroCluster per verificarne il corretto funzionamento.

Fasi

1. Verificare che i componenti di MetroCluster siano integri:

   `metrocluster check run`

   ```
   metrocluster_siteA::*> metrocluster check run
   ```

   L'operazione viene eseguita in background.

2. Dopo il `metrocluster check run` operazione completata, visualizzare i risultati:

   `metrocluster check show`

   Dopo circa cinque minuti, vengono visualizzati i seguenti risultati:

   ```
   metrocluster_siteA::*> metrocluster check show
   Last Checked On: 4/7/2019 21:15:05
   Component            Result
   ---------------      -------
   nodes                ok
   lifs                 ok
   config-replication   ok
   aggregates           warning
   clusters             ok
   connections          not-applicable
   volumes              ok
   7 entries were displayed.
   ```

3. Controllare lo stato dell'operazione di controllo MetroCluster in esecuzione:

```
metrocluster operation history show -job-id 38
```

4. Verificare che non siano presenti avvisi sullo stato di salute:

```
system health alert show
```

Verificare la presenza di errori di configurazione MetroCluster

È possibile utilizzare lo strumento Active IQ Config Advisor disponibile sul sito del supporto NetApp per verificare la presenza di errori di configurazione comuni.

Se non si dispone di una configurazione MetroCluster, ignorare questa sezione.

A proposito di questa attività

Active IQ Config Advisor è uno strumento per la convalida della configurazione e il controllo dello stato di salute. È possibile implementarlo sia in siti sicuri che in siti non sicuri per la raccolta di dati e l'analisi del sistema.

Il supporto per Config Advisor è limitato e disponibile solo online.

1. Scaricare il "Active IQ Config Advisor" tool.
2. Eseguire Active IQ Config Advisor, esaminare l'output e seguire i consigli per risolvere eventuali problemi.

Verificare lo switchover, la riparazione e lo switchback

Verificare le operazioni di switchover, riparazione e switchback della configurazione MetroCluster.

Fare riferimento a. "Riferimenti" Per collegarsi al contenuto di *Gestione MetroCluster e disaster recovery* e utilizzare le procedure indicate per lo switchover negoziato, la riparazione e lo switchback.

Scopri la sequenza di 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 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 di node1 siano online su node3, si riassegnano i dischi da node1 a node3 e si verifica l'installazione di node3. Se si utilizza NetApp Volume Encryption (NVE), viene ripristinata la configurazione del gestore delle chiavi. Se necessario, impostare la configurazione FC o UTA/UTA2 su node3. 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	Descrizione
"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 di node2 siano online su node4, si riassegnano i dischi da node2 a node4 e si verifica l'installazione di node4. Se si utilizza NVE, si ripristina la configurazione del gestore delle chiavi. Se necessario, impostare la configurazione FC o UTA/UTA2 su node4. 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

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
   ```

- A partire da ONTAP 9.10.1, la procedura di aggiornamento automatica basata su switchover negoziato (NSO) è l'impostazione predefinita per una configurazione FC MetroCluster a quattro nodi. Se si sta aggiornando una configurazione MetroCluster FC a quattro nodi, quando si esegue `system controller replace start` È necessario impedire l'avvio della procedura basata su NSO impostando il `-nso` parametro a. `false`:

  `system controller replace start -nodes node_names -nso false`

- È possibile eseguire il comando solo `system controller replace start` a livello di privilegi avanzati:

  `set -privilege advanced`

Viene visualizzato il seguente output:

```
Warning:
1. Current ONTAP version is 9.x
Before starting controller replacement operation, ensure that the new
controllers are running the version 9.x

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.

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.
MCC Cluster Check (controllo cluster MCC)	Verifica se il sistema è una configurazione MetroCluster. L'operazione rileva automaticamente se si tratta o meno di una configurazione MetroCluster ed esegue i controlli preliminari e di verifica specifici. È supportata solo la configurazione MetroCluster FC a 4 nodi. In caso di configurazione MetroCluster a 2 nodi e configurazione IP MetroCluster a 4 nodi, il controllo non riesce. Se la configurazione MetroCluster è in stato di switchover, il controllo non riesce.
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.
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. Se mancano dei dischi, fare riferimento al "Riferimenti"collegamento alla gestione *disco e aggregato con la CLI*, alla gestione *logica dello storage con la CLI* e alla gestione *coppia ha* 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.

Eseguire un controllo preliminare	Descrizione
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.

Se si dispone di un sistema con più di due porte cluster per nodo, ad esempio un sistema FAS8080 o AFF8080, prima di avviare l'aggiornamento, è necessario migrare e riassegnare le LIF del cluster a due porte cluster per nodo. Se si esegue l'aggiornamento del controller con più di due porte cluster per nodo, le LIF del cluster potrebbero non essere presenti sul nuovo controller dopo l'aggiornamento.

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 -node local`
   - `volume show -node local`
   - `storage array config show -switch switch_name`
   - `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)

   > Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha.
   >
   > È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

   "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

Alcune funzionalità richiedono licenze, emesse come *pacchetti* che includono una o più funzionalità. Ogni nodo del cluster deve disporre di una propria chiave per poter utilizzare ciascuna funzionalità nel cluster.

Se non si dispone di nuove chiavi di licenza, le funzionalità attualmente concesse in licenza nel cluster sono disponibili per il nuovo controller. Tuttavia, l'utilizzo di funzionalità senza licenza sul controller potrebbe non essere conforme al contratto di licenza, pertanto è necessario installare la nuova chiave di licenza o le nuove chiavi per il nuovo controller al termine dell'aggiornamento.

Fare riferimento a. "Riferimenti" Per accedere al *sito di supporto NetApp*, dove è possibile ottenere nuove chiavi di licenza di 28 caratteri per ONTAP. Le chiavi sono disponibili nella sezione *My Support* sotto *licenze software*. Se il sito non dispone delle chiavi di licenza necessarie, contattare il rappresentante commerciale NetApp.

Per informazioni dettagliate sulle licenze, fare riferimento a. "Riferimenti" Per collegarsi al *System Administration Reference*.

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

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 <aggregate_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`

Sposta gli aggregati falliti o sottoposti a veto sul nodo 2

Se uno qualsiasi degli aggregati non riesce a essere riposizionato o viene sottoposto a veto, è necessario riposizionarlo manualmente sul nodo 2 oppure, se necessario, ignorare i veti o i controlli di destinazione.

A proposito di questa attività

Il sistema interrompe l'operazione di ricollocazione 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 <aggregate_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 <aggregate_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 <aggregate_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.

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.

Per…	Quindi…

Sistemi della serie FAS/AFF8000	Estrarre il contenuto di `<ontap_version>_image.tgz` file nella directory di destinazione:
	`tar -zxvf <ontap_version>_image.tgz`
	Se si sta estraendo il contenuto su Windows, utilizzare 7-zip o WinRAR per estrarre l'immagine di netboot.
	L'elenco delle directory deve contenere una cartella netboot con un file kernel:
	`netboot/kernel`

Tutti gli altri sistemi	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

Installazione e boot node3

È necessario installare node3 nel rack, trasferire le connessioni del node1 al node3, fare il boot node3 e installare ONTAP. È quindi necessario riassegnare uno qualsiasi dei dischi spare di node1, tutti i dischi appartenenti al volume root e qualsiasi aggregato non root che non sia stato trasferito in node2 precedentemente nel 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, è necessario verificare che le LIF SAN siano state spostate correttamente in 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".

- Per un aggiornamento del controller AFF A800 o AFF C800 , è necessario assicurarsi che tutte le unità nello chassis siano saldamente posizionate contro il midplane prima di rimuovere node1. Per maggiori informazioni, vedere "Sostituire i moduli controller AFF A800 o AFF C800".
- Se si sta eseguendo l'aggiornamento di un sistema con dischi di storage, completare l'intera sezione e passare alla "Configurare le porte FC sul nodo 3" e. "Controllare e configurare le porte UTA/UTA2 sul nodo 3" sezioni, immissione dei comandi al prompt del cluster.

Fasi

1. assicurarsi di disporre di spazio rack per node3.

   Se node1 e node2 si trovano in uno chassis separato, è possibile inserire node3 nella stessa posizione rack del node1. Tuttavia, se il nodo 1 si trovava nello stesso chassis con il nodo 2, è necessario inserire il nodo 3 nel proprio spazio rack, preferibilmente vicino alla posizione del nodo 1.

2. installare node3 nel rack, seguendo le *istruzioni di installazione e configurazione* per il modello di nodo in uso.

   Se si esegue l'aggiornamento a un sistema con entrambi i nodi nello stesso chassis, installare node4 e node3 nello chassis. Se non si installano entrambi i nodi nello stesso chassis, quando si avvia node3, questo si comporta come se fosse in una configurazione a doppio chassis, mentre quando si avvia node4, l'interconnessione tra i nodi non si attiva.

3. cavo node3, spostamento delle connessioni da node1 a node3.

   Cablare le seguenti connessioni utilizzando le *Istruzioni di installazione e configurazione* per la piattaforma node3, il documento appropriato sullo scaffale dei dischi e la documentazione sulla *gestione delle coppie HA*.

   Fare riferimento a"Riferimenti" per collegarsi alla *gestione delle coppie HA*.

   - Console (porta di gestione remota)

- Porte del cluster
- Porte dati
- Porte di gestione di cluster e nodi
- Storage
- Configurazioni SAN: Porte switch FC e Ethernet iSCSI

> Potrebbe non essere necessario spostare la scheda di interconnessione o la connessione del cavo di interconnessione del cluster dal nodo 1 al nodo 3, poiché la maggior parte dei modelli di piattaforma dispone di un modello di scheda di interconnessione unico. Per la configurazione MetroCluster, è necessario spostare le connessioni del cavo FC-VI dal nodo 1 al nodo 3. Se il nuovo host non dispone di una scheda FC-VI, potrebbe essere necessario spostare la scheda FC-VI.

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.

   Se si sta eseguendo l'aggiornamento a un sistema con entrambi i nodi nello stesso chassis, anche node4 viene riavviato. Tuttavia, è possibile ignorare il node4 boot fino a tardi.

   > 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.

   > **Non ignorare il ritardo; se non si lascia caricare la batteria, si potrebbe verificare una 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 della LIF dati o potrebbe verificarsi una mancanza di disponibilità 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:

Per…	Quindi…
Sistemi della serie FAS/AFF8000	`netboot http://<web_server_ip/path_to_web-accessible_directory>/netboot/kernel`
Tutti gli altri sistemi	`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
    ```

    Se si dispone di una configurazione MetroCluster, utilizzare i seguenti comandi per modificare il controller e

lo chassis:

```
ha-config modify controller mcc
```

```
ha-config modify chassis mcc
```

14. Esci dalla modalità di manutenzione:

```
halt
```

Interrompere L'OPERAZIONE premendo Ctrl-C al prompt dell'ambiente di avvio.

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

```
date
```

16. al nodo 3, controllare la data utilizzando il seguente comando al prompt dell'ambiente di boot:

```
show date
```

17. se necessario, impostare la data sul node3:

```
set date mm/dd/yyyy
```

18. al nodo 3, controllare l'ora utilizzando il seguente comando al prompt dell'ambiente di boot:

```
show time
```

19. se necessario, impostare l'ora su node3:

```
set time hh:mm:ss
```

20. 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
```

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

```
printenv partner-sysid
```

1. Se sono installate unità NetApp Storage Encryption (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`**

> Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha. È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

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".

2. Avviare il nodo nel menu di avvio:

```
boot_ontap menu
```

Quali sono le prossime novità?

- Se si dispone di un sistema con una configurazione FC o UTA/UTA2,"imposta e configura le porte FC o UTA/UTA2 sul nodo 3" .
- Se non si dispone di una configurazione FC o UTA/UTA2,"riassegnare i dischi del nodo 1 al nodo 3, passaggio 1" in modo che node3 possa riconoscere i dischi di node1.
- Se si dispone di una configurazione MetroCluster ,"imposta e configura le porte FC o UTA/UTA2 sul nodo 3" per rilevare i dischi collegati al nodo.

Impostare la configurazione FC o UTA/UTA2 su node3

Se node3 dispone di porte FC integrate, porte UTA/UTA2 (onboard Unified target adapter) o una scheda UTA/UTA2, è necessario configurare le impostazioni prima di completare il resto della procedura.

A proposito di questa attività

Potrebbe essere necessario completare la sezione Configurare le porte FC sul nodo 3, la sezione Controllare e configurare le porte UTA/UTA2 sul nodo 3, o entrambe le sezioni.

> I materiali di marketing NetApp potrebbero utilizzare il termine UTA2 per fare riferimento alle porte e agli adattatori CNA (Converged Network Adapter). Tuttavia, la CLI utilizza il termine CNA.

Se node3 non dispone di porte FC integrate, porte UTA/UTA2 integrate o una scheda UTA/UTA2 (ad esempio, sistemi AFF e FAS introdotti a partire da ONTAP 9.15.1) e si sta aggiornando un sistema con dischi di archiviazione, è possibile passare a"Riassegnare dischi da node1 TB a node3 TB" .

Configurare le porte FC sul nodo 3

Se il nodo 3 dispone di porte FC, integrate o su un adattatore FC aggiuntivo, è necessario impostare le configurazioni delle porte sul nodo prima di metterlo in servizio, poiché le porte non sono preconfigurate al momento della spedizione dei sistemi. Se non si configurano le porte, si potrebbe verificare un'interruzione del servizio.

Prima di iniziare

È necessario disporre dei valori delle impostazioni della porta FC del nodo 1 salvati nella sezione "Preparare i nodi per l'aggiornamento".

A proposito di questa attività

È possibile saltare questa sezione se il sistema non dispone di configurazioni FC. Se il sistema dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2, configurarle in Controllare e configurare le porte UTA/UTA2 sul nodo 3.

Immettere i comandi in questa sezione al prompt della shell in modalità Manutenzione.

Fasi

1. Confronta le impostazioni FC sul nodo 3 con le impostazioni acquisite in precedenza dal nodo 1.
2. Eseguire una delle seguenti azioni per modificare le porte FC sul nodo 3, a seconda delle necessità:

   In modalità di manutenzione (opzione 5 nel menu di avvio):

   - Per programmare come porte di destinazione:

     `ucadmin modify -m fc -t target <adapter>`

     Per esempio: `ucadmin modify -m fc -t target 2a`

   - Per programmare le porte initiator:

     `ucadmin modify -m fc -t initiator <adapter>`

   Per esempio: `ucadmin modify -m fc -t initator 2b`

3. Verificare le nuove impostazioni utilizzando il seguente comando ed esaminando l'output:

   `ucadmin show`

4. Arrestare il nodo:

   `halt`

5. Avviare il sistema dal prompt del CARICATORE:

   `boot_ontap menu`

6. Dopo aver immesso il comando, attendere che il sistema si arresti al prompt dell'ambiente di avvio.
7. Selezionare l'opzione `5` dal menu di avvio per la modalità di manutenzione.
8. eseguire una delle seguenti operazioni:

Se il nodo 3…	Quindi…
Ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate	Vai aControllare e configurare le porte UTA/UTA2 sul nodo 3
Non ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate	Salta *Controlla e configura le porte UTA/UTA2 sul nodo 3* e vai a"Riassegnare dischi da node1 TB a node3 TB" .

Controllare e configurare le porte UTA/UTA2 sul nodo 3

Se node3 dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2, è necessario controllare la configurazione delle porte ed eventualmente riconfigurarle, a seconda di come si desidera utilizzare il sistema aggiornato.

Prima di iniziare

È necessario disporre dei moduli SFP+ corretti per le porte UTA/UTA2.

A proposito di questa attività

Se si desidera utilizzare una porta UTA/UTA2 (Unified Target Adapter) per FC, è necessario prima verificare la configurazione della porta.

> I materiali di marketing NetApp potrebbero utilizzare il termine UTA2 per fare riferimento agli adattatori e alle porte CNA. Tuttavia, la CLI utilizza il termine CNA.

Puoi usare il `ucadmin show` comando per visualizzare o verificare la configurazione della porta corrente, come mostrato nel seguente output di esempio:

```
*> ucadmin show
         Current  Current    Pending   Pending      Admin
Adapter  Mode     Type       Mode      Type         Status
-------  -------  -------    --------  ----------   --------
0e       fc       target     -         initiator    offline
0f       fc       target     -         initiator    offline
0g       fc       target     -         initiator    offline
0h       fc       target     -         initiator    offline
1a       fc       target     -         -            online
1b       fc       target     -         -            online
6 entries were displayed.
```

Le porte UTA/UTA2 possono essere configurate in modalità FC nativa o UTA/UTA2. La modalità FC supporta l'iniziatore FC e la destinazione FC; la modalità UTA/UTA2 consente la condivisione simultanea del traffico NIC e FCoE con la stessa interfaccia SFP+ 10 GbE e supporta le destinazioni FC.

Potresti trovare porte UTA/UTA2 su un adattatore aggiuntivo o sulla scheda madre del controller e avere le seguenti configurazioni, ma dovresti controllare la configurazione delle porte UTA/UTA2 sul nodo 3 e modificarla, se necessario:

- Le schede UTA/UTA2 ordinate al momento dell'ordine del controller vengono configurate prima della spedizione per avere la personalità richiesta.

- Le schede UTA/UTA2 ordinate separatamente dal controller vengono fornite con il linguaggio di destinazione FC predefinito.
- Le porte UTA/UTA2 integrate sui nuovi controller vengono configurate prima della spedizione in modo da avere la personalità richiesta.

> Per configurare le porte UTA/UTA2 è necessario essere in modalità di manutenzione. Immettere i comandi in questa sezione al prompt della shell in modalità Manutenzione.

Fasi

1. Se il modulo SFP+ corrente non corrisponde all'utilizzo desiderato, sostituirlo con il modulo SFP+ corretto.

   Contattare il rappresentante NetApp per ottenere il modulo SFP+ corretto.

2. Verificare le impostazioni della porta UTA/UTA2:

   ```
   ucadmin show
   ```

   Esaminare l'output e determinare se le porte UTA/UTA2 hanno la personalità desiderata.

   L'output nell'esempio seguente mostra che il tipo di adattatore "1b" sta cambiando in iniziatore e che la modalità degli adattatori "2a" e "2b" sta cambiando in "cna". La modalità CNA consente di utilizzare la scheda come adattatore di rete.

   ```
   *> ucadmin show
            Current    Current     Pending  Pending     Admin
   Adapter  Mode       Type        Mode     Type        Status
   -------  --------   ----------  -------  --------    --------
   1a       fc         initiator   -        -           online
   1b       fc         target      -        initiator   online
   2a       fc         target      cna      -           online
   2b       fc         target      cna      -           online
   *>
   ```

3. Eseguire una delle seguenti operazioni:

Se le porte UTA/UTA2…	Quindi…
Non avere la personalità che si desidera	Vai aFase 4 .
Avere la personalità che si desidera	Salta il passaggio 4 al passaggio 8 e vai aFase 9 .

4. Esegui una delle seguenti azioni:

Se si sta configurando…	Quindi…
Porte su una scheda UTA/UTA2	Vai aFase 5

Se si sta configurando…	Quindi…
Porte UTA/UTA2 integrate	Salta il passaggio 5 e vai aFase 6 .

5. Se l'adattatore è in modalità iniziatore e la porta UTA/UTA2 è online, metti offline la porta UTA/UTA2:

   `storage disable adapter <adapter_name>`

   Gli adattatori in modalità di destinazione sono automaticamente offline in modalità di manutenzione.

6. Se la configurazione corrente non corrisponde all'uso desiderato, modificare la configurazione secondo necessità:

   `ucadmin modify -m fc|cna -t initiator|target <adapter_name>`

   - `-m` è la modalità personality, `fc` oppure `cna`.
   - `-t` È di tipo FC4, `target` oppure `initiator`.

   > È necessario utilizzare l'iniziatore FC per le unità nastro e le configurazioni MetroCluster . Per i client SAN è necessario utilizzare la destinazione FC.

7. Mettere online tutte le porte di destinazione immettendo il seguente comando una volta per ogni porta:

   `storage enable adapter <adapter_name>`

8. Collegare la porta.

1. Uscire dalla modalità di manutenzione:

   `halt`

2. avviare il nodo nel menu di avvio:

   `boot_ontap menu`

Quali sono le prossime novità?

- Se stai effettuando l'aggiornamento a un sistema AFF A800 , vai a"Riassegnare node1 dischi a node3, passaggio 9" .
- Per tutti gli altri aggiornamenti di sistema, vai a"Riassegnare node1 dischi a node3, passaggio 1" .

Riassegnare dischi da node1 TB a node3 TB

È necessario riassegnare i dischi che appartenevano a node1 a node3 prima di verificare l'installazione di node3.

Fasi

1. Verificare che node1 si sia fermato al menu di avvio. Riassegnare i dischi del nodo 1 al nodo 3:

   `boot_after_controller_replacement`

   Dopo un breve intervallo di tempo, viene richiesto di inserire il nome del nodo da sostituire. Se sono

presenti dischi condivisi (chiamati anche Advanced Disk Partitioning (ADP) o dischi partizionati), viene richiesto di inserire il nome del nodo del partner ha.

Questi prompt potrebbero essere interrati nei messaggi della console. Se non si immette un nome di nodo o non si immette un nome corretto, viene richiesto di inserire nuovamente il nome.

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>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner 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).

2. Se il sistema entra in un ciclo di riavvio con il messaggio `no disks found` indica che il sistema ha reimpostato le porte FC o UTA/UTA2 sulla modalità di destinazione e pertanto non è in grado di vedere alcun disco. Selezionare una delle seguenti attività per risolvere questo problema:
   - EseguireFase 3 AFase 8 sul nodo 3
   - Vai alla sezione"Verificare l'installazione di node3"
3. premere Ctrl-C durante l'OPERAZIONE per arrestare il nodo al prompt Loader>.
4. Al prompt del CARICATORE, accedere alla modalità di manutenzione:

   ```
   boot_ontap maint
   ```

5. In modalità di manutenzione, visualizzare tutte le porte iniziatore precedentemente impostate che si trovano ora in modalità di destinazione:

   ```
   ucadmin show
   ```

   Riportare le porte in modalità initiator:

   ```
   ucadmin modify -m fc -t initiator -f adapter name
   ```

6. Verificare che le porte siano state modificate in modalità initiator:

   ```
   ucadmin show
   ```

7. Uscire dalla modalità di manutenzione:

```
halt
```

> Se si esegue l'aggiornamento da un sistema che supporta dischi esterni a un sistema che supporta anche dischi esterni, visitare il sito Fase 8.
>
> Se si esegue l'aggiornamento da un sistema che supporta dischi esterni a un sistema che supporta dischi interni ed esterni, ad esempio un sistema AFF A800, visitare il sito Fase 9.

8.]al prompt di Loader, 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
```

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

b. Invio `y` al seguente prompt:

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

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

d. 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.

e. 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 Fase 8 fino a quando il sistema non si avvia normalmente.

9. se si esegue l'aggiornamento da un sistema con dischi esterni a un sistema che supporta dischi interni ed esterni (ad esempio sistemi AFF A800), impostare l'aggregato node1 come aggregato root per confermare che node3 si avvia dall'aggregato root di node1. Per impostare l'aggregato root, andare al menu di avvio e selezionare l'opzione `5` per accedere alla modalità di manutenzione.

È necessario eseguire i seguenti passaggi secondari nell'ordine esatto indicato; in caso contrario, si potrebbe verificare un'interruzione o addirittura la perdita di dati.

La seguente procedura imposta node3 per l'avvio dall'aggregato root di node1:

a. Accedere alla modalità di manutenzione:

```
boot_ontap maint
```

b. Controllare le informazioni su RAID, plex e checksum per l'aggregato node1:

```
aggr status -r
```

c. Controllare lo stato dell'aggregato node1:

```
aggr status
```

d. Se necessario, portare online l'aggregato node1:

```
aggr_online root_aggr_from_node1
```

e. Impedire al node3 di avviarsi dal proprio aggregato root originale:

```
aggr offline root_aggr_on_node3
```

f. Impostare l'aggregato root node1 come nuovo aggregato root per node3:

```
aggr options aggr_from_node1 root
```

g. Verificare che l'aggregato root di node3 sia offline e che l'aggregato root per i dischi portati da node1 sia online e impostato su root:

```
aggr status
```

La mancata esecuzione del passaggio secondario precedente potrebbe causare l'avvio di node3 dall'aggregato root interno, oppure il sistema potrebbe presumere l'esistenza di una nuova configurazione del cluster o richiedere di identificarne una.

Di seguito viene riportato un esempio dell'output del comando:

```
-------------------------------------------------------------------
Aggr                  State    Status             Options

aggr0_nst_fas8080_15 online   raid_dp, aggr      root, nosnap=on
                              fast zeroed
                              64-bit

aggr0                 offline  raid_dp, aggr      diskroot
                              fast zeroed
                              64-bit
-------------------------------------------------------------------
```

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. In base alla versione di ONTAP in esecuzione sulla coppia ha sottoposta a upgrade, esegui una delle seguenti azioni:

Se la versione di ONTAP è…	Quindi…
da 9,8 a 9.11.1	Verificare che le LIF del cluster siano in ascolto sulla porta 7700: `::> network connections listening show -vserver Cluster`
9.12.1 o versione successiva	Saltare questo passaggio e passare a. Fase 5.

La porta 7700 in ascolto sulle porte del cluster è il risultato previsto, come mostrato nell'esempio seguente per un cluster a due nodi:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

4. Per ogni cluster LIF che non è in ascolto sulla porta 7700, imposta lo stato amministrativo della LIF su `down` e poi `up`:

   `::> net int modify -vserver Cluster -lif *cluster-lif* -status-admin down; net int modify -vserver Cluster -lif *cluster-lif* -status-admin up`

   Ripetere il passaggio 3 per verificare che la LIF del cluster sia in ascolto sulla porta 7700.

5. passare alla modalità privilegi avanzati:

   `set advanced`

6. 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`

7. Se si lavora su un sistema MetroCluster, verificare che il controller sostituito sia configurato correttamente per la configurazione MetroCluster; la configurazione MetroCluster dovrebbe essere in buono stato. Vedere "Verificare lo stato della configurazione MetroCluster".

   Riconfigurare le LIF dell'intercluster sul nodo MetroCluster node3 e controllare il peering del cluster per ripristinare la comunicazione tra i nodi MetroCluster prima di passare alla fase 6.

   Controllare lo stato del nodo MetroCluster:

```
metrocluster node show
```

8. Riprendere l'operazione di sostituzione del controller:

```
system controller replace resume
```

9. 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*.

10. 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*.

> Se si modifica la velocità delle porte del cluster e0a e E1a nei sistemi AFF A800 o AFF C800, è possibile che vengano ricevuti pacchetti non validi dopo la conversione della velocità. Vedere "Bug online di NetApp ID 1570339" e l'articolo della knowledge base "Errori CRC sulle porte T6 dopo la conversione da 40GbE a 100GbE" come guida.

Fasi

1. Elenca tutte le porte fisiche sul nodo aggiornato1 (indicato 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. Elenca i domini di trasmissione sul cluster:

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

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

   ```
   network port reachability show
   ```

   L'output dovrebbe essere simile al seguente esempio:

```
clusterA::*> reachability show -node node1_node3
(network port reachability show)
Node         Port       Expected Reachability   Reachability Status
-----------  ---------  ----------------------  ----------------------
node1_node3
             a0a        Default:Default         no-reachability
             a0a-822    Default:822             no-reachability
             a0a-823    Default:823             no-reachability
             e0M        Default:Mgmt            ok
             e0a        Cluster:Cluster         misconfigured-
reachability
             e0b        Cluster:Cluster         no-reachability
             e0c        Cluster:Cluster         no-reachability
             e0d        Cluster:Cluster         no-reachability
             e0e        Cluster:Cluster         ok
             e0e-822    -                       no-reachability
             e0e-823    -                       no-reachability
             e0f        Default:Default         no-reachability
             e0f-822    Default:822             no-reachability
             e0f-823    Default:823             no-reachability
             e0g        Default:Default         misconfigured-
reachability
             e0h        Default:Default         ok
             e0h-822    Default:822             ok
             e0h-823    Default:823             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 e0h
```

```
Warning: Repairing port "node1_node3: e0h" 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. [[fase 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` eseguire la trasmissione del dominio seguendo la procedura riportata di seguito:

   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 le 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
                  e0e       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 "e0e" in "e0h":

      ```
      Cluster::*> displaced-vlans restore -node node1_node3 -port e0e
      -destination-port e0h
      ```

      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. Elimina tutti i domini di broadcast vuoti dopo che tutte le riparazioni delle porte sono state completate:

```
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      ""           000000000000000002000000000000a008a81976
   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.

> Se si modifica la velocità delle porte delle schede di interfaccia di rete Ethernet basate su T6 o delle porte della scheda madre, è possibile che vengano ricevuti pacchetti non validi dopo la conversione della velocità. Vedere "Bug online di NetApp ID 1570339" e l'articolo della knowledge base "Errori CRC sulle porte T6 dopo la conversione da 40GbE a 100GbE" come guida.

Fasi

1. 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.

2. 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.

3. 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.

4. Se necessario, ripristinare e ripristinare i LIF spostati oppure migrare e modificare manualmente i LIF del nodo 1 che non sono riusciti a trasferirsi automaticamente nel nodo 3.

Ripristinare e ripristinare i LIF spostati

a. Elencare eventuali LIF spostati:

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

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

```
cluster controller-replacement network displaced-interface
restore-home-node -node <node3_nodename> -vserver <vserver name>
-lif-name <lif_name>
```

Migrare e modificare manualmente i LIF

a. Migrare i LIF che non sono riusciti a trasferirsi automaticamente al nodo 3:

```
network interface migrate -vserver <vserver name> -lif <lif_name>
-destination-node <node3_nodename> -destination-port
<port_on_node3>
```

b. Modificare il nodo home e la porta home per i LIF migrati:

```
network interface modify -vserver <vserver_name> -lif
<data_lif_name> -home-node <node3_nodename> -home-port
<home_port>
```

5. 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

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 <aggregate_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
```

Sposta gli aggregati falliti o sottoposti a veto sul nodo 3

Se uno qualsiasi degli aggregati non riesce a essere riposizionato o viene sottoposto a veto, è necessario riposizionarlo manualmente sul nodo 3 oppure, se necessario, ignorare i veti o i controlli di destinazione.

A proposito di questa attività

Il sistema interrompe l'operazione di ricollocazione 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 <node2> -destination <node3>
-aggregate-list <aggregate_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 node2 -destination node3 -aggregate-list <aggregate_list> -ndo-controller-upgrade true -override-vetoes true`
Ignorare i controlli di destinazione	Utilizzare il seguente comando: `storage aggregate relocation start -node node2 -destination node3 -aggregate-list <aggregate_list> -ndo-controller-upgrade true -override-vetoes true -override-destination-checks true`

Andare in pensione node2

Per dismettere node2, è necessario arrestare node2 correttamente e quindi 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

Installazione e boot node4

È necessario installare node4 nel rack, trasferire le connessioni node2 al node4, fare il boot node4 e installare ONTAP. È quindi necessario riassegnare uno qualsiasi dei dischi spare di node2, i dischi appartenenti al volume root e gli aggregati non root che non sono stati riallocati in node3 prima 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 l'avvio di rete del nodo 4 se la versione ONTAP sul nodo 4 è diversa dalla versione ONTAP sul nodo 2. Dopo aver installato node4, avviarlo dall'immagine ONTAP 9 memorizzata sul server web. È quindi possibile scaricare i file corretti sul dispositivo di supporto di avvio per i successivi avvii del sistema seguendo le istruzioni in "Preparatevi per il netboot".

- Per un aggiornamento del controller AFF A800 o AFF C800 , è necessario assicurarsi che tutte le unità nello chassis siano saldamente posizionate contro il midplane prima di rimuovere node2. Per maggiori informazioni, vedere "Sostituire i moduli controller AFF A800 o AFF C800".
- Se si sta aggiornando un sistema con dischi di archiviazione, è necessario completare l'intera sezione e quindi procedere a "Impostare la configurazione FC o UTA/UTA2 su node4" , immettendo comandi al prompt del cluster.

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.

   Cablare le seguenti connessioni, utilizzando le *Istruzioni di installazione e configurazione* per la piattaforma node4, il documento appropriato sullo scaffale dei dischi e la documentazione sulla *gestione delle coppie HA*.

   Fare riferimento a"Riferimenti" per collegarsi alla *gestione delle coppie HA*.

   - Console (porta di gestione remota)
   - Porte del cluster
   - Porte dati
   - Porte di gestione di cluster e nodi
   - Storage
   - Configurazioni SAN: Porte switch FC e Ethernet iSCSI

   Potrebbe non essere necessario spostare la connessione scheda di interconnessione/scheda FC-VI o cavo di interconnessione/FC-VI dal nodo 2 al nodo 4, poiché la maggior parte dei modelli di piattaforma dispone di modelli di schede di interconnessione univoci. Per la configurazione MetroCluster, è necessario spostare le connessioni del cavo FC-VI dal nodo 2 al nodo 4. Se il nuovo host non dispone di una scheda FC-VI, potrebbe essere necessario spostare la scheda FC-VI.

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 avvio.

   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.

   Non ignorare il ritardo; se non si lascia caricare la batteria, si potrebbe verificare una 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 della LIF dati o potrebbe verificarsi una mancanza di disponibilità 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`

Se DHCP (Dynamic host Configuration Protocol) è…	Quindi…
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:

Per…	Quindi…
Sistemi della serie FAS/AFF8000	`netboot http://<web_server_ip/path_to_web-accessible_directory>/netboot/kernel`
Tutti gli altri sistemi	`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`

    Se si dispone di una configurazione MetroCluster, utilizzare i seguenti comandi per modificare il controller e lo chassis:

    `ha-config modify controller mcc`

```
ha-config modify chassis mcc
```

14. Uscire dalla modalità di manutenzione:

```
halt
```

Interrompere L'OPERAZIONE premendo Ctrl-C al prompt dell'ambiente di avvio.

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

```
date
```

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

```
show date
```

17. Se necessario, impostare la data sul node4:

```
set date mm/dd/yyyy
```

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

```
show time
```

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

```
set time hh:mm:ss
```

20. 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
```

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

```
printenv partner-sysid
```

22. Se sono installate unità NetApp Storage Encryption (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**`

> Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha. È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

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".

23. Avviare il nodo nel menu di avvio:

```
boot_ontap menu
```

Quali sono le prossime novità?

- Se si dispone di una configurazione FC o UTA/UTA2,"imposta e configura le porte FC o UTA/UTA2 sul nodo 4" .
- Se non si dispone di una configurazione FC o UTA/UTA2,"riassegnare i dischi del nodo 2 al nodo 4, passaggio 1" in modo che node4 possa riconoscere i dischi di node2.
- Se si dispone di una configurazione MetroCluster ,"imposta e configura le porte FC o UTA/UTA2 sul nodo 4" per rilevare i dischi collegati al nodo.

Impostare la configurazione FC o UTA/UTA2 su node4

Se node4 dispone di porte FC integrate, porte UTA/UTA2 (onboard Unified target adapter) o una scheda UTA/UTA2, è necessario configurare le impostazioni prima di completare il resto della procedura.

A proposito di questa attività

Potrebbe essere necessario completareConfigurare le porte FC sul nodo 4 OControllare e configurare le porte UTA/UTA2 sul nodo 4 o entrambe le sezioni.

> Se node4 non dispone di porte FC integrate, porte UTA/UTA2 integrate o una scheda UTA/UTA2 (ad esempio, sistemi AFF e FAS introdotti a partire da ONTAP 9.15.1) e si sta aggiornando un sistema con dischi di archiviazione, è possibile passare a"Riassegnare dischi da node2 TB a node4 TB" .
>
> Assicurarsi che il 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.

Configurare le porte FC sul nodo 4

Se il nodo 4 dispone di porte FC, integrate o su un adattatore FC aggiuntivo, è necessario impostare le configurazioni delle porte sul nodo prima di metterlo in servizio, poiché le porte non sono preconfigurate al momento della spedizione dei sistemi. Se non si configurano le porte come richiesto, si potrebbe verificare un'interruzione del servizio.

Prima di iniziare

È necessario disporre dei valori delle impostazioni della porta FC del nodo 2 salvati nella sezione "Preparare i nodi per l'aggiornamento".

A proposito di questa attività

È possibile saltare questa sezione se il sistema non dispone di configurazioni FC. Se il sistema dispone di porte UTA/UTA2 integrate o di un adattatore UTA/UTA2, configurarle in Controllare e configurare le porte UTA/UTA2 sul nodo 4.

Immettere i comandi in questa sezione al prompt della shell in modalità Manutenzione.

Fasi

1. Visualizza informazioni su tutti gli adattatori di rete FC e convergenti sul sistema:

   ```
   system node hardware unified-connect show
   ```

2. Confrontare le impostazioni FC sul nodo 4 con quelle acquisite in precedenza dal nodo 1.
3. Modificare le porte FC sul nodo 4 in base alle necessità:
   - Per programmare come porte di destinazione:

     ```
     ucadmin modify -m fc -t target adapter
     ```

     Per esempio: `ucadmin modify -m fc -t target 2a`
   - Per programmare le porte initiator:

     ```
     ucadmin modify -m fc -t initiator adapter
     ```

     `-t` È il tipo FC4: Destinazione o iniziatore.

   Per esempio: `ucadmin modify -m fc -t initator 2b`
4. Arrestare il nodo:

   ```
   halt
   ```

5. Avviare il sistema dal prompt del CARICATORE:

   ```
   boot_ontap menu
   ```

6. Dopo aver immesso il comando, attendere che il sistema si arresti al prompt dell'ambiente di avvio.
7. Selezionare l'opzione `5` dal menu di avvio per la modalità di manutenzione.
8. eseguire una delle seguenti operazioni:

- Passare a. Controllare e configurare le porte UTA/UTA2 sul nodo 4 Se node4 ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate.
- Se node4 non ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate, saltare *Controllare e configurare le porte UTA/UTA2 su node4* e andare a"Riassegnare dischi da node2 TB a node4 TB" .

Controllare e configurare le porte UTA/UTA2 sul nodo 4

Se node4 dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2A, è necessario controllare la configurazione delle porte e configurarle, a seconda di come si desidera utilizzare il sistema aggiornato.

Prima di iniziare

È necessario disporre dei moduli SFP+ corretti per le porte UTA/UTA2.

A proposito di questa attività

Le porte UTA/UTA2 possono essere configurate in modalità FC nativa o UTA/UTA2A. La modalità FC supporta l'iniziatore FC e la destinazione FC; la modalità UTA/UTA2 consente al traffico simultaneo di NIC e FCoE di condividere la stessa interfaccia SFP+ 10 GbE e supporta la destinazione FC.

> I materiali di marketing NetApp potrebbero utilizzare il termine UTA2 per fare riferimento agli adattatori e alle porte CNA. Tuttavia, la CLI utilizza il termine CNA.

Le porte UTA/UTA2 potrebbero essere su un adattatore o sul controller con le seguenti configurazioni:

- Le schede UTA/UTA2 ordinate contemporaneamente al controller vengono configurate prima della spedizione in modo da avere la personalità richiesta.
- Le schede UTA/UTA2 ordinate separatamente dal controller vengono fornite con il linguaggio di destinazione FC predefinito.
- Le porte UTA/UTA2 integrate sui nuovi controller sono configurate (prima della spedizione) in modo da avere la personalità richiesta.

Tuttavia, è necessario controllare la configurazione delle porte UTA/UTA2 sul nodo 4 e modificarla, se necessario.

> Immettere i comandi in questa sezione al prompt della shell in modalità Manutenzione.

Fasi

1. Controlla come sono attualmente configurate le porte sul nodo 4:

   ```
   system node hardware unified-connect show
   ```

   Il sistema visualizza un output simile al seguente esempio:

```
*> ucadmin show
                Current  Current    Pending   Pending   Admin
Node   Adapter  Mode     Type       Mode      Type      Status
----   -------  ---      ---------  -------   --------  -------
f-a    0e       fc       initiator  -          -        online
f-a    0f       fc       initiator  -          -        online
f-a    0g       cna      target     -          -        online
f-a    0h       cna      target     -          -        online
f-a    0e       fc       initiator  -          -        online
f-a    0f       fc       initiator  -          -        online
f-a    0g       cna      target     -          -        online
f-a    0h       cna      target     -          -        online
*>
```

2. Se il modulo SFP+ corrente non corrisponde all'utilizzo desiderato, sostituirlo con il modulo SFP+ corretto.

   Contattare il rappresentante NetApp per ottenere il modulo SFP+ corretto.

3. Verificare le impostazioni:

   `ucadmin show`

   Esaminare l'output di `ucadmin show` Controllare e determinare se le porte UTA/UTA2 hanno la personalità desiderata.

   L'output degli esempi seguenti mostra che il tipo di adattatore FC4 "1b" sta cambiando in `initiator` e che la modalità degli adattatori "2a" e "2b" stia cambiando in `cna`:

```
*> ucadmin show
Node  Adapter  Current Mode  Current Type  Pending Mode  Pending Type
Admin Status
----  -------  ------------  ------------  ------------  ------------
------------
f-a   1a       fc             initiator    -             -
online
f-a   1b       fc             target       -             initiator
online
f-a   2a       fc             target       cna           -
online
f-a   2b       fc             target       cna           -
online
4 entries were displayed.
*>
```

4. Eseguire una delle seguenti operazioni:

Se la porta CNA…	Quindi…
Non avere la personalità che si desidera	Passare a. Fase 5.
Avere la personalità che si desidera	Salta il passaggio 5 al passaggio 9 e vai aFase 10 .

5. eseguire una delle seguenti operazioni:

Se si sta configurando…	Quindi…
Porte su una scheda UTA/UTA2	Vai aFase 6
Porte UTA/UTA2 integrate	Salta il passaggio 6 e vai aFase 7 .

6. Se l'adattatore è in modalità iniziatore e la porta UTA/UTA2 è online, metti offline la porta UTA/UTA2:

   `storage disable adapter adapter_name`

   Gli adattatori in modalità di destinazione sono automaticamente offline in modalità di manutenzione.

7. se la configurazione corrente non corrisponde all'utilizzo desiderato, modificare la configurazione in base alle necessità:

   `ucadmin modify -m fc|cna -t initiator|target <adapter_name>`

   - `-m` È la modalità Personality, FC o 10GbE UTA.
   - `-t` È di tipo FC4, `target` oppure `initiator`.

   > È necessario utilizzare l'iniziatore FC per le unità nastro e le configurazioni MetroCluster . Per i client SAN è necessario utilizzare la destinazione FC.

8. Mettere online tutte le porte di destinazione immettendo il seguente comando, una volta per ogni porta:

   `storage enable adapter <adapter_name>`

9. Collegare la porta.
10. Esci dalla modalità di manutenzione:

    `halt`

11. avviare il nodo nel menu di avvio:

    `boot_ontap menu`

Quali sono le prossime novità?

- Se si sta eseguendo l'aggiornamento a un sistema AFF A800, visitare il sito "Riassegnare i dischi del nodo 2 al nodo 4, fase 9".
- Per tutti gli altri aggiornamenti di sistema, vai a"Riassegnare node2 dischi a node4, passaggio 1" .

Riassegnare dischi da node2 TB a node4 TB

È necessario riassegnare i dischi che appartenevano a node2 a node4 prima di verificare l'installazione di node4.

Fasi

1. Verificare che node2 si sia fermato al menu di avvio e riassegnare i dischi di node2 a node4:

   ```
   boot_after_controller_replacement
   ```

   Dopo un breve intervallo di tempo, viene richiesto di inserire il nome del nodo da sostituire. Se sono presenti dischi condivisi (chiamati anche Advanced Disk Partitioning (ADP) o dischi partizionati), viene richiesto di inserire il nome del nodo del partner ha.

   Questi prompt potrebbero essere interrati nei messaggi della console. Se non si immette un nome di nodo o non si immette un nome corretto, viene richiesto di inserire nuovamente il nome.

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>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner 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).

2. Se il sistema entra in un ciclo di riavvio con il messaggio `no disks found` indica che il sistema ha reimpostato le porte FC o UTA/UTA2 sulla modalità di destinazione e pertanto non è in grado di vedere alcun disco. Selezionare una delle seguenti attività per risolvere questo problema:
   - EseguireFase 3 AFase 8 sul nodo 4
   - Vai alla sezione"Verificare l'installazione di node4"
3. premere Ctrl-C durante l'OPERAZIONE per arrestare il nodo al prompt Loader>.
4. Al prompt del CARICATORE, accedere alla modalità di manutenzione:

   ```
   boot_ontap maint
   ```

5. In modalità di manutenzione, visualizzare tutte le porte iniziatore precedentemente impostate che si trovano ora in modalità di destinazione:

   ```
   ucadmin show
   ```

   Riportare le porte in modalità initiator:

   ```
   ucadmin modify -m fc -t initiator -f adapter name
   ```

6. Verificare che le porte siano state modificate in modalità initiator:

   ```
   ucadmin show
   ```

7. Uscire dalla modalità di manutenzione:

   ```
   halt
   ```

   > Se si esegue l'aggiornamento da un sistema che supporta dischi esterni a un sistema che supporta anche dischi esterni, visitare il sito Fase 8.
   >
   > Se si esegue l'aggiornamento da un sistema che utilizza dischi esterni a un sistema che supporta dischi interni ed esterni, ad esempio un sistema AFF A800, visitare il sito Fase 9.

8.]al prompt di Loader, 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
```

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

b. Invio `y` al seguente prompt:

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

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

d. 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.

e. 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 Fase 8 fino a quando il sistema non si avvia normalmente.

9. Se si esegue l'aggiornamento da un sistema con dischi esterni a un sistema che supporta dischi interni ed esterni (ad esempio, sistemi AFF A800), impostare l'aggregato node2 come aggregato radice per garantire che node4 si avvii dall'aggregato radice di node2. Per impostare l'aggregato radice, vai al menu di avvio su node4 e seleziona l'opzione `5` per entrare in modalità manutenzione.

> **È necessario eseguire i seguenti passaggi secondari nell'ordine esatto indicato; in caso contrario, si potrebbe verificare un'interruzione o addirittura la perdita di dati.**

La seguente procedura imposta node4 per l'avvio dall'aggregato root di node2:

a. Accedere alla modalità di manutenzione:

```
boot_ontap maint
```

b. Controllare le informazioni su RAID, plex e checksum per l'aggregato node2:

```
aggr status -r
```

c. Controllare lo stato dell'aggregato node2:

```
aggr status
```

d. Se necessario, portare online l'aggregato node2:

```
aggr_online root_aggr_from_node2
```

e. Impedire al node4 di avviarsi dal proprio aggregato root originale:

```
aggr offline root_aggr_on_node4
```

f. Impostare l'aggregato root node2 come nuovo aggregato root per node4:

```
aggr options aggr_from_node2 root
```

g. Verificare che l'aggregato root di node4 sia offline e che l'aggregato root per i dischi portati da node2 sia online e impostato su root:

```
aggr status
```

> La mancata esecuzione del passaggio secondario precedente potrebbe causare l'avvio di node4 dall'aggregato root interno, oppure il sistema potrebbe assumere l'esistenza di una nuova configurazione del cluster o richiedere di identificarne una.

Di seguito viene riportato un esempio dell'output del comando:

```
------------------------------------------------------------------------
Aggr State                      Status              Options
aggr 0_nst_fas8080_15 online    raid_dp, aggr       root, nosnap=on
                                fast zeroed
                                64-bit
aggr0 offline                   raid_dp, aggr       diskroot
                                fast zeroed`
                                64-bit
------------------------------------------------------------------------
```

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. In base alla versione di ONTAP in esecuzione sulla coppia ha sottoposta a upgrade, esegui una delle seguenti azioni:

Se la versione di ONTAP è…	Quindi…
da 9,8 a 9.11.1	Verificare che le LIF del cluster siano in ascolto sulla porta 7700: `::> network connections listening show -vserver Cluster`
9.12.1 o versione successiva	Saltare questo passaggio e passare a. Fase 5.

   La porta 7700 in ascolto sulle porte del cluster è il risultato previsto, come mostrato nell'esempio seguente per un cluster a due nodi:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

4. Per ogni cluster LIF che non è in ascolto sulla porta 7700, imposta lo stato amministrativo della LIF su

`down` e poi `up`:

```
::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
int modify -vserver Cluster -lif cluster-lif -status-admin up
```

Ripetere il passaggio 3 per verificare che la LIF del cluster sia in ascolto sulla porta 7700.

5. passare alla modalità privilegi avanzati:

```
set advanced
```

6. 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
```

7. Se si lavora su un sistema MetroCluster, verificare che il controller sostituito sia configurato correttamente per la configurazione MetroCluster; la configurazione MetroCluster dovrebbe essere in buono stato. Fare riferimento a. "Verificare lo stato della configurazione MetroCluster".

   Riconfigurare le LIF dell'intercluster sul nodo MetroCluster node4 e controllare il peering del cluster per ripristinare la comunicazione tra i nodi MetroCluster prima di procedere Fase 6.

   Controllare lo stato del nodo MetroCluster:

```
metrocluster node show
```

8. riprendere l'operazione di sostituzione del controller:

```
system controller replace resume
```

9. 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*.

10. 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*.

> Se si modifica la velocità delle porte del cluster e0a e E1a nei sistemi AFF A800 o AFF C800, è possibile che vengano ricevuti pacchetti non validi dopo la conversione della velocità. Vedere "Bug online di NetApp ID 1570339" e l'articolo della knowledge base "Errori CRC sulle porte T6 dopo la conversione da 40GbE a 100GbE" come guida.

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::*> reachability show -node node2_node4
  (network port reachability show)
Node         Port       Expected Reachability       Reachability Status
---------    --------  --------------------------
---------------------
node2_node4
             a0a        Default:Default            no-reachability
             a0a-822    Default:822                no-reachability
             a0a-823    Default:823                no-reachability
             e0M        Default:Mgmt               ok
             e0a        Cluster:Cluster            misconfigured-
reachability
             e0b        Cluster:Cluster            no-reachability
             e0c        Cluster:Cluster            no-reachability
             e0d        Cluster:Cluster            no-reachability
             e0e        Cluster:Cluster            ok
             e0e-822    -                          no-reachability
             e0e-823    -                          no-reachability
             e0f        Default:Default            no-reachability
             e0f-822    Default:822                no-reachability
             e0f-823    Default:823                no-reachability
             e0g        Default:Default            misconfigured-
reachability
             e0h        Default:Default            ok
             e0h-822    Default:822                ok
             e0h-823    Default:823                ok
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 e0h
```

```
Warning: Repairing port "node2_node4: e0h" 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
                  e0e           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 "e0e" in "e0h":

      ```
      Cluster::*> displaced-vlans restore -node node2_node4 -port e0e
      -destination-port e0h
      ```

      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      ""           00000000000000000200000000000a008a81976
   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, è necessario spostare i LIF dei dati NAS di proprietà del nodo 2 dal nodo 3 al nodo 4 e confermare che i LIF SAN siano presenti sul nodo 4.

A proposito di questa attività

I LIF remoti gestiscono il traffico verso le LUN SAN durante la procedura di aggiornamento. Lo spostamento dei SAN LIF non è necessario per l'integrità del cluster o del servizio durante l'aggiornamento. I LIF SAN non vengono spostati a meno che non sia necessario mapparli su nuove porte.

Dopo aver portato online node4, è necessario verificare che i LIF siano integri e posizionati sulle porte corrette.

> Se si modifica la velocità delle porte delle schede di interfaccia di rete Ethernet basate su T6 o delle porte della scheda madre, è possibile che vengano ricevuti pacchetti non validi dopo la conversione della velocità. Vedere "Bug online di NetApp ID 1570339" e l'articolo della knowledge base "Errori CRC sulle porte T6 dopo la conversione da 40GbE a 100GbE" come guida.

Fasi

1. 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

In questa fase del controllo di raggiungibilità della rete, il sistema sospende l'operazione.

2. 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.

3. 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.

4. Se necessario, ripristinare e ripristinare i LIF spostati oppure migrare e modificare manualmente i LIF del nodo 2 che non sono riusciti a trasferirsi automaticamente nel nodo 4.

Ripristinare e ripristinare i LIF spostati

a. Elencare eventuali LIF spostati:

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

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

```
cluster controller-replacement network displaced-interface
restore-home-node -node <node4_nodename> -vserver <vserver name>
-lif-name <lif_name>
```

Migrare e modificare manualmente i LIF

a. Migrare i LIF che non sono riusciti a trasferirsi automaticamente al nodo 4:

```
network interface migrate -vserver <vserver name> -lif <lif_name>
-destination-node <node4_nodename> -destination-port
<port_on_node4>
```

b. Modificare il nodo home e la porta home per i LIF migrati:

```
network interface modify -vserver <vserver_name> -lif
<data_lif_name> -home-node <node4_nodename> -home-port
<home_port>
```

5. 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

Gestire l’autenticazione utilizzando i server KMIP

Con ONTAP 9.8 o versioni successive, è possibile 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 utilizzate unità auto-crittografanti e hai impostato `kmip.init.maxwait` variabile a `off` (ad esempio, in"Installa e avvia node4, passaggio 22"), 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

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

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.
"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.
"Gestione delle coppie HA"	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.
"Gestione MetroCluster e disaster recovery"	Descrive come eseguire le operazioni di switchover e switchback MetroCluster, sia nelle operazioni di manutenzione pianificate che in caso di disastro.
"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 9.0: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.0 supportati.

Contenuto	Descrizione
"Comandi di ONTAP 9.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.1 supportati.
"Comandi di ONTAP 9.2: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.2 supportati.
"Comandi di ONTAP 9.3: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.3 supportati.
"Comandi di ONTAP 9.4: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.4 supportati.
"Comandi di ONTAP 9.5: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.5 supportati.
"Comandi di ONTAP 9.6: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.6 supportati.
"Comandi di ONTAP 9.7: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.7 supportati.
"Comandi di ONTAP 9.8: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.8 supportati.
"Comandi di ONTAP 9.9.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.9.1 supportati.
"Comandi di ONTAP 9.10.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.10.1 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 "sostituzione controller di sistema" per aggiornare l'hardware del controller introdotto in ONTAP 9.15.1 e versioni successive"	Descrive le procedure di trasferimento degli aggregati necessarie per aggiornare senza interruzioni i controller introdotti in ONTAP 9.15.1 e versioni successive utilizzando i comandi "system controller replace".
"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.
"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".

Contenuto	Descrizione
"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.
"Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller che esegue ONTAP 9.5 a ONTAP 9.7"	Vengono descritte le procedure di riposizionamento degli aggregati necessarie per aggiornare senza interruzioni i controller che eseguono ONTAP 9.5 a ONTAP 9.7 utilizzando i comandi "system controller replace".
"Utilizzare il trasferimento di aggregati per aggiornare manualmente l'hardware del controller con ONTAP 9.7 o versione precedente"	Descrive le procedure di trasferimento degli aggregati necessarie per eseguire aggiornamenti manuali dei controller senza interruzioni con ONTAP 9.7 o versione precedente.

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.

Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller che esegue ONTAP 9.5 a 9.7

Scopri di più sulla procedura di aggiornamento ARL

Esistono diversi metodi di rilocazione aggregata (ARL) per aggiornare l'hardware del controller. Questa procedura descrive come aggiornare l'hardware del controller utilizzando ARL con "comandi di sostituzione del controller di sistema" su sistemi che eseguono ONTAP 9.7, 9.6 o 9.5.

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, "node1" viene sostituito da "node3" e "node2" da "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 lo stesso nome di "node1" e "node4" ha lo stesso nome di "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. Devi anche leggere e comprendere il "linee guida per l'aggiornamento dei controller con ARL" e il "Sequenza di 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 `wipeconfig` i comandi non sono inclusi in questa procedura. Se in precedenza è stato utilizzato l'hardware del controller sostitutivo, è necessario contattare il supporto tecnico, in particolare se i controller eseguivano Data ONTAP in 7-Mode.
- 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 ha nel cluster.
- Questa procedura si applica ai sistemi FAS e AFF .
- A partire da ONTAP 9.6, questa procedura si applica ai sistemi con configurazione MetroCluster a 4 nodi o superiore. Poiché i siti di configurazione MetroCluster possono trovarsi in due posizioni fisicamente diverse, l'aggiornamento automatizzato del controller deve essere eseguito singolarmente in ciascun sito MetroCluster per una coppia ha.
- Se si sta eseguendo l'aggiornamento da un sistema AFF A320, è possibile utilizzare i movimenti dei volumi per aggiornare l'hardware del controller o contattare il supporto tecnico. Se si desidera spostare il volume, fare riferimento a. "Riferimenti" Per collegarsi a *Upgrade spostando volumi o storage*.

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.

Le versioni precedenti di questo contenuto contenevano istruzioni per un processo di aggiornamento del controller senza interruzioni, che comprendeva passaggi interamente manuali. Questo contenuto fornisce i passaggi per la nuova procedura automatica.

Il processo manuale è stato lungo e complesso, ma in questa procedura semplificata è possibile implementare un aggiornamento del controller utilizzando il trasferimento degli aggregati, che consente aggiornamenti più efficienti e senza interruzioni per le coppie ha. Le procedure manuali sono notevolmente inferiori, in particolare per quanto riguarda la convalida, la raccolta di informazioni e i controlli successivi.

Decidere se utilizzare questa procedura di ricollocazione aggregata

Esistono diversi metodi di ricollocazione aggregata (ARL) per aggiornare l'hardware del controller. Questa procedura descrive come aggiornare l'hardware del controller utilizzando ARL con "comandi di sostituzione del controller di sistema" su sistemi che eseguono ONTAP 9.7, 9.6 o 9.5. Questa complessa procedura dovrebbe essere utilizzata solo da amministratori ONTAP esperti.

Per aiutarti a decidere se questa procedura ARL è adatta all'aggiornamento hardware del tuo controller, dovresti esaminare tutte le seguenti circostanze per gli aggiornamenti supportati:

- Stai aggiornando i controller NetApp che eseguono ONTAP 9.5, 9.6 o 9.7. Questo documento non è applicabile agli aggiornamenti a ONTAP 9.8.
- Non vuoi aggiungere i nuovi controller come nuova coppia ha al cluster e migrare i dati utilizzando gli spostamenti 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.

- La combinazione di aggiornamento hardware è elencata in matrice modello supportata .
- Se si sta aggiornando una configurazione MetroCluster, si tratta di una configurazione FC a 4 nodi o superiore e tutti i nodi eseguono ONTAP 9.6 o 9.7.

- Se si sta aggiornando un sistema scambiando i moduli del controller nello stesso chassis, come AFF A800 o AFF C800, NetApp consiglia vivamente di utilizzare la procedura di aggiornamento che"aggiorna i modelli di controller utilizzando ARL, mantenendo lo chassis e i dischi del sistema esistenti" . Questa procedura ARL include i passaggi che garantiscono che i dischi interni rimangano saldamente nello chassis quando si rimuovono e si installano i controller durante la procedura di aggiornamento.

  "Scopri le combinazioni di aggiornamento del sistema supportate utilizzando ARL, mantenendo lo chassis e i dischi del sistema esistenti".

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

Combinazioni di aggiornamento del sistema supportate

Le tabelle seguenti mostrano la matrice dei modelli supportati per l'aggiornamento del controller utilizzando questa procedura ARL.

Vecchio controller	Controller sostitutivo
FAS8020, FAS8040, FAS8060, FAS8080	FAS8200, FAS8300, FAS8700, FAS9000
AFF8020, AFF8040, AFF8060, AFF8080	AFF A300, AFF A400, AFF A700[1], AFF A800[2]
FAS8200	FAS8700, FAS9000, FAS8300[4, 5]
AFF A300	AFF A700[1], AFF A800[2, 3], AFF A400[4, 5]

Se la combinazione di modelli di upgrade del controller non è riportata nella tabella precedente, contattare il supporto tecnico.

[1]l'aggiornamento automatizzato ARL per il sistema AFF A700 è supportato da ONTAP 9.7P2.

[2]Se si esegue l'aggiornamento a un AFF A800 o a un sistema che supporta dischi interni ed esterni, è necessario seguire istruzioni specifiche per l'aggregazione root sui dischi NVMe interni. Fare riferimento a"Riassegnare node1 dischi a node3, passaggio 9" E"Riassegnare node2 dischi a node4, passaggio 9" .

[3]l'aggiornamento automatizzato ARL da un sistema AFF A300 a un sistema AFF A800 è supportato da ONTAP 9.7P5.

[4]ONTAP 9.7P8 supporta l'aggiornamento automatizzato ARL da un sistema AFF A300 a un sistema AFF A400 e FAS8200 a un sistema FAS8300.

[5]se si esegue l'aggiornamento da un sistema AFF A300 a un sistema AFF A400 o FAS8200 a un sistema FAS8300 in una configurazione cluster senza switch a due nodi, è necessario scegliere le porte cluster temporanee per l'aggiornamento del controller. I sistemi AFF A400 e FAS8300 sono disponibili in due configurazioni, come bundle Ethernet in cui le porte della scheda mezzanine sono di tipo Ethernet e come bundle FC in cui le porte mezzanine sono di tipo FC.

- Per un sistema AFF A400 o FAS8300 con configurazione di tipo Ethernet, è possibile utilizzare una qualsiasi delle due porte mezzanine come porte cluster temporanee.
- Per un sistema AFF A400 o FAS8300 con configurazione di tipo FC, è necessario aggiungere una scheda di interfaccia di rete 10GbE a quattro porte (codice X1147A) per fornire porte cluster temporanee.
- Dopo aver completato un aggiornamento del controller utilizzando porte cluster temporanee, è possibile migrare senza interruzioni le LIF del cluster a e3a ed e3b, porte 100GbE su un sistema AFF A400 e porte e0c ed e0d, 100GbE su un sistema FAS8300.

Scegli una procedura di aggiornamento hardware diversa

- "Esaminare i metodi ARL alternativi disponibili per l'aggiornamento dell'hardware del controller".
- 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*.

Informazioni correlate

Fare riferimento a "Riferimenti" per collegarsi alla *Documentazione 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 (aggregate relocation) per aggiornare una coppia di controller che eseguono ONTAP 9.5 a ONTAP 9.7, dipende dalla piattaforma e dalla configurazione dei controller originali e sostitutivi.

Aggiornamenti supportati per ARL

Quando si aggiorna una coppia di nodi utilizzando questa procedura ARL per ONTAP 9.5 a ONTAP 9.7, è necessario verificare che ARL possa essere eseguito sui controller originali e sostitutivi.

Controllare le dimensioni di tutti gli aggregati definiti e il numero di dischi supportati dal sistema originale. È quindi necessario confrontare le dimensioni e il numero di dischi aggregati supportati con le dimensioni e il numero di dischi aggregati supportati dal nuovo sistema. Fare riferimento a. "Riferimenti" Per collegarsi al *Hardware Universe* dove queste informazioni sono disponibili. 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.

È necessario verificare nelle regole di combinazione del cluster se i nuovi nodi possono diventare parte del cluster con i nodi esistenti, quando il controller originale viene sostituito. Per ulteriori informazioni sulle regole

di combinazione dei cluster, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*.

> Prima di eseguire un aggiornamento del sistema AFF, è necessario aggiornare ONTAP alla versione 9.5P1 o successiva. Questi livelli di release sono necessari per un aggiornamento corretto.

> Se si sta aggiornando un sistema che supporta dischi interni (ad esempio, un sistema FAS2700 o AFF A250) ma NON dispone di dischi interni, fare riferimento a. "Riferimenti" E utilizzare la procedura descritta nella sezione *aggregate Relocation to Manually Upgrade Controller hardware* content (trasferimento aggregato per aggiornare manualmente l'hardware del controller) corretta per la versione di ONTAP in uso.

Se si utilizza ONTAP 9.6P11, 9.7P8 o versioni successive, si consiglia di attivare il Takeover di connettività, livellosità e monitoraggio della disponibilità (CLAM) per riportare il cluster al quorum quando si verificano determinati guasti del nodo. Il `kernel-service` il comando richiede un accesso avanzato a livello di privilegio. Per ulteriori informazioni, consulta: "Articolo SU436 della Knowledge base di NetApp: Modifica della configurazione predefinita DI Takeover DI CLAM".

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 è possibile eseguire i seguenti aggiornamenti:

- Ai 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.

- Ai controller entry-level con dischi interni, ad esempio FAS 2500.

  Se si desidera aggiornare i controller entry-level con dischi interni, fare riferimento a. "Riferimenti" Per collegarsi a *Upgrade spostando volumi o storage* e passare alla procedura *aggiornamento di una coppia di nodi che eseguono Clustered Data ONTAP spostando volumi*.

Configurazione MetroCluster FC

In una configurazione FC MetroCluster, è necessario sostituire i nodi del sito di disaster recovery/failover il prima possibile. La mancata corrispondenza nei modelli di controller all'interno di una configurazione MetroCluster non è supportata perché la mancata corrispondenza del modello di controller può causare la disconnessione del mirroring del disaster recovery. Utilizzare `-skip-metrocluster-check true` comando per ignorare i controlli MetroCluster quando si sostituiscono i nodi nel secondo sito.

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.

Se si verificano problemi durante l'aggiornamento dei controller, fare riferimento a"Risolvere i problemi" sezione. Le informazioni sui guasti che possono verificarsi sono elencate in base alla fase della procedura nel"Sequenza di aggiornamento ARL" .

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

Verificare lo stato della configurazione MetroCluster

Prima di avviare un aggiornamento su una configurazione Fabric MetroCluster, è necessario verificare lo stato della configurazione MetroCluster per verificarne il corretto funzionamento.

Fasi

1. Verificare che i componenti di MetroCluster siano integri:

   `metrocluster check run`

   ```
   dpgqa-mcc-funct-8040-0403_siteA::*> metrocluster check run
   ```

   L'operazione viene eseguita in background.

2. Dopo il `metrocluster check run` operazione completata, visualizzare i risultati:

   `metrocluster check show`

   Dopo circa cinque minuti, vengono visualizzati i seguenti risultati:

   ```
   metrocluster_siteA::*> metrocluster check show
   Last Checked On: 4/7/2019 21:15:05
   Component            Result
   ---------------      -------
   nodes                ok
   lifs                 ok
   config-replication   ok
   aggregates           warning
   clusters             ok
   connections          not-applicable
   volumes              ok
   7 entries were displayed.
   ```

3. Controllare lo stato dell'operazione di controllo MetroCluster in esecuzione:

```
metrocluster operation history show -job-id 38
```

4. Verificare che non siano presenti avvisi sullo stato di salute:

```
system health alert show
```

Verificare la presenza di errori di configurazione MetroCluster

È possibile utilizzare lo strumento Active IQ Config Advisor disponibile sul sito del supporto NetApp per verificare la presenza di errori di configurazione comuni.

Se non si dispone di una configurazione MetroCluster, ignorare questa sezione.

A proposito di questa attività

Active IQ Config Advisor è uno strumento per la convalida della configurazione e il controllo dello stato di salute. È possibile implementarlo sia in siti sicuri che in siti non sicuri per la raccolta di dati e l'analisi del sistema.

Il supporto per Config Advisor è limitato e disponibile solo online.

1. Scaricare il "Active IQ Config Advisor" tool.
2. Eseguire Active IQ Config Advisor, esaminare l'output e seguire i consigli per risolvere eventuali problemi.

Verificare lo switchover, la riparazione e lo switchback

Verificare le operazioni di switchover, riparazione e switchback della configurazione MetroCluster.

Fare riferimento a. "Riferimenti" Per collegarsi al contenuto di *Gestione MetroCluster e disaster recovery* e utilizzare le procedure indicate per lo switchover negoziato, la riparazione e lo switchback.

Scopri la sequenza di 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	Fasi
"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 Onboard Key Manager ed è possibile 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. È necessario registrare le informazioni necessarie per il node1 da utilizzare più avanti nella procedura e quindi dismettere il node1. 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 3. Installazione e boot node3"	Durante la fase 3, è necessario installare e avviare node3, mappare il cluster e le porte di gestione dei nodi da node1 a node3, riassegnare i dischi da node1 a node3 e verificare l'installazione di node3. Se necessario, impostare la configurazione FC o UTA/UTA2 su node3 e confermare che node3 si è Unito al quorum. 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	Fasi
"Fase 4. Spostare e dismettere il node2"	Durante la fase 4, è possibile spostare node2 aggregati non root e LIF di dati non SAN in node3. È inoltre possibile registrare le informazioni necessarie per il node2, quindi dismettere il node2. 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, è necessario installare e avviare node4, mappare il cluster e le porte di gestione dei nodi da node2 a node4, riassegnare i dischi da node2 a node4 e verificare l'installazione di node4. Se necessario, impostare la configurazione FC o UTA/UTA2 su node4 e confermare che node4 si è Unito al quorum. 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, 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.

Fase 1. Preparatevi per l'aggiornamento

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 questo comando solo a livello di privilegi avanzati:
   `set -privilege advanced`

Viene visualizzato il seguente output:

```
Warning:
1. Current ONTAP version is 9.x
Before starting controller replacement operation, ensure that the new
controllers are running the version 9.x

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.

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.
MCC Cluster Check (controllo cluster MCC)	Verifica se il sistema è una configurazione MetroCluster. L'operazione rileva automaticamente se si tratta o meno di una configurazione MetroCluster ed esegue i controlli preliminari e di verifica specifici. È supportata solo la configurazione MetroCluster FC a 4 nodi. In caso di configurazione MetroCluster a 2 nodi e configurazione IP MetroCluster a 4 nodi, il controllo non riesce. Se la configurazione MetroCluster è in stato di switchover, il controllo non riesce.
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.

Eseguire un controllo preliminare	Descrizione
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.
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. Se mancano dei dischi, fare riferimento al "Riferimenti"collegamento alla gestione *disco e aggregato con la CLI*, alla gestione *logica dello storage con la CLI* e alla gestione *coppia ha* 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.
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,clustermgmt, 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`
- `network port vlan show`
- `system node show -instance -node local`
- `run -node local sysconfig`
- `storage aggregate show -node local`
- `volume show -node local`
- `network interface failover-groups show`
- `storage array config show -switch switch_name`
- `system license show -owner local`
- `storage encryption disk show`

> Se NetApp Volume Encryption (NVE) o NetApp aggregate Encryption (NAE) con Onboard Key Manager sono 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)

   > Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha.
   >
   > È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

   "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

Alcune funzionalità richiedono licenze, emesse come *pacchetti* che includono una o più funzionalità. Ogni nodo del cluster deve disporre di una propria chiave per poter utilizzare ciascuna funzionalità nel cluster.

Se non si dispone di nuove chiavi di licenza, le funzionalità attualmente concesse in licenza nel cluster sono disponibili per il nuovo controller. Tuttavia, l'utilizzo di funzionalità senza licenza sul controller potrebbe non essere conforme al contratto di licenza, pertanto è necessario installare la nuova chiave di licenza o le nuove chiavi per il nuovo controller al termine dell'aggiornamento.

Fare riferimento a. "Riferimenti" Per accedere al *sito di supporto NetApp*, dove è possibile ottenere nuove chiavi di licenza di 28 caratteri per ONTAP. Le chiavi sono disponibili nella sezione *My Support* sotto *licenze software*. Se il sito non dispone delle chiavi di licenza necessarie, contattare il rappresentante commerciale NetApp.

Per informazioni dettagliate sulle licenze, fare riferimento a. "Riferimenti" Per collegarsi al *System Administration Reference*.

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

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 deve essere già in pausa quando si avvia l'operazione; è necessario ripristinarla manualmente.

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. Dopo aver portato il nodo 3 online, è necessario verificare che i file LIF siano integri e posizionati su porte appropriate.

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 <aggregate_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 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`

6. 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` *`nodename`* `-status-admin up`

7. Se sono stati configurati gruppi di interfacce o VLAN, completare i seguenti passaggi secondari:

   a. Se non sono già state salvate, registrare le informazioni relative alla VLAN e al gruppo di interfacce in modo da poter ricreare le VLAN e i gruppi di interfacce sul nodo 3 dopo l'avvio del nodo 3.

   b. Rimuovere le VLAN dai gruppi di interfacce:

      `network port vlan delete -node` *`nodename`* `-port` *`ifgrp`* `-vlan-id` *`VLAN_ID`*

      Seguire l'azione correttiva per risolvere eventuali errori suggeriti dal comando di eliminazione della vlan.

   c. Immettere il seguente comando ed esaminare il relativo output per verificare l'eventuale presenza di gruppi di interfacce configurati sul nodo:

      `network port ifgrp show -node` *`nodename`* `-ifgrp` *`ifgrp_name`* `-instance`

      Il sistema visualizza le informazioni sul gruppo di interfacce per il nodo, come illustrato nell'esempio seguente:

```
cluster::> network port ifgrp show -node node1 -ifgrp a0a -instance
                  Node: node1
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode_lacp
          MAC Address: 02:a0:98:17:dc:d4
   Port Participation: partial
        Network Ports: e2c, e2d
             Up Ports: e2c
           Down Ports: e2d
```

   a. Se nel nodo sono configurati gruppi di interfacce, registrare i nomi di tali gruppi e le porte ad essi assegnate, quindi eliminare le porte immettendo il seguente comando, una volta per ciascuna porta:

      `network port ifgrp remove-port -node` *`nodename`* `-ifgrp` *`ifgrp_name`* `-port` *`netport`*

Spostare gli aggregati non riusciti o vetoed

Se gli aggregati non riescono a spostare o sono vetoed, è necessario spostare manualmente gli aggregati o eseguire l'override dei veti o dei controlli di destinazione, se necessario.

A proposito di questa attività

Il sistema interrompe l'operazione di ricollocazione a causa dell'errore.

Fasi

1. Controllare i registri EMS per determinare il motivo per cui l'aggregato non è riuscito a spostare o è stato vetoato.
2. Spostare eventuali aggregati guasti o vetoed:

   ```
   storage aggregate relocation start -node node1 -destination node2 aggregate-list * -ndocontroller-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	Immettere quanto segue: `storage aggregate relocation start -override -vetoes * -ndocontroller-upgrade true`
Ignorare i controlli di destinazione	Immettere quanto segue: `storage aggregate relocation start -overridedestination-checks * -ndo -controllerupgrade 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.

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.

Tuttavia, non è necessario eseguire il netboot dei controller se è installata la stessa versione di ONTAP 9 installata sui controller originali. In tal caso, saltare questa sezione e passare a. "Fase 3 Installazione e boot node3"

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.

Per…	Quindi…

Sistemi della serie FAS/AFF8000	Estrarre il contenuto di `<ontap_version>_image.tgz` file nella directory di destinazione:
	`tar -zxvf <ontap_version>_image.tgz`
	Se si sta estraendo il contenuto su Windows, utilizzare 7-zip o WinRAR per estrarre l'immagine di netboot.
	L'elenco delle directory deve contenere una cartella netboot con un file kernel:
	`netboot/kernel`

Tutti gli altri sistemi	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

Installazione e boot node3

È necessario installare node3 nel rack, trasferire le connessioni del node1 al node3, fare il boot node3 e installare ONTAP. È quindi necessario riassegnare uno qualsiasi dei dischi spare di node1, tutti i dischi appartenenti al volume root e qualsiasi aggregato non root che non sia stato trasferito in node2 precedentemente nel 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, è necessario verificare che le LIF SAN siano state spostate correttamente in 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".

- Per un aggiornamento del controller AFF A800 o AFF C800 , è necessario assicurarsi che tutte le unità nello chassis siano saldamente posizionate contro il midplane prima di rimuovere node1. Per maggiori informazioni, vedere "Sostituire i moduli controller AFF A800 o AFF C800".
- Se si sta eseguendo l'aggiornamento di un sistema con dischi di storage, completare l'intera sezione e passare alla "Configurare le porte FC sul nodo 3" e. "Controllare e configurare le porte UTA/UTA2 sul nodo 3" sezioni, immissione dei comandi al prompt del cluster.

Fasi

1. assicurarsi di disporre di spazio rack per node3.

   Se node1 e node2 si trovano in uno chassis separato, è possibile inserire node3 nella stessa posizione rack del node1. Tuttavia, se il nodo 1 si trovava nello stesso chassis con il nodo 2, è necessario inserire il nodo 3 nel proprio spazio rack, preferibilmente vicino alla posizione del nodo 1.

2. installare node3 nel rack, seguendo le *istruzioni di installazione e configurazione* per il modello di nodo in uso.

   Se si esegue l'aggiornamento a un sistema con entrambi i nodi nello stesso chassis, installare node4 e node3 nello chassis. Se non si installano entrambi i nodi nello stesso chassis, quando si avvia node3, questo si comporta come se fosse in una configurazione a doppio chassis, mentre quando si avvia node4, l'interconnessione tra i nodi non si attiva.

3. cavo node3, spostamento delle connessioni da node1 a node3.

   Cablare le seguenti connessioni utilizzando le *Istruzioni di installazione e configurazione* per la piattaforma node3, il documento appropriato sullo scaffale dei dischi e la documentazione sulla *gestione delle coppie HA*.

   Fare riferimento a"Riferimenti" per collegarsi alla *gestione delle coppie HA*.

- Console (porta di gestione remota)
- Porte del cluster
- Porte dati
- Porte di gestione di cluster e nodi
- Storage
- Configurazioni SAN: Porte switch FC e Ethernet iSCSI

> Potrebbe non essere necessario spostare la scheda di interconnessione o la connessione del cavo di interconnessione del cluster dal nodo 1 al nodo 3, poiché la maggior parte dei modelli di piattaforma dispone di un modello di scheda di interconnessione unico. Per la configurazione MetroCluster, è necessario spostare le connessioni del cavo FC-VI dal nodo 1 al nodo 3. Se il nuovo host non dispone di una scheda FC-VI, potrebbe essere necessario spostare la scheda FC-VI.

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.

   Se si sta eseguendo l'aggiornamento a un sistema con entrambi i nodi nello stesso chassis, anche node4 viene riavviato. Tuttavia, è possibile ignorare il node4 boot fino a tardi.

   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.

   > **Non ignorare il ritardo; se non si lascia caricare la batteria, si potrebbe verificare una 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 immettendo 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 (Domain Name Service). Se si utilizza questo parametro opzionale, non è necessario un nome di dominio completo nell'URL del server netboot; è necessario solo il nome host del server. Potrebbero essere necessari altri parametri per l'interfaccia. Invio `help ifconfig` al prompt del firmware per ulteriori informazioni.

7. Esegui netboot al nodo3:

Per…	Quindi…
Sistemi della serie FAS/AFF8000	`netboot http://<web_server_ip/path_to_web-accessible_directory>/netboot/kernel`
Tutti gli altri sistemi	`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
    ```

    Se si dispone di una configurazione MetroCluster, utilizzare i seguenti comandi per modificare il controller e

lo chassis:

```
ha-config modify controller mcc
```

```
ha-config modify chassis mcc
```

14. Esci dalla modalità di manutenzione:

```
halt
```

Interrompere L'OPERAZIONE premendo Ctrl-C al prompt dell'ambiente di avvio.

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

```
date
```

16. al nodo 3, controllare la data utilizzando il seguente comando al prompt dell'ambiente di boot:

```
show date
```

17. se necessario, impostare la data sul node3:

```
set date mm/dd/yyyy
```

18. al nodo 3, controllare l'ora utilizzando il seguente comando al prompt dell'ambiente di boot:

```
show time
```

19. se necessario, impostare l'ora su node3:

```
set time hh:mm:ss
```

20. 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
```

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

```
printenv partner-sysid
```

1. 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**`

> Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha. È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

b. Contattare il supporto NetApp per assistenza nel ripristino delle informazioni di gestione delle chiavi integrate.

2. Avviare il nodo nel menu di avvio:

```
boot_ontap menu
```

Quali sono le prossime novità?

- Se si dispone di un sistema con una configurazione FC o UTA/UTA2,"imposta la configurazione FC o UTA/UTA2 sul nodo 3" .
- Se non si dispone di una configurazione FC o UTA/UTA2,"riassegnare i dischi del nodo 1 al nodo 3" in modo che node3 possa riconoscere i dischi di node1.
- Se si dispone di una configurazione MetroCluster ,"riassegnare i dischi del nodo 1 al nodo 3" .

Impostare la configurazione FC o UTA/UTA2 su node3

Se node3 dispone di porte FC integrate, porte UTA/UTA2 (onboard Unified target adapter) o una scheda UTA/UTA2, è necessario configurare le impostazioni prima di completare il resto della procedura.

A proposito di questa attività

Potrebbe essere necessario completare la sezione Configurare le porte FC sul nodo 3, la sezione Controllare e configurare le porte UTA/UTA2 sul nodo 3, o entrambe le sezioni.

> I materiali di marketing NetApp potrebbero utilizzare il termine UTA2 per fare riferimento alle porte e agli adattatori CNA (Converged Network Adapter). Tuttavia, la CLI utilizza il termine CNA.

Se node3 non dispone di porte FC integrate, porte UTA/UTA2 integrate o una scheda UTA/UTA2 e si sta aggiornando un sistema con dischi di archiviazione, è possibile passare alla sezione "Riassegnare dischi da node1 TB a node3 TB".

Configurare le porte FC sul nodo 3

Se il nodo 3 dispone di porte FC, integrate o su un adattatore FC aggiuntivo, è necessario impostare le configurazioni delle porte sul nodo prima di metterlo in servizio, poiché le porte non sono preconfigurate al momento della spedizione dei sistemi. Se non si configurano le porte, si potrebbe verificare un'interruzione del servizio.

Prima di iniziare

È necessario disporre dei valori delle impostazioni della porta FC del nodo 1 salvati nella sezione "Preparare i nodi per l'aggiornamento".

A proposito di questa attività

È possibile saltare questa sezione se il sistema non dispone di configurazioni FC. Se il sistema dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2, configurarle in Controllare e configurare le porte UTA/UTA2 sul nodo 3.

Immettere i comandi in questa sezione al prompt della shell in modalità Manutenzione.

Fasi

1. Confronta le impostazioni FC sul nodo 3 con le impostazioni acquisite in precedenza dal nodo 1.
2. Eseguire una delle seguenti azioni per modificare le porte FC sul nodo 3, a seconda delle necessità:

   In modalità di manutenzione (opzione 5 nel menu di avvio):

   - Per programmare come porte di destinazione:

     `ucadmin modify -m fc -t target <adapter>`

     Per esempio: `ucadmin modify -m fc -t target 2a`

   - Per programmare le porte initiator:

     `ucadmin modify -m fc -t initiator <adapter>`

   Per esempio: `ucadmin modify -m fc -t initator 2b`

3. Verificare le nuove impostazioni utilizzando il seguente comando ed esaminando l'output:

   `ucadmin show`

4. Arrestare il nodo:

   `halt`

5. Avviare il sistema dal prompt del CARICATORE:

   `boot_ontap menu`

6. Dopo aver immesso il comando, attendere che il sistema si arresti al prompt dell'ambiente di avvio.
7. Selezionare l'opzione `5` dal menu di avvio per la modalità di manutenzione.
8. Eseguire una delle seguenti operazioni:
   - Se node3 ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate, passare a. Controllare e configurare le porte UTA/UTA2 sul nodo 3.
   - Se node3 non dispone di una scheda UTA/UTA2 o di porte onboard UTA/UTA2, ignorare Controllare e configurare le porte UTA/UTA2 sul nodo 3 e andare a "Riassegnare dischi da node1 TB a node3 TB".

Controllare e configurare le porte UTA/UTA2 sul nodo 3

Se node3 dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2, è necessario controllare la configurazione delle porte ed eventualmente riconfigurarle, a seconda di come si desidera utilizzare il sistema aggiornato.

Prima di iniziare

È necessario disporre dei moduli SFP+ corretti per le porte UTA/UTA2.

A proposito di questa attività

Se si desidera utilizzare una porta UTA/UTA2 (Unified Target Adapter) per FC, è necessario prima verificare la configurazione della porta.

> I materiali di marketing NetApp potrebbero utilizzare il termine UTA2 per fare riferimento agli adattatori e alle porte CNA. Tuttavia, la CLI utilizza il termine CNA.

Puoi usare il `ucadmin show` comando per visualizzare o verificare la configurazione della porta corrente, come mostrato nel seguente output di esempio:

```
*> ucadmin show
          Current  Current    Pending   Pending      Admin
Adapter   Mode     Type       Mode      Type         Status
-------   -------  -------    --------  ----------   --------
0e        fc       target     -         initiator    offline
0f        fc       target     -         initiator    offline
0g        fc       target     -         initiator    offline
0h        fc       target     -         initiator    offline
1a        fc       target     -         -            online
1b        fc       target     -         -            online
6 entries were displayed.
```

Le porte UTA/UTA2 possono essere configurate in modalità FC nativa o UTA/UTA2. La modalità FC supporta l'iniziatore FC e la destinazione FC; la modalità UTA/UTA2 consente la condivisione simultanea del traffico NIC e FCoE con la stessa interfaccia SFP+ 10 GbE e supporta le destinazioni FC.

Potresti trovare porte UTA/UTA2 su un adattatore aggiuntivo o sulla scheda madre del controller e avere le seguenti configurazioni, ma dovresti controllare la configurazione delle porte UTA/UTA2 sul nodo 3 e modificarla, se necessario:

- Le schede UTA/UTA2 ordinate al momento dell'ordine del controller vengono configurate prima della spedizione per avere la personalità richiesta.
- Le schede UTA/UTA2 ordinate separatamente dal controller vengono fornite con il linguaggio di destinazione FC predefinito.
- Le porte UTA/UTA2 integrate sui nuovi controller vengono configurate prima della spedizione in modo da avere la personalità richiesta.

> Per configurare le porte UTA/UTA2 è necessario essere in modalità di manutenzione. Immettere i comandi in questa sezione al prompt della shell in modalità Manutenzione.

Fasi

1. Se il modulo SFP+ corrente non corrisponde all'utilizzo desiderato, sostituirlo con il modulo SFP+ corretto.

   Contattare il rappresentante NetApp per ottenere il modulo SFP+ corretto.

2. Verificare le impostazioni della porta UTA/UTA2:

   ```
   ucadmin show
   ```

   Esaminare l'output e determinare se le porte UTA/UTA2 hanno la personalità desiderata.

   L'output nell'esempio seguente mostra che il tipo di adattatore "1b" sta cambiando in iniziatore e che la modalità degli adattatori "2a" e "2b" sta cambiando in "cna". La modalità CNA consente di utilizzare la scheda come adattatore di rete.

   ```
   *> ucadmin show
            Current    Current     Pending  Pending     Admin
   Adapter  Mode       Type        Mode     Type        Status
   -------  --------   ----------  -------  --------    --------
   1a       fc         initiator   -        -           online
   1b       fc         target      -        initiator   online
   2a       fc         target      cna      -           online
   2b       fc         target      cna      -           online
   *>
   ```

3. Eseguire una delle seguenti operazioni:

Se le porte UTA/UTA2…	Quindi…
Non avere la personalità che si desidera	Vai aFase 4 .
Avere la personalità che si desidera	Salta il passaggio 4 al passaggio 8 e vai aFase 9 .

4. Esegui una delle seguenti azioni:

Se si sta configurando…	Quindi…
Porte su una scheda UTA/UTA2	Vai aFase 5
Porte UTA/UTA2 integrate	Salta il passaggio 5 e vai aFase 6 .

5. Se l'adattatore è in modalità iniziatore e la porta UTA/UTA2 è online, metti offline la porta UTA/UTA2:

   ```
   storage disable adapter <adapter_name>
   ```

   Gli adattatori in modalità di destinazione sono automaticamente offline in modalità di manutenzione.

6. Se la configurazione corrente non corrisponde all'uso desiderato, modificare la configurazione secondo necessità:

```
ucadmin modify -m fc|cna -t initiator|target <adapter_name>
```

- `-m` è la modalità personality, `fc` oppure `cna`.
- `-t` È di tipo FC4, `target` oppure `initiator`.

> È necessario utilizzare l'iniziatore FC per le unità nastro e le configurazioni MetroCluster . Per i client SAN è necessario utilizzare la destinazione FC.

7. Mettere online tutte le porte di destinazione immettendo il seguente comando una volta per ogni porta:

```
storage enable adapter <adapter_name>
```

8. Collegare la porta.

1. Uscire dalla modalità di manutenzione:

```
halt
```

2. Avviare il nodo nel menu di avvio eseguendo `boot_ontap menu` .

Quali sono le prossime novità?

- Se stai effettuando l'aggiornamento a un sistema AFF A800 , vai a"Riassegnare node1 dischi a node3, passaggio 9" .
- Per tutti gli altri aggiornamenti di sistema, vai a"Riassegnare node1 dischi a node3, passaggio 1" .

Riassegnare dischi da node1 TB a node3 TB

È necessario riassegnare i dischi che appartenevano a node1 a node3 prima di verificare l'installazione di node3.

Fasi

1. Verificare che node1 si sia fermato al menu di avvio e riassegnare i dischi di node1 a node3:

```
boot_after_controller_replacement
```

Dopo un breve intervallo di tempo, viene richiesto di inserire il nome del nodo da sostituire. Se sono presenti dischi condivisi (chiamati anche Advanced Disk Partitioning (ADP) o dischi partizionati), viene richiesto di inserire il nome del nodo del partner ha.

Questi prompt potrebbero essere interrati nei messaggi della console. Se non si immette un nome di nodo o non si immette un nome corretto, viene richiesto di inserire nuovamente il nome.

Espandere l'esempio di output della console

```
LOADER-A> boot_ontap menu
...
******************************
*                            *
* Press Ctrl-C for Boot 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.
Selection (1-9)? 22/7
.
.
(boot_after_controller_replacement)   Boot after controller upgrade
(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.

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.
Selection (1-9)? 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
.
.
Controller Replacement: Provide name of the node you would like to
replace: <name of the node being replaced>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner of the node being replaced>
Changing sysid of node <node being replaced> disks.
Fetched sanown old_owner_sysid = 536953334 and calculated old sys id
= 536953334
Partner sysid = 4294967295, owner sysid = 536953334
.
.
.
Terminated
<node reboots>
.
.
System rebooting...
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
.
.
System rebooting...
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
Login:
...
```

2. Se il sistema entra in un ciclo di riavvio con il messaggio `no disks found`, questo perché ha reimpostato le porte sulla modalità di destinazione e quindi non è in grado di vedere alcun disco. EseguireFase 3 AFase 8 su node3 per risolvere questo problema.
3. premere Ctrl-C durante L'OPERAZIONE di AUTOBOOT per arrestare il nodo al prompt di Loader>.
4. al prompt DEL CARICATORE, accedere alla modalità di manutenzione:

```
boot_ontap maint
```

5. in modalità di manutenzione, visualizzare tutte le porte iniziatore precedentemente impostate che si trovano ora in modalità di destinazione:

   ```
   ucadmin show
   ```

   Riportare le porte in modalità initiator:

   ```
   ucadmin modify -m fc -t initiator -f adapter name
   ```

6. verificare che le porte siano state modificate in modalità initiator:

   ```
   ucadmin show
   ```

7. uscire dalla modalità di manutenzione:

   ```
   halt
   ```

   > Se si esegue l'aggiornamento da un sistema che supporta dischi esterni a un sistema che supporta anche dischi esterni, visitare il sito Fase 8.
   >
   > Se si esegue l'aggiornamento da un sistema che supporta dischi esterni a un sistema che supporta dischi interni ed esterni, ad esempio un sistema AFF A800, visitare il sito Fase 9.

8. 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:

   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
```

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

b. Invio `y` al seguente prompt:

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

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

d. 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.

e. 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 Fase 8 fino a quando il sistema non si avvia normalmente.

9. Se si esegue l'aggiornamento da un sistema con dischi esterni a un sistema che supporta dischi interni ed esterni (ad esempio, sistemi AFF A800), impostare l'aggregato node1 come aggregato radice per confermare che node3 si avvii dall'aggregato radice di node1. Per impostare l'aggregato radice, vai al menu di avvio su node3 e seleziona l'opzione `5` per entrare in modalità manutenzione.

> ⚠ **È necessario eseguire i seguenti passaggi secondari nell'ordine esatto indicato; in caso contrario, si potrebbe verificare un'interruzione o addirittura la perdita di dati.**

La seguente procedura imposta node3 per l'avvio dall'aggregato root di node1:

a. Accedere alla modalità di manutenzione:

```
boot_ontap maint
```

b. Controllare le informazioni su RAID, plex e checksum per l'aggregato node1:

```
aggr status -r
```

c. Controllare lo stato dell'aggregato node1:

```
aggr status
```

d. Se necessario, portare online l'aggregato node1:

```
aggr_online root_aggr_from_node1
```

e. Impedire al node3 di avviarsi dal proprio aggregato root originale:

```
aggr offline root_aggr_on_node3
```

f. Impostare l'aggregato root node1 come nuovo aggregato root per node3:

```
aggr options aggr_from_node1 root
```

g. Verificare che l'aggregato root di node3 sia offline e che l'aggregato root per i dischi portati da node1 sia online e impostato su root:

```
aggr status
```

> La mancata esecuzione del passaggio secondario precedente potrebbe causare l'avvio di node3 dall'aggregato root interno, oppure il sistema potrebbe presumere l'esistenza di una nuova configurazione del cluster o richiedere di identificarne una.

Di seguito viene riportato un esempio dell'output del comando:

```
------------------------------------------------------------------
Aggr                  State    Status             Options

aggr0_nst_fas8080_15 online   raid_dp, aggr      root, nosnap=on
                              fast zeroed
                              64-bit

aggr0                 offline  raid_dp, aggr      diskroot
                              fast zeroed
                              64-bit
------------------------------------------------------------------
```

Mappare le porte dal nodo 1 al nodo 3

È necessario verificare che le porte fisiche sul nodo 1 siano mappate correttamente alle porte fisiche sul nodo 3, consentendo al nodo 3 di 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.

Le impostazioni delle porte possono variare a seconda del modello dei nodi. È necessario rendere la porta e la configurazione LIF sul nodo originale compatibili con l'utilizzo pianificato e la configurazione del nuovo nodo. Questo perché il nuovo nodo riproduce la stessa configurazione all'avvio, il che significa che quando si avvia node3, ONTAP tenterà di ospitare le LIF sulle stesse porte utilizzate sul node1.

Pertanto, se le porte fisiche sul nodo 1 non vengono mappate direttamente alle porte fisiche sul nodo 3, saranno necessarie modifiche alla configurazione del software per ripristinare la connettività di cluster, gestione e rete dopo l'avvio. Inoltre, se le porte del cluster sul nodo 1 non vengono mappate direttamente alle porte del cluster sul nodo 3, il nodo 3 potrebbe non ricongiungersi automaticamente al quorum quando viene riavviato fino a quando non si modifica la configurazione software per ospitare le LIF del cluster sulle porte fisiche corrette.

Fasi

1. Annotare nella tabella tutte le informazioni relative al cablaggio node1 per il nodo 1, le porte, i domini di trasmissione e gli IPspaces:

LIF	Node1 porte	Node1 IPspaces	Node1 domini di broadcast	Node3 porte	Node3 IPspaces	Node3 domini di broadcast
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gestione dei nodi						
Gestione del cluster						
Dati 1						
Dati 2						
Dati 3						
Dati 4						
SAN						
Porta intercluster						

2. Annotare nella tabella tutte le informazioni relative al cablaggio per il nodo 3, le porte, i domini di trasmissione e gli IPspaces.
3. Per verificare se il setup è un cluster senza switch a due nodi, procedere come segue:

   a. Impostare il livello di privilegio su Advanced (avanzato):

      ```
      cluster::> set -privilege advanced
      ```

   b. Verificare se il setup è un cluster senza switch a due nodi:

```
cluster::> network options switchless-cluster show
```

```
cluster::*> network options switchless-cluster show

Enable Switchless Cluster: false/true
```

+
Il valore dell'output di questo comando deve corrispondere allo stato fisico del sistema.

a. Tornare al livello di privilegi di amministrazione:

```
cluster::*> set -privilege admin

cluster::>
```

4. Seguire questi passaggi per inserire il node3 nel quorum:

a. Punto di avvio3. Vedere "Installazione e boot node3" per avviare il nodo, se non è già stato fatto.

b. Verificare che le nuove porte del cluster si trovino nel dominio di trasmissione del cluster:

`network port show -node` *`node`* `-port` *`port`* `-fields broadcast-domain`

L'esempio seguente mostra che la porta "e0a" si trova nel dominio del cluster sul nodo 3:

```
 cluster::> network port show -node _node3_ -port e0a -fields
broadcast-domain

 node       port broadcast-domain
 ---------- ---- ----------------
 node3      e0a  Cluster
```

c. Se le porte del cluster non si trovano nel dominio di broadcast del cluster, aggiungerle con il seguente comando:

`broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports` *`node:port`*

Questo esempio aggiunge la porta cluster "e1b" al nodo 3:

```
network port modify -node node3 -port e1b -ipspace Cluster -mtu 9000
```

d. Aggiungere le porte corrette al dominio di trasmissione del cluster:

`network port modify -node -port -ipspace Cluster -mtu 9000`

Questo esempio aggiunge la porta cluster "e1b" al nodo 4:

```
network port modify -node node4 -port e1b -ipspace Cluster -mtu 9000
```

e. Migrare le LIF del cluster alle nuove porte, una volta per ogni LIF:

```
network interface migrate -vserver Cluster -lif lif_name -source-node node3
-destination-node node3 -destination-port port_name
```

f. Modificare la porta home delle LIF del cluster:

```
network interface modify -vserver Cluster -lif lif_name –home-port port_name
```

g. Rimuovere le vecchie porte dal dominio di trasmissione del cluster:

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

Il seguente comando rimuove la porta "e0d" sul nodo 3:

```
network port broadcast-domain remove-ports -ipspace Cluster -broadcast-domain
Cluster -ports node3:e0d
```

a. Verificare che node3 si sia riUnito al quorum:

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

5. regola i domini di broadcast che ospitano le LIF del cluster e le LIF di gestione dei nodi/gestione dei cluster. Verificare che ciascun dominio di trasmissione contenga le porte corrette. Una porta non può essere spostata tra domini di broadcast se è in hosting o è la sede di una LIF, quindi potrebbe essere necessario migrare e modificare le LIF come segue:

a. Visualizzare la porta home di una LIF:

```
network interface show -fields home-node,home-port
```

b. Visualizza il dominio di trasmissione contenente questa porta:

```
network port broadcast-domain show -ports node_name:port_name
```

c. Aggiungere o rimuovere le porte dai domini di broadcast:

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

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

a. Modificare la porta home di una LIF:

```
network interface modify -vserver vserver -lif lif_name –home-port port_name
```

6. Regolare l'appartenenza al dominio di broadcast delle porte di rete utilizzate per le LIF di intercluster utilizzando gli stessi comandi illustrati nella Fase 5.
7. Regolare gli altri domini di broadcast e migrare i file LIF dei dati, se necessario, utilizzando gli stessi

comandi illustrati nella Fase 5.

8. Se sul nodo 1 sono presenti porte che non esistono più sul nodo 3, attenersi alla seguente procedura per eliminarle:

   a. Accedere al livello di privilegio avanzato su uno dei nodi:

      ```
      set -privilege advanced
      ```

   b. Per eliminare le porte:

      ```
      network port delete -node node_name -port port_name
      ```

   c. Tornare al livello di amministrazione:

      ```
      set -privilege admin
      ```

9. Regolare tutti i gruppi di failover LIF:

   ```
   network interface modify -failover-group failover_group -failover-policy
   failover_policy
   ```

   Il seguente comando imposta il criterio di failover su `broadcast-domain-wide` E utilizza le porte del gruppo di failover "fg1" come destinazioni di failover per LIF "data1" sul node3:

   ```
   network interface modify -vserver node3 -lif data1 failover-policy broadcast-
   domainwide -failover-group fg1
   ```

   Fare riferimento a. "Riferimenti" Per ulteriori informazioni, fare riferimento a *Gestione di rete* o ai comandi di *ONTAP 9: Manuale di riferimento pagina*.

10. Verificare le modifiche al nodo 3:

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

11. Ogni LIF del cluster deve essere in ascolto sulla porta 7700. Verificare che le LIF del cluster siano in ascolto sulla porta 7700:

    ```
    ::> network connections listening show -vserver Cluster
    ```

    La porta 7700 in ascolto sulle porte del cluster è il risultato previsto, come mostrato nell'esempio seguente per un cluster a due nodi:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

12. Per ogni cluster LIF che non è in ascolto sulla porta 7700, imposta lo stato amministrativo della LIF su `down` e poi `up`:

    ```
    ::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
    int modify -vserver Cluster -lif cluster-lif -status-admin up
    ```

    Ripetere il passaggio 11 per verificare che la LIF del cluster sia in ascolto sulla porta 7700.

Unirsi al quorum quando un nodo dispone di un set diverso di porte di rete

Il nodo con il nuovo controller si avvia e tenta di connettersi automaticamente al cluster; tuttavia, se il nuovo nodo dispone di un set diverso di porte di rete, è necessario eseguire i seguenti passaggi per confermare che il nodo si connette correttamente al quorum.

A proposito di questa attività

È possibile utilizzare queste istruzioni per qualsiasi nodo pertinente. Node3 viene utilizzato per l'intero campione seguente.

Fasi

1. Verificare che le nuove porte del cluster si trovino nel dominio di trasmissione del cluster immettendo il seguente comando e verificandone l'output:

   ```
   network port show -node node -port port -fields broadcast-domain
   ```

   L'esempio seguente mostra che la porta "e1a" si trova nel dominio del cluster sul nodo 3:

   ```
   cluster::> network port show -node node3 -port e1a -fields broadcast-
   domain
   node   port broadcast-domain
   ------ ---- ----------------
   node3  e1a  Cluster
   ```

2. Aggiungere le porte corrette al dominio di trasmissione del cluster immettendo il seguente comando e controllandone l'output:

   ```
   network port modify -node -port -ipspace Cluster -mtu 9000
   ```

Questo esempio aggiunge la porta cluster "e1b" al nodo 3:

```
network port modify -node node3 -port e1b -ipspace Cluster -mtu 9000
```

3. Migrare le LIF del cluster alle nuove porte, una volta per ciascuna LIF, utilizzando il seguente comando:

   `network interface migrate -vserver Cluster -lif lif_name -source-node node3 -destination-node node3 -destination-port port_name`

4. Modificare la porta home delle LIF del cluster:

   `network interface modify -vserver Cluster -lif lif_name –home-port port_name`

5. Se le porte del cluster non si trovano nel dominio di broadcast del cluster, aggiungerle utilizzando il seguente comando:

   `network port broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster - ports node:port`

6. Rimuovere le vecchie porte dal dominio di trasmissione del cluster. È possibile utilizzare per qualsiasi nodo rilevante. Il seguente comando rimuove la porta "e0d" sul nodo 3:

   `network port broadcast-domain remove-ports network port broadcast-domain remove-ports ipspace Cluster -broadcast-domain Cluster -ports node3:e0d`

7. Verificare che il nodo abbia raggiunto nuovamente il quorum:

   `cluster show -node node3 -fields health`

8. Regolare i domini di broadcast che ospitano le LIF del cluster e le LIF di gestione dei nodi/cluster. Verificare che ciascun dominio di trasmissione contenga le porte corrette. Una porta non può essere spostata tra domini di broadcast se è in hosting o è la sede di una LIF, quindi potrebbe essere necessario migrare e modificare le LIF come segue:
   a. Visualizzare la porta home di una LIF:

      `network interface show -fields home-node,home-port`

   b. Visualizza il dominio di trasmissione contenente questa porta:

      `network port broadcast-domain show -ports node_name:port_name`

   c. Aggiungere o rimuovere le porte dai domini di broadcast:
      `network port broadcast-domain add-ports network port broadcast-domain remove-port`

   d. Modificare una porta home di una LIF:
      `network interface modify -vserver vserver -lif lif_name –home-port port_name`
      Regolare i domini di broadcast dell'intercluster e migrare le LIF dell'intercluster, se necessario. Le LIF dei dati rimangono invariate.

Verificare l'installazione di node3

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 proposito di questa attività

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
   ```

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

   ```
   cluster show
   ```

3. Controllare lo stato dell'operazione e verificare che le informazioni di configurazione per node3 siano le stesse di node1:

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

   Se la configurazione è diversa per node3, potrebbe verificarsi un'interruzione del sistema in seguito alla procedura.

4. Verificare che il controller sostituito sia configurato correttamente per la configurazione MetroCluster, che la configurazione MetroCluster sia in buono stato e non in modalità di commutazione. Fare riferimento a. "Verificare lo stato della configurazione MetroCluster".

Ricreare VLAN, gruppi di interfacce e domini di broadcast sul nodo 3

Dopo aver confermato che node3 è in quorum e può comunicare con node2, è necessario ricreare le VLAN, i gruppi di interfacce e i domini di broadcast di node1 sul node3. È inoltre necessario aggiungere le porte node3 ai domini di trasmissione appena ricreati.

A proposito di questa attività

Per ulteriori informazioni sulla creazione e la ricreazione di VLAN, gruppi di interfacce e domini di trasmissione, visitare il sito Web all'indirizzo "Riferimenti" E link a *Network Management*.

Fasi

1. Ricreare le VLAN sul nodo 3 utilizzando le informazioni sul nodo 1 registrate in "Spostare gli aggregati non root e le LIF dei dati NAS di proprietà del node1 al node2" sezione:

   ```
   network port vlan create -node node_name -vlan vlan-names
   ```

2. Ricreare i gruppi di interfacce sul nodo 3 utilizzando le informazioni sul nodo 1 registrate nel "Spostare gli aggregati non root e le LIF dei dati NAS di proprietà del node1 al node2" sezione:

   ```
   network port ifgrp create -node node_name -ifgrp port_ifgrp_names-distr-func
   ```

3. Ricreare i domini di trasmissione sul nodo 3 utilizzando le informazioni sul nodo 1 registrate nel "Spostare gli aggregati non root e le LIF dei dati NAS di proprietà del node1 al node2" sezione:

```
network port broadcast-domain create -ipspace Default -broadcast-domain
broadcast_domain_names -mtu mtu_size -ports
node_name:port_name,node_name:port_name
```

4. Aggiungere le 3 porte node3 ai domini di trasmissione appena ricreati:

```
network port broadcast-domain add-ports -broadcast-domain
broadcast_domain_names -ports node_name:port_name,node_name:port_name
```

Ripristinare la configurazione del gestore delle chiavi sul node3

Se si utilizza NetApp aggregate Encryption (NAE) o NetApp Volume Encryption (NVE) per crittografare i volumi sul sistema che si sta aggiornando, la configurazione della crittografia deve essere sincronizzata con i nuovi nodi. Se non si ripristina il gestore delle chiavi, quando si trasferiranno gli aggregati node1 da node2 a node3 utilizzando ARL, i volumi crittografati verranno portati offline.

Fasi

1. Per sincronizzare la configurazione della crittografia per Onboard Key Manager, eseguire il seguente comando al prompt del cluster:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 o 9.7	`security key-manager onboard sync`
ONTAP 9.5	`security key-manager setup -node node_name`

2. Immettere la passphrase a livello di cluster per Onboard Key Manager.

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

Dopo aver verificato l'installazione di node3 e prima di spostare gli aggregati da node2 a node3, è necessario spostare i dati NAS LIF appartenenti a node1 che sono attualmente su node2 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. 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.

2. Verificare manualmente che la rete e tutte le VLAN, i gruppi di interfacce e i domini di trasmissione siano stati configurati correttamente.
3. Riprendere l'operazione di trasferimento:

   ```
   system controller replace resume
   ```

   ```
   To complete the "Network Reachability" phase, ONTAP network
   configuration must
   be manually adjusted to match the new physical network configuration of
   the
   hardware. This includes assigning network ports to the correct broadcast
   domains, creating any required ifgrps and VLANs, and modifying the home-
   port
   parameter of network interfaces to the appropriate ports. Refer to the
   "Using
   aggregate relocation to upgrade controller hardware on a pair of nodes
   running
   ONTAP 9.x" documentation, Stages 3 and 5. Have all of these steps been
   manually
   completed? [y/n]
   ```

4. Invio `y` per continuare.
5. 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. Il sistema viene messo in pausa una volta completata la riallocazione delle risorse.

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

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

7. Verificare che gli aggregati non root e le LIF dei dati NAS siano stati ricollocati correttamente in node3.

   Se un aggregato non riesce a riallocare o viene vetoed, è necessario spostare manualmente gli aggregati o eseguire l'override dei veti o dei controlli di destinazione, se necessario. Vedere "Spostare gli aggregati non riusciti o vetoed" per ulteriori informazioni.

8. Verificare che le LIF SAN si trovino sulle porte corrette sul nodo 3 completando i seguenti passaggi secondari:

a. Immettere il seguente comando ed esaminarne l'output:

`network interface show -data-protocol iscsi|fcp -home-node node3`

Il sistema restituisce un output simile al seguente esempio:

```
cluster::> net int show -data-protocol iscsi|fcp -home-node node3

        Logical   Status     Network           Current  Current Is
Vserver Interface Admin/Oper Address/Mask      Node     Port    Home
------- --------- ---------- ----------------- -------- ------- ----
vs0
        a0a       up/down     10.63.0.53/24     node3   a0a     true
        data1     up/up       10.63.0.50/18     node3   e0c     true
        rads1     up/up       10.63.0.51/18     node3   e1a     true
        rads2     up/down     10.63.0.52/24     node3   e1b     true
vs1
        lif1      up/up       172.17.176.120/24 node3   e0c     true
        lif2      up/up       172.17.176.121/24 node3   e1a     true
```

b. Se node3 ha LIF SAN o gruppi DI LIF SAN che si trovano su una porta che non esisteva sul node1 o che devono essere mappati su una porta diversa, spostarli su una porta appropriata sul node3 completando i seguenti passaggi secondari:

i. Impostare lo stato LIF su DOWN (giù):

`network interface modify -vserver Vserver_name -lif LIF_name -status -admin down`

ii. Rimuovere la LIF dal set di porte:

`portset remove -vserver Vserver_name -portset portset_name -port-name port_name`

iii. Immettere uno dei seguenti comandi:

- Spostare una singola LIF:

  `network interface modify -vserver Vserver_name -lif LIF_name -home -port new_home_port`

- Spostare tutte le LIF su una singola porta inesistente o errata su una nuova porta:

  `network interface modify {-home-port port_on_node1 -home-node node1 -role data} -home-port new_home_port_on_node3`

- Aggiungere nuovamente i file LIF al set di porte:

  `portset add -vserver Vserver_name -portset portset_name -port-name port_name`

Devi confermare che hai spostato I file LIF SAN su una porta con la stessa velocità di collegamento della porta originale.

a. Modificare lo stato di tutte le LIF su "up" in modo che le LIF possano accettare e inviare traffico sul nodo:

   `network interface modify -home-port port_name -home-node node3 -lif data -status admin up`

b. Immettere il seguente comando su uno dei nodi ed esaminare l'output per verificare che le LIF siano state spostate nelle porte corrette e che le LIF abbiano lo stato di `up`:

   `network interface show -home-node node3 -role data`

c. 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 -status-admin up`

9. 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

Fase 4. Spostare e dismettere il 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 <aggregate_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 LIF di dati rimasti sul node2 immettendo il seguente comando ed esaminando l'output:

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

6. Se sono stati configurati gruppi di interfacce o VLAN, completare i seguenti passaggi secondari:

   a. Registrare le informazioni sulla VLAN e sul gruppo di interfacce in modo da poter ricreare le VLAN e i gruppi di interfacce sul nodo 3 dopo l'avvio del nodo 3.

   b. Rimuovere le VLAN dai gruppi di interfacce:

   ```
   network port vlan delete -node nodename -port ifgrp -vlan-id VLAN_ID
   ```

   c. Verificare se sono presenti gruppi di interfacce configurati sul nodo immettendo il seguente comando ed esaminandone l'output:

   ```
   network port ifgrp show -node node2 -ifgrp ifgrp_name -instance
   ```

   Il sistema visualizza le informazioni sul gruppo di interfacce per il nodo, come illustrato nell'esempio seguente:

```
cluster::> network port ifgrp show -node node2 -ifgrp a0a -instance
                  Node: node3
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode_lacp
          MAC Address: 02:a0:98:17:dc:d4
   Port Participation: partial
        Network Ports: e2c, e2d
             Up Ports: e2c
           Down Ports: e2d
```

   a. Se nel nodo sono configurati gruppi di interfacce, registrare i nomi di tali gruppi e le porte ad essi assegnate, quindi eliminare le porte immettendo il seguente comando, una volta per ciascuna porta:

   ```
   network port ifgrp remove-port -node nodename -ifgrp ifgrp_name -port
   netport
   ```

Andare in pensione node2

Per dismettere node2, è necessario arrestare node2 correttamente e quindi 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

Installazione e boot node4

È necessario installare node4 nel rack, trasferire le connessioni node2 a node4, fare il boot node4 e installare ONTAP. Quindi, è necessario riassegnare i dischi spare sul nodo 2, i dischi appartenenti al volume root e gli aggregati non root che non sono stati riallocati nel nodo 3 precedentemente durante il 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. Inoltre, è necessario verificare che le LIF dei dati NAS siano state spostate correttamente in node4.

È necessario eseguire l'avvio di rete del nodo 4 se la versione ONTAP sul nodo 4 è diversa dalla versione ONTAP sul nodo 2. Dopo aver installato node4, avviarlo dall'immagine ONTAP 9 memorizzata sul server web. È quindi possibile scaricare i file corretti sul dispositivo di supporto di avvio per i successivi avvii del sistema seguendo le istruzioni in "Preparatevi per il netboot".

- Per un aggiornamento del controller AFF A800 o AFF C800 , è necessario assicurarsi che tutte le unità nello chassis siano saldamente posizionate contro il midplane prima di rimuovere node2. Per maggiori informazioni, vedere "Sostituire i moduli controller AFF A800 o AFF C800".
- Se si sta aggiornando un sistema con dischi di archiviazione, è necessario completare l'intera sezione e quindi procedere a "Impostare la configurazione FC o UTA/UTA2 su node4" , immettendo comandi al prompt del cluster.

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.

   Cablare le seguenti connessioni, utilizzando le *Istruzioni di installazione e configurazione* per la piattaforma node4, il documento appropriato sullo scaffale dei dischi e la documentazione sulla *gestione delle coppie HA*.

   Fare riferimento a"Riferimenti" per collegarsi alla *gestione delle coppie HA*.

- Console (porta di gestione remota)
- Porte del cluster
- Porte dati
- Porte di gestione di cluster e nodi
- Storage
- Configurazioni SAN: Porte switch FC e Ethernet iSCSI

> Potrebbe non essere necessario spostare la connessione scheda di interconnessione/scheda FC-VI o cavo di interconnessione/FC-VI dal nodo 2 al nodo 4, poiché la maggior parte dei modelli di piattaforma dispone di modelli di schede di interconnessione univoci. Per la configurazione MetroCluster, è necessario spostare le connessioni del cavo FC-VI dal nodo 2 al nodo 4. Se il nuovo host non dispone di una scheda FC-VI, potrebbe essere necessario spostare la scheda FC-VI.

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 avvio.

> 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.

> **Non ignorare il ritardo; se non si lascia caricare la batteria, si potrebbe verificare una 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 immettendo 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 (Domain Name Service). Se si utilizza questo parametro opzionale, non è necessario un nome di dominio completo nell'URL del server netboot; è necessario solo il nome host del server. NOTA: Per l'interfaccia potrebbero essere necessari altri parametri. Invio `help ifconfig` al prompt del firmware per ulteriori informazioni.

7. Eseguire il netboot al nodo 4:

Per…	Quindi…
Sistemi della serie FAS/AFF8000	`netboot http://<web_server_ip/path_to_web-accessible_directory>/netboot/kernel`
Tutti gli altri sistemi	`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
```

Se si dispone di una configurazione MetroCluster, utilizzare i seguenti comandi per modificare il controller e lo chassis:

```
ha-config modify controller mcc
```

```
ha-config modify chassis mcc
```

14. Uscire dalla modalità di manutenzione:

```
halt
```

Interrompere L'OPERAZIONE premendo Ctrl-C al prompt dell'ambiente di avvio.

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

```
date
```

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

```
show date
```

17. Se necessario, impostare la data sul node4:

```
set date mm/dd/yyyy
```

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

```
show time
```

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

```
set time hh:mm:ss
```

20. 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
```

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

```
printenv partner-sysid
```

22. Se sono installate unità NetApp Storage Encryption (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`**

Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha. È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

b. Contattare il supporto NetApp per assistenza nel ripristino delle informazioni di gestione delle chiavi integrate.

23. Avviare il nodo nel menu di avvio:

```
boot_ontap menu
```

Quali sono le prossime novità?

- Se si dispone di un sistema con una configurazione FC o UTA/UTA2,"imposta la configurazione FC o UTA/UTA2 sul nodo 4" .
- Se non si dispone di una configurazione FC o UTA/UTA2,"riassegnare i dischi del nodo 2 al nodo 4, passaggio 1" in modo che node4 possa riconoscere i dischi di node2.
- Se si dispone di una configurazione MetroCluster ,"imposta la configurazione FC o UTA/UTA2 sul nodo 4" per rilevare i dischi collegati al nodo.

Impostare la configurazione FC o UTA/UTA2 su node4

Se node4 dispone di porte FC integrate, porte UTA/UTA2 (onboard Unified target adapter) o una scheda UTA/UTA2, è necessario configurare le impostazioni prima di completare il resto della procedura.

A proposito di questa attività

Potrebbe essere necessario completareConfigurare le porte FC sul nodo 4 OControllare e configurare le porte UTA/UTA2 sul nodo 4 o entrambe le sezioni.

Se node4 non dispone di porte FC integrate, porte UTA/UTA2 integrate o una scheda UTA/UTA2 e si sta aggiornando un sistema con dischi di archiviazione, è possibile passare alla sezione "Riassegnare dischi da node2 TB a node4 TB".

Assicurarsi che il 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.

Configurare le porte FC sul nodo 4

Se il nodo 4 dispone di porte FC, integrate o su un adattatore FC aggiuntivo, è necessario impostare le configurazioni delle porte sul nodo prima di metterlo in servizio, poiché le porte non sono preconfigurate al momento della spedizione dei sistemi. Se non si configurano le porte come richiesto, si potrebbe verificare un'interruzione del servizio.

Prima di iniziare

È necessario disporre dei valori delle impostazioni della porta FC del nodo 2 salvati nella sezione "Preparare i nodi per l'aggiornamento".

A proposito di questa attività

È possibile saltare questa sezione se il sistema non dispone di configurazioni FC. Se il sistema dispone di porte UTA/UTA2 integrate o di un adattatore UTA/UTA2, configurarle in Controllare e configurare le porte UTA/UTA2 sul nodo 4.

Immettere i comandi in questa sezione al prompt della shell in modalità Manutenzione.

Fasi

1. Visualizza informazioni su tutti gli adattatori di rete FC e convergenti sul sistema:

   ```
   system node hardware unified-connect show
   ```

2. Confrontare le impostazioni FC sul nodo 4 con quelle acquisite in precedenza dal nodo 1.
3. Modificare le porte FC sul nodo 4 in base alle necessità:
   - Per programmare come porte di destinazione:

     ```
     ucadmin modify -m fc -t target adapter
     ```

     Per esempio: `ucadmin modify -m fc -t target 2a`
   - Per programmare le porte initiator:

     ```
     ucadmin modify -m fc -t initiator adapter
     ```

     `-t` È il tipo FC4: Destinazione o iniziatore.

   Per esempio: `ucadmin modify -m fc -t initator 2b`
4. Arrestare il nodo:

   ```
   halt
   ```

5. Avviare il sistema dal prompt del CARICATORE:

   ```
   boot_ontap menu
   ```

6. Dopo aver immesso il comando, attendere che il sistema si arresti al prompt dell'ambiente di avvio.
7. Selezionare l'opzione `5` dal menu di avvio per la modalità di manutenzione.
8. eseguire una delle seguenti operazioni:

- Passare a. Controllare e configurare le porte UTA/UTA2 sul nodo 4 Se node4 ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate.
- Se node4 non ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate, saltare *Controllare e configurare le porte UTA/UTA2 su node4* e andare a"Riassegnare dischi da node2 TB a node4 TB" .

Controllare e configurare le porte UTA/UTA2 sul nodo 4

Se node4 dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2A, è necessario controllare la configurazione delle porte e configurarle, a seconda di come si desidera utilizzare il sistema aggiornato.

Prima di iniziare

È necessario disporre dei moduli SFP+ corretti per le porte UTA/UTA2.

A proposito di questa attività

Le porte UTA/UTA2 possono essere configurate in modalità FC nativa o UTA/UTA2A. La modalità FC supporta l'iniziatore FC e la destinazione FC; la modalità UTA/UTA2 consente al traffico simultaneo di NIC e FCoE di condividere la stessa interfaccia SFP+ 10 GbE e supporta la destinazione FC.

> I materiali di marketing NetApp potrebbero utilizzare il termine UTA2 per fare riferimento agli adattatori e alle porte CNA. Tuttavia, la CLI utilizza il termine CNA.

Le porte UTA/UTA2 potrebbero essere su un adattatore o sul controller con le seguenti configurazioni:

- Le schede UTA/UTA2 ordinate contemporaneamente al controller vengono configurate prima della spedizione in modo da avere la personalità richiesta.
- Le schede UTA/UTA2 ordinate separatamente dal controller vengono fornite con il linguaggio di destinazione FC predefinito.
- Le porte UTA/UTA2 integrate sui nuovi controller sono configurate (prima della spedizione) in modo da avere la personalità richiesta.

Tuttavia, è necessario controllare la configurazione delle porte UTA/UTA2 sul nodo 4 e modificarla, se necessario.

> Immettere i comandi in questa sezione al prompt della shell in modalità Manutenzione.

Fasi

1. Controlla come sono attualmente configurate le porte sul nodo 4:

   ```
   system node hardware unified-connect show
   ```

   Il sistema visualizza un output simile al seguente esempio:

```
*> ucadmin show
                Current  Current    Pending   Pending   Admin
Node   Adapter  Mode     Type       Mode      Type      Status
----   -------  ---      ---------  -------   --------  -------
f-a    0e       fc       initiator  -          -        online
f-a    0f       fc       initiator  -          -        online
f-a    0g       cna      target     -          -        online
f-a    0h       cna      target     -          -        online
f-a    0e       fc       initiator  -          -        online
f-a    0f       fc       initiator  -          -        online
f-a    0g       cna      target     -          -        online
f-a    0h       cna      target     -          -        online
*>
```

2. Se il modulo SFP+ corrente non corrisponde all'utilizzo desiderato, sostituirlo con il modulo SFP+ corretto.

   Contattare il rappresentante NetApp per ottenere il modulo SFP+ corretto.

3. Verificare le impostazioni:

   `ucadmin show`

   Esaminare l'output di `ucadmin show` Controllare e determinare se le porte UTA/UTA2 hanno la personalità desiderata.

   L'output degli esempi seguenti mostra che il tipo di adattatore FC4 "1b" sta cambiando in `initiator` e che la modalità degli adattatori "2a" e "2b" stia cambiando in `cna`:

```
*> ucadmin show
Node  Adapter  Current Mode  Current Type  Pending Mode  Pending Type
Admin Status
----  -------  ------------  ------------  ------------  ------------
------------
f-a   1a       fc             initiator    -             -
online
f-a   1b       fc             target       -             initiator
online
f-a   2a       fc             target       cna           -
online
f-a   2b       fc             target       cna           -
online
4 entries were displayed.
*>
```

4. Eseguire una delle seguenti operazioni:

Se la porta CNA…	Quindi…
Non avere la personalità che si desidera	Passare a. Fase 5.
Avere la personalità che si desidera	Salta il passaggio 5 al passaggio 9 e vai aFase 10 .

5. eseguire una delle seguenti operazioni:

Se si sta configurando…	Quindi…
Porte su una scheda UTA/UTA2	Vai aFase 6
Porte UTA/UTA2 integrate	Salta il passaggio 6 e vai aFase 7 .

6. Se l'adattatore è in modalità iniziatore e la porta UTA/UTA2 è online, metti offline la porta UTA/UTA2:

   `storage disable adapter adapter_name`

   Gli adattatori in modalità di destinazione sono automaticamente offline in modalità di manutenzione.

7. se la configurazione corrente non corrisponde all'utilizzo desiderato, modificare la configurazione in base alle necessità:

   `ucadmin modify -m fc|cna -t initiator|target <adapter_name>`

   - `-m` È la modalità Personality, FC o 10GbE UTA.
   - `-t` È di tipo FC4, `target` oppure `initiator`.

   > È necessario utilizzare l'iniziatore FC per le unità nastro e le configurazioni MetroCluster . Per i client SAN è necessario utilizzare la destinazione FC.

8. Mettere online tutte le porte di destinazione immettendo il seguente comando, una volta per ogni porta:

   `storage enable adapter <adapter_name>`

9. Collegare la porta.
10. Esci dalla modalità di manutenzione:

    `halt`

11. Avviare il nodo nel menu di avvio:

    `boot_ontap menu`

Quali sono le prossime novità?

- Se si sta eseguendo l'aggiornamento a un sistema AFF A800, visitare il sito "Riassegnare node2 dischi a node4, passaggio 9".
- Per tutti gli altri aggiornamenti di sistema, vai a"Riassegnare node2 dischi a node4, passaggio 1" .

Riassegnare dischi da node2 TB a node4 TB

È necessario riassegnare i dischi che appartenevano a node2 a node4 prima di verificare l'installazione di node4.

Fasi

1. Verificare che node2 si sia fermato al menu di avvio e riassegnare i dischi di node2 a node4:

   ```
   boot_after_controller_replacement
   ```

   Dopo un breve intervallo di tempo, viene richiesto di inserire il nome del nodo da sostituire. Se sono presenti dischi condivisi (chiamati anche Advanced Disk Partitioning (ADP) o dischi partizionati), viene richiesto di inserire il nome del nodo del partner ha.

   Questi prompt potrebbero essere interrati nei messaggi della console. Se non si immette un nome di nodo o non si immette un nome corretto, viene richiesto di inserire nuovamente il nome.

Espandere l'esempio di output della console

```
LOADER-A> boot_ontap menu ...
******************************
*                            *
* Press Ctrl-C for Boot 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.
Selection (1-9)? 22/7
.
.
(boot_after_controller_replacement) Boot after controller upgrade
(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.

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.
Selection (1-9)? 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
.
.
Controller Replacement: Provide name of the node you would like to
replace: <name of the node being replaced>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner of the node being replaced>
Changing sysid of node <node being replaced> disks.
Fetched sanown old_owner_sysid = 536953334 and calculated old sys id
= 536953334
Partner sysid = 4294967295, owner sysid = 536953334
.
.
.
Terminated
<node reboots>
.
.
System rebooting...
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
.
.
System rebooting...
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
Login: ...
```

2. Se il sistema entra in un ciclo di riavvio con il messaggio `no disks found`, questo perché ha reimpostato le porte sulla modalità di destinazione e quindi non è in grado di vedere alcun disco. EseguireFase 3 AttraversoFase 8 su node4 per risolvere questo problema.
3. premere Ctrl-C durante L'OPERAZIONE per arrestare il nodo al prompt Loader>.
4. Al prompt del CARICATORE, accedere alla modalità di manutenzione:

   ```
   boot_ontap maint
   ```

5. In modalità di manutenzione, visualizzare tutte le porte iniziatore precedentemente impostate che si trovano ora in modalità di destinazione:

```
ucadmin show
```

Riportare le porte in modalità initiator:

```
ucadmin modify -m fc -t initiator -f adapter name
```

6. Verificare che le porte siano state modificate in modalità initiator:

```
ucadmin show
```

7. Uscire dalla modalità di manutenzione:

```
halt
```

> Se si esegue l'aggiornamento da un sistema che supporta dischi esterni a un sistema che supporta anche dischi esterni, visitare il sito Fase 8.
>
> Se si esegue l'aggiornamento da un sistema che utilizza dischi esterni a un sistema che supporta dischi interni ed esterni, ad esempio un sistema AFF A800, visitare il sito Fase 9.

8. 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:

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
```

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

b. Invio `y` al seguente prompt:

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

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

d. 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.

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

> In questa fase potresti riscontrare un errore. Se si verifica un errore, ripetere i sottopassaggi inFase 8 finché il sistema non si avvia normalmente.

9. Se si esegue l'aggiornamento da un sistema con dischi esterni a un sistema che supporta dischi interni ed esterni (ad esempio, sistemi AFF A800), impostare l'aggregato node2 come aggregato radice per confermare che node4 si avvii dall'aggregato radice di node2. Per impostare l'aggregato radice, vai al menu di avvio su node4 e seleziona l'opzione `5` per entrare in modalità manutenzione.

> **È necessario eseguire i seguenti passaggi secondari nell'ordine esatto indicato; in caso contrario, si potrebbe verificare un'interruzione o addirittura la perdita di dati.**

La seguente procedura imposta node4 per l'avvio dall'aggregato root di node2:

a. Accedere alla modalità di manutenzione:

```
boot_ontap maint
```

b. Controllare le informazioni su RAID, plex e checksum per l'aggregato node2:

```
aggr status -r
```

c. Controllare lo stato dell'aggregato node2:

```
aggr status
```

d. Se necessario, portare online l'aggregato node2:

```
aggr_online root_aggr_from_node2
```

e. Impedire al node4 di avviarsi dal proprio aggregato root originale:

```
aggr offline root_aggr_on_node4
```

f. Impostare l'aggregato root node2 come nuovo aggregato root per node4:

```
aggr options aggr_from_node2 root
```

Mappare le porte dal nodo 2 al nodo 4

È necessario verificare che le porte fisiche sul nodo 2 siano mappate correttamente alle porte fisiche sul nodo 4, consentendo al nodo 4 di 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.

La configurazione software del nodo 4 deve corrispondere alla connettività fisica del nodo 4 e la connettività IP deve essere ripristinata prima di continuare con l'aggiornamento.

Le impostazioni delle porte possono variare a seconda del modello dei nodi. È necessario rendere la porta e la configurazione LIF del nodo originale compatibili con la configurazione del nuovo nodo. Questo perché il nuovo nodo riproduce la stessa configurazione all'avvio, il che significa che quando si avvia node4 Data ONTAP tenterà di ospitare le LIF sulle stesse porte utilizzate sul node2.

Pertanto, se le porte fisiche sul nodo 2 non vengono mappate direttamente alle porte fisiche sul nodo 4, saranno necessarie modifiche alla configurazione del software per ripristinare la connettività di cluster, gestione e rete dopo l'avvio. Inoltre, se le porte del cluster sul nodo 2 non vengono mappate direttamente alle porte del cluster sul nodo 4, il nodo 4 potrebbe non ricongiungersi automaticamente al quorum quando viene riavviato fino a quando non viene apportata una modifica alla configurazione software per ospitare le LIF del cluster sulle porte fisiche corrette.

Fasi

1. Annotare nella tabella tutte le informazioni di cablaggio node2 per il nodo 2, le porte, i domini di trasmissione e gli spazi IP,

LIF	Node2 porte	Node2 IPspaces	Node2 domini di trasmissione	Node4 porte	Node4 IPspaces	Node4 domini di trasmissione
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gestione dei nodi						
Gestione del cluster						
Dati 1						
Dati 2						
Dati 3						
Dati 4						
SAN						

LIF	Node2 porte	Node2 IPspaces	Node2 domini di trasmissione	Node4 porte	Node4 IPspaces	Node4 domini di trasmissione
Porta intercluster						

2. Annotare nella tabella tutte le informazioni di cablaggio per il nodo 4, le porte, i domini di trasmissione e gli IPspaces.
3. Per verificare se il setup è un cluster senza switch a due nodi, procedere come segue:
   a. Impostare il livello di privilegio su Advanced (avanzato):

      ```
      cluster::> set -privilege advanced
      ```

   b. Verificare se il setup è un cluster senza switch a due nodi:

      ```
      cluster::> network options switchless-cluster show
      ```

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

+
Il valore di questo comando deve corrispondere allo stato fisico del sistema.

   a. Tornare al livello di privilegi di amministrazione:

```
cluster::*> set -privilege admin
cluster::>
```

4. Seguire questi passaggi per inserire il node4 nel quorum:
   a. Punto di avvio4. Vedere "Installazione e boot node4" per avviare il nodo, se non è già stato fatto.
   b. Verificare che le nuove porte del cluster si trovino nel dominio di trasmissione del cluster:

      ```
      network port show -node node -port port -fields broadcast-domain
      ```

      L'esempio seguente mostra che la porta "e0a" si trova nel dominio del cluster sul nodo 4:

```
cluster::> network port show -node node4 -port e0a -fields broadcast-
domain
node       port broadcast-domain
---------- ---- ---------------
node4      e0a  Cluster
```

   c. Se le porte del cluster non si trovano nel dominio di broadcast del cluster, aggiungerle con il seguente comando:

```
broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports
node:port
```

d. Aggiungere le porte corrette al dominio di trasmissione del cluster:

```
network port modify -node -port -ipspace Cluster -mtu 9000
```

Questo esempio aggiunge la porta cluster "e1b" al nodo 4:

```
network port modify -node node4 -port e1b -ipspace Cluster -mtu 9000
```

e. Migrare le LIF del cluster alle nuove porte, una volta per ogni LIF:

```
network interface migrate -vserver Cluster -lif lif_name -source-node node4
destination-node node4 -destination-port port_name
```

f. Modificare la porta home delle LIF del cluster:

```
network interface modify -vserver Cluster -lif lif_name –home-port port_name
```

g. Rimuovere le vecchie porte dal dominio di trasmissione del cluster:

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

Questo comando rimuove la porta "e0d" sul nodo 4:

```
network port broadcast-domain remove-ports -ipspace Cluster -broadcast-domain
Cluster -ports node4:e0d
```

a. Verificare che node4 abbia raggiunto nuovamente il quorum:

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

5. regola i domini di broadcast che ospitano le LIF del cluster e le LIF di gestione dei nodi/gestione dei cluster. Verificare che ciascun dominio di trasmissione contenga le porte corrette. Una porta non può essere spostata tra domini di broadcast se è in hosting o è la sede di una LIF, quindi potrebbe essere necessario migrare e modificare le LIF come indicato di seguito:

a. Visualizzare la porta home di una LIF:

```
network interface show -fields home-node,home-port
```

b. Visualizza il dominio di trasmissione contenente questa porta:

```
network port broadcast-domain show -ports node_name:port_name
```

c. Aggiungere o rimuovere le porte dai domini di broadcast:

```
network port broadcast-domain add-ports
network port broadcast-domain remove-ports
```

d. Modificare la porta home di una LIF:

```
network interface modify -vserver vserver -lif lif_name –home-port port_name
```

6. Regolare i domini di broadcast dell'intercluster e migrare le LIF dell'intercluster, se necessario, utilizzando gli stessi comandi illustrati nella Fase 5.
7. Regolare gli altri domini di broadcast e migrare i file LIF dei dati, se necessario, utilizzando gli stessi comandi illustrati nella Fase 5.
8. Se sul nodo 2 sono presenti porte che non esistono più sul nodo 4, attenersi alla seguente procedura per eliminarle:
   a. Accedere al livello di privilegio avanzato su uno dei nodi:

      `set -privilege advanced`

   b. Per eliminare le porte:

      `network port delete -node node_name -port port_name`

   c. Tornare al livello di amministrazione:

      `set -privilege admin`
9. Regolare tutti i gruppi di failover LIF:

   `network interface modify -failover-group failover_group -failover-policy failover_policy`

   Il seguente comando imposta il criterio di failover su `broadcast-domain-wide` e utilizza le porte nel gruppo di failover `fg1` Come destinazioni di failover per LIF `data1` acceso `node4`:

   ```
   network interface modify -vserver node4 -lif data1 failover-policy broadcast-
   domainwide -failover-group fg1
   ```

   Fare riferimento a. "Riferimenti" Per il collegamento a *Gestione della rete* o ai *comandi di ONTAP 9: Guida di riferimento della pagina manuale* e per ulteriori informazioni vedere *Configurazione delle impostazioni di failover su un LIF*.
10. Verificare le modifiche al nodo 4:

    `network port show -node node4`
11. Ogni LIF del cluster deve essere in ascolto sulla porta 7700. Verificare che le LIF del cluster siano in ascolto sulla porta 7700:

    `::> network connections listening show -vserver Cluster`

    La porta 7700 in ascolto sulle porte del cluster è il risultato previsto, come mostrato nell'esempio seguente per un cluster a due nodi:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

12. Per ogni cluster LIF che non è in ascolto sulla porta 7700, imposta lo stato amministrativo della LIF su `down` e poi `up`:

    `::> net int modify -vserver Cluster -lif *cluster-lif* -status-admin down; net int modify -vserver Cluster -lif *cluster-lif* -status-admin up`

    Ripetere il passaggio 11 per verificare che la LIF del cluster sia in ascolto sulla porta 7700.

Unirsi al quorum quando un nodo dispone di un set diverso di porte di rete

Il nodo con il nuovo controller si avvia e tenta di connettersi automaticamente al cluster; tuttavia, se il nuovo nodo dispone di un set diverso di porte di rete, è necessario eseguire i seguenti passaggi per confermare che il nodo si connette correttamente al quorum.

A proposito di questa attività

È possibile utilizzare queste istruzioni per qualsiasi nodo pertinente. Node3 viene utilizzato per l'intero campione seguente.

Fasi

1. Verificare che le nuove porte del cluster si trovino nel dominio di trasmissione del cluster immettendo il seguente comando e controllando l'output:

   `network port show -node node -port port -fields broadcast-domain`

   L'esempio seguente mostra che la porta "e1a" si trova nel dominio del cluster sul nodo 3:

   ```
   cluster::> network port show -node node3 -port e1a -fields broadcast-
   domain
   node    port  broadcast-domain
   ------  ----  ----------------
   node3   e1a   Cluster
   ```

2. Aggiungere le porte corrette al dominio di trasmissione del cluster immettendo il seguente comando e controllando l'output:

   `network port modify -node -port -ipspace Cluster -mtu 9000`

Questo esempio aggiunge la porta cluster "e1b" al nodo 3:

```
network port modify -node node3 -port e1b -ipspace Cluster -mtu 9000
```

3. Migrare le LIF del cluster alle nuove porte, una volta per ciascuna LIF, utilizzando il seguente comando:

   `network interface migrate -vserver Cluster -lif lif_name -source-node node3 destination-node node3 -destination-port port_name`

4. Modificare la porta home delle LIF del cluster come segue:

   `network interface modify -vserver Cluster -lif lif_name –home-port port_name`

5. Se le porte del cluster non si trovano nel dominio di broadcast del cluster, aggiungerle con il seguente comando:

   `network port broadcast-domain add-ports -ipspace Cluster -broadcastdomain Cluster ports node:port`

6. Rimuovere le vecchie porte dal dominio di trasmissione del cluster. È possibile utilizzare per qualsiasi nodo rilevante. Il seguente comando rimuove la porta "e0d" sul nodo 3:

   `network port broadcast-domain remove-ports network port broadcast-domain remove-ports ipspace Cluster -broadcast-domain Cluster -ports node3:e0d`

7. Verificare che il nodo sia stato nuovamente collegato al quorum come segue:

   `cluster show -node node3 -fields health`

8. Regolare i domini di broadcast che ospitano le LIF del cluster e le LIF di gestione dei nodi/cluster. Verificare che ciascun dominio di trasmissione contenga le porte corrette. Una porta non può essere spostata tra domini di broadcast se è in hosting o è la sede di una LIF, quindi potrebbe essere necessario migrare e modificare le LIF come segue:

   a. Visualizzare la porta home di una LIF:

      `network interface show -fields home-node,home-port`

   b. Visualizza il dominio di trasmissione contenente questa porta:

      `network port broadcast-domain show -ports node_name:port_name`

   c. Aggiungere o rimuovere le porte dai domini di broadcast:

      `network port broadcast-domain add-ports network port broadcast-domain remove-port`

   d. Modificare una porta home di una LIF:

      `network interface modify -vserver vserver-name -lif lif_name –home-port port_name`

Regolare i domini di broadcast dell'intercluster e migrare le LIF dell'intercluster, se necessario. Le LIF dei dati rimangono invariate.

Verificare l'installazione di node4

Dopo aver installato e avviato il nodo 4, è necessario verificare che sia installato correttamente, che faccia parte del cluster e che sia in grado di comunicare con il nodo 3.

A proposito di questa attività

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
   ```

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

   ```
   cluster show
   ```

3. Controllare lo stato dell'operazione e verificare che le informazioni di configurazione per node4 siano le stesse di node2:

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

   Se la configurazione è diversa per node4, potrebbe verificarsi un'interruzione del sistema in seguito alla procedura.

4. Verificare che il controller sostituito sia configurato correttamente per la configurazione MetroCluster e non in modalità di switch-over.

   In questa fase la configurazione MetroCluster non sarà in uno stato normale e potrebbero esserci degli errori da risolvere. Vedere"Verificare lo stato della configurazione MetroCluster" .

Ricreare VLAN, gruppi di interfacce e domini di broadcast sul nodo 4

Dopo aver confermato che node4 è in quorum e può comunicare con node3, è necessario ricreare le VLAN, i gruppi di interfacce e i domini di broadcast di node2 sul node4. È inoltre necessario aggiungere le porte node3 ai domini di trasmissione appena ricreati.

A proposito di questa attività

Per ulteriori informazioni sulla creazione e la ricreazione di VLAN, gruppi di interfacce e domini di trasmissione, visitare il sito Web all'indirizzo "Riferimenti" E link a *Network Management*.

Fasi

1. Ricreare le VLAN sul nodo 4 utilizzando le informazioni sul nodo 2 registrate nel "Spostare aggregati non root e LIF dati NAS da node2 a node3" sezione:

   ```
   network port vlan create -node node4 -vlan vlan-names
   ```

2. Ricreare i gruppi di interfacce sul nodo 4 utilizzando le informazioni sul nodo 2 registrate nel "Spostare aggregati non root e LIF dati NAS da node2 a node3" sezione:

   `network port ifgrp create -node node4 -ifgrp port_ifgrp_names-distr-func`

3. Ricreare i domini di trasmissione sul nodo 4 utilizzando le informazioni sul nodo 2 registrate nel "Spostare aggregati non root e LIF dati NAS da node2 a node3" sezione:

   `network port broadcast-domain create -ipspace Default -broadcast-domain broadcast_domain_names -mtu mtu_size -ports node_name:port_name,node_name:port_name`

4. Aggiungere le 4 porte node4 ai domini di trasmissione appena ricreati:

   `network port broadcast-domain add-ports -broadcast-domain broadcast_domain_names -ports node_name:port_name,node_name:port_name`

Ripristinare la configurazione del gestore delle chiavi sul nodo 4

Se si utilizza NetApp aggregate Encryption (NAE) o NetApp Volume Encryption (NVE) per crittografare i volumi sul sistema che si sta aggiornando, la configurazione della crittografia deve essere sincronizzata con i nuovi nodi. Se non si ripristina il gestore delle chiavi, quando si trasferiranno gli aggregati node2 da node3 a node4 utilizzando ARL, i volumi crittografati verranno portati offline.

Fasi

1. Per sincronizzare la configurazione della crittografia per Onboard Key Manager, eseguire il seguente comando al prompt del cluster:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 o 9.7	`security key-manager onboard sync`
ONTAP 9.5	`security key-manager setup -node node_name`

2. Immettere la passphrase a livello di cluster per Onboard Key Manager.

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

Dopo aver verificato l'installazione di node4 e prima di spostare gli aggregati da node3 a node4, è necessario spostare le LIF dei dati NAS appartenenti a node2 che sono attualmente sul node3 da node3 a node4. È inoltre necessario verificare che le LIF SAN esistano sul nodo 4.

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. 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.

2. Verificare manualmente che la rete e tutte le VLAN, i gruppi di interfacce e i domini di trasmissione siano stati configurati correttamente.
3. Riprendere l'operazione di trasferimento:

```
system controller replace resume
```

```
To complete the "Network Reachability" phase, ONTAP network
configuration must be manually adjusted to match the new physical
network configuration of the hardware. This includes assigning network
ports to the correct broadcast domains,creating any required ifgrps and
VLANs, and modifying the home-port parameter of network interfaces to
the appropriate ports.Refer to the "Using aggregate relocation to
upgrade controller hardware on a pair of nodes running ONTAP 9.x"
documentation, Stages 3 and 5. Have all of these steps been manually
completed? [y/n]
```

4. Invio `y` per continuare.
5. 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. Il sistema viene messo in pausa una volta completata la riallocazione delle risorse.

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

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

7. Verificare manualmente che gli aggregati non root e le LIF dei dati NAS siano stati ricollocati correttamente in node4.

Se gli aggregati non riescono a spostare o sono vetoed, è necessario spostare manualmente gli aggregati o eseguire l'override dei veti o dei controlli di destinazione, se necessario. Vedere la sezione "Spostare gli aggregati non riusciti o vetoed" per ulteriori informazioni.

8. Verificare che le LIF SAN si trovino sulle porte corrette sul nodo 4 completando i seguenti passaggi secondari:

   a. Immettere il seguente comando ed esaminarne l'output:

      ```
      network interface show -data-protocol iscsi|fcp -home-node node4
      ```

      Il sistema restituisce un output simile al seguente esempio:

      ```
      cluster::> net int show -data-protocol iscsi|fcp -home-node node3
              Logical    Status     Network            Current Current Is
      Vserver Interface  Admin/Oper Address/Mask       Node    Port    Home
      ------- ---------- ---------- ------------------ ------- ------- ---
      vs0
              a0a        up/down    10.63.0.53/24      node3   a0a     true
              data1      up/up      10.63.0.50/18      node3   e0c     true
              rads1      up/up      10.63.0.51/18      node3   e1a     true
              rads2      up/down    10.63.0.52/24      node3   e1b     true
      vs1
              lif1       up/up      172.17.176.120/24  node3   e0c     true
              lif2       up/up      172.17.176.121/24  node3   e1a     true
      ```

   b. Se node4 ha LIF SAN o gruppi DI LIF SAN che si trovano su una porta che non esisteva sul node2 o che devono essere mappati su una porta diversa, spostarli su una porta appropriata sul node4 completando i seguenti passaggi secondari:

      i. Impostare lo stato LIF su DOWN immettendo il seguente comando:

         ```
         network interface modify -vserver vserver_name -lif lif_name -status
         -admin down
         ```

      ii. Rimuovere la LIF dal set di porte:

         ```
         portset remove -vserver vserver_name -portset portset_name -port-name
         port_name
         ```

      iii. Immettere uno dei seguenti comandi:

         - Spostare un singolo LIF immettendo il seguente comando:

           ```
           network interface modify -vserver vserver_name -lif lif_name -home
           -port new_home_port
           ```

         - Spostare tutte le LIF su una singola porta inesistente o errata in una nuova porta immettendo il seguente comando:

           ```
           network interface modify {-home-port port_on_node1 -home-node node1
           -role data} -home-port new_home_port_on_node3
           ```

         - Aggiungere nuovamente i file LIF al set di porte:

```
portset add -vserver vserver_name -portset portset_name -port-name
port_name
```

È necessario confermare di spostare I file LIF SAN su una porta con la stessa velocità di collegamento della porta originale.

a. Modificare lo stato di tutti i LIF in `up` In questo modo, i LIF possono accettare e inviare traffico sul nodo immettendo il seguente comando:

```
network interface modify -home-port port_name -home-node node4 -lif data
-statusadmin up
```

b. Immettere il seguente comando ed esaminare l'output per verificare che i file LIF siano stati spostati nelle porte corrette e che i file LIF abbiano lo stato di `up` immettendo il seguente comando su uno dei nodi ed esaminando l'output:

```
network interface show -home-node <node4> -role data
```

c. 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 -status-admin
up
```

9. 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

Fase 6. Completare l'aggiornamento

Gestire l'autenticazione utilizzando i server KMIP

Con ONTAP da 9.5 a 9.7, è possibile utilizzare i server KMIP (Key Management Interoperability Protocol) per gestire le chiavi di autenticazione.

Fasi

1. Aggiungere un nuovo controller:

```
security key-manager setup -node new_controller_name
```

2. Aggiungere il gestore delle chiavi:

   ```
   security key-manager -add 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 show -status
   ```

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

   ```
   security key-manager 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 utilizzate unità auto-crittografanti e hai impostato `kmip.init.maxwait` variabile a `off` (ad esempio, in"Installa e avvia node4, passaggio 22"), 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: 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 show -status

security key-manager query
```

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 -add 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 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 setup -node new_controller_name
      ```

   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 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.

ONTAP 9.6 e 9.7

Configurare NVE o NAE sui controller che eseguono ONTAP 9.6 o 9.7

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 -add 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 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 setup -node new_controller_name
      ```

   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.

   - Ripristinare l'autenticazione per il gestore delle chiavi esterno:

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

     Questo comando richiede la passphrase di Onboard Key Manager (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".

   - Ripristinare l'autenticazione per OKM:

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

ONTAP 9.5

Configurare NVE o NAE sui controller che eseguono ONTAP 9.5

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 show`

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 -add 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 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 setup -node new_controller_name`

   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.

   - Ripristinare l'autenticazione per il gestore delle chiavi esterno:

     `security key-manager external restore`

     Questo comando richiede la passphrase di Onboard Key Manager (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".

   - Ripristinare l'autenticazione per OKM:

     `security key-manager setup -node node_name`

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 di gestione delle chiavi esterne. Riportare online quei volumi 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

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: 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 poiché ha è già disattivato.

A proposito di questa attività

Esiste un'interruzione per gli aggregati non root che sono stati già ricollocati fino al riavvio del node3.

Fasi

1. Alzati il node3.

   Durante l'avvio di node3, si verifica un'interruzione del client per tutti gli aggregati.

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

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.
"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.
"Gestione delle coppie HA"	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.
"Gestione MetroCluster e disaster recovery"	Descrive come eseguire le operazioni di switchover e switchback MetroCluster, sia nelle operazioni di manutenzione pianificate che in caso di disastro.
"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 9.0: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.0 supportati.

Contenuto	Descrizione
"Comandi di ONTAP 9.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.1 supportati.
"Comandi di ONTAP 9.2: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.2 supportati.
"Comandi di ONTAP 9.3: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.3 supportati.
"Comandi di ONTAP 9.4: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.4 supportati.
"Comandi di ONTAP 9.5: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.5 supportati.
"Comandi di ONTAP 9.6: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.6 supportati.
"Comandi di ONTAP 9.7: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.7 supportati.
"Comandi di ONTAP 9.8: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.8 supportati.
"Comandi di ONTAP 9.9.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.9.1 supportati.
"Comandi di ONTAP 9.10.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.10.1 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 "sostituzione controller di sistema" per aggiornare l'hardware del controller introdotto in ONTAP 9.15.1 e versioni successive"	Descrive le procedure di trasferimento degli aggregati necessarie per aggiornare senza interruzioni i controller introdotti in ONTAP 9.15.1 e versioni successive utilizzando i comandi "system controller replace".
"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.
"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".

Contenuto	Descrizione
"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.
"Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller che esegue ONTAP 9.5 a ONTAP 9.7"	Vengono descritte le procedure di riposizionamento degli aggregati necessarie per aggiornare senza interruzioni i controller che eseguono ONTAP 9.5 a ONTAP 9.7 utilizzando i comandi "system controller replace".
"Utilizzare il trasferimento di aggregati per aggiornare manualmente l'hardware del controller con ONTAP 9.7 o versione precedente"	Descrive le procedure di trasferimento degli aggregati necessarie per eseguire aggiornamenti manuali dei controller senza interruzioni con ONTAP 9.7 o versione precedente.

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.

Aggiornare manualmente l'hardware del controller con ONTAP 9.8 o versione successiva

Scopri di più sulla procedura di aggiornamento ARL

Questa procedura descrive come aggiornare l'hardware del controller utilizzando la ricollocazione manuale degli aggregati (ARL) sui sistemi che eseguono ONTAP 9.8 o versioni successive.

È possibile utilizzare questa procedura ARL se si sta eseguendo uno dei seguenti aggiornamenti:

- Dal sistema FAS al sistema FAS
- Dal sistema AFF al sistema AFF

  È possibile eseguire l'aggiornamento a un sistema sostitutivo della stessa serie:

  - Dal sistema AFF A-Series al sistema AFF A-Series
  - Da sistema AFF C-Series a sistema AFF C-Series
- Dal sistema ASA al sistema ASA

  Gli aggiornamenti ASA a un sistema sostitutivo ASA R2 non sono supportati. Per informazioni sulla migrazione dei dati da ASA a ASA R2, vedere "Abilitare l'accesso ai dati dagli host SAN al sistema di storage ASA R2".

  È possibile eseguire l'aggiornamento a un sistema sostitutivo della stessa serie:

- Dal sistema ASA A-Series al sistema ASA A-Series
- Da sistema ASA C-Series a sistema ASA C-Series

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.

> In questo documento, i nodi originali sono chiamati *node1* e *node2*, mentre i nuovi nodi sono chiamati *node3* e *node4*. Durante la procedura descritta, il nodo 1 viene sostituito dal nodo 3 e il nodo 2 viene sostituito dal nodo 4. 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 originali e nuovi. 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. Devi anche leggere e comprendere il "linee guida per l'aggiornamento dei controller con ARL" e il "Workflow di upgrade 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 `wipeconfig` i comandi non sono inclusi in questa procedura. Se in precedenza è stato utilizzato l'hardware del controller sostitutivo, è necessario contattare il supporto tecnico, in particolare se i controller eseguivano Data ONTAP in 7-Mode.
- 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.
- Oltre alle configurazioni non MetroCluster, questa procedura si applica alle configurazioni Fabric MetroCluster a quattro e otto nodi con ONTAP 9.8 e versioni successive.
  - Per le configurazioni MetroCluster con ONTAP 9.7 e versioni precedenti, visitare il sito Web all'indirizzo "Riferimenti" Per collegarsi a *Using aggregate Relocation to Manually Upgrade Controller hardware running ONTAP 9.7 or antecedente*.
  - Per le configurazioni MetroCluster IP e le opzioni di aggiornamento aggiuntive per le configurazioni Fabric MetroCluster, visitare il sito Web all'indirizzo "Riferimenti" Per collegarsi al contenuto *aggiornamento ed espansione MetroCluster*.

Decidere se utilizzare questa procedura di ricollocazione aggregata

Questa procedura descrive come aggiornare l'hardware del controller utilizzando la rilocazione manuale degli aggregati (ARL) su sistemi che eseguono ONTAP 9.8 o versioni successive. Questa complessa procedura dovrebbe essere utilizzata solo da amministratori ONTAP esperti.

Utilizzare questo contenuto nelle seguenti circostanze:

- Non vuoi aggiungere i nuovi controller come nuova coppia ha al cluster e migrare i dati utilizzando gli spostamenti 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.

- I controller eseguono ONTAP 9.8 o versione successiva.
- Si dispone di un sistema che utilizza le configurazioni Fabric MetroCluster a 4 e 8 nodi con ONTAP 9.8 o versione successiva.
- Nel sistema sono presenti aggregati ibridi.

- Se si sta aggiornando un sistema scambiando i moduli del controller nello stesso chassis, come AFF A800 o AFF C800, NetApp consiglia vivamente di utilizzare la procedura di aggiornamento che"aggiorna i modelli di controller utilizzando ARL, mantenendo lo chassis e i dischi del sistema esistenti" . Questa procedura ARL include i passaggi che garantiscono che i dischi interni rimangano saldamente nello chassis quando si rimuovono e si installano i controller durante la procedura di aggiornamento.

  "Scopri le combinazioni di aggiornamento del sistema supportate utilizzando ARL, mantenendo lo chassis e i dischi del sistema esistenti".

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

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.

Scegli una procedura di aggiornamento hardware diversa

- "Esaminare i metodi ARL alternativi disponibili per l'aggiornamento dell'hardware del controller".
- 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*.

Informazioni correlate

Fare riferimento a "Riferimenti" per collegarsi alla *Documentazione ONTAP 9*.

Workflow di upgrade ARL

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

Aggiornare la coppia di nodi

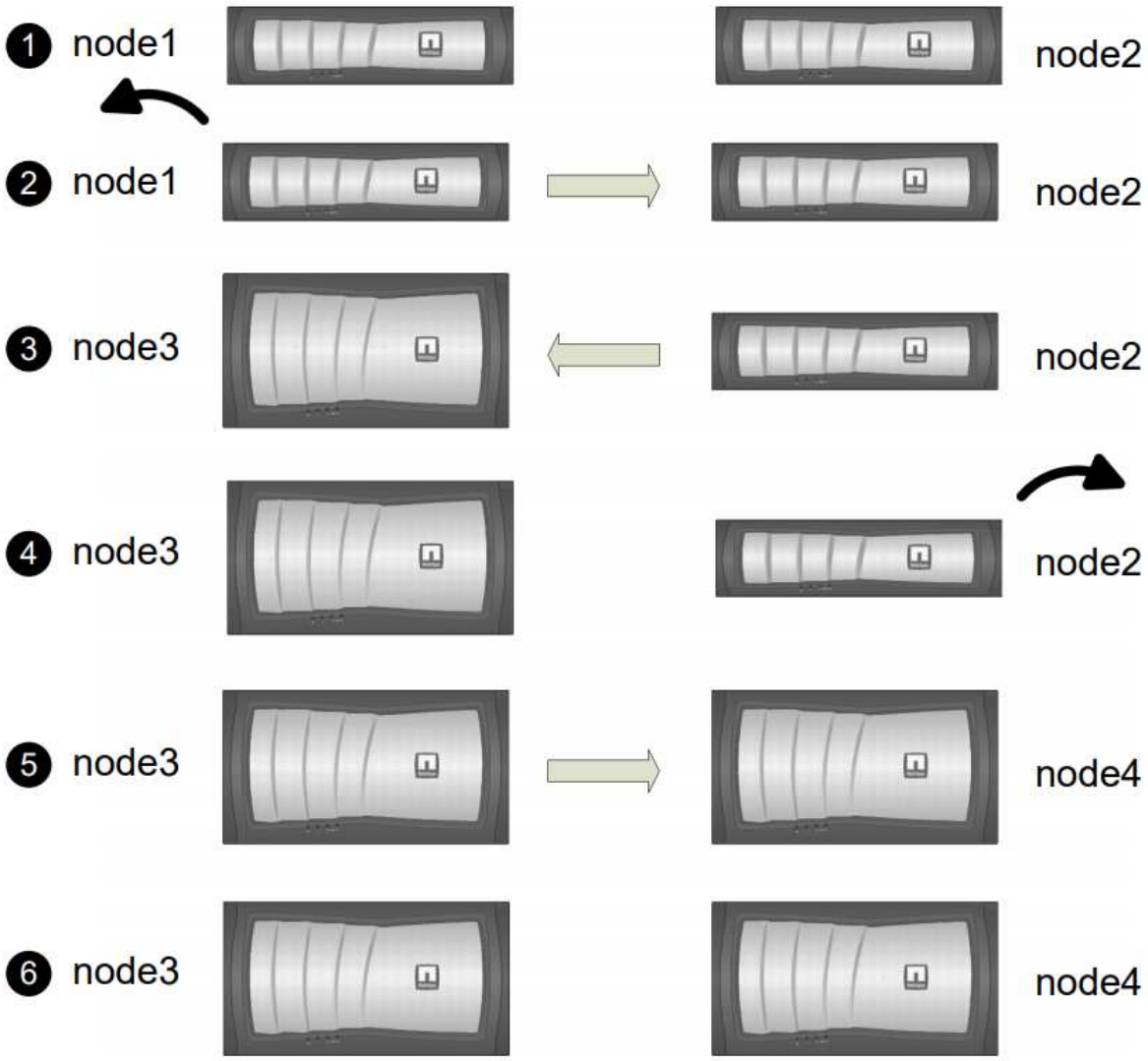
Per aggiornare la coppia di nodi, è necessario preparare i nodi originali ed eseguire una serie di passaggi sia sul nodo originale che su quello nuovo. È quindi possibile decommissionare i nodi originali.

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 figura seguente mostra le fasi della procedura. Le frecce spesse e grigio chiaro rappresentano il trasferimento degli aggregati e lo spostamento dei LIF, mentre le frecce nere più sottili rappresentano la rimozione dei nodi originali. Le immagini dei controller più piccole rappresentano i nodi originali, mentre quelle più grandi rappresentano i nuovi nodi.



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	Fasi
"Fase 1: Preparazione per l'aggiornamento"	Durante la fase 1, se necessario, si conferma che i dischi interni non contengono aggregati root o aggregati di dati, si preparano i nodi per l'aggiornamento ed eseguono una serie di controlli preliminari. Se necessario, occorre reimmettere i dischi per Storage Encryption e prepararsi all'avvio in rete dei nuovi controller. 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: Ritiro del node1"	Durante la fase 2, è possibile spostare aggregati non root da node1 a node2 e spostare le LIF di dati non SAN di proprietà di node1 a node2, inclusi gli aggregati non riusciti o vetoed. Inoltre, registrare le informazioni necessarie per il node1 da utilizzare in seguito nella procedura e dismettere il node1. Proprietà aggregata alla fine della fase 2: • Node1 è il proprietario domestico degli aggregati node1. • Node2 è l'attuale proprietario degli aggregati node1. • Node2 è il proprietario domestico e proprietario corrente degli aggregati node2.
"Fase 3: Installazione e boot node3"	Durante la fase 3, si installa e si avvia node3, si mappano le porte di gestione del cluster e dei nodi da node1 a node3 e si spostano le LIF dei dati e LE LIF SAN appartenenti al node1 da node2 a node3. Puoi anche spostare tutti gli aggregati da node2 a node3 e spostare i dati LIF e SAN di proprietà di node2 a node3. Proprietà aggregata alla fine della fase 3: • Node2 è il proprietario domestico degli aggregati node2 ma non il proprietario corrente. • Node3 è il proprietario della casa e il proprietario corrente degli aggregati originariamente appartenenti al node1. • Node2 è il proprietario domestico e proprietario corrente degli aggregati che appartengono al node2 ma non il proprietario domestico.
"Fase 4: Dismettere il node2"	Durante la fase 4, si registrano le informazioni necessarie per il node2 da utilizzare più avanti nella procedura, quindi si deve ritirare il node2. Non si verificano modifiche nella proprietà aggregata.

Fase	Fasi
"Fase 5: Installazione e boot node4"	Durante la fase 5, si installa e si avvia node4, si mappano le porte di gestione del cluster e dei nodi da node2 a node4 e si spostano le LIF dei dati e LE LIF SAN appartenenti a node2 da node3 a node4. È inoltre possibile spostare gli aggregati node2 da node3 a node4 e spostare i LIF dei dati e LE LIF SAN di proprietà di node2 a node3. 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, confermi che i nuovi nodi sono impostati correttamente e configuri Storage Encryption o NetApp Volume Encryption se i nuovi nodi sono abilitati alla crittografia. È inoltre necessario decommissionare i vecchi nodi per riprendere le operazioni di SnapMirror. Gli aggiornamenti per il disaster recovery della macchina virtuale per lo storage (SVM) non verranno interrotti in base alle pianificazioni assegnate. Non si verificano modifiche nella proprietà aggregata.

Linee guida per l'aggiornamento dei controller con ARL

Per capire se è possibile utilizzare il trasferimento aggregato (ARL) per aggiornare una coppia di controller che eseguono ONTAP 9.8, dipende dalla piattaforma e dalla configurazione dei controller originali e di quelli sostitutivi.

Aggiornamenti supportati per ARL

È possibile aggiornare una coppia di nodi utilizzando ARL nei seguenti casi:

- Prima dell'aggiornamento, sia i controller originali che quelli sostitutivi devono eseguire la stessa versione di ONTAP 9.8.
- I controller sostitutivi devono avere una capacità uguale o superiore a quella dei controller originali. Capacità uguale o superiore si riferisce agli attributi, ad esempio le dimensioni della NVRAM, il volume, il LUN o i limiti del numero di aggregati; si riferisce anche alle dimensioni massime del volume o dell'aggregato dei nuovi nodi.
- È possibile aggiornare i seguenti tipi di sistemi:
  - Da un sistema FAS a un sistema FAS.
  - Da un sistema AFF a un sistema AFF.
- Per alcuni aggiornamenti del controller ARL è possibile utilizzare porte cluster temporanee sul controller sostitutivo per l'aggiornamento. Ad esempio, se si esegue l'aggiornamento da un sistema AFF A300 a un sistema AFF A400, a seconda della configurazione di AFF A400, è possibile utilizzare una delle due porte

mezzanine o aggiungere una scheda di interfaccia di rete 10GbE a quattro porte per fornire porte cluster temporanee. Dopo aver completato un aggiornamento del controller utilizzando porte del cluster temporanee, è possibile migrare senza interruzioni i cluster alle porte 100 GbE del controller sostitutivo.

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

È necessario verificare se l'ARL può essere eseguito sui controller originali e sostitutivi. È necessario controllare le dimensioni di tutti gli aggregati definiti e il numero di dischi supportati dal sistema originale. Quindi confrontarli con la dimensione aggregata e il numero di dischi supportati dal nuovo sistema. Per accedere a queste informazioni, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*. 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.

È necessario verificare nelle regole di combinazione del cluster se i nuovi nodi possono diventare parte del cluster con i nodi esistenti quando il controller originale viene sostituito. Per ulteriori informazioni sulle regole di combinazione dei cluster, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*.

Entrambi i sistemi sono ad alta disponibilità (ha) o non ha. Entrambi i nodi devono avere la personalità abilitata o disabilitata; non è possibile combinare un nodo con la personalità ottimizzata per All Flash abilitata con un nodo che non ha la personalità abilitata nella stessa coppia ha. Se le personalità sono diverse, contattare il supporto tecnico.

Se il nuovo sistema dispone di meno slot rispetto al sistema originale o se dispone di un numero inferiore o di porte diverse, potrebbe essere necessario aggiungere un adattatore al nuovo sistema. Fare riferimento a. "Riferimenti" Per informazioni dettagliate su piattaforme specifiche, consultare il sito Web del supporto NetApp *Hardware Universe*.

Se si dispone di un sistema con più di due porte cluster per nodo, ad esempio un sistema FAS8080 o AFF8080, prima di avviare l'aggiornamento, è necessario migrare e riassegnare le LIF del cluster a due porte cluster per nodo. Se si esegue l'aggiornamento del controller con più di due porte cluster per nodo, le LIF del cluster potrebbero non essere presenti sul nuovo controller dopo l'aggiornamento.

Aggiornamenti non supportati per ARL

Non è possibile eseguire i seguenti aggiornamenti:

- Da o verso i controller che non possono eseguire ONTAP 9.8 o versioni successive.
- Ai controller sostitutivi che non supportano gli shelf di dischi collegati ai controller originali.

  Per informazioni sul supporto dei dischi, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*.

- Da controller con aggregati root o aggregati di dati su dischi interni.

  Se si desidera aggiornare i controller con aggregati root o aggregati di dati su dischi interni, fare riferimento a. "Riferimenti" Per collegarsi a *Upgrade spostando volumi o storage* e passare alla procedura *aggiornamento di una coppia di nodi che eseguono Clustered Data ONTAP spostando volumi*.

  Se si desidera aggiornare ONTAP sui nodi di un cluster, fare riferimento a. "Riferimenti" Collegamento a *Upgrade ONTAP*.

Presupposti e terminologia

Il presente documento si basa sui seguenti presupposti:

- L'hardware del controller sostitutivo è nuovo e non è stato utilizzato.

> I passaggi necessari per preparare i controller usati con il `wipeconfig` I comandi non sono inclusi in questa procedura perché questa presuppone che l'hardware del controller sostitutivo sia nuovo e non sia stato utilizzato. È necessario contattare l'assistenza tecnica se l'hardware del controller sostitutivo è stato utilizzato in precedenza, soprattutto se i controller eseguivano Data ONTAP in modalità 7.

- Hai letto e compreso le linee guida per l'aggiornamento della coppia di nodi.

> Non tentare di cancellare il contenuto NVRAM . Se è necessario cancellare il contenuto della NVRAM, contattare l'assistenza tecnica NetApp .

- Si sta eseguendo il comando appropriato prima e dopo `modify` e confrontando l'output di entrambi `show` comandi per verificare che il `modify` comando riuscito.
- Se si dispone di una configurazione SAN, si dispone di LIF locali e partner per ciascuna macchina virtuale di storage (SVM), sulla coppia ha. Se non si dispone di LIF locali e partner per ogni SVM, è necessario aggiungere LA LIF dei dati SAN sul nodo remoto e locale per tale SVM prima di iniziare l'aggiornamento.
- Se si dispone di set di porte in una configurazione SAN, è necessario verificare che ogni set di porte associato contenga almeno un LIF da ciascun nodo della coppia ha.

Questa procedura utilizza il termine *prompt dell'ambiente di boot* per fare riferimento al prompt di un nodo da cui è possibile eseguire determinate attività, come il riavvio del nodo e la stampa o l'impostazione di variabili ambientali. Il prompt viene a volte chiamato in modo informale *prompt del boot loader*.

Il prompt dell'ambiente di boot viene mostrato nell'esempio seguente:

```
LOADER>
```

Licensing in ONTAP 9.8 o versioni successive

Alcune funzionalità richiedono licenze, emesse come *pacchetti* che includono una o più funzionalità. Ogni nodo del cluster deve disporre di una propria chiave per poter utilizzare ciascuna funzionalità nel cluster.

Se non si dispone di nuove chiavi di licenza, le funzionalità attualmente concesse in licenza nel cluster sono disponibili per il nuovo controller e continueranno a funzionare. Tuttavia, l'utilizzo di funzionalità senza licenza sul controller potrebbe non essere conforme al contratto di licenza, pertanto è necessario installare la nuova chiave di licenza o le nuove chiavi per il nuovo controller al termine dell'aggiornamento.

Tutte le chiavi di licenza sono composte da 28 caratteri alfabetici maiuscoli. Fare riferimento a. "Riferimenti" Per accedere al *sito di supporto NetApp*, dove è possibile ottenere nuove chiavi di licenza di 28 caratteri per ONTAP 9.8. o versioni successive. Le chiavi sono disponibili nella sezione *My Support* sotto *licenze software*. Se il sito non dispone delle chiavi di licenza necessarie, contattare il rappresentante commerciale NetApp.

Per informazioni dettagliate sulle licenze, visitare il sito Web all'indirizzo "Riferimenti" Per collegarsi al *System Administration Reference*.

Crittografia dello storage

I nodi originali o i nuovi nodi potrebbero essere abilitati per Storage Encryption. In tal caso, è necessario eseguire ulteriori operazioni in questa procedura per verificare che Storage Encryption sia impostato correttamente.

Se si desidera utilizzare Storage Encryption, tutti i dischi associati ai nodi devono disporre di dischi con crittografia automatica.

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

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.

Se si verificano problemi durante l'aggiornamento dei controller, fare riferimento a "Risolvere i problemi" sezione. Le informazioni sui guasti che possono verificarsi sono elencate in base alla fase della procedura nella "Sequenza di aggiornamento ARL" .

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

Strumenti e documentazione richiesti

È necessario disporre di strumenti specifici per installare il nuovo hardware e consultare altri documenti durante il processo di aggiornamento. È inoltre necessario registrare le informazioni essenziali per completare l'aggiornamento del controller; viene fornito un foglio di lavoro per registrare le informazioni.

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 richiesti per questo aggiornamento.

Foglio di lavoro: Informazioni da raccogliere prima e durante l'aggiornamento del controller

È necessario raccogliere determinate informazioni per supportare l'aggiornamento dei nodi originali. Queste informazioni includono gli ID dei nodi, i dettagli di porta e LIF, le chiavi di licenza e gli indirizzi IP.

È possibile utilizzare il seguente foglio di lavoro per registrare le informazioni da utilizzare in seguito nella procedura:

Informazioni necessarie	Una volta raccolti	Se utilizzato	Informazioni raccolte
Modello, ID sistema, numero di serie dei nodi originali	Fase 1: *Preparare i nodi per l'aggiornamento*	Fase 3: *Installare e avviare node3* fase 5: *Installare e avviare node4* fase 6: *Rimuovere il vecchio sistema*	
Informazioni su shelf e dischi, dettagli dello storage flash, memoria, NVRAM e schede adattatore sui nodi originali	Fase 1: *Preparazione dei nodi per l'aggiornamento*	Durante l'intera procedura	
Aggregati e volumi online sui nodi originali	Fase 1: *Preparare i nodi per l'aggiornamento*	Durante l'intera procedura per verificare che aggregati e volumi rimangano online, tranne durante una breve delocalizzazione	
Output dei comandi `network port vlan show` e. `network port ifgrp show`	Fase 1: *Preparare i nodi per l'aggiornamento*	Fase 3: *Mappare le porte dal nodo 1 al nodo 3* fase 5: *Mappare le porte dal nodo 2 al nodo 4*	
(Solo ambienti SAN) Configurazione predefinita delle porte FC	Fase 1: *Preparare i nodi per l'aggiornamento*	Durante la configurazione delle porte FC sui nuovi nodi	
Indirizzo IP degli SP	Fase 1: *Preparare i nodi per l'aggiornamento*	Fase 6: *Verificare che i nuovi controller siano impostati correttamente*	
Chiavi di licenza	Fase 1: *Preparare i nodi per l'aggiornamento*	Fase 6: *Verificare che i nuovi controller siano impostati correttamente*	
Indirizzo IP per il server di gestione delle chiavi esterne	Fase 1: *Rekey disks for Storage Encryption*	Fase 6: *Impostare Storage Encryption sui nuovi nodi*	
Nome e percorso della directory accessibile dal web in cui si scaricano i file per avviare i nodi	Fase 1: *Prepararsi al netboot*	Fase 3: *Installare e avviare node3* fase 5: *Installare e avviare node4*	
LIF dati non SAN di proprietà di node1	Fase 2: *Spostare le LIF dei dati non SAN di proprietà del node1 in node2*	Più avanti nella sezione	
Cluster, intercluster, gestione dei nodi, gestione dei cluster e porte fisiche	Fase 2: *Registrare le informazioni del node1*	Fase 3: *Installare e avviare node3* fase 3: *Mappare le porte dal node1 al node3*	

Informazioni necessarie	Una volta raccolti	Se utilizzato	Informazioni raccolte
Porte su nuovi nodi	Fase 3: *Mappare le porte dal nodo 1 al nodo 3*	Più avanti nella sezione e nella sezione *Map ports from node2 to node4*	
Porte e domini di broadcast disponibili sul nodo 3	Fase 3: *Mappare le porte dal nodo 1 al nodo 3*	Più avanti nella sezione	
Le LIF di dati non SAN non sono di proprietà di node2	*Spostamento delle LIF di dati non SAN appartenenti al nodo 1 da node2 a node3 e verifica delle LIF SAN sul nodo 3*	Più avanti nella sezione	
LIF dati non SAN di proprietà di node2	Fase 3: *Spostare le LIF dei dati non SAN di proprietà del node2 in node3*	Più avanti nella sezione	
Cluster, intercluster, gestione dei nodi, gestione dei cluster e porte fisiche	Fase 4: *Registrare le informazioni node2*	Fase 5: *Installare e avviare node4* fase 5:_ mappare le porte da node2 a node4_	
Porte di rete del cluster sul nodo 4	Fase 5: *Mappare le porte dal nodo 2 al nodo 4*	Più avanti nella sezione	
Porte e domini di broadcast disponibili sul nodo 4	Fase 5: *Mappare le porte dal nodo 2 al nodo 4*	Più avanti nella sezione	
Certificati SSL pubblici e privati per il sistema di storage e certificati SSL privati per ciascun server di gestione delle chiavi	Fase 6: *Impostare Storage Encryption sui nuovi nodi*	Più avanti nella sezione	

Fase 1. Preparatevi per l'aggiornamento

Determinare se il controller dispone di aggregati su dischi interni

Se si stanno aggiornando i controller con dischi interni, è necessario completare diversi comandi ed esaminarne l'output per confermare che nessuno dei dischi interni contiene aggregati root o aggregati di dati.

A proposito di questa attività

Se non si stanno aggiornando controller con aggregati su dischi interni, saltare questa sezione e passare alla sezione "Preparare i nodi per l'aggiornamento".

Fasi

1. Inserisci il nodeshell, una volta per ciascuno dei nodi originali.

   ```
   system node run -node node_name
   ```

2. Visualizzare le unità interne:

   `sysconfig -av`

   Il sistema visualizza informazioni dettagliate sulla configurazione del nodo, incluso lo storage, come mostrato nell'output parziale mostrato nell'esempio seguente:

```
node> sysconfig -av
slot 0: SAS Host Adapter 0a (PMC-Sierra PM8001 rev. C, SAS, UP)
                Firmware rev: 01.11.06.00
                 Base WWN: 5:00a098:0008a3b:b0
                 Phy State: [0] Enabled, 6.0 Gb/s
                            [1] Enabled, 6.0 Gb/s
                            [2] Enabled, 6.0 Gb/s
                            [3] Enabled, 6.0 Gb/s
                ID Vendor Model FW Size
                00.0 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.1 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.2 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.3 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.4 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.5 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.6 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.7 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.8 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.9 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.10: NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.11: NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
...
```

3. Esaminare l'output dello storage di `sysconfig -av` per identificare i dischi interni e registrare le informazioni.

   I dischi interni hanno "00". All'inizio del proprio ID. Il "00." indica uno shelf di dischi interno e il numero dopo il punto decimale indica il singolo disco.

4. immettere il seguente comando su entrambi i controller:

   ```
   aggr status -r
   ```

   Il sistema visualizza lo stato aggregato del nodo, come mostrato nell'output parziale nell'esempio seguente:

   ```
   node> aggr status -r
   Aggregate aggr2 (online, raid_dp, parity uninit'd!) (block checksums)
   Plex /aggr2/plex0 (online, normal, active)
   RAID group /aggr2/plex0/rg0 (normal, block checksums)

   RAID Disk Device    HA SHELF BAY CHAN Pool Type RPM  Used (MB/blks)
   Phys (MB/blks)
   --------- --------- -- ----- --- ---- ---- ---- ---- ------------------
   ------------------
   dparity   0a.00.1   0a   0    1  SA:B  0   BSAS 7200 1695466/3472315904
   1695759/3472914816
   parity    0a.00.3   0a   0    3  SA:B  0   BSAS 7200 1695466/3472315904
   1695759/3472914816
   data      0a.00.9   0a   0    9  SA:B  0   BSAS 7200 1695466/3472315904
   1695759/3472914816
   ...
   ```

   Il dispositivo utilizzato per creare l'aggregato potrebbe non essere un disco fisico ma una partizione.

5. Esaminare l'output di `aggr status -r` per identificare gli aggregati utilizzando dischi interni e registrare le informazioni.

   Nell'esempio del passaggio precedente, "aggr2" utilizza dischi interni, come indicato dall'ID dello shelf "0".

6. Immettere il seguente comando su entrambi i controller:

   ```
   aggr status -v
   ```

   Il sistema visualizza le informazioni sui volumi sull'aggregato, come mostrato nell'output parziale nell'esempio seguente:

```
node> aggr status -v
...
 aggr2   online   raid_dp, aggr    nosnap=off, raidtype=raid_dp,
raidsize=14,
                  64-bit           raid_lost_write=on,
ignore_inconsistent=off,
                  rlw_on           snapmirrored=off, resyncsnaptime=60,
                                   fs_size_fixed=off,
lost_write_protect=on,
                                   ha_policy=cfo, hybrid_enabled=off,
percent_snapshot_space=0%,
                                   free_space_realloc=off, raid_cv=on,
thorough_scrub=off
         Volumes: vol6, vol5, vol14
...
 aggr0   online   raid_dp, aggr    root, diskroot, nosnap=off,
raidtype=raid_dp,
                  64-bit           raidsize=14, raid_lost_write=on,
ignore_inconsistent=off,
                  rlw_on           snapmirrored=off,  resyncsnaptime=60,
fs_size_fixed=off,
                                   lost_write_protect=on, ha_policy=cfo,
hybrid_enabled=off,
                                   percent_snapshot_space=0%,
free_space_realloc=off, raid_cv=on
         Volumes: vol0
```

In base all'output in Fase 4 Fase 6, aggr2 utilizza tre dischi interni, "0a.00.1", "0a.00.3" e "0a.00.9", mentre i volumi su "aggr2" sono "vol6", "vol5" e "vol14". Inoltre, nell'output della fase 6, la lettura per "aggr0" contiene la parola "root" all'inizio delle informazioni per l'aggregato. Che indica che contiene un volume root.

7. Esaminare l'output di `aggr status -v` comando per identificare i volumi appartenenti a qualsiasi aggregato presente su un disco interno e se uno di questi volumi contiene un volume root.
8. Uscire dal nodeshell immettendo il seguente comando su ciascun controller:

   `exit`

9. Eseguire una delle seguenti operazioni:

Se i controller	Quindi…
Non contenere aggregati sui dischi interni	Continuare con questa procedura.

Se i controller	Quindi…
Contengono aggregati ma non volumi sui dischi interni	Continuare con questa procedura. Prima di continuare, è necessario posizionare gli aggregati offline, quindi distruggere gli aggregati sui dischi interni. Fare riferimento a. "Riferimenti" Collegamento alla gestione di *dischi e aggregati con il contenuto CLI* per informazioni sulla gestione degli aggregati.
Contenere volumi non root sui dischi interni	Continuare con questa procedura. Prima di continuare, è necessario spostare i volumi su uno shelf di dischi esterno, posizionare gli aggregati offline e distruggere gli aggregati sui dischi interni. Fare riferimento a. "Riferimenti" Collegamento alla gestione di *dischi e aggregati con il contenuto CLI* per informazioni sullo spostamento dei volumi.
Contenere volumi root sui dischi interni	Non continuare con questa procedura. È possibile aggiornare i controller facendo riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* e utilizzare la procedura *aggiornamento dell'hardware del controller su una coppia di nodi che eseguono Clustered Data ONTAP spostando i volumi*.
Contengono volumi non root sui dischi interni e non è possibile spostare i volumi su uno storage esterno	Non continuare con questa procedura. È possibile aggiornare i controller utilizzando la procedura *aggiornamento dell'hardware del controller su una coppia di nodi che eseguono Clustered Data ONTAP spostando i volumi*. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp*, dove è possibile accedere a questa procedura.

Preparare i nodi per l'aggiornamento

Prima di poter sostituire i nodi originali, è necessario verificare che si trovino in una coppia ha, che non vi siano dischi mancanti o guasti, che possano accedere reciprocamente allo storage e che non dispongano di LIF dati assegnati agli altri nodi del cluster. È inoltre necessario raccogliere informazioni sui nodi originali e, se il cluster si trova in un ambiente SAN, confermare che tutti i nodi del cluster sono in quorum.

Fasi

1. Verificare che ciascuno dei nodi originali disponga di risorse sufficienti per supportare adeguatamente il carico di lavoro di entrambi i nodi durante la modalità Takeover.

   Fai riferimento "Riferimenti"al link *gestione coppia ha* e segui la sezione *Best practice per coppie ha*. Nessuno dei nodi originali deve essere eseguito con un utilizzo superiore al 50%; se un nodo viene eseguito con un utilizzo inferiore al 50%, può gestire i carichi per entrambi i nodi durante l'aggiornamento del controller.

2. Completare i seguenti passaggi secondari per creare una linea di base delle performance per i nodi

originali:

a. Assicurarsi che l'account utente diagnostico sia sbloccato.

> L'account utente diagnostico è destinato esclusivamente a scopi diagnostici di basso livello e deve essere utilizzato solo con le indicazioni del supporto tecnico.
>
> Per informazioni sullo sblocco degli account utente, fare riferimento a. "Riferimenti" Per collegarsi al *System Administration Reference*.

b. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* e scaricare il modulo di raccolta delle performance e delle statistiche (Perfstat Converged).

   Il tool Perfstat Converged consente di stabilire una linea di base per le performance da confrontare dopo l'aggiornamento.

c. Creare una linea di base per le performance seguendo le istruzioni sul NetApp Support Site.

3. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* e aprire un caso di supporto sul sito di supporto NetApp.

   È possibile utilizzare il caso per segnalare eventuali problemi che potrebbero verificarsi durante l'aggiornamento.

4. Verificare che le batterie NVMEM o NVRAM del nodo 3 e del nodo 4 siano cariche e, in caso contrario, ricaricarle.

   Controllare fisicamente il n. 3 e il n. 4 per verificare se le batterie NVMEM o NVRAM sono cariche. Per informazioni sui LED per il modello di node3 e node4, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*.

   > Non tentare di cancellare il contenuto NVRAM . Se è necessario cancellare il contenuto della NVRAM, contattare l'assistenza tecnica NetApp .

5. Controllare la versione di ONTAP su node3 e node4.

   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*.

   Le informazioni sulla versione di ONTAP su node3 e node4 devono essere incluse nelle confezioni di spedizione. La versione di ONTAP viene visualizzata all'avvio del nodo oppure è possibile avviare il nodo in modalità di manutenzione ed eseguire il comando:

   ```
   version
   ```

6. Controllare se sono presenti due o quattro LIF del cluster su node1 e node2:

   ```
   network interface show -role cluster
   ```

   Il sistema visualizza tutte le LIF del cluster, come mostrato nell'esempio seguente:

```
cluster::> network interface show -role cluster
        Logical    Status     Network          Current  Current Is
Vserver Interface  Admin/Oper Address/Mask     Node     Port    Home
------- ---------- ---------- ---------------- -------- ------- ----
node1
        clus1      up/up      172.17.177.2/24  node1    e0c     true
        clus2      up/up      172.17.177.6/24  node1    e0e     true
node2
        clus1      up/up      172.17.177.3/24  node2    e0c     true
        clus2      up/up      172.17.177.7/24  node2    e0e     true
```

7. Se si dispone di due o quattro LIF del cluster su node1 o node2, assicurarsi di poter eseguire il ping di entrambe le LIF del cluster in tutti i percorsi disponibili completando i seguenti passaggi secondari:

   a. Immettere il livello di privilegio avanzato:

      ```
      set -privilege advanced
      ```

      Il sistema visualizza il seguente messaggio:

      ```
      Warning: These advanced commands are potentially dangerous; use them
      only when directed to do so by NetApp personnel.
      Do you wish to continue? (y or n):
      ```

   b. Invio `y`.

   c. Eseguire il ping dei nodi e verificare la connettività:

      ```
      cluster ping-cluster -node node_name
      ```

      Il sistema visualizza un messaggio simile al seguente esempio:

```
cluster::*> cluster ping-cluster -node node1
Host is node1
Getting addresses from network interface table...
Local = 10.254.231.102 10.254.91.42
Remote = 10.254.42.25 10.254.16.228
Ping status:
...
Basic connectivity succeeds on 4 path(s) Basic connectivity fails on 0
path(s)
................
Detected 1500 byte MTU on 4 path(s):
Local 10.254.231.102 to Remote 10.254.16.228
Local 10.254.231.102 to Remote 10.254.42.25
Local 10.254.91.42 to Remote 10.254.16.228
Local 10.254.91.42 to Remote 10.254.42.25
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

+
Se il nodo utilizza due porte del cluster, si dovrebbe vedere che è in grado di comunicare su quattro percorsi, come mostrato nell'esempio.

a. Tornare al privilegio di livello amministrativo:

   ```
   set -privilege admin
   ```

8. Verificare che node1 e node2 si trovino in una coppia ha e che i nodi siano collegati tra loro e che sia possibile effettuare il takeover:

   ```
   storage failover show
   ```

   L'esempio seguente mostra l'output quando i nodi sono collegati tra loro ed è possibile effettuare il takeover:

   ```
   cluster::> storage failover show
                                Takeover
   Node           Partner        Possible State Description
   -------------- -------------- -------- -------------------------------
   node1          node2          true     Connected to node2
   node2          node1          true     Connected to node1
   ```

   Nessuno dei due nodi deve essere in giveback parziale. L'esempio seguente mostra che node1 è in giveback parziale:

```
cluster::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- -------------------------------
node1          node2          true     Connected to node2, Partial
giveback
node2          node1          true     Connected to node1
```

Se uno dei nodi è in un giveback parziale, utilizzare `storage failover giveback` il comando per eseguire il giveback e quindi utilizzare `storage failover show-giveback` il comando per assicurarsi che non venga restituito alcun aggregato. Per informazioni dettagliate sui comandi, fare riferimento al "Riferimenti"link a *ha Pair Management*.

9. Conferma che né node1 né node2 possiedono gli aggregati per i quali sono il proprietario corrente (ma non il proprietario domestico):

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

   Se né node1 né node2 possiedono aggregati per i quali è il proprietario corrente (ma non il proprietario domestico), il sistema restituirà un messaggio simile al seguente esempio:

```
cluster::> storage aggregate show -node node2 -is-home false -fields
owner-name,homename,state
There are no entries matching your query.
```

   L'esempio seguente mostra l'output del comando per un nodo denominato node2 che è il proprietario di casa, ma non il proprietario corrente, di quattro aggregati:

```
cluster::> storage aggregate show -node node2 -is-home false
               -fields owner-name,home-name,state

aggregate     home-name    owner-name   state
------------- ------------ ------------ ------
aggr1         node1        node2        online
aggr2         node1        node2        online
aggr3         node1        node2        online
aggr4         node1        node2        online

4 entries were displayed.
```

10. Eseguire una delle seguenti operazioni:

Se il comando è in Fase 9…	**Quindi…**
Con output vuoto	Saltare il passaggio 11 e passare a. Fase 12.

Se il comando è in Fase 9…	Quindi…
Ha avuto output	Passare a. Fase 11.

11. se node1 o node2 possiede aggregati per i quali è il proprietario corrente, ma non il proprietario della casa, completare i seguenti passaggi secondari:

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

    ```
    storage failover giveback -ofnode home_node_name
    ```

    b. 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.
```

12. verificare che node1 e node2 possano accedere reciprocamente allo storage e verificare che non manchino dischi:

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

    L'esempio seguente mostra l'output quando non mancano dischi:

```
cluster::> storage failover show -fields local-missing-disks,partner-
missing-disks

node     local-missing-disks partner-missing-disks
-------- ------------------- ---------------------
node1    None                None
node2    None                None
```

Se mancano dei dischi, fare riferimento al "Riferimenti"collegamento alla gestione *disco e aggregato con la*

CLI, alla gestione *logica dello storage con la CLI* e alla gestione *coppia ha* per configurare lo storage per la coppia ha.

13. Verificare che node1 e node2 siano integri e idonei a partecipare al cluster:

    `cluster show`

    L'esempio seguente mostra l'output quando entrambi i nodi sono idonei e integri:

```
cluster::> cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
```

14. Impostare il livello di privilegio su Advanced (avanzato):

    `set -privilege advanced`

15. verificare che node1 e node2 eseguano la stessa release di ONTAP:

    `system node image show -node node1,node2 -iscurrent true`

    L'esempio seguente mostra l'output del comando:

```
cluster::*> system node image show -node node1,node2 -iscurrent true

                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------- -------------------
node1
         image1   true    true    9.1         2/7/2017 20:22:06
node2
         image1   true    true    9.1         2/7/2017 20:20:48

2 entries were displayed.
```

16. Verificare che né node1 né node2 siano in possesso di LIF di dati appartenenti ad altri nodi del cluster e controllare `Current Node` e. `Is Home` colonne nell'output:

    `network interface show -role data -is-home false -curr-node node_name`

    L'esempio seguente mostra l'output quando node1 non ha LIF di proprietà di altri nodi nel cluster:

```
cluster::> network interface show -role data -is-home false -curr-node
node1
 There are no entries matching your query.
```

Nell'esempio seguente viene mostrato l'output quando node1 possiede le LIF dei dati di proprietà dell'altro nodo:

```
cluster::> network interface show -role data -is-home false -curr-node
node1

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data1      up/up      172.18.103.137/24  node1          e0d
false
            data2      up/up      172.18.103.143/24  node1          e0f
false

2 entries were displayed.
```

17. Se l'output è in Fase 15 Mostra che node1 o node2 possiede qualsiasi LIF di dati di proprietà di altri nodi nel cluster, migrare i LIF di dati lontano dal node1 o node2:

    `network interface revert -vserver * -lif *`

    Per informazioni dettagliate su `network interface revert` fare riferimento a. "Riferimenti" Per collegarsi ai comandi di *ONTAP 9: Manuale riferimento pagina*.

18. Controllare se node1 o node2 possiede dischi guasti:

    `storage disk show -nodelist node1,node2 -broken`

    Se uno dei dischi si è guastato, rimuoverli seguendo le istruzioni contenute in *Disk and aggregate management with the CLI*. (Fare riferimento a. "Riferimenti" Per collegarsi a *Disk and aggregate management with the CLI*.)

19. Raccogliere informazioni su node1 e node2 completando i seguenti passaggi secondari e registrando l'output di ciascun comando:

- Queste informazioni verranno utilizzate più avanti nella procedura.
- Se si dispone di un sistema con più di due porte cluster per nodo, ad esempio un sistema FAS8080 o AFF8080, prima di avviare l'aggiornamento, è necessario migrare e riassegnare le LIF del cluster a due porte cluster per nodo. Se si esegue l'aggiornamento del controller con più di due porte cluster per nodo, le LIF del cluster potrebbero non essere presenti sul nuovo controller dopo l'aggiornamento.

a. Registrare il modello, l'ID del sistema e il numero di serie di entrambi i nodi:

```
system node show -node node1,node2 -instance
```

Le informazioni verranno utilizzate per riassegnare i dischi e decommissionare i nodi originali.

b. Immettere il seguente comando sia sul nodo 1 che sul nodo 2 e registrare le informazioni sugli shelf, il numero di dischi in ogni shelf, i dettagli dello storage flash, la memoria, la NVRAM e le schede di rete dall'output:

```
run -node node_name sysconfig
```

È possibile utilizzare le informazioni per identificare parti o accessori che si desidera trasferire su node3 o node4.

c. Immettere il seguente comando sia su node1 che su node2 e registrare gli aggregati che sono online su entrambi i nodi:

```
storage aggregate show -node node_name -state online
```

È possibile utilizzare queste informazioni e le informazioni riportate nel seguente passaggio per verificare che gli aggregati e i volumi rimangano online durante l'intera procedura, ad eccezione del breve periodo in cui sono offline durante il trasferimento.

d. immettere il seguente comando sia su node1 che su node2 e registrare i volumi offline su entrambi i nodi:

```
volume show -node node_name -state offline
```

Dopo l'aggiornamento, eseguire di nuovo il comando e confrontare l'output con l'output in questa fase per verificare se altri volumi sono andati offline.

20. Immettere i seguenti comandi per verificare se sono configurati gruppi di interfacce o VLAN su node1 o node2:

```
network port ifgrp show

network port vlan show
```

Annotare se i gruppi di interfacce o le VLAN sono configurati su node1 o node2; tali informazioni sono necessarie nella fase successiva e successiva della procedura.

21. Completare i seguenti passaggi secondari su node1 e node2 per confermare che le porte fisiche possono

essere mappate correttamente più avanti nella procedura:

a. Immettere il seguente comando per verificare la presenza di gruppi di failover sul nodo diversi da `clusterwide`:

   `network interface failover-groups show`

   I gruppi di failover sono insiemi di porte di rete presenti nel sistema. Poiché l'aggiornamento dell'hardware del controller può modificare la posizione delle porte fisiche, i gruppi di failover possono essere modificati inavvertitamente durante l'aggiornamento.

   Il sistema visualizza i gruppi di failover sul nodo, come illustrato nell'esempio seguente:

```
cluster::> network interface failover-groups show

Vserver              Group              Targets
-------------------- ------------------ ----------
Cluster              Cluster            node1:e0a, node1:e0b
                                        node2:e0a, node2:e0b

fg_6210_e0c          Default            node1:e0c, node1:e0d
                                        node1:e0e, node2:e0c
                                        node2:e0d, node2:e0e

2 entries were displayed.
```

b. Se sono presenti gruppi di failover diversi da `clusterwide`, registrare i nomi dei gruppi di failover e le porte che appartengono ai gruppi di failover.

c. Immettere il seguente comando per verificare se nel nodo sono configurate VLAN:

   `network port vlan show -node *node_name*`

   Le VLAN sono configurate su porte fisiche. Se le porte fisiche cambiano, sarà necessario ricreare le VLAN in un secondo momento della procedura.

   Il sistema visualizza le VLAN configurate sul nodo, come illustrato nell'esempio seguente:

```
cluster::> network port vlan show

Network Network
Node    VLAN Name Port    VLAN ID MAC Address
------  --------- ------- ------- ------------------
node1   e1b-70    e1b     70      00:15:17:76:7b:69
```

a. Se nel nodo sono configurate VLAN, prendere nota di ogni associazione di porte di rete e ID VLAN.

22. Eseguire una delle seguenti operazioni:

Se i gruppi di interfacce o LE VLAN sono…	Quindi…
On node1 o node2	Completo Fase 23 e. Fase 24.
Non su node1 o node2	Passare a. Fase 24.

23. se non si sa se node1 e node2 si trovano in un ambiente SAN o non SAN, immettere il seguente comando ed esaminarne l'output:

    `network interface show -vserver vserver_name -data-protocol iscsi|fcp`

    Se non sono configurati né iSCSI né FC per SVM, il comando visualizza un messaggio simile all'esempio seguente:

    ```
    cluster::> network interface show -vserver Vserver8970 -data-protocol
    iscsi|fcp
    There are no entries matching your query.
    ```

    È possibile verificare che il nodo si trovi in un ambiente NAS utilizzando `network interface show` con il `-data-protocol nfs|cifs` parametri.

    Se iSCSI o FC sono configurati per SVM, il comando visualizza un messaggio simile all'esempio seguente:

    ```
    cluster::> network interface show -vserver vs1 -data-protocol iscsi|fcp

             Logical    Status     Network            Current  Current Is
    Vserver  Interface  Admin/Oper Address/Mask       Node     Port    Home
    -------- ---------- ---------- ------------------ -------- ------- ----
    vs1      vs1_lif1   up/down    172.17.176.20/24   node1    0d      true
    ```

24. verificare che tutti i nodi del cluster siano in quorum completando le seguenti fasi secondarie:

    a. Immettere il livello di privilegio avanzato:

       `set -privilege advanced`

       Il sistema visualizza il seguente messaggio:

       ```
       Warning: These advanced commands are potentially dangerous; use them
       only when directed to do so by NetApp personnel.
       Do you wish to continue? (y or n):
       ```

    b. Invio `y`.

    c. Verificare lo stato del servizio cluster nel kernel, una volta per ogni nodo:

       `cluster kernel-service show`

Il sistema visualizza un messaggio simile al seguente esempio:

```
cluster::*> cluster kernel-service show

Master        Cluster       Quorum        Availability  Operational
Node          Node          Status        Status        Status
------------- ------------- ------------- ------------- -------------
node1         node1         in-quorum     true          operational
              node2         in-quorum     true          operational

2 entries were displayed.
```

+
I nodi di un cluster sono in quorum quando una semplice maggioranza di nodi è in buone condizioni e può comunicare tra loro. Per ulteriori informazioni, fare riferimento a. "Riferimenti" Per collegarsi al *System Administration Reference*.

a. Tornare al livello di privilegi amministrativi:

   ```
   set -privilege admin
   ```

25. Eseguire una delle seguenti operazioni:

Se il cluster…	**Quindi…**
HA UNA SAN configurata	Passare a. Fase 26.
NON ha SAN configurato	Passare a. Fase 29.

26. verificare che vi siano LIF SAN su node1 e node2 per ogni SVM che ha UN servizio SAN iSCSI o FC abilitato immettendo il seguente comando ed esaminandone l'output:

    ```
    network interface show -data-protocol iscsi|fcp -home-node node_name
    ```

    Il comando visualizza le informazioni LIF SAN per node1 e node2. Gli esempi seguenti mostrano lo stato nella colonna Status Admin/Oper come up/up, indicando che SAN iSCSI e il servizio FC sono abilitati:

```
cluster::> network interface show -data-protocol iscsi|fcp
            Logical    Status     Network                  Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask             Node
Port    Home
----------- ---------- ---------- ------------------       ---------
------- ----
a_vs_iscsi  data1      up/up      10.228.32.190/21         node1     e0a
true
            data2      up/up      10.228.32.192/21         node2     e0a
true

b_vs_fcp    data1      up/up      20:09:00:a0:98:19:9f:b0  node1     0c
true
            data2      up/up      20:0a:00:a0:98:19:9f:b0  node2     0c
true

c_vs_iscsi_fcp data1   up/up      20:0d:00:a0:98:19:9f:b0  node2     0c
true
            data2      up/up      20:0e:00:a0:98:19:9f:b0  node2     0c
true
            data3      up/up      10.228.34.190/21         node2     e0b
true
            data4      up/up      10.228.34.192/21         node2     e0b
true
```

In alternativa, è possibile visualizzare informazioni LIF più dettagliate immettendo il seguente comando:

`network interface show -instance -data-protocol iscsi|fcp`

27. Acquisire la configurazione predefinita di qualsiasi porta FC sui nodi originali immettendo il seguente comando e registrando l'output dei sistemi:

    `ucadmin show`

    Il comando visualizza le informazioni su tutte le porte FC del cluster, come illustrato nell'esempio seguente:

```
cluster::> ucadmin show

                Current Current   Pending Pending   Admin
Node    Adapter Mode    Type      Mode    Type      Status
------- ------- ------- --------- ------- --------- -----------
node1   0a      fc      initiator -       -         online
node1   0b      fc      initiator -       -         online
node1   0c      fc      initiator -       -         online
node1   0d      fc      initiator -       -         online
node2   0a      fc      initiator -       -         online
node2   0b      fc      initiator -       -         online
node2   0c      fc      initiator -       -         online
node2   0d      fc      initiator -       -         online
8 entries were displayed.
```

È possibile utilizzare le informazioni dopo l'aggiornamento per impostare la configurazione delle porte FC sui nuovi nodi.

28. Completare i seguenti sotto-passaggi:

    a. Immettere il seguente comando su uno dei nodi originali e registrare l'output:

       `service-processor show -node * -instance`

    Il sistema visualizza informazioni dettagliate sull'SP su entrambi i nodi.

    a. Verificare che lo stato SP sia `online`.
    b. Verificare che la rete SP sia configurata.
    c. Registrare l'indirizzo IP e altre informazioni sull'SP.

       È possibile riutilizzare i parametri di rete dei dispositivi di gestione remota, in questo caso gli SP, dal sistema originale per gli SP sui nuovi nodi. Per informazioni dettagliate sull'SP, fare riferimento a. "Riferimenti" Per collegarsi al *riferimento per l'amministrazione del sistema* e ai comandi di *ONTAP 9: Riferimento pagina manuale*.

29. Se si desidera che i nuovi nodi abbiano le stesse funzionalità con licenza dei nodi originali, immettere il seguente comando per visualizzare le licenze del cluster sul sistema originale:

    `system license show -owner *`

    L'esempio seguente mostra le licenze del sito per il cluster1:

```
system license show -owner *
Serial Number: 1-80-000013
Owner: cluster1

Package           Type    Description           Expiration
----------------- ------- --------------------- -----------
Base              site    Cluster Base License  -
NFS               site    NFS License           -
CIFS              site    CIFS License          -
SnapMirror        site    SnapMirror License    -
FlexClone         site    FlexClone License     -
SnapVault         site    SnapVault License     -
6 entries were displayed.
```

30. Ottenere nuove chiavi di licenza per i nuovi nodi presso il *NetApp Support Site*. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp*.

    Se il sito non dispone delle chiavi di licenza necessarie, contattare il rappresentante commerciale NetApp.

31. Verificare se il sistema originale ha abilitato AutoSupport immettendo il seguente comando su ciascun nodo ed esaminandone l'output:

    `system node autosupport show -node node1,node2`

    L'output del comando indica se AutoSupport è attivato, come illustrato nell'esempio seguente:

```
cluster::> system node autosupport show -node node1,node2

Node              State     From          To                Mail Hosts
----------------- --------- ------------- ----------------  ----------
node1             enable    Postmaster    admin@netapp.com  mailhost

node2             enable    Postmaster    -                 mailhost
2 entries were displayed.
```

32. Eseguire una delle seguenti operazioni:

Se il sistema originale…	Quindi…
AutoSupport attivato…	Passare a. Fase 34.

Se il sistema originale…	Quindi…
AutoSupport non è abilitato…	Abilitare AutoSupport seguendo le istruzioni contenute nella sezione *riferimento per l'amministrazione del sistema*. (Fare riferimento a. "Riferimenti" Per collegarsi al *System Administration Reference*.) **Nota:** AutoSupport è attivato per impostazione predefinita quando si configura il sistema di storage per la prima volta. Sebbene sia possibile disattivare AutoSupport in qualsiasi momento, è necessario lasciarlo attivato. L'abilitazione di AutoSupport consente di identificare in modo significativo i problemi e le soluzioni in caso di problemi nel sistema storage.

33. verificare che AutoSupport sia configurato con i dettagli corretti dell'host di posta e gli ID di posta elettronica del destinatario immettendo il seguente comando su entrambi i nodi originali ed esaminando l'output:

```
system node autosupport show -node node_name -instance
```

Per informazioni dettagliate su AutoSupport, fare riferimento a. "Riferimenti" Per collegarsi al *riferimento per l'amministrazione del sistema* e ai comandi di *ONTAP 9: Riferimento pagina manuale*.

34. Invia un messaggio AutoSupport a NetApp per node1 immettendo il seguente comando:

```
system node autosupport invoke -node node1 -type all -message "Upgrading node1
from platform_old to platform_new"
```

> Non inviare un messaggio AutoSupport a NetApp per node2 a questo punto; lo si esegue più avanti nella procedura.

35. verificare che il messaggio AutoSupport sia stato inviato immettendo il seguente comando ed esaminandone l'output:

```
system node autosupport show -node node1 -instance
```

I campi `Last Subject Sent:` e. `Last Time Sent:` contiene il titolo dell'ultimo messaggio inviato e l'ora in cui il messaggio è stato inviato.

36. 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)

> Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha.
>
> È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

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

Gestire le chiavi di autenticazione utilizzando Onboard Key Manager

È possibile utilizzare Onboard Key Manager (OKM) per gestire le chiavi di autenticazione. 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

Prima di avviare il sistema dalla rete, è necessario verificare che tutte le relazioni SnapMirror siano state rinunciate. 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 `Transferring`, è necessario interrompere questi trasferimenti: `snapmirror abort -destination-vserver` *`vserver name`*

   L'interruzione non riesce se la relazione SnapMirror non si trova in `Transferring` stato.

2. Interrompere tutte le relazioni tra il cluster:

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

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. Durante la preparazione per il netboot, è necessario inserire una copia dell'immagine di boot di ONTAP 9 su un server Web a cui il sistema può accedere.

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.

Tuttavia, non è necessario eseguire il netboot dei controller se è installata la stessa versione di ONTAP 9 installata sui controller originali. In tal caso, saltare questa sezione e passare a. "Fase 3: Installazione e boot node3".

Fasi

1. accedere al sito di supporto NetApp per scaricare i file utilizzati per eseguire il netboot 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.

Per…	Quindi…

Sistemi della serie FAS/AFF8000	Estrarre il contenuto di `<ontap_version>_image.tgz` file nella directory di destinazione:
	
	`tar -zxvf <ontap_version>_image.tgz`
	
	Se si sta estraendo il contenuto su Windows, utilizzare 7-zip o WinRAR per estrarre l'immagine di netboot.
	
	L'elenco delle directory deve contenere una cartella netboot con un file kernel:
	
	`netboot/kernel`

Tutti gli altri sistemi	L'elenco delle directory deve contenere il seguente file: `<ontap_version>_image.tgz`NOTA: Non è necessario estrarre il contenuto di `<ontap_version>_image.tgz` file.

Utilizzerai le informazioni nelle directory in "Fase 3" .

Fase 2. Spostare e dismettere il node1

Spostare gli aggregati non root dal nodo 1 al nodo 2

Prima di poter sostituire il nodo 1 con il nodo 3, è necessario spostare gli aggregati non root da node1 a node2 utilizzando il comando di trasferimento degli aggregati di storage e verificando quindi il trasferimento.

Fasi

1. Riposizionare gli aggregati non radice completando i seguenti sottopassaggi:
   a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

b. Immettere il seguente comando:

```
storage aggregate relocation start -node node1 -destination node2 -aggregate
-list * -ndo-controller-upgrade true
```

c. Quando richiesto, immettere `y`.

Il trasferimento avverrà in background. La riposizionamento di un aggregato potrebbe richiedere da pochi secondi a un paio di minuti. Il tempo include sia le parti di fuori servizio del client che quelle di non fuori servizio. Il comando non ricolloca nessun aggregato offline o limitato.

d. Tornare al livello admin immettendo il seguente comando:

```
set -privilege admin
```

2. Controllare lo stato di rilocazione immettendo il seguente comando sul nodo 1:

```
storage aggregate relocation show -node node1
```

Viene visualizzato l'output `Done` per un aggregato dopo che è stato trasferito.

Attendere che tutti gli aggregati non root di proprietà di node1 siano stati riallocati in node2 prima di procedere con la fase successiva.

3. Eseguire una delle seguenti operazioni:

In caso di trasferimento…	Quindi…
Di tutti gli aggregati ha successo	Passare a. Fase 4.

In caso di trasferimento…	Quindi…

Di qualsiasi aggregato non funziona o viene vetoato	a. Controllare i registri EMS per l'azione correttiva.
	b. Eseguire l'azione correttiva.
	c. Spostare eventuali aggregati guasti o vetoed:
	`storage aggregate relocation start -node node1 - destination node2 -aggregate-list * -ndo -controller-upgrade true`
	d. Quando richiesto, immettere `y`.
	e. Tornare al livello di amministrazione:
	`set -privilege admin`Se necessario, è possibile forzare il trasferimento utilizzando uno dei seguenti metodi:
	◦ Ignora i controlli di veto:
	`storage aggregate relocation start -override -vetoes true -ndo-controller-upgrade`
	◦ Ignora controlli destinazione:
	`storage aggregate relocation start -override -destination-checks true -ndo-controller -upgrade`
	Fare riferimento a. "Riferimenti" Per collegarsi alla gestione di *dischi e aggregati con il contenuto CLI* e i comandi di *ONTAP 9: Manuale di riferimento pagina* per ulteriori informazioni sui comandi di spostamento degli aggregati di storage.

4.] verifica che tutti gli aggregati non root siano online e che il loro stato sia 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`*

5. Verificare che tutti i volumi siano online sul nodo 2 immettendo 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.

6. Immettere il seguente comando su node2:

   `storage failover show -node` *`node2`*

   L'output dovrebbe visualizzare il seguente messaggio:

   ```
   Node owns partner's aggregates as part of the nondisruptive controller
   upgrade procedure.
   ```

7. Verificare che node1 non possiedi aggregati non root online:

   `storage aggregate show -owner-name` *`node1`* `-ha-policy sfo -state online`

   L'output non dovrebbe visualizzare alcun aggregato non root online, che è già stato trasferito in node2.

Spostare le LIF dei dati NAS di proprietà del node1 in node2

Prima di poter sostituire il nodo 1 con il nodo 3, è necessario spostare le LIF dati NAS di proprietà del nodo 1 in node2 se si dispone di un cluster a due nodi o in un terzo nodo se il cluster ha più di due nodi. Il metodo utilizzato dipende dalla configurazione del cluster per NAS o SAN.

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. Dopo aver portato il nodo 3 online, è necessario verificare che i file LIF siano integri e posizionati su porte appropriate.

Fasi

1. Elencare tutte le LIF dei dati NAS ospitate sul nodo 1 immettendo il seguente comando e acquisendo l'output:

   `network interface show -data-protocol nfs|cifs -curr-node node1`

```
 cluster::> network interface show -data-protocol nfs|cifs -curr-node
node1

          Logical     Status      Network             Current   Current
Is
 Vserver  Interface   Admin/Oper  Address/Mask        Node      Port
Home
 -------- ----------  ----------  ------------------  --------- -------
----
 vs0
          a0a         up/down     10.63.0.53/24       node1     a0a
true
          data1       up/up       10.63.0.50/18       node1     e0c
true
          rads1       up/up       10.63.0.51/18       node1     e1a
true
          rads2       up/down     10.63.0.52/24       node1     e1b
true
 vs1
          lif1        up/up       192.17.176.120/24   node1     e0c
true
          lif2        up/up       172.17.176.121/24   node1     e1a
true
```

2. Modifica le impostazioni di ripristino automatico di tutte le LIF su node1 e node2:

   `network interface modify -vserver Vserver_name -lif LIF_name -auto-revert false`

3. eseguire i seguenti passaggi per migrare qualsiasi file LIF dati NAS ospitati su gruppi di interfacce e VLAN sul node1:

   a. Migrate le LIF ospitate su qualsiasi gruppo di interfacce e le VLAN sul node1 a una porta sul node2 in grado di ospitare LIF sulla stessa rete dei gruppi di interfacce immettendo il seguente comando, una volta per ogni LIF:

   ```
   network interface migrate -vserver Vserver_name -lif LIF_name -destination
   -node node2 –destination-port netport|ifgrp
   ```

   b. Modificare la porta home e il nodo home di LIF e VLAN in Sotto-fase A. Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

   ```
   network interface modify -vserver Vserver_name -lif LIF_name -home-node
   node2 - home-port netport|ifgrp
   ```

4. eseguire una delle seguenti operazioni:

Se il cluster è configurato per…	Quindi…
NAS	Completo Fase 5 attraverso Fase 8.
SAN	Disattivare tutte le LIF SAN sul nodo per disattivarle per l'aggiornamento: `network interface modify -vserver *Vserver-name* -lif *LIF_name* -home-node *node_to_upgrade* -home-port _netport

5. Migrare i LIF dei dati NAS da node1 a node2 immettendo il seguente comando, una volta per ciascun LIF dei dati:

   ```
   network interface migrate -vserver Vserver-name -lif LIF_name -destination
   -node node2 -destination-port data_port
   ```

6. immettere il seguente comando ed esaminare l'output per verificare che i file LIF siano stati spostati nelle porte corrette e che i file LIF abbiano lo stato di up immettendo il seguente comando su entrambi i nodi ed esaminando l'output:

   ```
   network interface show -curr-node node2 -data-protocol nfs|cifs
   ```

7. Modifica del nodo principale delle LIF migrate:

   ```
   network interface modify -vserver Vserver-name -lif LIF_name -home-node node2
   -home-port port_name
   ```

8. verificare se LIF sta utilizzando la porta come porta principale o corrente. Se la porta non è domestica o corrente, passare a. Fase 9:

   ```
   network interface show -home-node node2 -home-port port_name

   network interface show -curr-node node_name -curr-port port_name
   ```

9. se le LIF utilizzano la porta come porta home o porta corrente, modificare la LIF in modo che utilizzi una porta diversa:

   ```
   network interface migrate -vserver Vserver-name -lif LIF_name
   ```

```
-destination-node node_name -destination-port port_name

network interface modify -vserver Vserver-name -lif LIF_name -home-node
node_name -home-port port_name
```

10. se i LIF non sono attivi, imposta lo stato amministrativo dei LIF su "up" immettendo il seguente comando, una volta per ciascun LIF:

```
network interface modify -vserver Vserver-name -lif LIF_name -home-node
nodename -status-admin up
```

> Per le configurazioni MetroCluster, potrebbe non essere possibile modificare il dominio di trasmissione di una porta perché è associata a una porta che ospita la LIF di una macchina virtuale di storage di destinazione (SVM). Immettere il seguente comando dalla SVM di origine corrispondente sul sito remoto per riallocare la LIF di destinazione su una porta appropriata:
> `metrocluster vserver resync -vserver Vserver_name`

11. immettere il seguente comando ed esaminarne l'output per verificare che non vi siano LIF di dati rimasti sul node1:

```
network interface show -curr-node node1 -role data
```

Registrare le informazioni del nodo 1

Prima di spegnere e dismettere il node1, è necessario registrare le informazioni relative alla rete del cluster, alla gestione e alle porte FC, nonché l'ID del sistema NVRAM. Queste informazioni sono necessarie più avanti nella procedura quando si esegue il mapping del nodo 1 al nodo 3 e si riassegnano i dischi.

Fasi

1. immettere il seguente comando e acquisirne l'output:

```
network route show
```

Il sistema visualizza un output simile al seguente esempio:

```
cluster::> network route show

Vserver         Destination    Gateway      Metric
 -------------- -------------- ----------- -------
 iscsi vserver  0.0.0.0/0       10.10.50.1  20
 node1          0.0.0.0/0       10.10.20.1  10
 ....
 node2          0.0.0.0/0       192.169.1.1 20
```

2. Immettere il seguente comando e acquisire l'output:

```
vserver services name-service dns show
```

Il sistema visualizza un output simile al seguente esempio:

```
 cluster::> vserver services name-service dns show
                                                                 Name
 Vserver        State     Domains                               Servers
 -------------- --------- ------------------------------------
---------------
 node 1 2       enabled   alpha.beta.gamma.netapp.com
10.10.60.10,

10.10.60.20
 vs_base1       enabled   alpha.beta.gamma.netapp.com,
10.10.60.10,
                          beta.gamma.netapp.com,
10.10.60.20
 ...
 ...
 vs peer1        enabled  alpha.beta.gamma.netapp.com,
10.10.60.10,
                          gamma.netapp.com
10.10.60.20
```

3. trova la rete del cluster e le porte di gestione dei nodi sul node1 immettendo il seguente comando su uno dei controller:

   `network interface show -curr-node` *`node1`* `-role cluster,intercluster,node-mgmt,cluster-mgmt`

   Il sistema visualizza le LIF di cluster, intercluster, gestione dei nodi e gestione dei cluster per il nodo del cluster, come illustrato nell'esempio seguente:

```
 cluster::> network interface show -curr-node <node1>
            -role cluster,intercluster,node-mgmt,cluster-mgmt

              Logical       Status     Network            Current
Current Is
  Vserver     Interface     Admin/Oper Address/Mask       Node     Port
Home
  ----------- ------------- ---------- ------------------ --------
------- ----
  vserver1
              cluster mgmt   up/up     192.168.x.xxx/24   node1    e0c
true
  node1
              intercluster   up/up     192.168.x.xxx/24   node1    e0e
true
              clus1          up/up     169.254.xx.xx/24   node1    e0a
true
              clus2          up/up     169.254.xx.xx/24   node1    e0b
true
              mgmt1          up/up     192.168.x.xxx/24   node1    e0c
true
 5 entries were displayed.
```

Il sistema potrebbe non disporre di LIF intercluster.

4. Acquisire le informazioni nell'output del comando in Fase 3 da utilizzare nella sezione "Mappare le porte dal nodo 1 al nodo 3".

   Le informazioni di output sono necessarie per mappare le nuove porte del controller alle vecchie porte del controller.

5. Immettere il seguente comando su node1:

   `network port show -node node1 -type physical`

   Il sistema visualizza le porte fisiche sul nodo, come mostrato nell'esempio seguente:

```
 sti8080mcc-htp-008::> network port show -node sti8080mcc-htp-008 -type
physical

 Node: sti8080mcc-htp-008

                                                                        Ignore
                                                  Speed(Mbps)  Health   Health
 Port   IPspace  Broadcast Domain Link MTU   Admin/Oper   Status   Status
 ----   -------  ---------------- ---- ----  -----------  -------
-------
 e0M    Default  Mgmt             up   1500  auto/1000    healthy  false
 e0a    Default  Default          up   9000  auto/10000   healthy  false
 e0b    Default  -                up   9000  auto/10000   healthy  false
 e0c    Default  -                down 9000  auto/-       -        false
 e0d    Default  -                down 9000  auto/-       -        false
 e0e    Cluster  Cluster          up   9000  auto/10000   healthy  false
 e0f    Default  -                up   9000  auto/10000   healthy  false
 e0g    Cluster  Cluster          up   9000  auto/10000   healthy  false
 e0h    Default  Default          up   9000  auto/10000   healthy  false
 9 entries were displayed.
```

6. Registrare le porte e i relativi domini di trasmissione.

   I domini di broadcast dovranno essere mappati alle nuove porte sul nuovo controller più avanti nella procedura.

7. Immettere il seguente comando su node1:

   `network fcp adapter show -node *node1*`

   Il sistema visualizza le porte FC sul nodo, come mostrato nell'esempio seguente:

```
 cluster::> fcp adapter show -node <node1>
                      Connection  Host
 Node         Adapter Established Port Address
 ------------ ------- ----------- ------------
 node1
               0a     ptp         11400
 node1
               0c     ptp         11700
 node1
               6a     loop        0
 node1
               6b     loop        0
 4 entries were displayed.
```

8. Registrare le porte.

   Le informazioni di output sono necessarie per mappare le nuove porte FC sul nuovo controller più avanti nella procedura.

9. In caso contrario, controllare se ci sono gruppi di interfacce o VLAN configurati sul nodo 1 immettendo i seguenti comandi:

   ```
   network port ifgrp show

   network port vlan show
   ```

   Verranno utilizzate le informazioni contenute nella sezione "Mappare le porte dal nodo 1 al nodo 3".

10. Eseguire una delle seguenti operazioni:

Se…	Quindi…
Il numero dell'ID del sistema NVRAM è stato registrato nella sezione "Preparare i nodi per l'aggiornamento".	Passare alla sezione successiva, "Ritirare il node1".
Il numero dell'ID del sistema NVRAM non è stato registrato nella sezione "Preparare i nodi per l'aggiornamento"	Completo Fase 11 e. Fase 12 quindi passare a. "Ritirare il node1".

11. immettere il seguente comando su uno dei controller:

    ```
    system node show -instance -node node1
    ```

    Il sistema visualizza le informazioni relative al nodo 1 come mostrato nell'esempio seguente:

    ```
    cluster::> system node show -instance -node <node1>
                                Node: node1
                               Owner:
                            Location: GDl
                               Model: FAS6240
                       Serial Number: 700000484678
                           Asset Tag: -
                              Uptime: 20 days 00:07
                     NVRAM System ID: 1873757983
                           System ID: 1873757983
                              Vendor: NetApp
                              Health: true
                         Eligibility: true
    ```

12. registrare il numero di ID del sistema NVRAM da utilizzare nella sezione "Installazione e boot node3".

Ritirare il node1

Per dismettere il node1, è necessario disattivare la coppia ha con node2, chiudere il node1 correttamente e rimuoverlo dal rack o dallo chassis.

Fasi

1. Verificare il numero di nodi nel cluster:

   `cluster show`

   Il sistema visualizza i nodi nel cluster, come illustrato nell'esempio seguente:

   ```
   cluster::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node1                 true    true
   node2                 true    true
   2 entries were displayed.
   ```

2. Disattiva il failover dello storage, a seconda dei casi:

Se il cluster è…	Quindi…

Un cluster a due nodi	a. Disattivare la disponibilità elevata del cluster immettendo il seguente comando su uno dei nodi:
	`cluster ha modify -configured false`
	a. Disattivare il failover dello storage:
	`storage failover modify -node node1 -enabled false`

Un cluster con più di due nodi	Disattivare il failover dello storage: `storage failover modify -node node1 -enabled false`

   Se non si disattiva il failover dello storage, può verificarsi un errore di upgrade del controller che può interrompere l'accesso ai dati e causare la perdita di dati.

3. Verificare che il failover dello storage sia stato disattivato:

   `storage failover show`

   L'esempio seguente mostra l'output di `storage failover show` comando quando il failover dello storage è stato disattivato per un nodo:

```
 cluster::> storage failover show
                                 Takeover
 Node           Partner         Possible State Description
 -------------- -------------- --------
-------------------------------------
 node1          node2          false    Connected to node2, Takeover
                                        is not possible: Storage
failover is
                                        disabled

 node2          node1          false    Node owns partner's aggregates
as part
                                        of the nondisruptive controller
upgrade
                                        procedure. Takeover is not
possible:
                                        Storage failover is disabled
 2 entries were displayed.
```

4. Verificare lo stato LIF dei dati:

   `network interface show -role data -curr-node` *`node2`* `-home-node` *`node1`*

   Controllare nella colonna **Status Admin/Oper** (Amministrazione stato/Oper*) se le LIF non sono attive. Se uno qualsiasi dei LIF è inattivo, consultare il "Troubleshoot" sezione.

5. Eseguire una delle seguenti operazioni:

Se il cluster è…	Quindi…
Un cluster a due nodi	Passare a. Fase 6.
Un cluster con più di due nodi	Passare a. Fase 8.

6. Accedi al livello di privilegio avanzato su uno dei nodi:

   `set -privilege advanced`

7. verificare che il cluster ha sia stato disattivato:

   `cluster ha show`

   Il sistema visualizza il seguente messaggio:

```
High Availability Configured: false
```

   Se il cluster ha non è stato disattivato, ripetere Fase 2.

8. Controlla se il node1 attualmente contiene epsilon:

   `cluster show`

   Poiché esiste la possibilità di un legame in un cluster con un numero pari di nodi, un nodo ha un peso di voto frazionario aggiuntivo chiamato epsilon. Fare riferimento a. "Riferimenti" Per ulteriori informazioni, fare riferimento a *System Administration Reference*.

   > Se si dispone di un cluster a quattro nodi, epsilon potrebbe trovarsi su un nodo di una coppia ha diversa nel cluster.
   >
   > Se si sta aggiornando una coppia HA in un cluster con più coppie HA, è necessario spostare epsilon sul nodo di una coppia HA che non è in fase di aggiornamento del controller. Ad esempio, se si sta aggiornando NodeA/NodeB in un cluster con la configurazione della coppia ha NodeA/NodeB e NODEC/NODed, è necessario spostare epsilon in NODEC o NODed.

   Il seguente esempio mostra che node1 contiene epsilon:

   ```
   cluster::*> cluster show

   Node                  Health  Eligibility  Epsilon
   --------------------- ------- ------------ ------------
   node1                 true    true         true
   node2                 true    true         false
   ```

9. Se node1 contiene epsilon, contrassegnare epsilon `false` sul nodo in modo che possa essere trasferito al nodo 2:

   `cluster modify -node node1 -epsilon false`

10. Trasferire epsilon al nodo 2 contrassegnando epsilon `true` al nodo 2:

    `cluster modify -node node2 -epsilon true`

11. Verificare che si sia verificata la modifica in node2:

    `cluster show`

    ```
    cluster::*> cluster show
    Node                  Health  Eligibility  Epsilon
    --------------------- ------- ------------ ------------
    node1                 true    true         false
    node2                 true    true         true
    ```

    L'epsilon per il node2 dovrebbe ora essere vero e l'epsilon per il node1 dovrebbe essere falso.

12. Verificare se il setup è un cluster senza switch a due nodi:

```
network options switchless-cluster show
```

```
cluster::*> network options switchless-cluster show

Enable Switchless Cluster: false/true
```

Il valore di questo comando deve corrispondere allo stato fisico del sistema.

13. Tornare al livello di amministrazione:

```
set -privilege admin
```

14. Arrestare il node1 dal prompt node1:

```
system node halt -node node1
```

> Se il nodo 1 si trova nello stesso chassis del nodo 2, non spegnere lo chassis utilizzando l'interruttore di alimentazione o tirando il cavo di alimentazione. In tal caso, il nodo 2, che fornisce i dati, non funzionerà.

15. Quando il sistema richiede di confermare che si desidera arrestare il sistema, immettere `y`.

    Il nodo si arresta al prompt dell'ambiente di boot.

16. Quando node1 visualizza il prompt dell'ambiente di avvio, rimuoverlo dallo chassis o dal rack.

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

Fase 3. Installazione e boot node3

Installazione e boot node3

È necessario installare node3 nel rack, trasferire le connessioni del node1 al node3, fare il boot node3 e installare ONTAP. È inoltre necessario riassegnare i dischi spare di node1, i dischi appartenenti al volume root e gli aggregati non root non ricollocati in node2 in precedenza.

A proposito di questa attività

È necessario eseguire l'avvio di rete del nodo 3 se non ha la stessa versione di ONTAP 9 installata sul nodo 1. 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 avvii del sistema. Vedere "Preparatevi per il netboot".

Tuttavia, non è necessario eseguire l'avvio di rete di node3 se è installata la stessa versione o una versione successiva di ONTAP 9 su node1.

- Per un aggiornamento del controller AFF A800 o AFF C800 , è necessario assicurarsi che tutte le unità nello chassis siano saldamente posizionate contro il midplane prima di rimuovere node1. Per maggiori informazioni, vedere "Sostituire i moduli controller AFF A800 o AFF C800".
- Se si sta aggiornando un sistema con dischi di archiviazione, è necessario completare l'intera sezione e quindi andare a "Configurare le porte FC sul nodo 3" E "Controllare e configurare le porte UTA/UTA2 sul nodo 3" , immettendo comandi al prompt del cluster.

Fasi

1. assicurarsi di disporre di spazio rack per node3.

   Se node1 e node2 si trovano in uno chassis separato, è possibile inserire node3 nella stessa posizione rack del node1. Tuttavia, se il nodo 1 si trovava nello stesso chassis con il nodo 2, è necessario inserire il nodo 3 nel proprio spazio rack, preferibilmente vicino alla posizione del nodo 1.

2. [[fase 2]]installare il nodo 3 nel rack seguendo le *istruzioni di installazione e configurazione* relative al modello di nodo in uso.

   Se si esegue l'aggiornamento a un sistema con entrambi i nodi nello stesso chassis, installare node4 e node3 nello chassis. Se non si installano entrambi i nodi nello stesso chassis, quando si avvia node3, questo si comporta come se fosse in una configurazione a doppio chassis, mentre quando si avvia node4, l'interconnessione tra i nodi non si attiva.

3. cavo node3, spostamento delle connessioni da node1 a node3.

   I seguenti riferimenti consentono di stabilire i collegamenti dei cavi corretti. Passare a. "Riferimenti" per collegarli.

   - *Istruzioni di installazione e configurazione* per la piattaforma node3
   - La procedura di shelf di dischi appropriata
   - La documentazione *ha Pair Management*

   Collegare i seguenti cavi:

   - Console (porta di gestione remota)
   - Porte del cluster
   - Porte dati
   - Porte di gestione di cluster e nodi
   - Storage
   - Configurazioni SAN: Porte switch FC e Ethernet iSCSI

   Potrebbe non essere necessario spostare la scheda di interconnessione o la connessione del cavo di interconnessione del cluster dal nodo 1 al nodo 3, poiché la maggior parte dei modelli di piattaforma dispone di un modello di scheda di interconnessione unico. Per la configurazione MetroCluster, è necessario spostare le connessioni del cavo FC-VI dal nodo 1 al nodo 3. Se il nuovo host non dispone di una scheda FC-VI, potrebbe essere necessario spostare la scheda FC-VI.

4. accendere il computer su node3, quindi interrompere il processo di boot premendo Ctrl-C sul terminale

della console per accedere al prompt dell'ambiente di boot.

Se si sta eseguendo l'aggiornamento a un sistema con entrambi i nodi nello stesso chassis, anche node4 viene riavviato. Tuttavia, è possibile ignorare il node4 boot fino a tardi.

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.

   Non ignorare il ritardo; se non si lascia caricare la batteria, si potrebbe verificare una perdita di dati.

6. Al prompt della modalità di manutenzione, immettere il seguente comando:

   ```
   halt
   ```

   Il sistema si arresta al prompt dell'ambiente di avvio.

7. Eseguire una delle seguenti operazioni:

Se il sistema a cui si esegue l'aggiornamento si trova in una…	Quindi…
Configurazione a doppio chassis (con controller in chassis diversi)	Vai aFase 8 .

Se il sistema a cui si esegue l'aggiornamento si trova in una…	Quindi…
Configurazione a unico chassis (con controller nello stesso chassis)	a. Spostare il cavo della console dal nodo 3 al nodo 4. b. 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 avvio. L'alimentazione dovrebbe essere già attiva se entrambi i controller si trovano nello stesso chassis. ⓘ Lasciare node4 al prompt dell'ambiente di boot; si tornerà a node4 in "Installazione e boot node4". c. Se viene visualizzato il messaggio di avviso nella Fase 4, seguire le istruzioni in Fase 5 d. Riportare il cavo della console dal nodo 4 al nodo 3. e. Vai aFase 8 .

8. Configura node3 per ONTAP:

```
set-defaults
```

9. Se sono installate unità NetApp Storage Encryption (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`**

ⓘ Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha.

È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

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 le chiavi di autenticazione utilizzando Onboard Key Manager".

10.] se la versione di ONTAP installata su node3 è uguale o successiva alla versione di ONTAP 9 installata su node1, elencare e riassegnare i dischi al nuovo node3:

`boot_ontap`

> Se questo nuovo nodo è stato utilizzato in qualsiasi altro cluster o coppia ha, è necessario eseguire `wipeconfig` prima di procedere. In caso contrario, potrebbero verificarsi interruzioni del servizio o perdita di dati. Contattare il supporto tecnico se il controller sostitutivo è stato utilizzato in precedenza, in particolare se i controller eseguivano ONTAP in 7-Mode.

11. Premere CTRL-C per visualizzare il menu di avvio.
12. eseguire una delle seguenti operazioni:

Se il sistema che si sta aggiornando…	**Quindi…**
Non ha la versione ONTAP corretta o corrente sul nodo 3	Vai aFase 13 .
Ha la versione corretta o attuale di ONTAP al nodo 3	Vai aFase 18 .

13. Configurare la connessione netboot scegliendo una delle seguenti azioni.

> 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 immettendo il seguente comando al prompt dell'ambiente di boot: `ifconfig e0M -auto`

Se DHCP (Dynamic host Configuration Protocol) è…	Quindi…
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 (Domain Name Service). Se si utilizza questo parametro opzionale, non è necessario un nome di dominio completo nell'URL del server netboot; è necessario solo il nome host del server. Potrebbero essere necessari altri parametri per l'interfaccia. Invio `help ifconfig` al prompt del firmware per ulteriori informazioni.

14. Eseguire netboot sul nodo 3:

Per…	Quindi…
Sistemi della serie FAS/AFF8000	`netboot http://<web_server_ip>/<path_to_webaccessible_directory>/netboot/kernel`
Tutti gli altri sistemi	`netboot http://<web_server_ip>/<path_to_webaccessible_directory>/<ontap_version>_image.tgz`

Il `<path_to_the_web-accessible_directory>` consente di accedere alla posizione in cui è stato scaricato `<ontap_version>_image.tgz` poll "Fase 1" Nella sezione *Prepare for netboot*.

Non interrompere l'avvio.

15. Dal menu di avvio, seleziona prima l'opzione **(7) Installa nuovo software**.

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 essere errata. 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 ONTAP su entrambe le partizioni dell'immagine.

16. Se ti viene chiesto di continuare la procedura, inserisci `y` e quando ti viene richiesto il pacchetto, inserisci il seguente URL:

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

17. Completare i seguenti passaggi secondari:

    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.

18. Seleziona **(5) Avvio in modalità di manutenzione** inserendo `5` , e poi inserisci `y` quando viene richiesto di continuare con l'avvio.

19. prima di continuare, visitare il sito "Impostare la configurazione FC o UTA/UTA2 su node3" Apportare le modifiche necessarie alle porte FC o UTA/UTA2 del nodo.

    Apportare le modifiche consigliate in queste sezioni, riavviare il nodo e passare alla modalità di manutenzione.

20. Trova l'ID di sistema del nodo 3:

    `disk show -a`

    Il sistema visualizza l'ID di sistema del nodo e le informazioni relative ai dischi, come mostrato nell'esempio seguente:

```
 *> disk show -a
 Local System ID: 536881109
 DISK     OWNER                    POOL   SERIAL    HOME          DR
 HOME                                     NUMBER
 -------- -------------            -----  -------- -------------
-------------
 0b.02.23 nst-fas2520-2(536880939) Pool0  KPG2RK6F nst-fas2520-
2(536880939)
 0b.02.13 nst-fas2520-2(536880939) Pool0  KPG3DE4F nst-fas2520-
2(536880939)
 0b.01.13 nst-fas2520-2(536880939) Pool0  PPG4KLAA nst-fas2520-
2(536880939)
 ......
 0a.00.0               (536881109) Pool0  YFKSX6JG
(536881109)
 ......
```

Potrebbe essere visualizzato il messaggio `disk show: No disks match option -a.` dopo aver immesso il comando. Non si tratta di un messaggio di errore, pertanto è possibile continuare con la procedura.

21. Riassegnare i dischi di riserva del nodo 1, tutti i dischi appartenenti alla radice e tutti gli aggregati non radice che non sono stati trasferiti in precedenza al nodo 2 in"Spostare gli aggregati non root dal nodo 1 al nodo 2" .

Inserire il modulo appropriato di `disk reassign` comando basato sulla presenza di dischi condivisi nel sistema:

Se nel sistema sono presenti dischi condivisi, aggregati ibridi o entrambi, è necessario utilizzare il corretto `disk reassign` dalla seguente tabella.

Se il tipo di disco è…	Quindi eseguire il comando…
Con dischi condivisi	`disk reassign -s` *`node1_sysid`* `-d` *`node3_sysid`* `-p` *`node2_sysid`*
Senza dischi condivisi	`disk reassign -s` *`node1_sysid`* `-d` *`node3_sysid`*

Per *`node1_sysid`* utilizzare le informazioni acquisite in "Registrare le informazioni del nodo 1". Per ottenere il valore per *`node3_sysid`*, utilizzare `sysconfig` comando.

Il `-p` l'opzione è richiesta solo in modalità di manutenzione quando sono presenti dischi condivisi.

Il `disk reassign` il comando riassegna solo i dischi per i quali *`node1_sysid`* è il proprietario corrente.

Il sistema visualizza il seguente messaggio:

```
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)?
```

22. Invio `n`.

Il sistema visualizza il seguente messaggio:

```
After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)?
```

23. Invio `y`

Il sistema visualizza il seguente messaggio:

```
Disk ownership will be updated on all disks previously belonging to
Filer with sysid <sysid>.
Do you want to continue (y/n)?
```

24. Invio `y`.

25. se si esegue l'aggiornamento da un sistema con dischi esterni a un sistema che supporta dischi interni ed esterni (ad esempio, sistemi AFF A800), impostare l'aggregato node1 come root per confermare che node3 si avvia dall'aggregato root di node1.

Attenzione: È necessario eseguire le seguenti fasi secondarie nell'ordine esatto indicato; in caso contrario, si potrebbe verificare un'interruzione o addirittura la perdita di dati.

La seguente procedura imposta node3 per l'avvio dall'aggregato root di node1:

a. Controllare le informazioni su RAID, plex e checksum per l'aggregato node1:

```
aggr status -r
```

b. Controllare lo stato dell'aggregato node1:

```
aggr status
```

c. Se necessario, portare online l'aggregato node1:

```
aggr_online root_aggr_from_node1
```

d. Impedire al node3 di avviarsi dal proprio aggregato root originale:

```
aggr offline root_aggr_on_node3
```

e. Impostare l'aggregato root node1 come nuovo aggregato root per node3:

```
aggr options aggr_from_node1 root
```

f. Verificare che l'aggregato root di node3 sia offline e che l'aggregato root per i dischi portati da node1 sia online e impostato su root:

```
aggr status
```

> La mancata esecuzione del passaggio secondario precedente potrebbe causare l'avvio di node3 dall'aggregato root interno, oppure il sistema potrebbe presumere l'esistenza di una nuova configurazione del cluster o richiedere di identificarne una.

Di seguito viene riportato un esempio dell'output del comando:

```
-------------------------------------------------------------
     Aggr State               Status          Options
aggr0_nst_fas8080_15 online   raid_dp, aggr   root, nosnap=on
                              fast zeroed
                              64-bit

  aggr0 offline               raid_dp, aggr   diskroot
                              fast zeroed
                              64-bit
-------------------------------------------------------------
```

26. verificare che il controller e lo chassis siano configurati come `ha`:

```
ha-config show
```

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

```
*> ha-config show
   Chassis HA configuration: ha
   Controller HA configuration: ha
```

I sistemi registrano in una ROM programmabile (PROM) se si trovano in una configurazione a coppia ha o standalone. Lo stato deve essere lo stesso su tutti i componenti all'interno del sistema standalone o della coppia ha.

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
```

Se si dispone di una configurazione MetroCluster, utilizzare i seguenti comandi per modificare il controller e lo chassis:

```
ha-config modify controller mcc

ha-config modify chassis mcc
```

27. distruggere le caselle di posta sul node3:

```
mailbox destroy local
```

La console visualizza il seguente messaggio:

```
Destroying mailboxes forces a node to create new empty mailboxes, which
clears any takeover state, removes all knowledge of out-of-date plexes
of mirrored volumes, and will prevent management services from going
online in 2-node cluster HA configurations. Are you sure you want to
destroy the local mailboxes?
```

28. Invio `y` quando viene richiesto di confermare che si desidera distruggere le caselle postali locali.
29. Esci dalla modalità di manutenzione:

```
halt
```

Il sistema si arresta al prompt dell'ambiente di avvio.

30. al node2, controllare la data, l'ora e il fuso orario del sistema:

```
date
```

31. al node3, controllare la data al prompt dell'ambiente di boot:

```
show date
```

32. se necessario, impostare la data su node3:

```
set date mm/dd/yyyy
```

33. al node3, controllare l'ora al prompt dell'ambiente di boot:

```
show time
```

34. se necessario, impostare l'ora su node3:

```
set time hh:mm:ss
```

35. Verificare che l'ID del sistema partner sia impostato correttamente come indicato inFase 21 con l'opzione -p:

```
printenv partner-sysid
```

36. se necessario, impostare l'ID di sistema del partner su node3:

```
setenv partner-sysid node2_sysid
```

Salvare le impostazioni:

```
saveenv
```

37. accedere al menu di boot al prompt dell'ambiente di boot:

```
boot_ontap menu
```

38. dal menu di avvio, selezionare l'opzione **(6) Aggiorna flash dalla configurazione di backup** immettendo `6` quando richiesto.

Il sistema visualizza il seguente messaggio:

```
This will replace all flash-based configuration with the last backup to
disks. Are you sure you want to continue?:
```

39. Invio `y` quando richiesto.

L'avvio procede normalmente e il sistema chiede di confermare la mancata corrispondenza dell'ID di sistema.

> Il sistema potrebbe riavviarsi due volte prima di visualizzare l'avviso di mancata corrispondenza.

40. confermare la mancata corrispondenza come mostrato nell'esempio seguente:

```
WARNING: System id mismatch. This usually occurs when replacing CF or
NVRAM cards!
Override system id (y|n) ? [n] y
```

Il nodo potrebbe essere sottoposto a un ciclo di riavvio prima dell'avvio normale.

41. Accedi a node3.

Impostare la configurazione FC o UTA/UTA2 su node3

Se node3 dispone di porte FC integrate, porte UTA/UTA2 (onboard Unified target adapter) o una scheda UTA/UTA2, è necessario configurare le impostazioni prima di completare il resto della procedura.

A proposito di questa attività

Potrebbe essere necessario completareConfigurare le porte FC sul nodo 3 OControllare e configurare le porte UTA/UTA2 sul nodo 3 o entrambe le sezioni.

I materiali di marketing NetApp potrebbero utilizzare il termine "UTA2" per fare riferimento agli adattatori e alle porte CNA. Tuttavia, la CLI utilizza il termine "CNA".

Se node3 non dispone di porte FC integrate, porte UTA/UTA2 integrate o una scheda UTA/UTA2 (ad esempio, sistemi AFF e FAS introdotti a partire da ONTAP 9.15.1) e si sta aggiornando un sistema con dischi di archiviazione, è possibile passare alla sezione"Mappare le porte dal nodo 1 al nodo 3" .

Configurare le porte FC sul nodo 3

Se il nodo 3 dispone di porte FC, integrate o su un adattatore FC aggiuntivo, è necessario impostare le configurazioni delle porte sul nodo prima di metterlo in servizio, poiché le porte non sono preconfigurate al momento della spedizione dei sistemi. Se non si configurano le porte, si potrebbe verificare un'interruzione del servizio.

Prima di iniziare

È necessario disporre dei valori delle impostazioni della porta FC da node1 salvati in "Preparare i nodi per l'aggiornamento".

A proposito di questa attività

È possibile saltare questa sezione se il sistema non dispone di configurazioni FC. Se il sistema dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2, configurarle in Controllare e configurare le porte UTA/UTA2 sul nodo 3.

Immettere i comandi in questa sezione al prompt del cluster.

Fasi

1. Visualizza informazioni su tutti gli adattatori di rete FC e convergenti presenti sul sistema.

   ```
   system node hardware unified-connect show
   ```

2. Confronta le impostazioni FC del nodo 3 con le impostazioni acquisite in precedenza dal nodo 1.
3. Esegui una delle seguenti azioni:

Se le impostazioni FC predefinite sui nuovi nodi sono…	Quindi…
Le stesse di quelle che hai catturato sul node1	Vai aFase 9 .
Diverso da quelli che avete catturato sul node1	Vai aFase 4 .

4. Modificare le porte FC sul nodo 3 secondo necessità immettendo uno dei seguenti comandi:
   - Per programmare le porte di destinazione:

     ```
     system node hardware unified-connect modify -type \| -t target -adapter port_name
     ```

   - Per programmare le porte initiator:

     ```
     system node hardware unified-connect modify -type \| -t initiator -adapter port_name
     ```

`-t` È il tipo FC4: Destinazione o iniziatore.

5. Verificare le nuove impostazioni immettendo il seguente comando ed esaminando l'output:

   ```
   system node hardware unified-connect show
   ```

6. Uscire dalla modalità di manutenzione:

   ```
   halt
   ```

7. Dopo aver immesso il comando, attendere che il sistema si arresti al prompt dell'ambiente di avvio.
8. Avviare node3 al prompt dell'ambiente di avvio:

   ```
   boot_ontap
   ```

9. Esegui una delle seguenti azioni:
   - Se node3 ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate, passare a. Controllare e configurare le porte UTA/UTA2 sul nodo 3.
   - Se node3 non dispone di una scheda UTA/UTA2 o di porte UTA/UTA2 integrate, saltare Controllare e configurare le porte UTA/UTA2 sul nodo 3 e passare a. "Mappare le porte dal nodo 1 al nodo 3".

Controllare e configurare le porte UTA/UTA2 sul nodo 3

Se node3 dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2, è necessario controllare la configurazione delle porte ed eventualmente riconfigurarle, a seconda di come si desidera utilizzare il sistema aggiornato.

Prima di iniziare

È necessario disporre dei moduli SFP+ corretti per le porte UTA/UTA2.

A proposito di questa attività

Se si desidera utilizzare una porta UTA/UTA2 (Unified Target Adapter) per FC, è necessario prima verificare la configurazione della porta.

> I materiali di marketing NetApp potrebbero utilizzare il termine UTA2 per fare riferimento agli adattatori e alle porte CNA. Tuttavia, la CLI utilizza il termine CNA.

È possibile utilizzare `ucadmin show` comando per verificare la configurazione corrente della porta:

```
*> ucadmin show
          Current  Current    Pending  Pending    Admin
 Adapter  Mode     Type       Mode     Type       Status
 -------  -------  ---------  -------  ---------  -----------
 0e       fc       target     -        initiator  offline
 0f       fc       target     -        initiator  offline
 0g       fc       target     -        initiator  offline
 0h       fc       target     -        initiator  offline
 1a       fc       target     -        -          online
 1b       fc       target     -        -          online
6 entries were displayed.
```

Le porte UTA/UTA2 possono essere configurate in modalità FC nativa o UTA/UTA2. La modalità FC supporta l'iniziatore FC e la destinazione FC; la modalità UTA/UTA2 consente la condivisione simultanea del traffico NIC e FCoE con la stessa interfaccia SFP+ 10 GbE e supporta le destinazioni FC.

Le porte UTA/UTA2 potrebbero essere presenti su un adattatore o sul controller e presentano le seguenti configurazioni, ma è necessario controllare la configurazione delle porte UTA/UTA2 sul nodo 3 e modificarla, se necessario:

- Le schede UTA/UTA2 ordinate al momento dell'ordine del controller vengono configurate prima della spedizione per avere la personalità richiesta.
- Le schede UTA/UTA2 ordinate separatamente dal controller vengono fornite con il linguaggio di destinazione FC predefinito.
- Le porte UTA/UTA2 integrate sui nuovi controller vengono configurate prima della spedizione in modo da avere la personalità richiesta.

> Immettere i comandi in questa sezione al prompt del cluster, a meno che non venga richiesto di entrare in modalità Manutenzione.

Fasi

1. Verificare la configurazione attuale della porta immettendo il seguente comando sul nodo 3:

   ```
   system node hardware unified-connect show
   ```

   Il sistema visualizza un output simile al seguente esempio:

```
cluster1::> system node hardware unified-connect show

                Current  Current    Pending  Pending  Admin
Node  Adapter   Mode     Type       Mode     Type     Status
----  -------   -------  ---------  -------  -------  ------
f-a   0e        fc       initiator  -        -        online
f-a   0f        fc       initiator  -        -        online
f-a   0g        cna      target     -        -        online
f-a   0h        cna      target     -        -        online
f-b   0e        fc       initiator  -        -        online
f-b   0f        fc       initiator  -        -        online
f-b   0g        cna      target     -        -        online
f-b   0h        cna      target     -        -        online
12 entries were displayed.
```

2. [[fase 2]]se il modulo SFP+ corrente non corrisponde all'utilizzo desiderato, sostituirlo con il modulo SFP+ corretto.

   Contattare il rappresentante NetApp per ottenere il modulo SFP+ corretto.

3. esaminare l'output di `system node hardware unified-connect show` oppure `ucadmin show` Per determinare se le porte UTA/UTA2 hanno la personalità desiderata.
4. eseguire una delle seguenti operazioni:

Se le porte UTA/UTA2…	**Quindi…**
Non avere la personalità che si desidera	Passare a. Fase 5.
Avere la personalità che si desidera	Salta il passaggio 5 al passaggio 13 e vai aFase 14 .

5. Se il sistema dispone di dischi di archiviazione ed esegue Data ONTAP 8.3 in cluster, avviare node3 ed entrare in modalità di manutenzione:

   `boot_ontap maint`

6. Verificare le impostazioni:

   `ucadmin show`

7. Eseguire una delle seguenti operazioni:

Se si sta configurando…	**Quindi…**
Porte su una scheda UTA/UTA2	Vai aFase 8 .
Porte UTA/UTA2 integrate	Salta il passaggio 8 e vai aFase 9 .

8. Se l'adattatore è in modalità iniziatore e la porta UTA/UTA2 è online, metti offline la porta UTA/UTA2:

   `storage disable adapter` *`adapter_name`*

Gli adattatori in modalità di destinazione sono automaticamente offline in modalità di manutenzione.

9. Se la configurazione corrente non corrisponde all'uso desiderato, modificare la configurazione secondo necessità:

   `ucadmin modify -m fc|cna -t initiator|target adapter_name`

   - `-m` è la modalità personality, `fc` oppure `cna`.
   - `-t` È di tipo FC4, `target` oppure `initiator`.

   > È necessario utilizzare l'iniziatore FC per le unità nastro e le configurazioni MetroCluster . Per i client SAN è necessario utilizzare la destinazione FC.

10. Arrestare il sistema:

    `halt`

    Il sistema si arresta al prompt dell'ambiente di avvio.

11. Immettere il seguente comando:

    `boot_ontap`

12. verificare le impostazioni:

    `system node hardware unified-connect show`

    L'output degli esempi seguenti mostra che il tipo di adattatore FC4 "1b" sta cambiando in `initiator` e che la modalità degli adattatori "2a" e "2b" stia cambiando in `cna`:

```
cluster1::> system node hardware unified-connect show

                Current  Current    Pending  Pending      Admin
Node  Adapter  Mode     Type       Mode     Type         Status
----  -------  -------  ---------  -------  -----------  ------
f-a   1a       fc       initiator  -        -            online
f-a   1b       fc       target     -        initiator    online
f-a   2a       fc       target     cna      -            online
f-a   2b       fc       target     cna      -            online

4 entries were displayed.
```

13. Metti online tutte le porte di destinazione immettendo il seguente comando, una volta per ogni porta:

    `network fcp adapter modify -node node_name -adapter adapter_name -state up`

14. Cablare la porta.

Mappare le porte dal nodo 1 al nodo 3

È necessario assicurarsi che le porte fisiche sul nodo 1 siano mappate correttamente alle porte fisiche sul nodo 3, che consentirà al nodo 3 di comunicare con gli altri nodi del cluster e con la rete dopo l'aggiornamento.

Prima di iniziare

È necessario disporre già delle informazioni relative alle porte sui nuovi nodi di *Hardware Universe*. (Passare a. "Riferimenti" Per collegarsi a *Hardware Universe*). Le informazioni vengono utilizzate più avanti in questa sezione e in "Mappare le porte dal nodo 2 al nodo 4".

La configurazione software di node3 deve corrispondere alla connettività fisica di node3 e la connettività di rete deve essere ripristinata prima di continuare con l'aggiornamento.

A proposito di questa attività

Le impostazioni delle porte possono variare a seconda del modello dei nodi.

Fasi

1. [[fase 1]]eseguire i seguenti passaggi per verificare se l'installazione è un cluster senza switch a due nodi:

   a. Impostare il livello di privilegio su Advanced (avanzato):

      `set -privilege advanced`

   b. Verificare se il setup è un cluster senza switch a due nodi:

      `network options switchless-cluster show`

      Ad esempio:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

   +
   Il valore di questo comando deve corrispondere allo stato fisico del sistema.

   a. Tornare al livello di privilegi di amministrazione:

      `set -privilege admin`

2. apportare le seguenti modifiche:

   a. Modificare le porte che faranno parte del dominio di broadcast del cluster:

      `network port modify -node node_name -port port_name -mtu 9000 -ipspace Cluster`

      Questo esempio aggiunge la porta del cluster e1b su "node1":

```
network port modify -node node1 -port e1b -ipspace Cluster -mtu 9000
```

b. Migrare le LIF del cluster alle nuove porte, una volta per ogni LIF:

```
network interface migrate -vserver Vserver_name -lif lif_name -source-node
node1 -destination-node node1 -destination-port port_name
```

Una volta migrate tutte le LIF del cluster e stabilita la comunicazione del cluster, il cluster deve entrare in quorum.

c. Modificare la porta home delle LIF del cluster:

```
network interface modify -vserver Cluster -lif lif_name –home-port port_name
```

d. Rimuovere le vecchie porte dal dominio di trasmissione del cluster:

```
network port broadcast-domain remove-ports -ipspace Cluster -broadcast
-domain Cluster -ports node1:port
```

e. Visualizza lo stato di salute di node1 e node3:

```
cluster show -node node1 -fields health
```

f. In base alla versione di ONTAP in esecuzione sulla coppia ha sottoposta a upgrade, esegui una delle seguenti azioni:

Se la versione di ONTAP è…	**Quindi…**
da 9,8 a 9.11.1	Verificare che le LIF del cluster siano in ascolto sulla porta 7700: `::> network connections listening show -vserver Cluster`
9.12.1 o versione successiva	Saltare questo passaggio e passare a. Fase 3.

La porta 7700 in ascolto sulle porte del cluster è il risultato previsto, come mostrato nell'esempio seguente per un cluster a due nodi:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

g. Per ogni cluster LIF che non è in ascolto sulla porta 7700, imposta lo stato amministrativo della LIF su `down` e poi `up`:

```
::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
int modify -vserver Cluster -lif cluster-lif -status-admin up
```

Ripetere il passaggio secondario (f) per verificare che la LIF del cluster sia in ascolto sulla porta 7700.

3. Modifica l'appartenenza al dominio di broadcast delle porte fisiche che ospitano i file LIF dei dati.

   a. Elencare lo stato di raggiungibilità di tutte le porte:

      ```
      network port reachability show
      ```

   b. Riparare la raggiungibilità delle porte fisiche, seguita dalle porte VLAN, eseguendo il seguente comando su ciascuna porta, una alla volta:

      ```
      reachability repair -node node_name -port port_name
      ```

      È previsto un avviso simile a quello riportato di seguito. Rivedere e accedere `y` oppure `n` a seconda dei casi:

      ```
      WARNING: Repairing port "node_name:port" might 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}:
      ```

   c. Per consentire a ONTAP di completare la riparazione, attendere circa un minuto dopo aver eseguito `reachability repair` sull'ultima porta.

   d. Elencare tutti i domini di broadcast sul cluster:

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

   e. 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 corrisponde a nessuno dei domini di broadcast esistenti, ONTAP creerà nuovi domini di broadcast per queste porte. Se necessario, è possibile eliminare i domini di broadcast appena creati se tutte le porte membri diventeranno porte membri dei gruppi di interfacce. Elimina domini di broadcast:

      ```
      broadcast-domain delete -broadcast-domain broadcast_domain
      ```

   f. Esaminare la configurazione del gruppo di interfacce e, se necessario, aggiungere o eliminare le porte membro.

      Aggiungere porte membro alle porte del gruppo di interfacce:

      ```
      ifgrp add-port -node node_name -ifgrp ifgrp_port -port port_name
      ```

      Rimuovere le porte membro dalle porte del gruppo di interfacce:

      ```
      ifgrp remove-port -node node_name -ifgrp ifgrp_port -port port_name
      ```

   g. Eliminare e ricreare le porte VLAN in base alle necessità. Elimina porte VLAN:

      ```
      vlan delete -node node_name -vlan-name vlan_port
      ```

Creazione delle porte VLAN:

```
vlan create -node node_name -vlan-name vlan_port
```

> A seconda della complessità della configurazione di rete del sistema da aggiornare, potrebbe essere necessario ripetere i passaggi secondari da (a) a (g) fino a quando tutte le porte non vengono posizionate correttamente dove necessario.

4. [[fase 4]]se nel sistema non sono configurate VLAN, passare a. Fase 5. Se sono configurate VLAN, ripristinare le VLAN smontate precedentemente configurate su porte che non esistono più o che sono state configurate su porte spostate in un altro dominio di trasmissione.
   a. Visualizzare le VLAN smontate:

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

   b. Ripristinare le VLAN spostate sulla porta di destinazione desiderata:

      ```
      displaced-vlans restore -node node_name -port port_name -destination-port
      destination_port
      ```

   c. Verificare che tutte le VLAN smontate siano state ripristinate:

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

   d. Le VLAN vengono automaticamente collocate nei domini di trasmissione appropriati circa un minuto dopo la loro creazione. Verificare che le VLAN ripristinate siano state collocate nei domini di trasmissione appropriati:

      ```
      network port reachability show
      ```

5. a partire da ONTAP 9.8, ONTAP modificherà automaticamente le porte home delle LIF se le porte vengono spostate tra domini di broadcast durante la procedura di riparazione della raggiungibilità delle porte di rete. Se la porta home di una LIF è stata spostata in un altro nodo o non è assegnata, tale LIF viene presentata come LIF spostato. Ripristinare le porte home dei file LIF spostati le cui porte home non esistono più o sono state spostate in un altro nodo.
   a. Visualizzare le LIF le cui porte home potrebbero essere state spostate in un altro nodo o non esistere più:

      ```
      displaced-interface show
      ```

   b. Ripristinare la porta home di ciascun LIF:

      ```
      displaced-interface restore -vserver Vserver_name -lif-name LIF_name
      ```

   c. Verificare che tutte le porte LIF home siano state ripristinate:

      ```
      displaced-interface 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 le porte senza connettività fisica. Se una delle porte riporta uno stato diverso da questi due, riparare la raggiungibilità come descritto in Fase 3.

6. verifica che tutte le LIF siano amministrativamente up sulle porte appartenenti ai domini di broadcast corretti.

   a. Verificare la presenza di eventuali LIF amministrativamente non disponibili:

      `network interface show -vserver Vserver_name -status-admin down`

   b. Verificare la presenza di eventuali LIF non attivi dal punto di vista operativo:

      `network interface show -vserver Vserver_name -status-oper down`

   c. Modificare le LIF che devono essere modificate in modo da avere una porta home diversa:

      `network interface modify -vserver Vserver_name -lif LIF_name -home-port home_port`

      Per le LIF iSCSI, la modifica della porta home richiede che la LIF sia amministrativamente inattiva.

   a. Ripristinare le LIF che non si trovano nelle rispettive porte home:

      `network interface revert *`

Spostare le LIF dei dati NAS di proprietà del node1 da node2 a node3 e verificare le LIF SAN sul node3

Prima di spostare gli aggregati da node2 a node3, è necessario spostare le LIF dei dati NAS appartenenti a node1 che sono attualmente su node2 da node2 a node3. È inoltre necessario verificare le LIF SAN sul nodo 3.

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. Elenca tutte le LIF dati NAS non possedute da node2 immettendo il seguente comando su entrambi i nodi e catturando l'output:

   `network interface show -role data -curr-node node2 -is-home false -home-node node3`

2. se il cluster è configurato per le LIF SAN, registrare le LIF SAN `adapter` e. `switch-port` informazioni di configurazione in questo "foglio di lavoro" da utilizzare in seguito nella procedura.

   a. Elencare le LIF SAN sul node2 ed esaminare l'output:

      `network interface show -data-protocol fc*`

      Il sistema restituisce un output simile al seguente esempio:

```
cluster1::> net int show -data-protocol fc*
  (network interface show)
            Logical     Status     Network            Current
Current Is
Vserver     Interface   Admin/Oper Address/Mask       Node
Port    Home
----------  ----------  ---------- ------------------ -------------
------- ----
svm2_cluster1
            lif_svm2_cluster1_340
                        up/up      20:02:00:50:56:b0:39:99
                                                      cluster1-01
1b      true
            lif_svm2_cluster1_398
                        up/up      20:03:00:50:56:b0:39:99
                                                      cluster1-02
1a      true
            lif_svm2_cluster1_691
                        up/up      20:01:00:50:56:b0:39:99
                                                      cluster1-01
1a      true
            lif_svm2_cluster1_925
                        up/up      20:04:00:50:56:b0:39:99
                                                      cluster1-02
1b      true
4 entries were displayed.
```

b. Elencare le configurazioni esistenti ed esaminare l'output:

   `fcp adapter show -fields switch-port,fc-wwpn`

   Il sistema restituisce un output simile al seguente esempio:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  -----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

3. eseguire una delle seguenti operazioni:

Se nodo1…	Quindi…
Ha configurato gruppi di interfacce o VLAN	Passare a. Fase 4.
Non sono stati configurati gruppi di interfacce o VLAN	Saltare la fase 4 e passare a. Fase 5.

4. eseguire i seguenti passaggi secondari per migrare qualsiasi LIF di dati NAS ospitata su gruppi di interfacce e VLAN originariamente presenti sul nodo 1 da node2 a node3:

   a. Migrate qualsiasi LIF di dati ospitata su node2 che in precedenza apparteneva a node1 su un gruppo di interfacce a una porta sul node3 in grado di ospitare LIF sulla stessa rete immettendo il seguente comando, una volta per ogni LIF:

      `network interface migrate -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-destination -node` *`node3`* `-destination-port` *`netport|ifgrp`*

   b. Modificare la porta home e il nodo home di LIF in Sotto-fase A. Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

      `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home-node` *`node3`* `-home-port` *`netport|ifgrp`*

   c. Migrare tutti i dati LIF ospitati su node2 che in precedenza appartenevano a node1 su una porta VLAN a una porta su node3 in grado di ospitare LIF sulla stessa rete immettendo il seguente comando,

una volta per ogni LIF:

```
network interface migrate -vserver vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

d. Modificare la porta home e il nodo home dei file LIF in Sotto-fase c Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node
node3 -home-port netport|ifgrp
```

5. eseguire una delle seguenti operazioni:

Se il cluster è configurato per…	**Quindi…**
NAS	Completo Fase 6 e. Fase 7, Saltare il passaggio 8 e completare Fase 9 attraverso Fase 12.
SAN	Disattivare tutte le LIF SAN sul nodo per disattivarle per l'aggiornamento: `network interface modify -vserver *vserver_name* -lif *LIF_name* -home-node *node_to_upgrade* -home-port _netport

6. se si dispone di porte dati non uguali sulle piattaforme, aggiungere le porte al dominio di trasmissione:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt -ports node:port
```

Nell'esempio seguente viene aggiunta la porta "e0a" sul nodo "8200-1" e la porta "e0i" sul nodo "8060-1" al dominio di trasmissione "mgmt" nell'IPSpace "Default":

```
cluster::> network port broadcast-domain add-ports -ipspace Default
-broadcast-domain mgmt -ports 8200-1:e0a, 8060-1:e0i
```

7. Migrare ciascun LIF dati NAS in node3 immettendo il seguente comando, una volta per ogni LIF:

```
network interface migrate -vserver vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

8. assicurarsi che la migrazione dei dati sia persistente:

```
network interface modify -vserver vserver_name -lif LIF_name-home-port
netport|ifgrp -home-node node3
```

9. verificare che le LIF SAN si trovino sulle porte corrette sul nodo 3:

a. Immettere il seguente comando ed esaminarne l'output:

```
network interface show -data-protocol iscsi|fcp -home-node node3
```

Il sistema restituisce un output simile al seguente esempio:

```
cluster::> net int show -data-protocol iscsi|fcp -home-node node3
              Logical     Status      Network             Current
Current  Is
 Vserver      Interface   Admin/Oper  Address/Mask        Node
Port     Home
 -----------  ----------  ----------  ------------------
-------------  -------  ----
 vs0
              a0a         up/down     10.63.0.53/24       node3
a0a      true
              data1       up/up       10.63.0.50/18       node3
e0c      true
              rads1       up/up       10.63.0.51/18       node3
e1a      true
              rads2       up/down     10.63.0.52/24       node3
e1b      true
 vs1
              lif1        up/up       172.17.176.120/24   node3
e0c      true
              lif2        up/up       172.17.176.121/24   node3
e1a      true
```

b. Verificare che i nuovi e. `adapter` e. `switch-port` le configurazioni sono corrette confrontando l'output di `fcp adapter show` con le informazioni di configurazione registrate nel foglio di lavoro in Fase 2.

   Elencare le nuove configurazioni LIF SAN al nodo 3:

   `fcp adapter show -fields switch-port,fc-wwpn`

   Il sistema restituisce un output simile al seguente esempio:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node        adapter fc-wwpn                 switch-port
----------- ------- ----------------------- -------------
cluster1-01 0a      50:0a:09:82:9c:13:38:00 ACME Switch:0
cluster1-01 0b      50:0a:09:82:9c:13:38:01 ACME Switch:1
cluster1-01 0c      50:0a:09:82:9c:13:38:02 ACME Switch:2
cluster1-01 0d      50:0a:09:82:9c:13:38:03 ACME Switch:3
cluster1-01 0e      50:0a:09:82:9c:13:38:04 ACME Switch:4
cluster1-01 0f      50:0a:09:82:9c:13:38:05 ACME Switch:5
cluster1-01 1a      50:0a:09:82:9c:13:38:06 ACME Switch:6
cluster1-01 1b      50:0a:09:82:9c:13:38:07 ACME Switch:7
cluster1-02 0a      50:0a:09:82:9c:6c:36:00 ACME Switch:0
cluster1-02 0b      50:0a:09:82:9c:6c:36:01 ACME Switch:1
cluster1-02 0c      50:0a:09:82:9c:6c:36:02 ACME Switch:2
cluster1-02 0d      50:0a:09:82:9c:6c:36:03 ACME Switch:3
cluster1-02 0e      50:0a:09:82:9c:6c:36:04 ACME Switch:4
cluster1-02 0f      50:0a:09:82:9c:6c:36:05 ACME Switch:5
cluster1-02 1a      50:0a:09:82:9c:6c:36:06 ACME Switch:6
cluster1-02 1b      50:0a:09:82:9c:6c:36:07 ACME Switch:7
16 entries were displayed
```

Se un LIF SAN nella nuova configurazione non si trova su un adattatore ancora collegato allo stesso `switch-port`, potrebbe causare un'interruzione del sistema quando si riavvia il nodo.

c. Se node3 ha LIF SAN o gruppi DI LIF SAN che si trovano su una porta che non esisteva sul node1 o che devono essere mappati su una porta diversa, spostarli su una porta appropriata sul node3 completando i seguenti passaggi secondari:

   i. Impostare lo stato LIF su "DOWN" (giù):

      `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-status -admin down`

   ii. Rimuovere la LIF dal set di porte:

      `portset remove -vserver` *`vserver_name`* `-portset` *`portset_name`* `-port-name` *`port_name`*

   iii. Immettere uno dei seguenti comandi:

      - Spostare una singola LIF:

        `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home -port` *`new_home_port`*

      - Spostare tutte le LIF su una singola porta inesistente o errata su una nuova porta:

```
network interface modify {-home-port port_on_node1 -home-node node1
-role data} -home-port new_home_port_on_node3
```

- Aggiungere nuovamente i file LIF al set di porte:

```
portset add -vserver vserver_name -portset portset_name -port-name
port_name
```

> È necessario spostare I file LIF SAN su una porta con la stessa velocità di collegamento della porta originale.

10. Modificare lo stato di tutte le LIF su "up" in modo che le LIF possano accettare e inviare traffico sul nodo:

```
network interface modify -home-port port_name -home-node node3 -lif data
-status-admin up
```

11. Immettere il seguente comando su uno dei nodi ed esaminare l'output per verificare che le LIF siano state spostate nelle porte corrette e che le LIF abbiano lo stato di "up" immettendo il seguente comando su uno dei nodi ed esaminando l'output:

```
network interface show -home-node node3 -role data
```

12. se le LIF non sono attive, impostare lo stato amministrativo delle LIF su "up" immettendo il seguente comando, una volta per ciascuna LIF:

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

13. Invia un messaggio AutoSupport post-upgrade a NetApp per il node1:

```
system node autosupport invoke -node node3 -type all -message "node1
successfully upgraded from platform_old to platform_new"
```

Foglio di lavoro: Informazioni da registrare prima di spostare i file LIF dei dati NAS in node3

Per verificare di disporre della configurazione corretta dopo aver spostato LE LIF SAN da node2 a node3, è possibile utilizzare il seguente foglio di lavoro per registrare `adapter` e. `switch-port` Informazioni per ciascun LIF.

Registrare la LIF `adapter` informazioni da `network interface show -data-protocol fc*` output del comando e il `switch-port` informazioni da `fcp adapter show -fields switch-port,fc-wwpn` output del comando per node2.

Dopo aver completato la migrazione al nodo 3, registrare il LIF `adapter` e. `switch-port` Informazioni per i LIF sul node3 e verificare che ciascun LIF sia ancora connesso allo stesso `switch-port`.

Node2			**Node3**		
LIF	`adapter`	`switch-port`	LIF	`adapter`	`switch-port`

Node2			Node3		

Spostare gli aggregati non root dal nodo 2 al nodo 3

Prima di sostituire node2 con node4, è necessario inviare un messaggio AutoSupport per node2 e spostare gli aggregati non root di proprietà di node2 a node3.

> Durante questa procedura, non spostare gli aggregati da node3 a node2. In questo modo, gli aggregati vengono portati offline e si verifica una mancanza di servizio dei dati per gli aggregati che vengono ricollocati.

Fasi

1. Verificare che l'ID del sistema partner sia impostato correttamente sul nodo 3:

   a. Immettere il livello di privilegio avanzato:

      ```
      set -privilege advanced
      ```

   b. Mostra l'ID del sistema del partner su node3:

      ```
      ha interconnect config show -node <node3-node1>
      ```

      Il sistema visualizza un output simile al seguente esempio:

   Mostra esempio

   ```
   cluster::*> ha interconnect config show -node <node>
     (system ha interconnect config show)

                           Node: node3-node1
              Interconnect Type: RoCE
                Local System ID: <node3-system-id>
              Partner System ID: <node2-system-id>
           Connection Initiator: local
                     Interface: external

   Port   IP Address
   ----   -----------------
   e4a-17   0.0.0.0
   e4b-18   0.0.0.0
   ```

2. Se "ID sistema partner" non è corretto per node3:

a. Arresto node3:

```
halt
```

b. Al prompt di Loader, impostare il valore corretto "partner-sysid".

Il node3 "partner-sysid" è l'ID di sistema di node2, che è possibile trovare nell' `ha interconnect config show`output in Fase 1.

c. Salvare le impostazioni:

```
saveenv
```

d. Al prompt di Loader, avviare node3 nel menu di avvio:

```
boot_ontap menu
```

e. Accedere a node3.

3. Manda un messaggio a "AutoSupport" a "NetApp for node2:

```
system node autosupport invoke -node <node2> -type all -message "Upgrading
<node2> from <platform_old> to <platform_new>"
```

4. Verificare che il messaggio AutoSupport sia stato inviato:

```
system node autosupport show -node <node2> -instance
```

I campi "ultimo oggetto inviato:" e "ultimo invio:" contengono il titolo dell'ultimo messaggio inviato e l'ora in cui il messaggio è stato inviato.

5. Riposiziona gli aggregati non radice:

a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

b. Elencare gli aggregati di proprietà di node2:

```
storage aggregate show -owner-name <node2>
```

c. Avviare il trasferimento degli aggregati:

```
storage aggregate relocation start -node <node2> -destination <node3>
-aggregate-list * -ndo-controller-upgrade true
```

Il comando individua solo gli aggregati non root.

a. Quando richiesto, immettere `y`.

Il trasferimento avviene in background. La riposizionamento di un aggregato può richiedere da pochi secondi a un paio di minuti. Il tempo include sia le parti di fuori servizio del client che quelle di non fuori servizio. Il comando non sposta aggregati non in linea o con restrizioni.

b. Tornare al livello di privilegio admin:

```
set -privilege admin
```

6. Verificare lo stato di trasferimento del nodo 2:

```
storage aggregate relocation show -node <node2>
```

L'output visualizza "Done" (eseguito) per un aggregato dopo che è stato spostato.

> Prima di passare alla fase successiva, è necessario attendere che tutti gli aggregati di proprietà di node2 siano stati ricollocati in node3.

7. Eseguire una delle seguenti operazioni:

In caso di trasferimento di…	Quindi…
Tutti gli aggregati hanno avuto successo	Andare a Fase 8.

In caso di trasferimento di…	Quindi…

Qualsiasi aggregato ha avuto esito negativo o è stato vetoato	a. Visualizzare un messaggio di stato dettagliato:
	
	`storage aggregate show -instance`
	
	È inoltre possibile controllare i registri EMS per visualizzare l'azione correttiva necessaria.
	
	Il `event log show` command elenca gli errori che si sono verificati.
	
	b. Eseguire l'azione correttiva.
	c. Impostare il livello di privilegio su Advanced (avanzato):
	
	`set -privilege advanced`
	
	d. Spostare eventuali aggregati guasti o vetoed:
	
	`storage aggregate relocation start -node <node2> -destination <node3> -aggregate-list * -ndo-controllerupgrade true`
	
	e. Quando richiesto, immettere `y`.
	f. Tornare al livello di privilegio admin:
	
	`set -privilege admin`
	
	Se necessario, è possibile forzare il trasferimento utilizzando uno dei seguenti metodi:
	
	• Sovrascrivendo i veto check:
	
	`storage aggregate relocation start -override -vetoes true -ndo-controller-upgrade`
	
	• Sovrascrivendo i controlli di destinazione:
	
	`storage aggregate relocation start -override -destination-checks true -ndocontroller-upgrade`
	
	Per ulteriori informazioni sui comandi di trasferimento degli aggregati di storage, visitare il sito Web all'indirizzo "Riferimenti" Per collegarsi alla gestione di *dischi e aggregati con i comandi CLI* e *ONTAP 9: Manuale riferimento pagina*.

8. verificare che tutti gli aggregati non root siano online su node3:

`storage aggregate show -node <node3> -state offline -root false`

Se alcuni aggregati sono andati offline o sono diventati estranei, è necessario portarli online una volta per

ciascun aggregato:

```
storage aggregate online -aggregate <aggregate_name>
```

9. Verificare che tutti i volumi siano online al nodo3:

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

   Se alcuni volumi sono offline sul node3, è necessario portarli online, una volta per ciascun volume:

   ```
   volume online -vserver <Vserver-name> -volume <volume-name>
   ```

10. Verificare che node2 non disponga di aggregati non root online:

    ```
    storage aggregate show -owner-name <node2> -ha-policy sfo -state online
    ```

    L'output del comando non dovrebbe visualizzare gli aggregati online non root perché tutti gli aggregati online non root sono già stati riallocati in node3.

Spostare le LIF dei dati NAS di proprietà del node2 al node3

Dopo aver spostato gli aggregati da node2 a node3, è necessario spostare i dati NAS LIF di proprietà di 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. LE LIF SAN non vengono spostate a meno che non sia necessario mapparle su nuove porte. È necessario verificare che le LIF siano integre e ubicate sulle porte appropriate dopo aver spostato le LIF da node3 a node4 e aver portato node4 online.

Fasi

1. Elenca tutte le LIF dei dati NAS di proprietà di node2 immettendo il seguente comando su uno dei nodi e acquisendo l'output:

   ```
   network interface show -data-protocol nfs|cifs -home-node node2
   ```

   L'esempio seguente mostra l'output del comando per node2:

```
cluster::> network interface show -data-protocol nfs|cifs -home-node
node2
              Logical     Status      Network             Current
Current  Is
 Vserver      Interface   Admin/Oper  Address/Mask        Node     Port
Home
 -----------  ----------  ----------  ------------------  -------
-------  ----
 vs0
              a0a         up/down     10.63.0.53/24       node2    a0a
true
              data1       up/up       10.63.0.50/18       node2    e0c
true
              rads1       up/up       10.63.0.51/18       node2    e1a
true
              rads2       up/down     10.63.0.52/24       node2    e1b
true
 vs1
              lif1        up/up       172.17.176.120/24   node2    e0c
true
              lif2        up/up       172.17.176.121/24   node2    e1a
true
```

2. eseguire una delle seguenti operazioni:

In caso di node2…	Quindi…
Dispone di gruppi di interfacce o VLAN configurati	Passare a. Fase 3.
Non ha gruppi di interfacce o VLAN configurati	Saltare la fase 3 e passare a. Fase 4.

3. eseguire i seguenti passaggi per migrare i dati NAS LIF ospitati su gruppi di interfacce e VLAN sul nodo 2:

   a. Migrate qualsiasi LIF di dati ospitata su un gruppo di interfacce su node2 a una porta su node3 in grado di ospitare LIF sulla stessa rete immettendo il seguente comando, una volta per ogni LIF:

      `network interface migrate -vserver` *`Vserver_name`* `-lif` *`LIF_name`* `-destination -node` *`node3`* `-destination-port` *`netport|ifgrp`*

   b. Modificare la porta home e il nodo home dei file LIF in Sotto-fase A. Alla porta e al nodo che attualmente ospitano i LIF immettendo il seguente comando, una volta per ogni nodo:

      `network interface modify -vserver` *`Vserver_name`* `-lif` *`LIF_name`* `-home-node` *`node3`* `-homeport` *`netport|ifgrp`*

   c. Migrare le LIF ospitate su VLAN su node2 a una porta su node3 in grado di ospitare LIF sulla stessa rete delle VLAN immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface migrate -vserver Vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

d. Modificare la porta home e il nodo home dei file LIF in Sotto-fase c Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface modify -vserver Vserver_name -lif LIF_name -home-node
node3 -homeport netport|ifgrp
```

4. eseguire una delle seguenti operazioni:

Se il cluster è configurato per…	Quindi…
NAS	Completo Fase 5 attraverso Fase 8.
SAN	Saltare i passaggi da 5 a 8, quindi completare Fase 9.
NAS e SAN	Completo Fase 5 attraverso Fase 9.

5. se si dispone di porte dati non uguali sulle piattaforme, aggiungere le porte al dominio di trasmissione:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt -ports node:port
```

Nell'esempio seguente viene aggiunta la porta "e0a" sul nodo "6280-1" e la porta "e0i" sul nodo "8060-1" al dominio di trasmissione "mgmt" nell'IPSpace "Default":

```
cluster::> network port broadcast-domain add-ports -ipspace Default
           -broadcast-domain mgmt -ports 6280-1:e0a, 8060-1:e0i
```

6. Migrare ciascun LIF dati NAS in node3 immettendo il seguente comando, una volta per ogni LIF:

```
network interface migrate -vserver Vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

7. verificare che le LIF NAS siano state spostate nelle porte corrette e che le LIF abbiano lo stato di up immettendo il seguente comando su entrambi i nodi ed esaminando l'output:

```
network interface show -curr-node node3 -data-protocol cifs|nfs
```

8. se le LIF non sono attive, imposta lo stato amministrativo delle LIF su "up" immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface modify -vserver Vserver_name -lif LIF_name -status-admin up
```

9. se sono configurati gruppi di interfacce o VLAN, completare i seguenti passaggi secondari:

a. Rimuovere le VLAN dai gruppi di interfacce:

```
network port vlan delete -node node_name -port ifgrp -vlan-id VLAN_ID
```

b. Immettere il seguente comando ed esaminarne l'output per determinare se nel nodo sono configurati gruppi di interfacce:

```
network port ifgrp show -node node_name -ifgrp ifgrp_name -instance
```

Il sistema visualizza le informazioni sul gruppo di interfacce per il nodo, come illustrato nell'esempio seguente:

```
cluster::> network port ifgrp show -node node2 -ifgrp a0a -instance
                  Node: node2
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode_lacp
          MAC Address: MAC_address
    ort Participation: partial
        Network Ports: e2c, e2d
             Up Ports: e2c
           Down Ports: e2d
```

a. Se nel nodo sono configurati gruppi di interfacce, registrare i nomi dei gruppi di interfacce e le porte ad essi assegnate, quindi eliminare le porte immettendo il seguente comando, una volta per ciascuna porta:

   ```
   network port ifgrp remove-port -node node_name -ifgrp ifgrp_name -port port_name
   ```

Fase 4. Registrare le informazioni e dismettere il node2

Registrare le informazioni del nodo 2

Prima di spegnere e dismettere il nodo 2, è necessario registrare le informazioni relative alla rete del cluster, alla gestione e alle porte FC, nonché l'ID del sistema NVRAM. Queste informazioni sono necessarie più avanti nella procedura quando si esegue il mapping del nodo 2 al nodo 4 e si riassegnano i dischi.

Fasi

1. Trova le porte di rete cluster, gestione nodi, intercluster e gestione cluster sul nodo 2:

   ```
   network interface show -curr-node node_name -role
   cluster,intercluster,nodemgmt,cluster-mgmt
   ```

   Il sistema visualizza le LIF per quel nodo e per gli altri nodi nel cluster, come mostrato nell'esempio seguente:

```
cluster::> network interface show -curr-node node2 -role
cluster,intercluster,node-mgmt,cluster-mgmt
         Logical     Status     Network            Current     Current
Is
Vserver  Interface   Admin/Oper Address/Mask       Node        Port
Home
-------- ----------  ---------- ------------------ ----------  -------
----
node2
         intercluster up/up     192.168.1.202/24   node2       e0e
true
         clus1        up/up     169.254.xx.xx/24   node2       e0a
true
         clus2        up/up     169.254.xx.xx/24   node2       e0b
true
         mgmt1        up/up     192.168.0.xxx/24   node2       e0c
true
4 entries were displayed.
```

Il sistema potrebbe non disporre di LIF intercluster. Si avrà una LIF di gestione del cluster solo su un nodo di una coppia di nodi. Una LIF di gestione cluster viene visualizzata nell'output di esempio di "Fase 1" In *Record node1 port information*.

2. Acquisire le informazioni nell'output da utilizzare nella sezione "Mappare le porte dal nodo 2 al nodo 4".

   Le informazioni di output sono necessarie per mappare le nuove porte del controller alle vecchie porte del controller.

3. Determinare le porte fisiche sul nodo 2:

   `network port show -node node_name -type physical +`

   `node_name` è il nodo che viene migrato.

   Il sistema visualizza le porte fisiche sul nodo 2, come mostrato nell'esempio seguente:

```
cluster::> network port show -node node2 -type physical

                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- -----------
node2
       e0M       Default      IP_address       up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

4. Registrare le porte e i relativi domini di trasmissione.

   I domini di broadcast dovranno essere mappati alle porte sul nuovo controller più avanti nella procedura.

5. Determinare le porte FC sul nodo 2:

   `network fcp adapter show`

   Il sistema visualizza le porte FC sul nodo 2, come mostrato nell'esempio seguente:

```
cluster::> network fcp adapter show -node node2
                     Connection  Host
Node         Adapter Established Port Address
------------ ------- ----------- ------------
node2
             0a      ptp         11400
node2
             0c      ptp         11700
node2
             6a      loop        0
node2
             6b      loop        0
4 entries were displayed.
```

6. Registrare le porte.

   Le informazioni di output sono necessarie per mappare le nuove porte FC sul nuovo controller più avanti nella procedura.

7. Se non è stato fatto in precedenza, controllare se ci sono gruppi di interfacce o VLAN configurati su node2:

   `ifgrp show`

```
vlan show
```

Verranno utilizzate le informazioni contenute nella sezione "Mappare le porte dal nodo 2 al nodo 4".

8. Eseguire una delle seguenti operazioni:

Se…	Quindi…
Numero ID sistema NVRAM registrato in "Preparare i nodi per l'aggiornamento"	Passare a. "Andare in pensione node2".
Il numero dell'ID del sistema NVRAM non è stato registrato in "Preparare i nodi per l'aggiornamento"	Completo Fase 9 e. Fase 10 quindi passare alla sezione successiva, "Andare in pensione node2".

9. Visualizza gli attributi del node2:

```
system node show -instance -node node2
```

```
cluster::> system node show -instance -node node2
                              ...
                NVRAM System ID: system_ID
                              ...
```

10. registrare l'ID del sistema NVRAM da utilizzare nella sezione "Installazione e boot node4".

Andare in pensione node2

Per dismettere il node2, è necessario chiudere il node2 correttamente e rimuoverlo dal rack o dallo chassis. Se il cluster si trova in un ambiente SAN, è necessario eliminare anche le LIF SAN.

Fasi

1. Eseguire una delle seguenti operazioni:

Se il cluster è…	Quindi…
Un cluster a due nodi	Passare a. Fase 2.
Un cluster con più di due nodi	Passare a. Fase 9.

2. accedere al livello di privilegio avanzato immettendo il seguente comando su uno dei nodi:

```
set -privilege advanced
```

3. Verificare che l'ha del cluster sia stato disattivato immettendo il seguente comando ed esaminandone l'output:

```
cluster ha show
```

Il sistema visualizza il seguente messaggio:

```
High Availability Configured: false
```

4. Verificare se node2 attualmente contiene epsilon immettendo il seguente comando ed esaminandone l'output:

   `cluster show`

   Il seguente esempio mostra che node2 contiene epsilon:

```
cluster*::> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -----------
node1                 true    true          false
node2                 true    true          true

Warning: Cluster HA has not been configured. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

2 entries were displayed.
```

   Se si sta aggiornando una coppia HA in un cluster con più coppie HA, è necessario spostare epsilon sul nodo di una coppia HA che non è in fase di aggiornamento del controller. Ad esempio, se si sta aggiornando NodeA/NodeB in un cluster con la configurazione della coppia ha NodeA/NodeB e NODEC/NODed, è necessario spostare epsilon in NODEC o NODed.

5. Se il node2 contiene epsilon, contrassegnare epsilon come `false` sul nodo in modo che possa essere trasferito al nodo 3:

   `cluster modify -node node2 -epsilon false`

6. Trasferire epsilon al nodo 3 contrassegnando epsilon `true` al nodo 3:

   `cluster modify -node node3 -epsilon true`

7. Verificare se il setup è un cluster senza switch a due nodi:

   `network options switchless-cluster show`

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

Il valore di questo comando deve corrispondere allo stato fisico del sistema.

8. Verificare se il setup è un cluster senza switch a due nodi:

   `network options switchless-cluster show`

   ```
   cluster::*> network options switchless-cluster show
   Enable Switchless Cluster: false/true
   ```

   Il valore di questo comando deve corrispondere allo stato fisico del sistema.

9. Torna al livello di amministrazione:

   `set -privilege admin`

10. Arrestare il node2 immettendo il seguente comando su uno dei controller:
    `system node halt -node node2`
11. Dopo lo spegnimento completo del node2, rimuoverlo dallo chassis o dal rack. È possibile decommissionare il node2 una volta completato l'aggiornamento. Vedere "Decommissionare il vecchio sistema".

Fase 5. Installazione e boot node4

Installazione e boot node4

È necessario installare node4 nel rack, trasferire node2 connessioni al node4 e fare il boot node4. È inoltre necessario riassegnare eventuali spare node2, dischi appartenenti a root e aggregati non root che non sono stati riallocati in precedenza in node3.

A proposito di questa attività

È necessario eseguire l'avvio di rete del nodo 4 se la versione ONTAP sul nodo 4 è diversa dalla versione ONTAP sul nodo 2. Dopo aver installato node4, avviarlo dall'immagine ONTAP 9 memorizzata sul server web. È quindi possibile scaricare i file corretti sul dispositivo di supporto di avvio per i successivi avvii del sistema seguendo le istruzioni in "Preparatevi per il netboot"

Tuttavia, non è necessario eseguire l'avvio di rete del nodo 4 se la versione ONTAP sul nodo 4 è uguale o successiva alla versione ONTAP sul nodo 2.

- Per un aggiornamento del controller AFF A800 o AFF C800 , è necessario assicurarsi che tutte le unità nello chassis siano saldamente posizionate contro il midplane prima di rimuovere node2. Per maggiori informazioni, vedere "Sostituire i moduli controller AFF A800 o AFF C800".
- Se si sta aggiornando un sistema con dischi di archiviazione, è necessario completare l'intera sezione e quindi procedere alla sezione "Impostare la configurazione FC o UTA/UTA2 su node4" , immettendo comandi al prompt del cluster.

Fasi

1. eseguire una delle seguenti operazioni:

Se node4 sarà in …	Quindi…
Uno chassis separato dal node3	Passare a. Fase 2.
Lo stesso chassis con node3	Saltare i passaggi 2 e 3 e passare a. Fase 4.

2. assicurarsi che node4 disponga di spazio rack sufficiente.

   Se il nodo 4 si trova in uno chassis separato dal nodo 3, è possibile inserire il nodo 4 nella stessa posizione del nodo 2. Se node3 e node4 si trovano nello stesso chassis, node4 si trova già nella posizione rack appropriata.

3. Installare il nodo 4 nel rack seguendo le istruzioni contenute nelle *istruzioni di installazione e configurazione* relative al modello di nodo.
4. cavo node4, spostamento delle connessioni da node2 a node4.

   I seguenti riferimenti consentono di stabilire i collegamenti dei cavi corretti. Passare a. "Riferimenti" per collegarli.

   - *Istruzioni di installazione e configurazione* per la piattaforma node4
   - La procedura di shelf di dischi appropriata
   - La documentazione *ha Pair Management*

   Collegare i seguenti cavi:

   - Console (porta di gestione remota)
   - Porte del cluster
   - Porte dati
   - Porte di gestione di cluster e nodi
   - Storage
   - Configurazioni SAN: Porte switch FC e Ethernet iSCSI

   Non è necessario spostare la scheda di interconnessione/scheda FC_VI o la connessione del cavo Interconnect/FC_VI dal nodo 2 al nodo 4, poiché la maggior parte dei modelli di piattaforma dispone di modelli di schede di interconnessione univoci.

5. Eseguire una delle seguenti operazioni:

Se il nodo 4 è in…	Quindi…
Lo stesso chassis del node3	Passare a. Fase 8.
Uno chassis separato dal node3	Passare a. Fase 6.

6. accendere l'alimentazione a node4, quindi interrompere l'avvio premendo Ctrl-C per accedere al prompt dell'ambiente di avvio.

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

```
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'
```

7. se viene visualizzato il messaggio di avviso nella fase 6, 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 sia terminato.

   Non ignorare il ritardo. Se la batteria non viene caricata, si potrebbe verificare una perdita di dati.

8. Al prompt della modalità di manutenzione, immettere il seguente comando:

   `halt`

   Il sistema si arresta al prompt dell'ambiente di avvio.

9. Configurare il nodo 4 per ONTAP:

   `set-defaults`

10. Se sono installate unità NetApp Storage Encryption (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`**

    Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha.

    È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

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 le chiavi di autenticazione utilizzando Onboard Key Manager".

11. Se la versione di ONTAP installata sul nodo 4 è la stessa o successiva alla versione di ONTAP 9 installata sul nodo 2, immettere il seguente comando:

```
boot_ontap menu
```

12. Eseguire una delle seguenti operazioni:

Se il sistema che si sta aggiornando…	Quindi…
Non dispone della versione ONTAP corretta o corrente sul nodo 4	Vai aFase 13 .
Ha la versione corretta o attuale di ONTAP al nodo 4	Vai aFase 18 .

13. Configurare la connessione netboot scegliendo una delle seguenti azioni.

> Come connessione di netboot, è necessario utilizzare la porta di gestione e l'indirizzo IP. Non utilizzare un indirizzo 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 immettendo 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 (Domain Name Service). Se si utilizza questo parametro opzionale, non è necessario un nome di dominio completo nell'URL del server netboot; è necessario solo il nome host del server. Potrebbero essere necessari altri parametri per l'interfaccia. Invio `help ifconfig` al prompt del firmware per ulteriori informazioni.

14. Eseguire il netboot al nodo 4:

Per…	Quindi…
Sistemi della serie FAS/AFF8000	`netboot http://<web_server_ip/path_to_webaccessible_directory>/netboot/kernel`
Tutti gli altri sistemi	`netboot http://<web_server_ip/path_to_webaccessible_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` poll "Fase 1" Nella sezione *Prepare for netboot*.

Non interrompere l'avvio.

15. Dal menu di avvio, selezionare `option (7) Install new software first`.

Questa opzione di menu consente di scaricare e installare la nuova immagine Data 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 Data 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.

16. se viene richiesto di continuare la procedura, inserire y e, quando richiesto, inserire l'URL:

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

17. Completare i seguenti passaggi secondari:

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.

18. Seleziona la modalità di manutenzione `5` dal menu di avvio e inserisci `y` quando ti viene chiesto di continuare con l'avvio.
19. Prima di continuare, vai a"Impostare la configurazione FC o UTA/UTA2 su node4" per apportare le modifiche necessarie alle porte FC o UTA/UTA2 sul nodo. Apportare le modifiche consigliate in quelle sezioni, riavviare il nodo e passare alla modalità di manutenzione.
20. Immettere il seguente comando ed esaminare l'output per trovare l'ID di sistema di node4:

    `disk show -a`

    Il sistema visualizza l'ID di sistema del nodo e le informazioni relative ai dischi, come mostrato nell'esempio seguente:

```
*> disk show -a
Local System ID: 536881109
DISK         OWNER                      POOL   SERIAL NUMBER   HOME
------------ -------------              -----  -------------
-------------
0b.02.23     nst-fas2520-2(536880939)    Pool0  KPG2RK6F        nst-
fas2520-2(536880939)
0b.02.13     nst-fas2520-2(536880939)    Pool0  KPG3DE4F        nst-
fas2520-2(536880939)
0b.01.13     nst-fas2520-2(536880939)    Pool0  PPG4KLAA        nst-
fas2520-2(536880939)
......
0a.00.0                   (536881109)    Pool0  YFKSX6JG
(536881109)
......
```

21. Riassegnare le parti di ricambio di node2, i dischi appartenenti alla root e gli aggregati non root che non sono stati ricollocati in node3 precedentemente nella sezione "Spostare gli aggregati non root dal nodo 2 al nodo 3":

    Se nel sistema sono presenti dischi condivisi, aggregati ibridi o entrambi, è necessario utilizzare il corretto `disk reassign` dalla seguente tabella.

Tipo di disco…	Eseguire il comando…
Con dischi condivisi	`disk reassign -s` *`node2_sysid`* `-d` *`node4_sysid`* `-p` *`node3_sysid`*

Tipo di disco…	Eseguire il comando…
Senza condivisione	`disks disk reassign -s` *`node2_sysid`* `-d` *`node4_sysid`*

Per `<node2_sysid>` utilizzare le informazioni acquisite in "Fase 10" Della sezione *Record node2 information*. Per *`node4_sysid`*, utilizzare le informazioni acquisite in Fase 23.

> Il `-p` l'opzione è richiesta solo in modalità di manutenzione quando sono presenti dischi condivisi.

Il `disk reassign` command riassegna solo i dischi per i quali *`node2_sysid`* è il proprietario corrente.

Il sistema visualizza il seguente messaggio:

```
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n
```

Invio `n` quando viene richiesto di interrompere la riassegnazione del disco.

Quando viene richiesto di interrompere la riassegnazione del disco, è necessario rispondere a una serie di richieste come indicato di seguito:

a. Il sistema visualizza il seguente messaggio:

```
After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
```

b. Invio `y` per continuare.

Il sistema visualizza il seguente messaggio:

```
Disk ownership will be updated on all disks previously belonging to
Filer with sysid <sysid>.
Do you want to continue (y/n)? y
```

a. Invio `y` per consentire l'aggiornamento della proprietà del disco.

22. Se si esegue l'aggiornamento da un sistema con dischi esterni a un sistema che supporta dischi interni ed esterni (ad esempio, sistemi A800), impostare node4 come root per confermare che si avvia dall'aggregato root di node2.

Attenzione: È necessario eseguire le seguenti procedure secondarie nell'ordine esatto indicato; in caso contrario, si potrebbe verificare un'interruzione o persino la perdita di dati.

La seguente procedura imposta node4 per l'avvio dall'aggregato root di node2:

a. Controllare le informazioni su RAID, plex e checksum per l'aggregato node2:

   `aggr status -r`

b. Controllare lo stato generale dell'aggregato node2:

   `aggr status`

c. Se necessario, portare online l'aggregato node2:

   `aggr_online root_aggr_from_node2`

d. Impedire al node4 di avviarsi dal proprio aggregato root originale:

   `aggr offline root_aggr_on_node4`

e. Impostare l'aggregato root node2 come nuovo aggregato root per node4:

   `aggr options aggr_from_node2 root`

23. Verificare che il controller e lo chassis siano configurati come `ha` immettendo il seguente comando e osservando l'output:

    `ha-config show`

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

    ```
    *> ha-config show
       Chassis HA configuration: ha
       Controller HA configuration: ha
    ```

    I sistemi registrano in una PROM se si trovano 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.

    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.`

    Se si dispone di una configurazione MetroCluster, utilizzare i seguenti comandi per correggere la configurazione:

    `ha-config modify controller mcc`

```
ha-config modify chassis mcc.
```

24. Distruggere le caselle di posta sul node4:

```
mailbox destroy local
```

25. Uscire dalla modalità di manutenzione:

```
halt
```

Il sistema si arresta al prompt dell'ambiente di avvio.

26. Al nodo 3, controllare la data, l'ora e il fuso orario del sistema:

```
date
```

27. Al nodo 4, controllare la data al prompt dell'ambiente di boot:

```
show date
```

28. Se necessario, impostare la data sul node4:

```
set date mm/dd/yyyy
```

29. Al nodo 4, controllare l'ora al prompt dell'ambiente di boot:

```
show time
```

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

```
set time hh:mm:ss
```

31. Verificare che l'ID del sistema partner sia impostato correttamente come indicato inFase 19 in opzione.

```
printenv partner-sysid
```

32. Se necessario, impostare l'ID di sistema del partner su node4:

```
setenv partner-sysid node3_sysid
```

a. Salvare le impostazioni:

```
saveenv
```

33. Al prompt dell'ambiente di boot, accedere al menu di boot:

```
boot_ontap menu
```

34. Nel menu di avvio, selezionare l'opzione **(6) Aggiorna flash dalla configurazione di backup** immettendo `6` quando richiesto.

Il sistema visualizza il seguente messaggio:

```
This will replace all flash-based configuration with the last backup to
disks. Are you sure you want to continue?:
```

35. Invio `y` quando richiesto.

    L'avvio procede normalmente e il sistema richiede di confermare la mancata corrispondenza dell'ID di sistema.

    > Il sistema potrebbe riavviarsi due volte prima di visualizzare l'avviso di mancata corrispondenza.

36. Confermare la mancata corrispondenza. Il nodo potrebbe completare un ciclo di riavvio prima di avviarsi normalmente.
37. Accedere a node4.

Impostare la configurazione FC o UTA/UTA2 su node4

Se node4 dispone di porte FC integrate, porte UTA/UTA2 (onboard Unified target adapter) o una scheda UTA/UTA2, è necessario configurare le impostazioni prima di completare il resto della procedura.

A proposito di questa attività

Potrebbe essere necessario completareConfigurare le porte FC sul nodo 4 OControllare e configurare le porte UTA/UTA2 sul nodo 4 o entrambe le sezioni.

Se node4 non dispone di porte FC integrate, porte UTA/UTA2 integrate o una scheda UTA/UTA2 (ad esempio, sistemi AFF e FAS introdotti a partire da ONTAP 9.15.1) e si sta aggiornando un sistema con dischi di archiviazione, è possibile passare a"Mappare le porte dal nodo 2 al nodo 4" .

Configurare le porte FC sul nodo 4

Se node4 dispone di porte FC, integrate o su un adattatore FC, è necessario impostare le configurazioni delle porte sul nodo prima di metterlo in servizio, perché le porte non sono preconfigurate. Se le porte non sono configurate, si potrebbe verificare un'interruzione del servizio.

Prima di iniziare

È necessario disporre dei valori delle impostazioni della porta FC del nodo 2 salvati nella sezione "Preparare i nodi per l'aggiornamento".

A proposito di questa attività

È possibile saltare questa sezione se il sistema non dispone di configurazioni FC. Se il sistema dispone di porte UTA/UTA2 integrate o di un adattatore UTA/UTA2, configurarle in Controllare e configurare le porte UTA/UTA2 sul nodo 4.

> Immettere i comandi in questa sezione al prompt del cluster.

Fasi

1. Visualizza informazioni su tutti gli adattatori di rete FC e convergenti sul sistema:

```
system node hardware unified-connect show
```

2. Confrontare le impostazioni FC sui nuovi nodi con quelle acquisite in precedenza dal nodo originale.
3. Modificare le porte FC sul nodo 4 in base alle necessità:
   - Per programmare le porte di destinazione:

     ```
     system node hardware unified-connect modify -type \| -t target -adapter port_name
     ```

   - Per programmare le porte initiator:

     ```
     system node unified-connect modify type \| -t initiator -adapter port_name
     ```

   `-type` È il tipo, la destinazione o l'iniziatore FC4.
4. Verificare le nuove impostazioni immettendo il seguente comando ed esaminando l'output:

   ```
   system node unified-connect show
   ```

5. Eseguire una delle seguenti operazioni:

Se le impostazioni FC predefinite sui nuovi nodi sono…	**Quindi…**
Le stesse di quelle acquisite sui nodi originali	Vai aFase 9 .
Diverso da quelli acquisiti sui nodi originali	Vai aStep6 .

6. Esci dalla modalità di manutenzione:

   ```
   halt
   ```

7. Dopo aver immesso il comando, attendere che il sistema si arresti al prompt dell'ambiente di avvio.
8. Avviare node4 immettendo il seguente comando al prompt dell'ambiente di avvio:

   ```
   boot_ontap
   ```

9. Esegui una delle seguenti azioni:
   - Passare a. Controllare e configurare le porte UTA/UTA2 sul nodo 4 Se node4 ha una scheda UTA/UTA2A o porte UTA/UTA2 integrate.
   - Saltare la sezione e passare a. "Mappare le porte dal nodo 2 al nodo 4" Se node4 non dispone di una scheda UTA/UTA2 o di porte UTA/UTA2 integrate.

Controllare e configurare le porte UTA/UTA2 sul nodo 4

Se node4 dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2A, è necessario controllare la configurazione delle porte e configurarle, a seconda di come si desidera utilizzare il sistema aggiornato.

Prima di iniziare

È necessario disporre dei moduli SFP+ corretti per le porte UTA/UTA2.

A proposito di questa attività

Le porte UTA/UTA2 possono essere configurate in modalità FC nativa o UTA/UTA2A. La modalità FC supporta l'iniziatore FC e la destinazione FC; la modalità UTA/UTA2 consente al traffico simultaneo di NIC e FCoE di condividere la stessa interfaccia SFP+ 10 GbE e supporta la destinazione FC.

I materiali di marketing NetApp potrebbero utilizzare il termine UTA2 per fare riferimento agli adattatori e alle porte CNA. Tuttavia, la CLI utilizza il termine CNA.

Le porte UTA/UTA2 potrebbero essere su un adattatore o sul controller con le seguenti configurazioni:

- Le schede UTA/UTA2 ordinate contemporaneamente al controller vengono configurate prima della spedizione in modo da avere la personalità richiesta.
- Le schede UTA/UTA2 ordinate separatamente dal controller vengono fornite con il linguaggio di destinazione FC predefinito.
- Le porte UTA/UTA2 integrate sui nuovi controller sono configurate (prima della spedizione) in modo da avere la personalità richiesta.

Tuttavia, è possibile controllare la configurazione delle porte UTA/UTA2 sul nodo 4 e modificarla, se necessario.

Immettere i comandi in questa sezione al prompt del cluster, a meno che non venga richiesto di entrare in modalità Manutenzione. Se si dispone di un sistema MetroCluster FC, è necessario essere in modalità di manutenzione per configurare le porte UTA/UTA2.

Fasi

1. Controlla come sono attualmente configurate le porte sul nodo 4:

   ```
   system node hardware unified-connect show
   ```

2. Se il modulo SFP+ corrente non corrisponde all'utilizzo desiderato, sostituirlo con il modulo SFP+ corretto.

   Contattare il rappresentante NetApp per ottenere il modulo SFP+ corretto.

3. Esaminare l'output di `system node hardware unified-connect show` oppure `ucadmin show` Controllare e determinare se le porte UTA/UTA2 hanno la personalità desiderata.
4. Eseguire una delle seguenti operazioni:

Se la porta CNA…	Quindi…
Non avere la personalità che si desidera	Passare a. Fase 5.
Avere la personalità che si desidera	Saltare i passaggi da 5 a 12 e passare a. Fase 13.

5. Se il sistema dispone di dischi di archiviazione ed esegue Data ONTAP 8.3, avviare node4 ed entrare in modalità di manutenzione:

   ```
   boot_ontap maint
   ```

6. Verificare le impostazioni immettendo il seguente comando ed esaminandone l'output:

   ```
   ucadmin show
   ```

7. Eseguire una delle seguenti operazioni:

Se si sta configurando…	Quindi…
Porte su una scheda UTA/UTA2A	Vai aFase 8 .
Porte UTA/UTA2 integrate	Salta il passaggio 8 e vai aFase 9 .

8. Se l'adattatore è in modalità iniziatore e la porta UTA/UTA2 è online, metti offline la porta UTA/UTA2:

   `storage disable adapter` *`adapter_name`*

   Gli adattatori in modalità di destinazione sono automaticamente offline in modalità di manutenzione.

9. Se la configurazione corrente non corrisponde all'uso desiderato, immettere il seguente comando per modificare la configurazione in base alle esigenze:

   `ucadmin modify -m fc|cna -t initiator|target` *`adapter_name`*

   - `-m` È la modalità Personality: FC o 10GbE UTA.
   - `-t` È il tipo FC4: Destinazione o iniziatore.

   > È necessario utilizzare l'iniziatore FC per le unità nastro e la destinazione FC per i client SAN.

10. Se il sistema dispone di dischi di archiviazione, immettere il seguente comando:

    `halt`

    Il sistema si arresta al prompt dell'ambiente di avvio.

    a. Immettere il seguente comando:

       `boot_ontap`

11. Se il sistema dispone di dischi di archiviazione, immettere il seguente comando:

    `system node hardware unified-connect show`

    L'output degli esempi seguenti mostra che il tipo di adattatore FC4 "1b" sta cambiando in `initiator` e che la modalità degli adattatori "2a" e "2b" stia cambiando in `cna`.

```
cluster1::> system node hardware unified-connect show
                Current  Current    Pending  Pending    Admin
Node  Adapter  Mode     Type       Mode     Type       Status
----  -------  -------  ---------  -------  -------    -----
f-a    1a      fc       initiator  -        -          online
f-a    1b      fc       target     -        initiator  online
f-a    2a      fc       target     cna      -          online
f-a    2b      fc       target     cna      -          online
4 entries were displayed.
```

12. Inserire le porte di destinazione in linea immettendo uno dei seguenti comandi, una volta per ciascuna porta:

    `network fcp adapter modify -node node_name -adapter adapter_name -state up`

13. collegare la porta via cavo.

Mappare le porte dal nodo 2 al nodo 4

È necessario assicurarsi che le porte fisiche sul nodo 2 siano mappate correttamente alle porte fisiche sul nodo 4, in modo che il nodo 4 comunichi con gli altri nodi del cluster e con la rete dopo l'aggiornamento.

Prima di iniziare

È necessario disporre già di informazioni sulle porte dei nuovi nodi; per accedere a queste informazioni, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*. Le informazioni vengono utilizzate più avanti in questa sezione.

La configurazione software del nodo 4 deve corrispondere alla connettività fisica del nodo 4 e la connettività IP deve essere ripristinata prima di continuare con l'aggiornamento.

A proposito di questa attività

Le impostazioni delle porte possono variare a seconda del modello dei nodi.

Fasi

1. Per verificare se l'installazione è un cluster senza switch a due nodi, procedere come segue:

    a. Impostare il livello di privilegio su Advanced (avanzato):

    `set -privilege advanced`

    b. Verificare se il setup è un cluster senza switch a due nodi:

    `network options switchless-cluster show`

    Ad esempio:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster:  false/true
```

    +
    Il valore di questo comando deve corrispondere allo stato fisico del sistema.

    a. Tornare al livello di privilegi di amministrazione utilizzando il seguente comando:

    `set -privilege admin`

2. Apportare le seguenti modifiche:

    a. Modificare le porte che fanno parte di `Cluster` dominio di broadcast:

```
network port modify -node node_name -port port_name -mtu 9000 -ipspace
Cluster
```

Questo esempio aggiunge la porta cluster "e1b" su "node2":

```
network port modify -node node2 -port e1b -ipspace Cluster -mtu 9000
```

b. Migrare le LIF del cluster alle nuove porte, una volta per ogni LIF:

```
network interface migrate -vserver vserver_name -lif lif_name source-node
node2 -destination-node node2 -destination-port port_name
```

Una volta migrate tutte le LIF del cluster e stabilita la comunicazione del cluster, il cluster deve entrare in quorum.

c. Modificare la porta home delle LIF del cluster:

```
network interface modify -vserver Cluster -lif lif_name –home-port port_name
```

d. Rimuovere le vecchie porte da `Cluster` dominio di broadcast:

```
network port broadcast-domain remove-ports -ipspace Cluster -broadcast
-domain Cluster -ports node2:port
```

e. Visualizzare il `health` stato di node2/node4:

```
cluster show -node node2 -fields health
```

f. In base alla versione di ONTAP in esecuzione sulla coppia ha sottoposta a upgrade, esegui una delle seguenti azioni:

Se la versione di ONTAP è…	**Quindi…**
da 9,8 a 9.11.1	Verificare che le LIF del cluster siano in ascolto sulla porta 7700: `::> network connections listening show -vserver Cluster`
9.12.1 o versione successiva	Saltare questo passaggio e passare a. Fase 3.

La porta 7700 in ascolto sulle porte del cluster è il risultato previsto, come mostrato nell'esempio seguente per un cluster a due nodi:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

g. Per ogni cluster LIF che non è in ascolto sulla porta 7700, imposta lo stato amministrativo della LIF su `down` e poi `up`:

```
::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
int modify -vserver Cluster -lif cluster-lif -status-admin up
```

Ripetere il passaggio secondario (f) per verificare che la LIF del cluster sia in ascolto sulla porta 7700.

3. Modifica l'appartenenza al dominio di broadcast delle porte fisiche che ospitano i file LIF dei dati.

a. Elencare lo stato di raggiungibilità di tutte le porte:

```
network port reachability show
```

b. Riparare la raggiungibilità delle porte fisiche, seguita dalle porte VLAN, eseguendo il seguente comando su ciascuna porta, una alla volta:

```
reachability repair -node node_name -port port_name
```

È previsto un avviso simile a quello riportato di seguito. Rivedere e inserire y o n, a seconda dei casi:

```
Warning: Repairing port "node_name:port" 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}:
```

c. Per consentire a ONTAP di completare la riparazione, attendere circa un minuto dopo aver eseguito `reachability repair` sull'ultima porta.

d. Elencare tutti i domini di broadcast sul cluster:

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

e. 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 corrisponde a nessuno dei domini di broadcast esistenti, ONTAP creerà nuovi domini di broadcast per queste porte. Se necessario, è possibile eliminare i domini di broadcast appena creati se tutte le porte membri diventeranno porte membri dei gruppi di interfacce. Elimina domini di broadcast:

```
broadcast-domain delete -broadcast-domain broadcast_domain
```

f. Esaminare la configurazione del gruppo di interfacce e, se necessario, aggiungere o eliminare le porte membro.

Aggiungere porte membro alle porte del gruppo di interfacce:

```
ifgrp add-port -node node_name -ifgrp ifgrp_port -port port_name
```

Rimuovere le porte membro dalle porte del gruppo di interfacce:

```
ifgrp remove-port -node node_name -ifgrp ifgrp_port -port port_name
```

g. Eliminare e ricreare le porte VLAN in base alle necessità. Elimina porte VLAN:

```
vlan delete -node node_name -vlan-name vlan_port
```

Creazione delle porte VLAN:

```
vlan create -node node_name -vlan-name vlan_port
```

A seconda della complessità della configurazione di rete del sistema da aggiornare, potrebbe essere necessario ripetere i passaggi secondari da (a) a (g) fino a quando tutte le porte non vengono posizionate correttamente dove necessario.

4. Se nel sistema non sono configurate VLAN, passare a. Fase 5. Se sono configurate VLAN, ripristinare le VLAN smontate precedentemente configurate su porte che non esistono più o che sono state configurate su porte spostate in un altro dominio di trasmissione.

a. Visualizzare le VLAN smontate:

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

b. Ripristinare le VLAN spostate sulla porta di destinazione desiderata:

```
displaced-vlans restore -node node_name -port port_name -destination-port
destination_port
```

c. Verificare che tutte le VLAN smontate siano state ripristinate:

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

d. Le VLAN vengono automaticamente collocate nei domini di trasmissione appropriati circa un minuto dopo la loro creazione. Verificare che le VLAN ripristinate siano state collocate nei domini di trasmissione appropriati:

```
network port reachability show
```

5. a partire da ONTAP 9.8, ONTAP modificherà automaticamente le porte home delle LIF se le porte vengono spostate tra domini di broadcast durante la procedura di riparazione della raggiungibilità delle porte di rete. Se la porta home di una LIF è stata spostata in un altro nodo o non è assegnata, tale LIF viene presentata come LIF spostato. Ripristinare le porte home dei file LIF spostati le cui porte home non esistono più o sono state spostate in un altro nodo.

a. Visualizzare le LIF le cui porte home potrebbero essere state spostate in un altro nodo o non esistere più:

```
displaced-interface show
```

b. Ripristinare la porta home di ciascun LIF:

```
displaced-interface restore -vserver vserver_name -lif-name lif_name
```

c. Verificare che tutte le porte LIF home siano state ripristinate:

```
displaced-interface 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, riparare la raggiungibilità come descritto in Fase 3.

6. Verificare che tutte le LIF siano amministrativamente up sulle porte appartenenti ai domini di broadcast corretti.

a. Verificare la presenza di eventuali LIF amministrativamente non disponibili:

```
network interface show -vserver vserver_name -status-admin down
```

b. Verificare la presenza di eventuali LIF non attivi dal punto di vista operativo:

```
network interface show -vserver vserver_name -status-oper down
```

c. Modificare le LIF che devono essere modificate in modo da avere una porta home diversa:

```
network interface modify -vserver vserver_name -lif lif_name -home-port
home_port
```

Per le LIF iSCSI, la modifica della porta home richiede che la LIF sia amministrativamente inattiva.

a. Ripristinare le LIF che non si trovano nelle rispettive porte home:

```
network interface revert *
```

Spostare le LIF dei dati NAS di proprietà di node2 da node3 a node4 e verificare le LIF SAN sul node4

Dopo aver mappato le porte da node2 a node4 e prima di spostare gli aggregati node2 da node3 a node4, è necessario spostare i dati NAS LIF di proprietà di node2 attualmente su node3 da node3 a node4. È inoltre necessario verificare le LIF SAN sul nodo 4.

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. Verifica che i file LIF siano integri

e posizionati sulle porte appropriate dopo aver portato il node4 online.

Fasi

1. Elencare tutte le LIF dei dati NAS che non sono di proprietà di node3 immettendo il seguente comando su entrambi i nodi e acquisendo l'output:

   ```
   network interface show -role data -curr-node node3 -is-home false
   ```

2. se il cluster è configurato per le LIF SAN, registrare le LIF SAN e le informazioni di configurazione esistenti "foglio di lavoro" da utilizzare in seguito nella procedura.

   a. Elencare le LIF SAN sul node3 ed esaminare l'output:

      ```
      network interface show -data-protocol fc*
      ```

      Il sistema restituisce un output simile al seguente esempio:

      ```
      cluster1::> net int show -data-protocol fc*
        (network interface show)
                  Logical     Status     Network            Current
      Current Is
      Vserver     Interface   Admin/Oper Address/Mask       Node
      Port    Home
      ----------  ----------  ---------- ------------------ -------------
      ------- ----
      svm2_cluster1
                  lif_svm2_cluster1_340
                              up/up      20:02:00:50:56:b0:39:99
                                                            cluster1-01
      1b      true
                  lif_svm2_cluster1_398
                              up/up      20:03:00:50:56:b0:39:99
                                                            cluster1-02
      1a      true
                  lif_svm2_cluster1_691
                              up/up      20:01:00:50:56:b0:39:99
                                                            cluster1-01
      1a      true
                  lif_svm2_cluster1_925
                              up/up      20:04:00:50:56:b0:39:99
                                                            cluster1-02
      1b      true
      4 entries were displayed.
      ```

   b. Elencare le configurazioni esistenti ed esaminare l'output:

      ```
      fcp adapter show -fields switch-port,fc-wwpn
      ```

Il sistema restituisce un output simile al seguente esempio:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  -----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

3. Eseguire una delle seguenti operazioni:

In caso di node2…	Descrizione
Ha configurato gruppi di interfacce o VLAN	Passare a. Fase 4.
Non sono stati configurati gruppi di interfacce o VLAN	Saltare la fase 4 e passare a. Fase 5.

4. eseguire i seguenti passaggi per migrare qualsiasi file LIF dati NAS ospitati su gruppi di interfacce e VLAN che erano originariamente sul nodo 2 dal nodo 3 al nodo 4.

   a. Migrare le LIF ospitate su node3 che in precedenza appartenevano a node2 su un gruppo di interfacce a una porta su node4 in grado di ospitare LIF sulla stessa rete immettendo il seguente comando, una volta per ciascuna LIF:

      ```
      network interface migrate -vserver vserver_name -lif lif_name -destination
      -node node4 -destination-port netport|ifgrp
      ```

   b. Modificare la porta home e il nodo home dei file LIF in Sotto-fase A. Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

      ```
      network interface modify -vserver vserver_name -lif datalif_name -home-node
      node4 home-port netport|ifgrp
      ```

c. Migrate le LIF ospitate su node3 che in precedenza appartenevano a node2 su una porta VLAN a una porta su node4 in grado di ospitare LIF sulla stessa rete immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface migrate -vserver vserver_name -lif datalif_name
-destination-node node4 -destination-port netport|ifgrp
```

d. Modificare la porta home e il nodo home dei file LIF in Sotto-fase c Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface modify -vserver vserver_name -lif datalif_name -home-node
node4 home-port netport|ifgrp
```

5. eseguire una delle seguenti operazioni:

Se il cluster è configurato per…	Quindi…
NAS	Completo Fase 6 attraverso Fase 9, Saltare il passaggio 10 e completare Fase 11 attraverso Fase 14.
SAN	Saltare i passaggi da 6 a 9 e completare Fase 10 attraverso Fase 14.
NAS e SAN	Completo Fase 6 attraverso Fase 14.

6. se si dispone di porte dati non uguali sulle piattaforme, immettere il seguente comando per aggiungere le porte al dominio di trasmissione:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt ports node:port
```

Nell'esempio seguente viene aggiunta la porta "e0a" sul nodo "6280-1" e la porta "e0i" sul nodo "8060-1" per trasmettere la gestione del dominio in IPSpace Default:

```
cluster::> network port broadcast-domain add-ports -ipspace Default
-broadcast-domain mgmt -ports 6280-1:e0a, 8060-1:e0i
```

7. Migrare ciascun LIF dati NAS in node4 immettendo il seguente comando, una volta per ogni LIF:

```
network interface migrate -vserver vserver-name -lif datalif-name -destination
-node node4 -destination-port netport|ifgrp -home-node node4
```

8. Assicurarsi che la migrazione dei dati sia persistente:

```
network interface modify -vserver vserver_name -lif datalif_name -home-port
netport|ifgrp
```

9. verifica lo stato di tutti i collegamenti come `up` immettendo il seguente comando per elencare tutte le porte di rete ed esaminarne l'output:

```
network port show
```

L'esempio seguente mostra l'output di `network port show` Comando con alcune LIF in alto e altre in

basso:

```
cluster::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- -----------
node3
       a0a       Default      -                up       1500  auto/1000
       e0M       Default      172.17.178.19/24 up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0a-1     Default      172.17.178.19/24 up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
node4
       e0M       Default      172.17.178.19/24 up       1500  auto/100
       e0a       Default      172.17.178.19/24 up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
12 entries were displayed.
```

10. se l'output di `network port show` il comando visualizza le porte di rete che non sono disponibili nel nuovo nodo e che sono presenti nei nodi precedenti, eliminare le porte di rete precedenti completando le seguenti operazioni secondarie:

    a. Immettere il livello di privilegio avanzato immettendo il seguente comando:

       `set -privilege advanced`

    b. Immettere il seguente comando, una volta per ogni vecchia porta di rete:

       `network port delete -node` *`node_name`* `-port` *`port_name`*

    c. Tornare al livello admin immettendo il seguente comando:

       `set -privilege admin`

11. verificare che le LIF SAN si trovino sulle porte corrette sul node4 completando i seguenti passaggi secondari:

    a. Immettere il seguente comando ed esaminarne l'output:

       `network interface show -data-protocol iscsi|fcp -home-node node4`

       Il sistema restituisce un output simile al seguente esempio:

```
cluster::> network interface show -data-protocol iscsi|fcp -home-node
node4
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            a0a          up/down  10.63.0.53/24      node4
a0a     true
            data1        up/up    10.63.0.50/18      node4
e0c     true
            rads1        up/up    10.63.0.51/18      node4
e1a     true
            rads2        up/down  10.63.0.52/24      node4
e1b     true
vs1
            lif1         up/up    172.17.176.120/24  node4
e0c     true
            lif2         up/up    172.17.176.121/24  node4
```

b. Verificare che il nuovo `adapter` e. `switch-port` le configurazioni sono corrette confrontando l'output di `fcp adapter show` con le nuove informazioni di configurazione registrate nel foglio di lavoro in Fase 2.

   Elencare le nuove configurazioni LIF SAN al nodo 4:

   `fcp adapter show -fields switch-port,fc-wwpn`

   Il sistema restituisce un output simile al seguente esempio:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  -----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

Se un LIF SAN nella nuova configurazione non si trova su un adattatore ancora collegato allo stesso `switch-port`, potrebbe causare un'interruzione del sistema quando si riavvia il nodo.

c. Se node4 ha LIF SAN o gruppi DI LIF SAN che si trovano su una porta che non esisteva sul node2, spostarli su una porta appropriata sul node4 immettendo uno dei seguenti comandi:

   i. Impostare lo stato LIF su DOWN (giù):

      `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-status -admin down`

   ii. Rimuovere la LIF dal set di porte:

      `portset remove -vserver` *`vserver_name`* `-portset` *`portset_name`* `-port-name` *`port_name`*

   iii. Immettere uno dei seguenti comandi:

      - Spostare una singola LIF:

        `network interface modify -lif` *`lif_name`* `-home-port` *`new_home_port`*

      - Spostare tutte le LIF su una singola porta inesistente o errata su una nuova porta:

        `network interface modify {-home-port` *`port_on_node2`* `-home-node` *`node2`* `-role data} -home-port` *`new_home_port_on_node4`*

- Aggiungere nuovamente i file LIF al set di porte:

  `portset add -vserver vserver_name -portset portset_name -port-name port_name`

> È necessario spostare I file LIF SAN su una porta con la stessa velocità di collegamento della porta originale.

12. Modificare lo stato di tutti i LIF in `up` In questo modo, i LIF possono accettare e inviare traffico sul nodo immettendo il seguente comando:

    `network interface modify -vserver vserver_name -home-port port_name -home-node node4 lif lif_name -status-admin up`

13. Verificare che le LIF SAN siano state spostate nelle porte corrette e che le LIF abbiano lo stato di `up` immettendo il seguente comando su uno dei nodi ed esaminando l'output:

    `network interface show -home-node node4 -role data`

14. 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 -status-admin up`

Foglio di lavoro: Informazioni da registrare prima di spostare i file LIF dei dati NAS in node4

Per verificare di disporre della configurazione corretta dopo aver spostato LE LIF SAN da node3 a node4, è possibile utilizzare il seguente foglio di lavoro per registrare `adapter` e. `switch-port` Informazioni per ciascun LIF.

Registrare la LIF `adapter` informazioni da `network interface show -data-protocol fc*` output del comando e il `switch-port` informazioni da `fcp adapter show -fields switch-port,fc-wwpn` output del comando per node3.

Dopo aver completato la migrazione al nodo 4, registrare il LIF `adapter` e. `switch-port` Informazioni per i LIF sul node4 e verificare che ciascun LIF sia ancora connesso allo stesso `switch-port`.

Node3			**Node4**		
LIF	`adapter`	`switch-port`	LIF	`adapter`	`switch-port`

Spostare gli aggregati non root node2 da node3 a node4

Dopo aver trasferito gli aggregati non root di node2 in node3, è necessario trasferirli da node3 a node4.

Fasi

1. immettere il seguente comando su uno dei controller ed esaminare l'output per identificare gli aggregati non root da spostare:

   `storage aggregate show -owner-name` *`node3`* `-home-id` *`node2_system_id`*

2. Spostare gli aggregati completando le seguenti fasi secondarie:

   a. Accedere al livello di privilegio avanzato immettendo il seguente comando su uno dei nodi:

      `set -privilege advanced`

   b. Immettere il seguente comando:

      `storage aggregate relocation start -node` *`node3`* `-destination` *`node4`* `-aggregate -list` *`aggr_name1, aggr_name2…`* `-ndo-controller-upgrade true`

   L'elenco aggregato è l'elenco degli aggregati di proprietà del node4 ottenuti in Fase 1.

   a. Quando richiesto, immettere `y`.

      Il trasferimento avviene in background. La riposizionamento di un aggregato potrebbe richiedere da pochi secondi a un paio di minuti. Il tempo include sia le parti di fuori servizio del client che quelle di non fuori servizio. Il comando non ricolloca nessun aggregato offline o limitato.

   b. Tornare al livello di amministrazione:

      `set -privilege admin`

3. controllare lo stato del trasferimento:

   `storage aggregate relocation show -node` *`node3`*

   Viene visualizzato l'output `Done` per un aggregato dopo che è stato trasferito.

   Attendere che tutti gli aggregati node2 siano stati riposizionati al node4 prima di passare alla fase successiva.

4. Eseguire una delle seguenti operazioni:

In caso di trasferimento di…	Quindi…
Tutti gli aggregati hanno avuto successo	Passare a. Fase 5.

In caso di trasferimento di…	Quindi…

Qualsiasi aggregato ha avuto esito negativo o è stato vetoato	a. Controllare i registri EMS per l'azione correttiva.
	b. Eseguire l'azione correttiva.
	c. Accedere al livello di privilegio avanzato immettendo il seguente comando su uno dei nodi:
	`set -privilege advanced`
	d. Spostare eventuali aggregati guasti o vetoed:
	`storage aggregate relocation start -node node3 destination node4 -aggregate-list aggr_name1, aggr_name2… ndo-controller-upgrade true`
	L'elenco aggregato è l'elenco degli aggregati non riusciti o vetoati.
	e. Quando richiesto, immettere `y`.
	f. Tornare al livello admin immettendo il seguente comando:
	`set -privilege admin`
	Se necessario, è possibile forzare il trasferimento utilizzando uno dei seguenti metodi:
	• Ignorare i controlli di veto:
	`storage aggregate relocation start -override -vetoes -ndo-controller-upgrade`
	• Esclusione dei controlli di destinazione:
	`storage aggregate relocation start -override -destination-checks -ndocontroller-upgrade`
	Per ulteriori informazioni sui comandi di trasferimento degli aggregati di storage, fare riferimento a. "Riferimenti" Per collegarsi alla gestione di *dischi e aggregati con i comandi CLI* e *ONTAP 9: Manuale riferimento pagina*.

5. verificare che tutti gli aggregati non root node2 siano online e che il loro stato sia su node4:

   `storage aggregate show -node node4 -state offline -root false`

   Gli aggregati node2 sono stati elencati nell'output del comando in Fase 1.

6. Se un aggregato è diventato offline o straniero, portarlo online utilizzando il seguente comando per ogni aggregato:

   `storage aggregate online -aggregate aggr_name`

7. Verificare che tutti i volumi negli aggregati node2 siano online sul node4:

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

8. Se alcuni volumi sono offline al nodo4, portarli online:

   ```
   volume online -vserver vserver-name -volume volume_name
   ```

9. Invia un messaggio AutoSupport post-upgrade a NetApp per il node4:

   ```
   system node autosupport invoke -node node4 -type all -message "node2
   successfully upgraded from platform_old to platform_new"
   ```

Fase 6. Completare l'aggiornamento

Gestire l'autenticazione utilizzando i server KMIP

Con ONTAP 9.5 e versioni successive, è possibile utilizzare i server KMIP (Key Management Interoperability Protocol) per gestire le chiavi di autenticazione.

Fasi

1. Aggiungere un nuovo controller:

   ```
   security key-manager setup -node new_controller_name
   ```

2. Aggiungere il gestore delle chiavi:

   ```
   security key-manager -add 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 show -status
   ```

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

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

Verificare che i nuovi controller siano impostati correttamente

Per confermare la corretta configurazione, attivare la coppia ha. Inoltre, è possibile verificare che node3 e node4 possano accedere reciprocamente allo storage e che nessuno dei due possieda le LIF dei dati appartenenti ad altri nodi del cluster. Inoltre, confermi 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. Abilitare il failover dello storage immettendo il seguente comando su uno dei nodi:

   ```
   storage failover modify -enabled true -node <node3>
   ```

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. Eseguire una delle seguenti operazioni:

Se il cluster è un…	Descrizione
Cluster a due nodi	Abilitare la disponibilità elevata del cluster immettendo il seguente comando su uno dei nodi: `cluster ha modify -configured true`
Cluster con più di due nodi	Passare a. Fase 4.

4. verificare che node3 e node4 appartengano allo stesso cluster immettendo il seguente comando ed esaminando l'output:

   `cluster show`

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

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

6. Verificare che né node3 né node4 detengano le LIF dei dati di proprietà di altri nodi del cluster immettendo il seguente comando ed esaminando l'output:

   `network interface show`

   Se il nodo 3 o il nodo 4 possiede le LIF dei dati di proprietà di altri nodi del cluster, utilizzare il `network interface revert` Comando per ripristinare le LIF dei dati al proprietario di casa.

7. 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>
   ```

8. Determinare se i volumi sono offline:

   ```
   volume show -node <node3> -state offline
   volume show -node <node4> -state offline
   ```

9. Se alcuni volumi non sono in linea, confrontarli con l'elenco dei volumi non in linea in cui sono stati acquisiti "Fase 19 (d)" In *preparare i nodi per l'aggiornamento* e portare online qualsiasi volume offline, come richiesto, immettendo il seguente comando, una volta per ogni volume:

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

10. Installare nuove licenze per i nuovi nodi immettendo 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, ciascuna chiave di licenza separata da una virgola.

11. se nella configurazione vengono utilizzati dischi con crittografia automatica ed è stato impostato `kmip.init.maxwait` variabile a. `off` (ad esempio, in "Fase 16" Of *Install and boot node3*), devi disimpostare la variabile:

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

12. Per rimuovere tutte le vecchie licenze dai nodi originali, immettere uno dei seguenti comandi:

    ```
    system license clean-up -unused -expired
    system license delete -serial-number <node_serial_number> -package
    <licensable_package>
    ```

    - Per eliminare tutte le licenze scadute, immettere:

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

    - Per eliminare tutte le licenze inutilizzate, immettere:

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

    - Per eliminare una licenza specifica da un cluster, immettere 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.

13. Verificare che le licenze siano installate correttamente immettendo il seguente comando ed esaminandone l'output:

```
system license show
```

Puoi confrontare l'output con l'output che hai catturato in"Fase 29" di *Preparare i nodi per l'aggiornamento*.

14. Configurare gli SP eseguendo il seguente comando su entrambi i nodi:

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

Passare a. "Riferimenti" Per informazioni dettagliate su, fare riferimento alla sezione *Guida all'amministrazione del sistema* e ai *comandi di ONTAP 9: Guida di riferimento alla pagina* `system service- processor network modify` comando.

15. Se si desidera configurare un cluster senza switch sui nuovi nodi, visitare il sito Web all'indirizzo "Riferimenti" Per collegarsi al *sito di supporto di rete* 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 procedura descritta in "Impostare Storage Encryption sul nuovo modulo controller". In caso contrario, completare la procedura descritta in "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 show -status

security key-manager query
```

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 -add 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 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 setup -node new_controller_name`

   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 restore -node new_controller_name`

Configurare NetApp Volume o Aggregte 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.

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 utilizzando il seguente comando:

      `security key-manager -add 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 utilizzando il seguente comando:

      `security key-manager 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 utilizzando il seguente comando:

```
security key-manager setup -node new_controller_name
```

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:

Per…	Utilizzare questo comando…
Gestore delle chiavi esterno	`security key-manager external restore`Questo comando richiede la passphrase OKM
Onboard Key Manager (OKM)	`security key-manager onboard sync`

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 di gestione delle chiavi esterne. Riportare online quei volumi 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

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: 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 deve 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. Confronta l'output di Fase 1 con l'output acquisito per node1 nella sezione "Preparare i nodi per l'aggiornamento" e annotare eventuali aggregati che non sono stati correttamente ricollocati.
3. ricollocare gli aggregati rimasti al nodo4:

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

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

4. Immettere il seguente comando per 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.

Riavvio, panic o cicli di alimentazione durante la fase 2

Gli arresti anomali possono verificarsi prima, durante o subito dopo la fase 2, durante la quale si spostano gli aggregati da node1 a node2, si spostano le LIF dei dati e LE LIF SAN di proprietà di node1 in node2, si registrano le informazioni node1 e si ritirano node1.

Node1 o node2 si blocca prima della fase 2 con ha ancora attivato

Se node1 o node2 si bloccano prima della fase 2, nessun aggregato è stato ancora trasferito e la configurazione ha è ancora attivata.

A proposito di questa attività

Il takeover e il giveback possono procedere normalmente.

Fasi

1. Verificare la presenza di messaggi EMS emessi dal sistema nella console ed eseguire l'azione correttiva consigliata.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node1 si blocca durante o subito dopo la fase 2 con ha ancora attivato

Alcuni o tutti gli aggregati sono stati riallocati da node1 a node2 e ha è ancora abilitato. Node2 prenderà il controllo del volume root di 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 restituirà tutti gli aggregati non root node1.

Fasi

1. Completare"Fase 1" nella sezione *Spostare gli aggregati non radice dal nodo 1 al nodo 2* di nuovo.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node1 si blocca dopo la fase 2 mentre ha è disattivato

Node2 non prenderà 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.

   È possibile che vengano visualizzate alcune modifiche nell'output di `storage failover show` comando, ma questo è tipico e non influisce sulla procedura. Consultare la sezione relativa alla risoluzione dei problemi "Il failover dello storage non previsto mostra l'output del comando".

Node2 non funziona durante o dopo la fase 2 con ha ancora attivato

Node1 ha trasferito alcuni o tutti i suoi aggregati al node2. HA è attivato.

A proposito di questa attività

Node1 prenderà il controllo di tutti gli aggregati del node2 e di tutti i suoi aggregati che aveva trasferito al node2. Quando noda2 entra in `Waiting for Giveback` state, node1 restituisce tutti gli aggregati del node2.

Fasi

1. Completare"Fase 1" nella sezione *Spostare gli aggregati non radice dal nodo 1 al nodo 2* di nuovo.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node2 si blocca dopo la fase 2 e dopo la disattivazione di ha

Node1 non prenderà il posto.

Fasi

1. Alzati il node2.

   Durante l'avvio di node2 si verifica un'interruzione del client per tutti gli aggregati.

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

Riavvio, panic o cicli di alimentazione durante la fase 3

Gli errori possono verificarsi durante o subito dopo la fase 3, durante la quale si installa e si avvia node3, si mappano le porte da node1 a node3, si spostano le LIF dei dati e LE LIF SAN appartenenti a node1 e node2 in node3 e si spostano tutti gli aggregati da node2 a node3.

Node2 si blocca durante la fase 3 con ha disattivato e prima di spostare qualsiasi aggregato

Node3 non si prenderà il controllo in seguito a un crash node2, in quanto ha è già disattivato.

Fasi

1. Alzati il node2.

   Durante l'avvio di node2 si verifica un'interruzione del client per tutti gli aggregati.

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

Node2 si blocca durante la fase 3 dopo aver riallocato alcuni o tutti gli aggregati

Node2 ha trasferito alcuni o tutti i suoi aggregati al node3, che servirà i dati degli aggregati che sono stati ricollocati. HA disattivato.

A proposito di questa attività

Si verificherà un'interruzione del client per gli aggregati che non sono stati ricollocati.

Fasi

1. Alzati il node2.
2. Riposizionare gli aggregati rimanenti completando"Fase 1" Attraverso"Fase 5" nella sezione *Spostare gli aggregati non radice dal nodo 2 al nodo 3*.
3. Continuare con la procedura di aggiornamento della coppia di nodi.

Node3 si blocca durante la fase 3 e prima che node2 abbia riallocato gli aggregati

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.

Node3 si blocca durante la fase 3 durante il trasferimento dell'aggregato

Se il nodo 3 si blocca mentre il nodo 2 sta spostando gli aggregati al nodo 3, il nodo 2 interrompe il trasferimento degli aggregati rimanenti.

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. Completare"Fase 5" di nuovo nella sezione *Spostare gli aggregati non radice dal nodo 2 al nodo 3*.
3. Continuare con la procedura di aggiornamento della coppia di nodi.

Node3 non riesce ad avviarsi dopo il blocco nella fase 3

A causa di un guasto catastrofico, il node3 non può essere avviato in seguito a un crash durante la fase 3.

Fase

1. Contattare il supporto tecnico.

Node2 si blocca dopo la fase 3 ma prima della fase 5

Node3 continua a fornire dati per tutti gli aggregati. La coppia ha è disattivata.

Fasi

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

Node3 si blocca dopo la fase 3 ma prima della fase 5

Node3 si blocca dopo la fase 3 ma prima della fase 5. La coppia ha è disattivata.

Fasi

1. Alzati il node3.

   Si verificherà un'interruzione del servizio client per tutti gli aggregati.

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

Riavvio, panic o cicli di alimentazione durante la fase 5

I crash possono verificarsi durante la fase 5, in cui si installa e si avvia node4, si mappano le porte da node2 a node4, si spostano le LIF dei dati e LE LIF SAN appartenenti a node2 da node3 a node4 e si spostano tutti gli aggregati di node2 da node3 a node4.

Node3 si blocca durante la fase 5

Node3 ha trasferito alcuni o tutti gli aggregati del node2 al node4. Node4 non prende il controllo, ma continua a servire aggregati non root che node3 ha già trasferito. La coppia ha è disattivata.

A proposito di questa attività

Si verifica un'interruzione per il resto degli aggregati fino a quando il node3 non viene riavviato.

Fasi

1. Alzati il node3.
2. Riallocare gli aggregati rimanenti che appartenevano al node2 ripetendo "Fase 1" attraverso "Fase 3" Nella sezione *spostare gli aggregati non root di node2 da node3 a node4*.

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

Node4 si blocca durante la fase 5

Node3 ha trasferito alcuni o tutti gli aggregati del node2 al node4. Node3 non prende il controllo, ma continua a servire aggregati non root che node3 possiede e quelli che non sono stati ricollocati. HA disattivato.

A proposito di questa attività

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

Fasi

1. Far salire il node4.
2. Riposizionare gli aggregati rimanenti che appartenevano al nodo 2 completando nuovamente"Fase 1" Attraverso"Fase 3" in *Sposta gli aggregati non radice del nodo2 dal nodo3 al nodo4*.
3. 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 "inattivo".

Le LIF si trovano su porte non valide dopo l'aggiornamento

Una volta completato l'aggiornamento, se si dispone di una configurazione MetroCluster, è possibile che le interfacce logiche FC (LIF) vengano lasciate su porte non corrette. È possibile eseguire un'operazione di risincronizzazione per riassegnare i LIF alle porte corrette.

Fase

1. Inserire il `metrocluster vserver resync` Comando per riallocare le LIF alle porte corrette.

   `metrocluster vserver resync -vserver` *`vserver_name`* `fcp-mc.headupgrade.test.vs`

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

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.
"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.
"Gestione delle coppie HA"	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.
"Gestione MetroCluster e disaster recovery"	Descrive come eseguire le operazioni di switchover e switchback MetroCluster, sia nelle operazioni di manutenzione pianificate che in caso di disastro.
"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 9.0: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.0 supportati.
"Comandi di ONTAP 9.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.1 supportati.
"Comandi di ONTAP 9.2: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.2 supportati.
"Comandi di ONTAP 9.3: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.3 supportati.
"Comandi di ONTAP 9.4: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.4 supportati.
"Comandi di ONTAP 9.5: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.5 supportati.
"Comandi di ONTAP 9.6: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.6 supportati.

Contenuto	Descrizione
"Comandi di ONTAP 9.7: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.7 supportati.
"Comandi di ONTAP 9.8: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.8 supportati.
"Comandi di ONTAP 9.9.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.9.1 supportati.
"Comandi di ONTAP 9.10.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.10.1 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 "sostituzione controller di sistema" per aggiornare l'hardware del controller introdotto in ONTAP 9.15.1 e versioni successive"	Descrive le procedure di trasferimento degli aggregati necessarie per aggiornare senza interruzioni i controller introdotti in ONTAP 9.15.1 e versioni successive utilizzando i comandi "system controller replace".
"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.
"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.
"Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller che esegue ONTAP 9.5 a ONTAP 9.7"	Vengono descritte le procedure di riposizionamento degli aggregati necessarie per aggiornare senza interruzioni i controller che eseguono ONTAP 9.5 a ONTAP 9.7 utilizzando i comandi "system controller replace".
"Utilizzare il trasferimento di aggregati per aggiornare manualmente l'hardware del controller con ONTAP 9.7 o versione precedente"	Descrive le procedure di trasferimento degli aggregati necessarie per eseguire aggiornamenti manuali dei controller senza interruzioni con ONTAP 9.7 o versione precedente.

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.

Aggiornare manualmente l'hardware del controller con ONTAP 9.7 o versione precedente

Scopri di più sulla procedura di aggiornamento ARL

Questa procedura descrive come aggiornare l'hardware del controller utilizzando la rilocazione manuale degli aggregati (ARL) sui sistemi che eseguono ONTAP 9.7 o versioni precedenti.

È possibile utilizzare questa procedura ARL se si sta eseguendo uno dei seguenti aggiornamenti:

- Dal sistema FAS al sistema FAS
- Dal sistema AFF al sistema AFF

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.

> In questo documento, i nodi originali sono chiamati *node1* e *node2*, mentre i nuovi nodi sono chiamati *node3* e *node4*. Durante la procedura descritta, il nodo 1 viene sostituito dal nodo 3 e il nodo 2 viene sostituito dal nodo 4. 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 originali e nuovi. 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. Devi anche leggere e comprendere il "linee guida per l'aggiornamento dei controller con ARL" e il "Workflow di upgrade 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 `wipeconfig` i comandi non sono inclusi in questa procedura. Se in precedenza è stato utilizzato l'hardware del controller sostitutivo, è necessario contattare il supporto tecnico, in particolare se i controller eseguivano Data ONTAP in 7-Mode.
- 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.
- Questa procedura si applica alle configurazioni MetroCluster a quattro e otto nodi che eseguono ONTAP 9.5 e versioni precedenti. Per le configurazioni MetroCluster con ONTAP 9.6 e versioni successive, visitare il sito Web all'indirizzo "Riferimenti" Per collegarsi a *utilizzando i comandi "sostituzione controller di sistema" per aggiornare l'hardware del controller che esegue ONTAP 9,5 a ONTAP 9,7*.

Decidere se utilizzare questa procedura di ricollocazione aggregata

Questa procedura descrive come aggiornare l'hardware del controller utilizzando la rilocazione manuale degli aggregati (ARL) su sistemi che eseguono ONTAP 9.7 o versioni precedenti. Questa complessa procedura dovrebbe essere utilizzata solo da amministratori ONTAP esperti.

Utilizzare questo contenuto nelle seguenti circostanze:

- Non vuoi aggiungere i nuovi controller come nuova coppia ha al cluster e migrare i dati utilizzando gli spostamenti 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.
- I controller utilizzano ONTAP 9.7 o una versione precedente.
- Si dispone di un sistema che utilizza le configurazioni Fabric MetroCluster a 4 e 8 nodi con ONTAP 9.5 o versione precedente.

- Se si sta aggiornando un sistema scambiando i moduli del controller nello stesso chassis, come AFF A800 o AFF C800, NetApp consiglia vivamente di utilizzare la procedura di aggiornamento che"aggiorna i modelli di controller utilizzando ARL, mantenendo lo chassis e i dischi del sistema esistenti" . Questa procedura ARL include i passaggi che garantiscono che i dischi interni rimangano saldamente nello chassis quando si rimuovono e si installano i controller durante la procedura di aggiornamento.

  "Scopri le combinazioni di aggiornamento del sistema supportate utilizzando ARL, mantenendo lo chassis e i dischi del sistema esistenti".

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

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.

Scegli una procedura di aggiornamento hardware diversa

- "Esaminare i metodi ARL alternativi disponibili per l'aggiornamento dell'hardware del controller".
- 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*.

Informazioni correlate

Fare riferimento a "Riferimenti" per collegarsi alla *Documentazione ONTAP 9*.

Workflow di upgrade ARL

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

Aggiornare la coppia di nodi

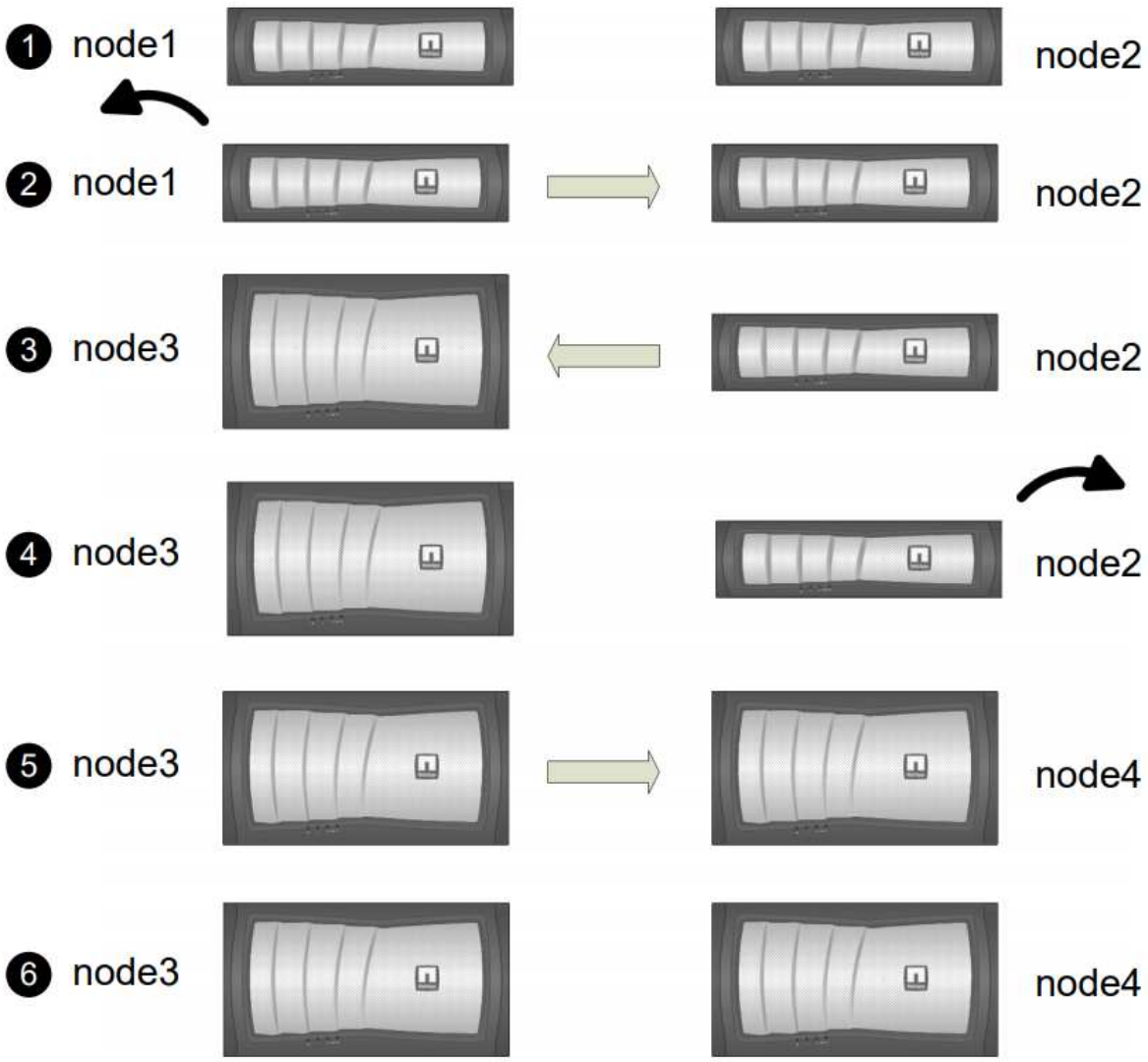
Per aggiornare la coppia di nodi, è necessario preparare i nodi originali ed eseguire una serie di passaggi sia sul nodo originale che su quello nuovo. È quindi possibile decommissionare i nodi originali.

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 figura seguente mostra le fasi della procedura. Le frecce spesse e grigio chiaro rappresentano il trasferimento degli aggregati e lo spostamento dei LIF, mentre le frecce nere più sottili rappresentano la rimozione dei nodi originali. Le immagini dei controller più piccole rappresentano i nodi originali, mentre quelle più grandi rappresentano i nuovi nodi.



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: Preparazione per l'aggiornamento"	Durante la fase 1, se necessario, si conferma che i dischi interni non contengono aggregati root o aggregati di dati, si preparano i nodi per l'aggiornamento ed eseguono una serie di controlli preliminari. Se necessario, occorre reimmettere i dischi per Storage Encryption e prepararsi all'avvio in rete dei nuovi controller. 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: Ritiro del node1"	Durante la fase 2, è possibile spostare aggregati non root da node1 a node2 e spostare le LIF di dati non SAN di proprietà di node1 a node2, inclusi gli aggregati non riusciti o vetoed. Registrare le informazioni necessarie per l'utilizzo1 più avanti nella procedura, quindi dismettere il node1. Proprietà aggregata alla fine della fase 2: • Node1 è il proprietario domestico degli aggregati node1. • Node2 è l'attuale proprietario degli aggregati node1. • Node2 è il proprietario domestico e proprietario corrente degli aggregati node2.
"Fase 3: Installazione e boot node3"	Durante la fase 3, si installa e si avvia node3, si mappano le porte di gestione del cluster e dei nodi da node1 a node3, si verifica l'installazione node3 e si spostano le LIF dei dati e LE LIF SAN appartenenti al node1 da node2 a node3. Puoi anche spostare tutti gli aggregati da node2 a node3 e spostare i dati LIF e SAN LIF di proprietà di node2 a node3. Proprietà aggregata alla fine della fase 3: • Node2 è il proprietario domestico degli aggregati node2 ma non il proprietario corrente. • Node3 è il proprietario della casa e il proprietario corrente degli aggregati originariamente appartenenti al node1. • Node2 è il proprietario domestico e proprietario corrente degli aggregati che appartengono al node2 ma non il proprietario domestico.

Fase	Descrizione
"Fase 4: Dismettere il node2"	Durante la fase 4, si registrano le informazioni necessarie per il node2 da utilizzare più avanti nella procedura, quindi si deve ritirare il node2. Non si verificano modifiche nella proprietà aggregata.
"Fase 5: Installazione e boot node4"	Durante la fase 5, si installa e si avvia node4, si mappano le porte di gestione del cluster e dei nodi da node2 a node4, si verifica l'installazione node4 e si spostano le LIF dei dati e LE LIF SAN appartenenti al node2 da node3 a node4. È inoltre possibile spostare gli aggregati node2 da node3 a node4 e spostare i dati node2 NAS LIF da node3 a 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, confermi che i nuovi nodi sono impostati correttamente e configuri Storage Encryption o NetApp Volume Encryption se i nuovi nodi sono abilitati alla crittografia. È inoltre necessario decommissionare i vecchi nodi e riprendere le operazioni di SnapMirror. Gli aggiornamenti per il disaster recovery della macchina virtuale per lo storage (SVM) non verranno interrotti in base alle pianificazioni assegnate. Non si verificano modifiche nella proprietà aggregata.

Linee guida per l'aggiornamento dei controller con ARL

Per capire se è possibile utilizzare il trasferimento aggregato (ARL) per aggiornare una coppia di controller che eseguono ONTAP da 9.0 a 9.7, dipende dalla piattaforma e dalla configurazione dei controller originali e di quelli sostitutivi.

Aggiornamenti supportati per ARL

È possibile aggiornare una coppia di nodi utilizzando ARL nei seguenti casi:

- Sia i controller originali che quelli sostitutivi devono eseguire la stessa versione di ONTAP 9.x prima dell'aggiornamento.
- I controller sostitutivi devono avere una capacità uguale o superiore a quella dei controller originali. Capacità uguale o superiore si riferisce agli attributi, ad esempio le dimensioni della NVRAM, il volume, il LUN o i limiti del numero di aggregati; si riferisce anche alle dimensioni massime del volume o dell'aggregato dei nuovi nodi.
- È possibile aggiornare i seguenti tipi di sistemi:

- Da un sistema FAS a un sistema FAS.
- Da un sistema AFF a un sistema AFF.

> Prima di eseguire un aggiornamento del sistema AFF, è necessario aggiornare ONTAP alle versioni 9.3P12, 9.4P6 o 9.5P1 o successive. Questi livelli di release sono necessari per un aggiornamento corretto.

- Per alcuni aggiornamenti del controller ARL è possibile utilizzare porte cluster temporanee sul controller sostitutivo per l'aggiornamento. Ad esempio, se si esegue l'aggiornamento da un sistema AFF A300 a un sistema AFF A400, a seconda della configurazione di AFF A400, è possibile utilizzare una delle due porte mezzanine o aggiungere una scheda di interfaccia di rete 10GbE a quattro porte per fornire porte cluster temporanee. Dopo aver completato un aggiornamento del controller utilizzando porte del cluster temporanee, è possibile migrare senza interruzioni i cluster alle porte 100 GbE del controller sostitutivo.
- Se si utilizza ONTAP 9.6P11, 9.7P8 o versioni successive, si consiglia di attivare il Takeover di connettività, livellosità e monitoraggio della disponibilità (CLAM) per riportare il cluster al quorum quando si verificano determinati guasti del nodo. Il `kernel-service` il comando richiede un accesso avanzato a livello di privilegio. Per ulteriori informazioni, consulta: "Articolo SU436 della Knowledge base di NetApp: Modifica della configurazione predefinita DI Takeover DI CLAM".
- L'upgrade del controller tramite ARL è supportato sui sistemi configurati con volumi di conformità SnapLock Enterprise e SnapLock.

È necessario verificare se l'ARL può essere eseguito sui controller originali e sostitutivi. È necessario controllare le dimensioni di tutti gli aggregati definiti e il numero di dischi supportati dal sistema originale. Quindi confrontarli con la dimensione aggregata e il numero di dischi supportati dal nuovo sistema. Per accedere a queste informazioni, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*. 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.

È necessario verificare nelle regole di combinazione del cluster se i nuovi nodi possono diventare parte del cluster con i nodi esistenti quando il controller originale viene sostituito. Per ulteriori informazioni sulle regole di combinazione dei cluster, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*.

> Entrambi i sistemi sono ad alta disponibilità (ha) o non ha. Entrambi i nodi devono avere la personalità abilitata o disabilitata; non è possibile combinare un nodo con la personalità ottimizzata per All Flash abilitata con un nodo che non ha la personalità abilitata nella stessa coppia ha. Se le personalità sono diverse, contattare il supporto tecnico.

> Se il nuovo sistema dispone di meno slot rispetto al sistema originale o se dispone di un numero inferiore o di porte diverse, potrebbe essere necessario aggiungere un adattatore al nuovo sistema. Fare riferimento a. "Riferimenti" Per informazioni dettagliate su piattaforme specifiche, consultare il sito Web del supporto NetApp *Hardware Universe*.

Aggiornamenti non supportati per ARL

Non è possibile eseguire i seguenti aggiornamenti:

- Da o verso i controller che non possono eseguire una versione di ONTAP da ONTAP 9.0 a ONTAP 9.7.

  Per informazioni sugli aggiornamenti dei controller per i sistemi che eseguono Data ONTAP in modalità 7, fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp*.

- Ai controller sostitutivi che non supportano gli shelf di dischi collegati ai controller originali.

  Per informazioni sul supporto dei dischi, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*.

- Da controller con aggregati root o aggregati di dati su dischi interni.

  Se si desidera aggiornare i controller con aggregati root o aggregati di dati su dischi interni, fare riferimento a. "Riferimenti" Per collegarsi a *Upgrade spostando volumi o storage* e passare alla procedura *aggiornamento di una coppia di nodi che eseguono Clustered Data ONTAP spostando volumi*.

  Se si desidera aggiornare ONTAP sui nodi di un cluster, fare riferimento a. "Riferimenti" Collegamento a *Upgrade ONTAP*.

Presupposti e terminologia

Il presente documento si basa sui seguenti presupposti:

- L'hardware del controller sostitutivo è nuovo e non è stato utilizzato.

  I passaggi necessari per preparare i controller usati con il `wipeconfig` I comandi non sono inclusi in questa procedura perché questa presuppone che l'hardware del controller sostitutivo sia nuovo e non sia stato utilizzato. È necessario contattare l'assistenza tecnica se l'hardware del controller sostitutivo è stato utilizzato in precedenza, soprattutto se i controller eseguivano Data ONTAP in modalità 7.

- Hai letto e compreso le linee guida per l'aggiornamento della coppia di nodi.

  Non tentare di cancellare il contenuto NVRAM . Se è necessario cancellare il contenuto della NVRAM, contattare l'assistenza tecnica NetApp .

- Si sta eseguendo il comando appropriato prima e dopo `modify` e confrontando l'output di entrambi `show` comandi per verificare che il `modify` comando riuscito.
- Se si dispone di una configurazione SAN, si dispone di LIF locali e partner per ciascuna macchina virtuale di storage (SVM), sulla coppia ha. Se non si dispone di LIF locali e partner per ogni SVM, è necessario aggiungere LA LIF dei dati SAN sul nodo remoto e locale per tale SVM prima di iniziare l'aggiornamento.
- Se si dispone di set di porte in una configurazione SAN, è necessario verificare che ogni set di porte associato contenga almeno un LIF da ciascun nodo della coppia ha.

Questa procedura utilizza il termine *prompt dell'ambiente di boot* per fare riferimento al prompt di un nodo da cui è possibile eseguire determinate attività, come il riavvio del nodo e la stampa o l'impostazione di variabili ambientali. Il prompt viene a volte chiamato in modo informale *prompt del boot loader*.

Il prompt dell'ambiente di boot viene mostrato nell'esempio seguente:

```
LOADER>
```

Licensing in ONTAP 9.7 o versioni precedenti

Alcune funzionalità richiedono licenze, emesse come *pacchetti* che includono una o più funzionalità. Ogni nodo del cluster deve disporre di una propria chiave per poter utilizzare ciascuna funzionalità nel cluster.

Se non si dispone di nuove chiavi di licenza, le funzionalità attualmente concesse in licenza nel cluster sono disponibili per il nuovo controller e continueranno a funzionare. Tuttavia, l'utilizzo di funzionalità senza licenza sul controller potrebbe non essere conforme al contratto di licenza, pertanto è necessario installare la nuova chiave di licenza o le nuove chiavi per il nuovo controller al termine dell'aggiornamento.

Tutte le chiavi di licenza sono composte da 28 caratteri alfabetici maiuscoli. Fare riferimento a. "Riferimenti" Per accedere al *sito di supporto NetApp*, dove è possibile ottenere nuove chiavi di licenza di 28 caratteri per ONTAP 9.7. o prima. Le chiavi sono disponibili nella sezione *My Support* sotto *licenze software*. Se il sito non dispone delle chiavi di licenza necessarie, contattare il rappresentante commerciale NetApp.

Per informazioni dettagliate sulle licenze, visitare il sito Web all'indirizzo "Riferimenti" Per collegarsi al *System Administration Reference*.

Crittografia dello storage

I nodi originali o i nuovi nodi potrebbero essere abilitati per Storage Encryption. In tal caso, è necessario eseguire ulteriori operazioni in questa procedura per verificare che Storage Encryption sia impostato correttamente.

Se si desidera utilizzare Storage Encryption, tutti i dischi associati ai nodi devono disporre di dischi con crittografia automatica.

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.

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.

Se si verificano problemi durante l'aggiornamento dei controller, fare riferimento a "Risolvere i problemi" sezione. Le informazioni sui guasti che possono verificarsi sono elencate in base alla fase della procedura nella "Sequenza di aggiornamento ARL" .

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

Strumenti e documentazione richiesti

È necessario disporre di strumenti specifici per installare il nuovo hardware e consultare altri documenti durante il processo di aggiornamento. È inoltre necessario registrare le informazioni essenziali per completare l'aggiornamento del controller; viene fornito un foglio di lavoro per registrare le informazioni.

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 richiesti per questo aggiornamento.

Foglio di lavoro: Informazioni da raccogliere prima e durante l'aggiornamento del controller

È necessario raccogliere determinate informazioni per supportare l'aggiornamento dei nodi originali. Queste informazioni includono gli ID dei nodi, i dettagli di porta e LIF, le chiavi di licenza e gli indirizzi IP.

È possibile utilizzare il seguente foglio di lavoro per registrare le informazioni da utilizzare in seguito nella procedura:

Informazioni necessarie	Una volta raccolti	Se utilizzato	Informazioni raccolte
Modello, ID sistema, numero di serie dei nodi originali	Fase 1: *Preparare i nodi per l'aggiornamento*	Fase 3: *Installare e avviare node3* fase 5: *Installare e avviare node4* fase 6: *Rimuovere il vecchio sistema*	
Informazioni su shelf e dischi, dettagli dello storage flash, memoria, NVRAM e schede adattatore sui nodi originali	Fase 1: *Preparazione dei nodi per l'aggiornamento*	Durante l'intera procedura	
Aggregati e volumi online sui nodi originali	Fase 1: *Preparare i nodi per l'aggiornamento*	Durante l'intera procedura per verificare che aggregati e volumi rimangano online, tranne durante una breve delocalizzazione	
Output dei comandi `network port vlan show` e. `network port ifgrp show`	Fase 1: *Preparare i nodi per l'aggiornamento*	Fase 3: *Mappare le porte dal nodo 1 al nodo 3* fase 5: *Mappare le porte dal nodo 2 al nodo 4*	
(Solo ambienti SAN) Configurazione predefinita delle porte FC	Fase 1: *Preparare i nodi per l'aggiornamento*	Durante la configurazione delle porte FC sui nuovi nodi	
Indirizzo IP degli SP	Fase 1: *Preparare i nodi per l'aggiornamento*	Fase 6: *Verificare che i nuovi controller siano impostati correttamente*	
Chiavi di licenza	Fase 1: *Preparare i nodi per l'aggiornamento*	Fase 6: *Verificare che i nuovi controller siano impostati correttamente*	

Informazioni necessarie	Una volta raccolti	Se utilizzato	Informazioni raccolte
Indirizzo IP per il server di gestione delle chiavi esterne	Fase 1: *Rekey disks for Storage Encryption*	Fase 6: *Impostare Storage Encryption sui nuovi nodi*	
Nome e percorso della directory accessibile dal web in cui si scaricano i file per avviare i nodi	Fase 1: *Prepararsi al netboot*	Fase 3: *Installare e avviare node3* fase 5: *Installare e avviare node4*	
LIF dati non SAN di proprietà di node1	Fase 2: *Spostare le LIF dei dati non SAN di proprietà del node1 in node2*	Più avanti nella sezione	
Cluster, intercluster, gestione dei nodi, gestione dei cluster e porte fisiche	Fase 2: *Registrare le informazioni del node1*	Fase 3: *Installare e avviare node3* fase 3: *Mappare le porte dal node1 al node3*	
Porte su nuovi nodi	Fase 3: *Mappare le porte dal nodo 1 al nodo 3*	Più avanti nella sezione e nella sezione *Map ports from node2 to node4*	
Porte e domini di broadcast disponibili sul nodo 3	Fase 3: *Mappare le porte dal nodo 1 al nodo 3*	Più avanti nella sezione	
Le LIF di dati non SAN non sono di proprietà di node2	*Spostamento delle LIF di dati non SAN appartenenti al nodo 1 da node2 a node3 e verifica delle LIF SAN sul nodo 3*	Più avanti nella sezione	
LIF dati non SAN di proprietà di node2	Fase 3: *Spostare le LIF dei dati non SAN di proprietà del node2 in node3*	Più avanti nella sezione	
Cluster, intercluster, gestione dei nodi, gestione dei cluster e porte fisiche	Fase 4: *Registrare le informazioni node2*	Fase 5: *Installare e avviare node4* fase 5:_ mappare le porte da node2 a node4_	
Porte di rete del cluster sul nodo 4	Fase 5: *Mappare le porte dal nodo 2 al nodo 4*	Più avanti nella sezione	
Porte e domini di broadcast disponibili sul nodo 4	Fase 5: *Mappare le porte dal nodo 2 al nodo 4*	Più avanti nella sezione	
Certificati SSL pubblici e privati per il sistema di storage e certificati SSL privati per ciascun server di gestione delle chiavi	Fase 6: *Impostare Storage Encryption sui nuovi nodi*	Più avanti nella sezione	

Riconfigurare il layout dello switch FC per ONTAP 9.1 o versione successiva

Riconfigurare il layout dello switch FC per ONTAP 9.1 o versione successiva

Se il layout dello switch FC esistente è stato configurato prima di ONTAP 9.1, è necessario riconfigurare il layout delle porte e applicare i file di configurazione di riferimento (RCF) più recenti. Questa procedura si applica solo alle configurazioni MetroCluster FC.

Prima di iniziare

È necessario identificare gli switch FC presenti nel dominio fabric.

È necessaria la password admin e l'accesso a un server FTP o SCP.

A proposito di questa attività

È necessario eseguire questa attività se il layout dello switch FC esistente è stato configurato prima di ONTAP 9.1 e si sta eseguendo l'aggiornamento a un modello di piattaforma supportato in ONTAP 9.1 o versione successiva. Non è necessario eseguire l'aggiornamento da un layout di switch esistente configurato per ONTAP 9.1 o versione successiva.

Questa procedura è senza interruzioni e richiede circa quattro ore per il completamento (esclusi rack e stack) quando i dischi vengono azzerati.

Fasi

1. "Inviare un messaggio AutoSupport personalizzato prima di riconfigurare gli switch"
2. "Verificare lo stato della configurazione MetroCluster"
3. "Verificare la presenza di errori di configurazione MetroCluster"
4. "Disattivare in modo persistente gli switch"
5. "Determinare il nuovo layout del cablaggio"
6. "Applicare i file RCF e recuperare gli switch"
7. "Abilitare gli switch in modo persistente"
8. "Verificare lo switchover, la riparazione e lo switchback"

Inviare un messaggio AutoSupport personalizzato prima di riconfigurare gli switch

Prima di riconfigurare gli switch, è necessario inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Accedere al cluster.
2. Richiamare un messaggio AutoSupport che indica l'inizio della manutenzione:

```
system node autosupport invoke -node * -type all -message MAINT=maintenance-
```

window-in-hours

Il `maintenance-window-in-hours` value specifica la lunghezza della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

3. Ripetere questi passaggi sul sito del partner.

Verificare lo stato della configurazione MetroCluster

Verificare lo stato della configurazione MetroCluster per verificarne il corretto funzionamento.

Fasi

1. Verificare che i componenti di MetroCluster siano integri:

```
metrocluster check run
```

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2017 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

2. Verificare che non siano presenti avvisi sullo stato di salute:

```
system health alert show
```

Verificare la presenza di errori di configurazione MetroCluster

È possibile utilizzare lo strumento Active IQ Config Advisor disponibile sul sito del supporto NetApp per verificare la presenza di errori di configurazione comuni.

Se non si dispone di una configurazione MetroCluster, ignorare questa sezione.

A proposito di questa attività

Active IQ Config Advisor è uno strumento per la convalida della configurazione e il controllo dello stato di salute. È possibile implementarlo sia in siti sicuri che in siti non sicuri per la raccolta di dati e l'analisi del sistema.

Il supporto per Config Advisor è limitato e disponibile solo online.

1. Scaricare il "Active IQ Config Advisor" tool.
2. Eseguire Active IQ Config Advisor, esaminare l'output e seguire i consigli per risolvere eventuali problemi.

Disattivare gli switch in modo indisabile

È necessario disattivare gli switch nel fabric in modo persistente per modificarne la configurazione.

A proposito di questa attività

Per disattivare gli switch, eseguire i comandi sulla riga di comando dello switch; i comandi utilizzati per questo non sono comandi ONTAP.

Fase

Disattivare in modo persistente lo switch:

- Per gli switch Brocade, utilizzare `switchCfgPersistentDisable` comando.
- Per gli switch Cisco, utilizzare `suspend` comando.

Il seguente comando disattiva uno switch Brocade in modo persistente:

```
FC_switch_A_1:admin> switchCfgPersistentDisable
```

Il seguente comando disattiva uno switch Cisco:

```
vsan [vsna #] suspend
```

Determinare il nuovo layout del cablaggio

È necessario determinare il cablaggio dei nuovi moduli controller e dei nuovi shelf di dischi per gli switch FC esistenti.

A proposito di questa attività

Questa attività deve essere eseguita in ogni sito MetroCluster.

Fase

Utilizzare il contenuto *Fabric-Attached MetroCluster Installation and Configuration* per determinare il layout del cablaggio per il tipo di switch in uso, utilizzando l'utilizzo della porta per una configurazione MetroCluster a otto nodi. L'utilizzo della porta dello switch FC deve corrispondere all'utilizzo descritto nel contenuto, in modo da poter utilizzare i file di configurazione di riferimento (RCF).

Passare a. "Riferimenti" Per collegarsi al contenuto di *installazione e configurazione del MetroCluster collegato al fabric*.

Se l'ambiente non può essere cablato in modo da poter utilizzare gli RCF, contattare il supporto tecnico. Non utilizzare questa procedura se il cablaggio non può utilizzare RCF.

Applicare i file RCF e recuperare gli switch

È necessario applicare i file di configurazione di riferimento (RCF) appropriati per riconfigurare gli switch in modo da ospitare i nuovi nodi. Dopo aver applicato gli RCF, è possibile recuperare gli switch.

Prima di iniziare

L'utilizzo della porta dello switch FC deve corrispondere all'utilizzo descritto nel contenuto *Fabric-Attached MetroCluster Installation and Configuration*, in modo da poter utilizzare gli RCF. Passare a. "Riferimenti" Per collegarsi al contenuto di *installazione e configurazione del MetroCluster collegato al fabric*.

Fasi

1. Accedere alla "Download di MetroCluster RCF" E selezionare gli RCF per la configurazione dello switch.

   È necessario utilizzare gli RCF corrispondenti ai modelli di switch.

2. Installare gli RCF dello switch FC selezionando la procedura corrispondente ai modelli di switch in uso e seguendo le istruzioni di installazione:
   - "Installare uno switch FC Brocade RCF"
   - "Installare uno switch FC Cisco RCF"
3. Verificare che la configurazione dello switch sia stata salvata.
4. Collegare entrambi i bridge FC-SAS agli switch FC, utilizzando il layout di cablaggio creato in "Determinare il nuovo layout del cablaggio".
5. Verificare che le porte siano in linea:
   - Per gli switch Brocade, utilizzare `switchshow` comando.
   - Per gli switch Cisco, utilizzare il programma `interface brief` comando.
6. Collegare le porte FC-VI dai controller agli switch.
7. Dai nodi esistenti, verificare che le porte FC-VI siano in linea:

   ```
   metrocluster interconnect adapter show

   metrocluster interconnect mirror show
   ```

Abilitare gli switch in modo persistente

È necessario abilitare gli switch nel fabric in modo persistente.

Fase

Abilitare costantemente lo switch:

- Per gli switch Brocade, utilizzare `switchCfgPersistentenable` comando.

```
FC_switch_A_1:admin> switchCfgPersistentenable
```

- Per gli switch Cisco, utilizzare `no suspend` comando.

```
vsan [vsna #]no suspend
```

Verificare lo switchover, la riparazione e lo switchback

Verificare le operazioni di switchover, riparazione e switchback della configurazione MetroCluster.

Fase

Fare riferimento a. "Riferimenti" Per collegarsi al contenuto di *Gestione MetroCluster e disaster recovery* e seguire le procedure per lo switchover negoziato, la riparazione e lo switchback.

Fase 1. Preparatevi per l'aggiornamento

Determinare se il controller dispone di aggregati su dischi interni

Se si stanno aggiornando i controller con dischi interni, è necessario completare diversi comandi ed esaminarne l'output per confermare che nessuno dei dischi interni contiene aggregati root o aggregati di dati.

A proposito di questa attività

Se non si stanno aggiornando controller con aggregati su dischi interni, saltare questa sezione e passare alla sezione "Preparare i nodi per l'aggiornamento".

Fasi

1. Inserisci il nodeshell, una volta per ciascuno dei nodi originali.

   `system node run -node node_name`

2. Visualizzare le unità interne:

   `sysconfig -av`

   Il sistema visualizza informazioni dettagliate sulla configurazione del nodo, incluso lo storage, come mostrato nell'output parziale mostrato nell'esempio seguente:

```
node> sysconfig -av
slot 0: SAS Host Adapter 0a (PMC-Sierra PM8001 rev. C, SAS, UP)
                Firmware rev: 01.11.06.00
                 Base WWN: 5:00a098:0008a3b:b0
                 Phy State: [0] Enabled, 6.0 Gb/s
                            [1] Enabled, 6.0 Gb/s
                            [2] Enabled, 6.0 Gb/s
                            [3] Enabled, 6.0 Gb/s
                ID Vendor Model FW Size
                00.0 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.1 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.2 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.3 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.4 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.5 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.6 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.7 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.8 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.9 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.10: NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.11: NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
...
```

3. Esaminare l'output dello storage di `sysconfig -av` per identificare i dischi interni e registrare le informazioni.

   I dischi interni hanno "00". All'inizio del proprio ID. Il "00." indica uno shelf di dischi interno e il numero dopo il punto decimale indica il singolo disco.

4. immettere il seguente comando su entrambi i controller:

   `aggr status -r`

   Il sistema visualizza lo stato aggregato del nodo, come mostrato nell'output parziale nell'esempio seguente:

```
node> aggr status -r
Aggregate aggr2 (online, raid_dp, parity uninit'd!) (block checksums)
Plex /aggr2/plex0 (online, normal, active)
RAID group /aggr2/plex0/rg0 (normal, block checksums)

RAID Disk Device    HA SHELF BAY CHAN Pool Type RPM  Used (MB/blks)
Phys (MB/blks)
--------- --------- -- ----- --- ---- ---- ---- ---- ------------------
------------------
dparity   0a.00.1   0a   0    1  SA:B  0   BSAS 7200 1695466/3472315904
1695759/3472914816
parity    0a.00.3   0a   0    3  SA:B  0   BSAS 7200 1695466/3472315904
1695759/3472914816
data      0a.00.9   0a   0    9  SA:B  0   BSAS 7200 1695466/3472315904
1695759/3472914816
...
```

Il dispositivo utilizzato per creare l'aggregato potrebbe non essere un disco fisico ma una partizione.

5. Esaminare l'output di `aggr status -r` per identificare gli aggregati utilizzando dischi interni e registrare le informazioni.

   Nell'esempio del passaggio precedente, "aggr2" utilizza dischi interni, come indicato dall'ID dello shelf "0".

6. Immettere il seguente comando su entrambi i controller:

   `aggr status -v`

   Il sistema visualizza le informazioni sui volumi sull'aggregato, come mostrato nell'output parziale nell'esempio seguente:

```
node> aggr status -v
...
 aggr2   online   raid_dp, aggr    nosnap=off, raidtype=raid_dp,
raidsize=14,
                  64-bit           raid_lost_write=on,
ignore_inconsistent=off,
                  rlw_on           snapmirrored=off, resyncsnaptime=60,
                                   fs_size_fixed=off,
lost_write_protect=on,
                                   ha_policy=cfo, hybrid_enabled=off,
percent_snapshot_space=0%,
                                   free_space_realloc=off, raid_cv=on,
thorough_scrub=off
         Volumes: vol6, vol5, vol14
...
 aggr0   online   raid_dp, aggr    root, diskroot, nosnap=off,
raidtype=raid_dp,
                  64-bit           raidsize=14, raid_lost_write=on,
ignore_inconsistent=off,
                  rlw_on           snapmirrored=off,  resyncsnaptime=60,
fs_size_fixed=off,
                                   lost_write_protect=on, ha_policy=cfo,
hybrid_enabled=off,
                                   percent_snapshot_space=0%,
free_space_realloc=off, raid_cv=on
         Volumes: vol0
```

In base all'output in Fase 4 Fase 6, aggr2 utilizza tre dischi interni, "0a.00.1", "0a.00.3" e "0a.00.9", mentre i volumi su "aggr2" sono "vol6", "vol5" e "vol14". Inoltre, nell'output della fase 6, la lettura per "aggr0" contiene la parola "root" all'inizio delle informazioni per l'aggregato. Che indica che contiene un volume root.

7. Esaminare l'output di `aggr status -v` comando per identificare i volumi appartenenti a qualsiasi aggregato presente su un disco interno e se uno di questi volumi contiene un volume root.
8. Uscire dal nodeshell immettendo il seguente comando su ciascun controller:

   `exit`

9. Eseguire una delle seguenti operazioni:

Se i controller	Quindi…
Non contenere aggregati sui dischi interni	Continuare con questa procedura.

Se i controller	Quindi…
Contengono aggregati ma non volumi sui dischi interni	Continuare con questa procedura. Prima di continuare, è necessario posizionare gli aggregati offline, quindi distruggere gli aggregati sui dischi interni. Fare riferimento a. "Riferimenti" Collegamento alla gestione di *dischi e aggregati con il contenuto CLI* per informazioni sulla gestione degli aggregati.
Contenere volumi non root sui dischi interni	Continuare con questa procedura. Prima di continuare, è necessario spostare i volumi su uno shelf di dischi esterno, posizionare gli aggregati offline e distruggere gli aggregati sui dischi interni. Fare riferimento a. "Riferimenti" Collegamento alla gestione di *dischi e aggregati con il contenuto CLI* per informazioni sullo spostamento dei volumi.
Contenere volumi root sui dischi interni	Non continuare con questa procedura. È possibile aggiornare i controller facendo riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* e utilizzare la procedura *aggiornamento dell'hardware del controller su una coppia di nodi che eseguono Clustered Data ONTAP spostando i volumi*.
Contengono volumi non root sui dischi interni e non è possibile spostare i volumi su uno storage esterno	Non continuare con questa procedura. È possibile aggiornare i controller utilizzando la procedura *aggiornamento dell'hardware del controller su una coppia di nodi che eseguono Clustered Data ONTAP spostando i volumi*. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp*, dove è possibile accedere a questa procedura.

Preparare i nodi per l'aggiornamento

Prima di poter sostituire i nodi originali, è necessario verificare che si trovino in una coppia ha, che non vi siano dischi mancanti o guasti, che possano accedere reciprocamente allo storage e che non dispongano di LIF dati assegnati agli altri nodi del cluster. È inoltre necessario raccogliere informazioni sui nodi originali e, se il cluster si trova in un ambiente SAN, confermare che tutti i nodi del cluster sono in quorum.

Fasi

1. Verificare che ciascuno dei nodi originali disponga di risorse sufficienti per supportare adeguatamente il carico di lavoro di entrambi i nodi durante la modalità Takeover.

   Fai riferimento "Riferimenti"al link *gestione coppia ha* e segui la sezione *Best practice per coppie ha*. Nessuno dei nodi originali deve essere eseguito con un utilizzo superiore al 50%; se un nodo viene eseguito con un utilizzo inferiore al 50%, può gestire i carichi per entrambi i nodi durante l'aggiornamento del controller.

2. Completare i seguenti passaggi secondari per creare una linea di base delle performance per i nodi

originali:

a. Assicurarsi che l'account utente diagnostico sia sbloccato.

> L'account utente diagnostico è destinato esclusivamente a scopi diagnostici di basso livello e deve essere utilizzato solo con le indicazioni del supporto tecnico.
>
> Per informazioni sullo sblocco degli account utente, fare riferimento a. "Riferimenti" Per collegarsi al *System Administration Reference*.

b. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* e scaricare il modulo di raccolta delle performance e delle statistiche (Perfstat Converged).

   Il tool Perfstat Converged consente di stabilire una linea di base per le performance da confrontare dopo l'aggiornamento.

c. Creare una linea di base per le performance seguendo le istruzioni sul NetApp Support Site.

3. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* e aprire un caso di supporto sul sito di supporto NetApp.

   È possibile utilizzare il caso per segnalare eventuali problemi che potrebbero verificarsi durante l'aggiornamento.

4. Verificare che le batterie NVMEM o NVRAM del nodo 3 e del nodo 4 siano cariche e, in caso contrario, ricaricarle.

   Controllare fisicamente il n. 3 e il n. 4 per verificare se le batterie NVMEM o NVRAM sono cariche. Per informazioni sui LED per il modello di node3 e node4, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*.

   > Non tentare di cancellare il contenuto NVRAM . Se è necessario cancellare il contenuto della NVRAM, contattare l'assistenza tecnica NetApp .

5. Controllare la versione di ONTAP su node3 e node4.

   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*.

   Le informazioni sulla versione di ONTAP su node3 e node4 devono essere incluse nelle confezioni di spedizione. La versione di ONTAP viene visualizzata all'avvio del nodo oppure è possibile avviare il nodo in modalità di manutenzione ed eseguire il comando:

   ```
   version
   ```

6. Controllare se sono presenti due o quattro LIF del cluster su node1 e node2:

   ```
   network interface show -role cluster
   ```

   Il sistema visualizza tutte le LIF del cluster, come mostrato nell'esempio seguente:

```
cluster::> network interface show -role cluster
        Logical    Status     Network          Current  Current Is
Vserver Interface  Admin/Oper Address/Mask     Node     Port    Home
------- ---------- ---------- ---------------- -------- ------- ----
node1
        clus1      up/up      172.17.177.2/24  node1    e0c     true
        clus2      up/up      172.17.177.6/24  node1    e0e     true
node2
        clus1      up/up      172.17.177.3/24  node2    e0c     true
        clus2      up/up      172.17.177.7/24  node2    e0e     true
```

7. Se si dispone di due o quattro LIF del cluster su node1 o node2, assicurarsi di poter eseguire il ping di entrambe le LIF del cluster in tutti i percorsi disponibili completando i seguenti passaggi secondari:

   a. Immettere il livello di privilegio avanzato:

      ```
      set -privilege advanced
      ```

      Il sistema visualizza il seguente messaggio:

      ```
      Warning: These advanced commands are potentially dangerous; use them
      only when directed to do so by NetApp personnel.
      Do you wish to continue? (y or n):
      ```

   b. Invio `y`.

   c. Eseguire il ping dei nodi e verificare la connettività:

      ```
      cluster ping-cluster -node node_name
      ```

      Il sistema visualizza un messaggio simile al seguente esempio:

```
cluster::*> cluster ping-cluster -node node1
Host is node1
Getting addresses from network interface table...
Local = 10.254.231.102 10.254.91.42
Remote = 10.254.42.25 10.254.16.228
Ping status:
...
Basic connectivity succeeds on 4 path(s) Basic connectivity fails on 0
path(s)
................
Detected 1500 byte MTU on 4 path(s):
Local 10.254.231.102 to Remote 10.254.16.228
Local 10.254.231.102 to Remote 10.254.42.25
Local 10.254.91.42 to Remote 10.254.16.228
Local 10.254.91.42 to Remote 10.254.42.25
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

+
Se il nodo utilizza due porte del cluster, si dovrebbe vedere che è in grado di comunicare su quattro percorsi, come mostrato nell'esempio.

a. Tornare al privilegio di livello amministrativo:

   ```
   set -privilege admin
   ```

8. Verificare che node1 e node2 si trovino in una coppia ha e che i nodi siano collegati tra loro e che sia possibile effettuare il takeover:

   ```
   storage failover show
   ```

   L'esempio seguente mostra l'output quando i nodi sono collegati tra loro ed è possibile effettuare il takeover:

   ```
   cluster::> storage failover show
                                Takeover
   Node           Partner        Possible State Description
   -------------- -------------- -------- -------------------------------
   node1          node2          true     Connected to node2
   node2          node1          true     Connected to node1
   ```

   Nessuno dei due nodi deve essere in giveback parziale. L'esempio seguente mostra che node1 è in giveback parziale:

```
cluster::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- -------------------------------
node1          node2          true     Connected to node2, Partial
giveback
node2          node1          true     Connected to node1
```

Se uno dei nodi è in un giveback parziale, utilizzare `storage failover giveback` il comando per eseguire il giveback e quindi utilizzare `storage failover show-giveback` il comando per assicurarsi che non venga restituito alcun aggregato. Per informazioni dettagliate sui comandi, fare riferimento al "Riferimenti"link a *ha Pair Management*.

9. Conferma che né node1 né node2 possiedono gli aggregati per i quali sono il proprietario corrente (ma non il proprietario domestico):

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

   Se né node1 né node2 possiedono aggregati per i quali è il proprietario corrente (ma non il proprietario domestico), il sistema restituirà un messaggio simile al seguente esempio:

```
cluster::> storage aggregate show -node node2 -is-home false -fields
owner-name,homename,state
There are no entries matching your query.
```

   L'esempio seguente mostra l'output del comando per un nodo denominato node2 che è il proprietario di casa, ma non il proprietario corrente, di quattro aggregati:

```
cluster::> storage aggregate show -node node2 -is-home false
               -fields owner-name,home-name,state

aggregate     home-name    owner-name   state
------------- ------------ ------------ ------
aggr1         node1        node2        online
aggr2         node1        node2        online
aggr3         node1        node2        online
aggr4         node1        node2        online

4 entries were displayed.
```

10. Eseguire una delle seguenti operazioni:

Se il comando è in Fase 9…	**Quindi…**
Con output vuoto	Saltare il passaggio 11 e passare a. Fase 12.

Se il comando è in Fase 9…	Quindi…
Ha avuto output	Passare a. Fase 11.

11. se node1 o node2 possiede aggregati per i quali è il proprietario corrente, ma non il proprietario della casa, completare i seguenti passaggi secondari:

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

    ```
    storage failover giveback -ofnode home_node_name
    ```

    b. 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.
```

12. verificare che node1 e node2 possano accedere reciprocamente allo storage e verificare che non manchino dischi:

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

    L'esempio seguente mostra l'output quando non mancano dischi:

```
cluster::> storage failover show -fields local-missing-disks,partner-
missing-disks

node     local-missing-disks partner-missing-disks
-------- ------------------- ---------------------
node1    None                None
node2    None                None
```

    Se mancano dei dischi, fare riferimento al "Riferimenti"collegamento alla gestione *disco e aggregato con la*

CLI, alla gestione *logica dello storage con la CLI* e alla gestione *coppia ha* per configurare lo storage per la coppia ha.

13. Verificare che node1 e node2 siano integri e idonei a partecipare al cluster:

    `cluster show`

    L'esempio seguente mostra l'output quando entrambi i nodi sono idonei e integri:

```
cluster::> cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
```

14. Impostare il livello di privilegio su Advanced (avanzato):

    `set -privilege advanced`

15. verificare che node1 e node2 eseguano la stessa release di ONTAP:

    `system node image show -node node1,node2 -iscurrent true`

    L'esempio seguente mostra l'output del comando:

```
cluster::*> system node image show -node node1,node2 -iscurrent true

                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- ------- ------- ------- --------- -------------------
node1
         image1   true    true    9.1         2/7/2017 20:22:06
node2
         image1   true    true    9.1         2/7/2017 20:20:48

2 entries were displayed.
```

16. Verificare che né node1 né node2 siano in possesso di LIF di dati appartenenti ad altri nodi del cluster e controllare `Current Node` e. `Is Home` colonne nell'output:

    `network interface show -role data -is-home false -curr-node node_name`

    L'esempio seguente mostra l'output quando node1 non ha LIF di proprietà di altri nodi nel cluster:

```
cluster::> network interface show -role data -is-home false -curr-node
node1
 There are no entries matching your query.
```

Nell'esempio seguente viene mostrato l'output quando node1 possiede le LIF dei dati di proprietà dell'altro nodo:

```
cluster::> network interface show -role data -is-home false -curr-node
node1

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data1      up/up      172.18.103.137/24  node1          e0d
false
            data2      up/up      172.18.103.143/24  node1          e0f
false

2 entries were displayed.
```

17. Se l'output è in Fase 15 Mostra che node1 o node2 possiede qualsiasi LIF di dati di proprietà di altri nodi nel cluster, migrare i LIF di dati lontano dal node1 o node2:

    `network interface revert -vserver * -lif *`

    Per informazioni dettagliate su `network interface revert` fare riferimento a. "Riferimenti" Per collegarsi ai comandi di *ONTAP 9: Manuale riferimento pagina*.

18. Controllare se node1 o node2 possiede dischi guasti:

    `storage disk show -nodelist node1,node2 -broken`

    Se uno dei dischi si è guastato, rimuoverli seguendo le istruzioni contenute in *Disk and aggregate management with the CLI*. (Fare riferimento a. "Riferimenti" Per collegarsi a *Disk and aggregate management with the CLI*.)

19. Raccogliere informazioni su node1 e node2 completando i seguenti passaggi secondari e registrando l'output di ciascun comando:

    Queste informazioni verranno utilizzate più avanti nella procedura.

    a. Registrare il modello, l'ID del sistema e il numero di serie di entrambi i nodi:

```
system node show -node node1,node2 -instance
```

Le informazioni verranno utilizzate per riassegnare i dischi e decommissionare i nodi originali.

b. Immettere il seguente comando sia sul nodo 1 che sul nodo 2 e registrare le informazioni sugli shelf, il numero di dischi in ogni shelf, i dettagli dello storage flash, la memoria, la NVRAM e le schede di rete dall'output:

```
run -node node_name sysconfig
```

È possibile utilizzare le informazioni per identificare parti o accessori che si desidera trasferire su node3 o node4.

c. Immettere il seguente comando sia su node1 che su node2 e registrare gli aggregati che sono online su entrambi i nodi:

```
storage aggregate show -node node_name -state online
```

È possibile utilizzare queste informazioni e le informazioni riportate nel seguente passaggio per verificare che gli aggregati e i volumi rimangano online durante l'intera procedura, ad eccezione del breve periodo in cui sono offline durante il trasferimento.

d. immettere il seguente comando sia su node1 che su node2 e registrare i volumi offline su entrambi i nodi:

```
volume show -node node_name -state offline
```

Dopo l'aggiornamento, eseguire di nuovo il comando e confrontare l'output con l'output in questa fase per verificare se altri volumi sono andati offline.

20. Immettere i seguenti comandi per verificare se sono configurati gruppi di interfacce o VLAN su node1 o node2:

```
network port ifgrp show

network port vlan show
```

Annotare se i gruppi di interfacce o le VLAN sono configurati su node1 o node2; tali informazioni sono necessarie nella fase successiva e successiva della procedura.

21. Completare i seguenti passaggi secondari su node1 e node2 per confermare che le porte fisiche possono essere mappate correttamente più avanti nella procedura:

a. Immettere il seguente comando per verificare la presenza di gruppi di failover sul nodo diversi da `clusterwide`:

```
network interface failover-groups show
```

I gruppi di failover sono insiemi di porte di rete presenti nel sistema. Poiché l'aggiornamento dell'hardware del controller può modificare la posizione delle porte fisiche, i gruppi di failover possono essere modificati inavvertitamente durante l'aggiornamento.

Il sistema visualizza i gruppi di failover sul nodo, come illustrato nell'esempio seguente:

```
cluster::> network interface failover-groups show

Vserver              Group              Targets
-------------------- ------------------ ----------
Cluster              Cluster            node1:e0a, node1:e0b
                                        node2:e0a, node2:e0b

fg_6210_e0c          Default            node1:e0c, node1:e0d
                                        node1:e0e, node2:e0c
                                        node2:e0d, node2:e0e

2 entries were displayed.
```

b. Se sono presenti gruppi di failover diversi da `clusterwide`, registrare i nomi dei gruppi di failover e le porte che appartengono ai gruppi di failover.

c. Immettere il seguente comando per verificare se nel nodo sono configurate VLAN:

`network port vlan show -node node_name`

Le VLAN sono configurate su porte fisiche. Se le porte fisiche cambiano, sarà necessario ricreare le VLAN in un secondo momento della procedura.

Il sistema visualizza le VLAN configurate sul nodo, come illustrato nell'esempio seguente:

```
cluster::> network port vlan show

Network Network
Node    VLAN Name Port    VLAN ID MAC Address
------  --------- ------- ------- ------------------
node1   e1b-70    e1b     70      00:15:17:76:7b:69
```

a. Se nel nodo sono configurate VLAN, prendere nota di ogni associazione di porte di rete e ID VLAN.

22. Eseguire una delle seguenti operazioni:

Se i gruppi di interfacce o LE VLAN sono…	Quindi…
On node1 o node2	Completo Fase 23 e. Fase 24.
Non su node1 o node2	Passare a. Fase 24.

23. se non si sa se node1 e node2 si trovano in un ambiente SAN o non SAN, immettere il seguente comando ed esaminarne l'output:

`network interface show -vserver vserver_name -data-protocol iscsi|fcp`

Se non sono configurati né iSCSI né FC per SVM, il comando visualizza un messaggio simile all'esempio seguente:

```
cluster::> network interface show -vserver Vserver8970 -data-protocol
iscsi|fcp
There are no entries matching your query.
```

È possibile verificare che il nodo si trovi in un ambiente NAS utilizzando `network interface show` con il `-data-protocol nfs|cifs` parametri.

Se iSCSI o FC sono configurati per SVM, il comando visualizza un messaggio simile all'esempio seguente:

```
cluster::> network interface show -vserver vs1 -data-protocol iscsi|fcp

         Logical    Status     Network            Current  Current Is
Vserver  Interface  Admin/Oper Address/Mask       Node     Port    Home
-------- ---------- ---------- ------------------ -------- ------- ----
vs1      vs1_lif1   up/down    172.17.176.20/24   node1    0d      true
```

24. verificare che tutti i nodi del cluster siano in quorum completando le seguenti fasi secondarie:

    a. Immettere il livello di privilegio avanzato:

       `set -privilege advanced`

       Il sistema visualizza il seguente messaggio:

       ```
       Warning: These advanced commands are potentially dangerous; use them
       only when directed to do so by NetApp personnel.
       Do you wish to continue? (y or n):
       ```

    b. Invio `y`.

    c. Verificare lo stato del servizio cluster nel kernel, una volta per ogni nodo:

       `cluster kernel-service show`

       Il sistema visualizza un messaggio simile al seguente esempio:

```
cluster::*> cluster kernel-service show

Master        Cluster       Quorum        Availability  Operational
Node          Node          Status        Status        Status
------------- ------------- ------------- ------------- -------------
node1         node1         in-quorum     true          operational
              node2         in-quorum     true          operational

2 entries were displayed.
```

+
I nodi di un cluster sono in quorum quando una semplice maggioranza di nodi è in buone condizioni e può comunicare tra loro. Per ulteriori informazioni, fare riferimento a. "Riferimenti" Per collegarsi al *System Administration Reference*.

a. Tornare al livello di privilegi amministrativi:

```
set -privilege admin
```

25. Eseguire una delle seguenti operazioni:

Se il cluster…	**Quindi…**
HA UNA SAN configurata	Passare a. Fase 26.
NON ha SAN configurato	Passare a. Fase 29.

26. verificare che vi siano LIF SAN su node1 e node2 per ogni SVM che ha UN servizio SAN iSCSI o FC abilitato immettendo il seguente comando ed esaminandone l'output:

```
network interface show -data-protocol iscsi|fcp -home-node node_name
```

Il comando visualizza le informazioni LIF SAN per node1 e node2. Gli esempi seguenti mostrano lo stato nella colonna Status Admin/Oper come up/up, indicando che SAN iSCSI e il servizio FC sono abilitati:

```
cluster::> network interface show -data-protocol iscsi|fcp
            Logical    Status     Network                  Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask             Node
Port    Home
----------- ---------- ---------- ------------------       ---------
------- ----
a_vs_iscsi  data1      up/up      10.228.32.190/21         node1     e0a
true
            data2      up/up      10.228.32.192/21         node2     e0a
true

b_vs_fcp    data1      up/up      20:09:00:a0:98:19:9f:b0  node1     0c
true
            data2      up/up      20:0a:00:a0:98:19:9f:b0  node2     0c
true

c_vs_iscsi_fcp data1   up/up      20:0d:00:a0:98:19:9f:b0  node2     0c
true
            data2      up/up      20:0e:00:a0:98:19:9f:b0  node2     0c
true
            data3      up/up      10.228.34.190/21         node2     e0b
true
            data4      up/up      10.228.34.192/21         node2     e0b
true
```

In alternativa, è possibile visualizzare informazioni LIF più dettagliate immettendo il seguente comando:

`network interface show -instance -data-protocol iscsi|fcp`

27. Acquisire la configurazione predefinita di qualsiasi porta FC sui nodi originali immettendo il seguente comando e registrando l'output dei sistemi:

    `ucadmin show`

    Il comando visualizza le informazioni su tutte le porte FC del cluster, come illustrato nell'esempio seguente:

```
cluster::> ucadmin show

                Current Current   Pending Pending   Admin
Node    Adapter Mode    Type      Mode    Type      Status
------- ------- ------- --------- ------- --------- -----------
node1   0a      fc      initiator -       -         online
node1   0b      fc      initiator -       -         online
node1   0c      fc      initiator -       -         online
node1   0d      fc      initiator -       -         online
node2   0a      fc      initiator -       -         online
node2   0b      fc      initiator -       -         online
node2   0c      fc      initiator -       -         online
node2   0d      fc      initiator -       -         online
8 entries were displayed.
```

È possibile utilizzare le informazioni dopo l'aggiornamento per impostare la configurazione delle porte FC sui nuovi nodi.

28. Completare i seguenti sotto-passaggi:

    a. Immettere il seguente comando su uno dei nodi originali e registrare l'output:

       `service-processor show -node * -instance`

    Il sistema visualizza informazioni dettagliate sull'SP su entrambi i nodi.

    a. Verificare che lo stato SP sia `online`.
    b. Verificare che la rete SP sia configurata.
    c. Registrare l'indirizzo IP e altre informazioni sull'SP.

       È possibile riutilizzare i parametri di rete dei dispositivi di gestione remota, in questo caso gli SP, dal sistema originale per gli SP sui nuovi nodi. Per informazioni dettagliate sull'SP, fare riferimento a. "Riferimenti" Per collegarsi al *riferimento per l'amministrazione del sistema* e ai comandi di *ONTAP 9: Riferimento pagina manuale*.

29. Se si desidera che i nuovi nodi abbiano le stesse funzionalità con licenza dei nodi originali, immettere il seguente comando per visualizzare le licenze del cluster sul sistema originale:

    `system license show -owner *`

    L'esempio seguente mostra le licenze del sito per il cluster1:

```
system license show -owner *
Serial Number: 1-80-000013
Owner: cluster1

Package           Type    Description           Expiration
----------------- ------- --------------------- -----------
Base              site    Cluster Base License  -
NFS               site    NFS License           -
CIFS              site    CIFS License          -
SnapMirror        site    SnapMirror License    -
FlexClone         site    FlexClone License     -
SnapVault         site    SnapVault License     -
6 entries were displayed.
```

30. Ottenere nuove chiavi di licenza per i nuovi nodi presso il *NetApp Support Site*. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp*.

    Se il sito non dispone delle chiavi di licenza necessarie, contattare il rappresentante commerciale NetApp.

31. Verificare se il sistema originale ha abilitato AutoSupport immettendo il seguente comando su ciascun nodo ed esaminandone l'output:

    `system node autosupport show -node node1,node2`

    L'output del comando indica se AutoSupport è attivato, come illustrato nell'esempio seguente:

```
cluster::> system node autosupport show -node node1,node2

Node              State     From          To                Mail Hosts
----------------- --------- ------------- ----------------  ----------
node1             enable    Postmaster    admin@netapp.com  mailhost

node2             enable    Postmaster    -                 mailhost
2 entries were displayed.
```

32. Eseguire una delle seguenti operazioni:

Se il sistema originale…	Quindi…
AutoSupport attivato…	Passare a. Fase 34.

Se il sistema originale…	Quindi…
AutoSupport non è abilitato…	Abilitare AutoSupport seguendo le istruzioni contenute nella sezione *riferimento per l'amministrazione del sistema*. (Fare riferimento a. "Riferimenti" Per collegarsi al *System Administration Reference*.) **Nota:** AutoSupport è attivato per impostazione predefinita quando si configura il sistema di storage per la prima volta. Sebbene sia possibile disattivare AutoSupport in qualsiasi momento, è necessario lasciarlo attivato. L'abilitazione di AutoSupport consente di identificare in modo significativo i problemi e le soluzioni in caso di problemi nel sistema storage.

33. verificare che AutoSupport sia configurato con i dettagli corretti dell'host di posta e gli ID di posta elettronica del destinatario immettendo il seguente comando su entrambi i nodi originali ed esaminando l'output:

    ```
    system node autosupport show -node node_name -instance
    ```

    Per informazioni dettagliate su AutoSupport, fare riferimento a. "Riferimenti" Per collegarsi al *riferimento per l'amministrazione del sistema* e ai comandi di *ONTAP 9: Riferimento pagina manuale*.

34. Invia un messaggio AutoSupport a NetApp per node1 immettendo il seguente comando:

    ```
    system node autosupport invoke -node node1 -type all -message "Upgrading node1 from platform_old to platform_new"
    ```

    > Non inviare un messaggio AutoSupport a NetApp per node2 a questo punto; lo si esegue più avanti nella procedura.

35. verificare che il messaggio AutoSupport sia stato inviato immettendo il seguente comando ed esaminandone l'output:

    ```
    system node autosupport show -node node1 -instance
    ```

    I campi `Last Subject Sent:` e. `Last Time Sent:` contiene il titolo dell'ultimo messaggio inviato e l'ora in cui il messaggio è stato inviato.

36. 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)

    > Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha.
    >
    > È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

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

Gestire le chiavi di autenticazione utilizzando Onboard Key Manager

È possibile utilizzare Onboard Key Manager (OKM) per gestire le chiavi di autenticazione. 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

Prima di avviare il sistema dalla rete, è necessario verificare che tutte le relazioni SnapMirror siano state rinunciate. 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 `Transferring`, è necessario interrompere questi trasferimenti: `snapmirror abort -destination-vserver` *`vserver name`*

   L'interruzione non riesce se la relazione SnapMirror non si trova in `Transferring` stato.

2. Interrompere tutte le relazioni tra il cluster:

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

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. Durante la preparazione per il netboot, è necessario inserire una copia dell'immagine di boot di ONTAP 9 su un server Web a cui il sistema può accedere.

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.

Tuttavia, non è necessario eseguire il netboot dei controller se è installata la stessa versione di ONTAP 9 installata sui controller originali. In tal caso, saltare questa sezione e passare a. "Fase 3: Installazione e boot node3".

Fasi

1. accedere al sito di supporto NetApp per scaricare i file utilizzati per eseguire il netboot 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.

Per…	Quindi…

Sistemi della serie FAS/AFF8000	Estrarre il contenuto di `<ontap_version>_image.tgz` file nella directory di destinazione:
	
	`tar -zxvf <ontap_version>_image.tgz`
	
	Se si sta estraendo il contenuto su Windows, utilizzare 7-zip o WinRAR per estrarre l'immagine di netboot.
	
	L'elenco delle directory deve contenere una cartella netboot con un file kernel:
	
	`netboot/kernel`

Tutti gli altri sistemi	L'elenco delle directory deve contenere il seguente file: `<ontap_version>_image.tgz`NOTA: Non è necessario estrarre il contenuto di `<ontap_version>_image.tgz` file.

Utilizzerai le informazioni nelle directory in "Fase 3" .

Fase 2. Spostare e dismettere il node1

Spostare gli aggregati non root dal nodo 1 al nodo 2

Prima di poter sostituire il nodo 1 con il nodo 3, è necessario spostare gli aggregati non root da node1 a node2 utilizzando il comando di trasferimento degli aggregati di storage e verificando quindi il trasferimento.

Fasi

1. Riposizionare gli aggregati non radice completando i seguenti sottopassaggi:
   a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

b. Immettere il seguente comando:

```
storage aggregate relocation start -node node1 -destination node2 -aggregate
-list * -ndo-controller-upgrade true
```

c. Quando richiesto, immettere `y`.

Il trasferimento avverrà in background. La riposizionamento di un aggregato potrebbe richiedere da pochi secondi a un paio di minuti. Il tempo include sia le parti di fuori servizio del client che quelle di non fuori servizio. Il comando non ricolloca nessun aggregato offline o limitato.

d. Tornare al livello admin immettendo il seguente comando:

```
set -privilege admin
```

2. Controllare lo stato di rilocazione immettendo il seguente comando sul nodo 1:

```
storage aggregate relocation show -node node1
```

Viene visualizzato l'output `Done` per un aggregato dopo che è stato trasferito.

Attendere che tutti gli aggregati non root di proprietà di node1 siano stati riallocati in node2 prima di procedere con la fase successiva.

3. Eseguire una delle seguenti operazioni:

In caso di trasferimento…	Quindi…
Di tutti gli aggregati ha successo	Passare a. Fase 4.

In caso di trasferimento…	Quindi…

Di qualsiasi aggregato non funziona o viene vetoato	a. Controllare i registri EMS per l'azione correttiva.
	b. Eseguire l'azione correttiva.
	c. Spostare eventuali aggregati guasti o vetoed:
	`storage aggregate relocation start -node node1 - destination node2 -aggregate-list * -ndo -controller-upgrade true`
	d. Quando richiesto, immettere `y`.
	e. Tornare al livello di amministrazione:
	`set -privilege admin`Se necessario, è possibile forzare il trasferimento utilizzando uno dei seguenti metodi:
	◦ Ignora i controlli di veto:
	`storage aggregate relocation start -override -vetoes true -ndo-controller-upgrade`
	◦ Ignora controlli destinazione:
	`storage aggregate relocation start -override -destination-checks true -ndo-controller -upgrade`
	Fare riferimento a. "Riferimenti" Per collegarsi alla gestione di *dischi e aggregati con il contenuto CLI* e i comandi di *ONTAP 9: Manuale di riferimento pagina* per ulteriori informazioni sui comandi di spostamento degli aggregati di storage.

4.] verifica che tutti gli aggregati non root siano online e che il loro stato sia 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`*

5. Verificare che tutti i volumi siano online sul nodo 2 immettendo 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.

6. Immettere il seguente comando su node2:

   `storage failover show -node` *`node2`*

   L'output dovrebbe visualizzare il seguente messaggio:

   ```
   Node owns partner's aggregates as part of the nondisruptive controller
   upgrade procedure.
   ```

7. Verificare che node1 non possiedi aggregati non root online:

   `storage aggregate show -owner-name` *`node1`* `-ha-policy sfo -state online`

   L'output non dovrebbe visualizzare alcun aggregato non root online, che è già stato trasferito in node2.

Spostare le LIF dei dati NAS di proprietà del node1 in node2

Prima di poter sostituire il nodo 1 con il nodo 3, è necessario spostare le LIF dati NAS di proprietà del nodo 1 in node2 se si dispone di un cluster a due nodi o in un terzo nodo se il cluster ha più di due nodi. Il metodo utilizzato dipende dalla configurazione del cluster per NAS o SAN.

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. Dopo aver portato il nodo 3 online, è necessario verificare che i file LIF siano integri e posizionati su porte appropriate.

Fasi

1. Elencare tutte le LIF dei dati NAS ospitate sul nodo 1 immettendo il seguente comando e acquisendo l'output:

   `network interface show -data-protocol nfs|cifs -curr-node` *`node1`*

   Il sistema visualizza i dati NAS LIF sul nodo 1, come mostrato nell'esempio seguente:

```
 cluster::> network interface show -data-protocol nfs|cifs -curr-node
node1

          Logical     Status      Network             Current   Current
Is
 Vserver  Interface   Admin/Oper  Address/Mask        Node      Port
Home
 -------- ----------  ----------  ------------------  --------- -------
----
 vs0
          a0a         up/down     10.63.0.53/24       node1     a0a
true
          data1       up/up       10.63.0.50/18       node1     e0c
true
          rads1       up/up       10.63.0.51/18       node1     e1a
true
          rads2       up/down     10.63.0.52/24       node1     e1b
true
 vs1
          lif1        up/up       192.17.176.120/24   node1     e0c
true
          lif2        up/up       172.17.176.121/24   node1     e1a
true
```

2. Eseguire una delle seguenti operazioni:

Se nodo1…	Quindi…
Dispone di gruppi di interfacce di VLAN configurati	Passare a. Fase 3.
Non ha gruppi di interfacce o VLAN configurati	Saltare la fase 3 e passare a. Fase 4.

Utilizzare `network port vlan show` Per visualizzare le informazioni sulle porte di rete collegate alle VLAN e utilizzare `network port ifgrp show` comando per visualizzare le informazioni sui gruppi di interfaccia delle porte.

3. eseguire i seguenti passaggi per migrare qualsiasi LIF di dati NAS ospitata su gruppi di interfacce e VLAN sul nodo 1:

   a. Migrare le LIF ospitate su qualsiasi gruppo di interfacce e le VLAN sul node1 a una porta sul node2 in grado di ospitare LIF sulla stessa rete dei gruppi di interfacce immettendo il seguente comando, una volta per ogni LIF:

   ```
   network interface migrate -vserver Vserver_name -lif LIF_name -destination
   -node node2 -destination-port netport|ifgrp
   ```

   b. Modificare la porta home e il nodo home di LIF e VLAN in Sotto-fase A. Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

   ```
   network interface modify -vserver Vserver_name -lif LIF_name -home-node
   node2 - home-port netport|ifgrp
   ```

4. eseguire una delle seguenti operazioni:

Se il cluster è configurato per…	Quindi…
NAS	Completo Fase 5 attraverso Fase 8.
SAN	Disattivare tutte le LIF SAN sul nodo per disattivarle per l'aggiornamento: `network interface modify -vserver *Vserver-name* -lif *LIF_name* -home-node *node_to_upgrade* -home-port _netport

5. migrazione dei dati NAS LIF da node1 a node2 immettendo il seguente comando, una volta per ciascun LIF di dati:

   ```
   network interface migrate -vserver Vserver-name -lif LIF_name -destination
   -node node2 -destination-port data_port
   ```

6. immettere il seguente comando ed esaminare l'output per verificare che i file LIF siano stati spostati nelle porte corrette e che i file LIF abbiano lo stato di up immettendo il seguente comando su entrambi i nodi ed esaminando l'output:

   ```
   network interface show -curr-node node2 -data-protocol nfs|cifs
   ```

7. immettere il seguente comando per modificare il nodo home delle LIF migrate:

   ```
   network interface modify -vserver Vserver-name -lif LIF_name -home-node node2
   -home-port port_name
   ```

8. verifica se LIF sta utilizzando la porta come porta principale o corrente. Se la porta non è domestica o corrente, passare a. Fase 9:

   ```
   network interface show -home-node node2 -home-port port_name

   network interface show -curr-node node_name -curr-port port_name
   ```

9. se le LIF utilizzano la porta come porta home o porta corrente, modificare la LIF per utilizzare una porta diversa:

   ```
   network interface migrate -vserver Vserver-name -lif LIF_name
   -destination-node node_name -destination-port port_name

   network interface modify -vserver Vserver-name -lif LIF_name -home-node
   node_name -home-port port_name
   ```

10. se le porte che attualmente ospitano i file LIF dei dati non saranno presenti sul nuovo hardware, rimuoverle dal dominio di trasmissione:

    ```
    network port broadcast-domain remove-ports -ipspace Default -broadcast-domain
    Default -ports node:port
    ```

11. se i LIF non sono attivi, imposta lo stato amministrativo dei LIF su "up" immettendo il seguente comando, una volta per ciascun LIF:

    ```
    network interface modify -vserver Vserver-name -lif LIF_name -home-node
    nodename -status-admin up
    ```

    > Per le configurazioni MetroCluster, potrebbe non essere possibile modificare il dominio di trasmissione di una porta perché è associata a una porta che ospita la LIF di una macchina virtuale di storage di destinazione (SVM). Immettere il seguente comando dalla SVM di origine corrispondente sul sito remoto per riallocare la LIF di destinazione su una porta appropriata:
    > `metrocluster vserver resync -vserver Vserver_name`

12. immettere il seguente comando ed esaminarne l'output per verificare che non vi siano LIF di dati rimasti sul node1:

    ```
    network interface show -curr-node node1 -role data
    ```

13. se sono configurati gruppi di interfacce o VLAN, completare i seguenti passaggi secondari:

    a. Rimuovere le VLAN dai gruppi di interfacce immettendo il seguente comando:

       ```
       network port vlan delete -node nodename -port ifgrp_name -vlan-id VLAN_ID
       ```

    b. Immettere il seguente comando ed esaminare il relativo output per verificare l'eventuale presenza di gruppi di interfacce configurati sul nodo:

       ```
       network port ifgrp show -node nodename -ifgrp ifgrp_name -instance
       ```

       Il sistema visualizza le informazioni sul gruppo di interfacce per il nodo, come illustrato nell'esempio seguente:

```
cluster::> network port ifgrp show -node node1 -ifgrp a0a -instance
                  Node: node1
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode_lacp
          MAC Address: 02:a0:98:17:dc:d4
   Port Participation: partial
        Network Ports: e2c, e2d
             Up Ports: e2c
           Down Ports: e2d
```

a. Se nel nodo sono configurati gruppi di interfacce, registrare i nomi di tali gruppi e le porte ad essi assegnate, quindi eliminare le porte immettendo il seguente comando, una volta per ciascuna porta:

   `network port ifgrp remove-port -node` *`nodename`* `-ifgrp` *`ifgrp_name`* `-port` *`netport`*

Registrare le informazioni del nodo 1

Prima di spegnere e dismettere il node1, è necessario registrare le informazioni relative alla rete del cluster, alla gestione e alle porte FC, nonché l'ID del sistema NVRAM. Queste informazioni sono necessarie più avanti nella procedura quando si esegue il mapping del nodo 1 al nodo 3 e si riassegnano i dischi.

Fasi

1. immettere il seguente comando e acquisirne l'output:

   `network route show`

   Il sistema visualizza un output simile al seguente esempio:

```
cluster::> network route show

Vserver         Destination    Gateway      Metric
 -------------- -------------- ----------- -------
 iscsi vserver  0.0.0.0/0       10.10.50.1  20
 node1          0.0.0.0/0       10.10.20.1  10
 ....
 node2          0.0.0.0/0       192.169.1.1 20
```

2. Immettere il seguente comando e acquisire l'output:

   `vserver services name-service dns show`

   Il sistema visualizza un output simile al seguente esempio:

```
 cluster::> vserver services name-service dns show
                                                                  Name
 Vserver        State     Domains                                 Servers
 -------------- --------- ------------------------------------
---------------
 node 1 2       enabled   alpha.beta.gamma.netapp.com
10.10.60.10,

10.10.60.20
 vs_base1       enabled   alpha.beta.gamma.netapp.com,
10.10.60.10,
                          beta.gamma.netapp.com,
10.10.60.20
 ...
 ...
 vs peer1        enabled  alpha.beta.gamma.netapp.com,
10.10.60.10,
                          gamma.netapp.com
10.10.60.20
```

3. trova la rete del cluster e le porte di gestione dei nodi sul node1 immettendo il seguente comando su uno dei controller:

   `network interface show -curr-node` *`node1`* `-role cluster,intercluster,node-mgmt,cluster-mgmt`

   Il sistema visualizza le LIF di cluster, intercluster, gestione dei nodi e gestione dei cluster per il nodo del cluster, come illustrato nell'esempio seguente:

```
 cluster::> network interface show -curr-node <node1>
            -role cluster,intercluster,node-mgmt,cluster-mgmt

              Logical       Status     Network            Current
Current Is
  Vserver     Interface     Admin/Oper Address/Mask       Node     Port
Home
  ----------- ------------- ---------- ------------------ --------
------- ----
  vserver1
              cluster mgmt   up/up     192.168.x.xxx/24   node1    e0c
true
  node1
              intercluster   up/up     192.168.x.xxx/24   node1    e0e
true
              clus1          up/up     169.254.xx.xx/24   node1    e0a
true
              clus2          up/up     169.254.xx.xx/24   node1    e0b
true
              mgmt1          up/up     192.168.x.xxx/24   node1    e0c
true
 5 entries were displayed.
```

Il sistema potrebbe non disporre di LIF intercluster.

4. Acquisire le informazioni nell'output del comando in Fase 3 da utilizzare nella sezione "Mappare le porte dal nodo 1 al nodo 3".

   Le informazioni di output sono necessarie per mappare le nuove porte del controller alle vecchie porte del controller.

5. Immettere il seguente comando su node1:

   `network port show -node node1 -type physical`

   Il sistema visualizza le porte fisiche sul nodo, come mostrato nell'esempio seguente:

```
 sti8080mcc-htp-008::> network port show -node sti8080mcc-htp-008 -type
physical

 Node: sti8080mcc-htp-008

                                                                    Ignore
                                              Speed(Mbps)  Health   Health
 Port  IPspace  Broadcast Domain Link MTU   Admin/Oper   Status   Status
 ----  -------  ---------------- ---- ----  -----------  -------
-------
 e0M   Default  Mgmt             up   1500  auto/1000    healthy  false
 e0a   Default  Default          up   9000  auto/10000   healthy  false
 e0b   Default  -                up   9000  auto/10000   healthy  false
 e0c   Default  -                down 9000  auto/-       -        false
 e0d   Default  -                down 9000  auto/-       -        false
 e0e   Cluster  Cluster          up   9000  auto/10000   healthy  false
 e0f   Default  -                up   9000  auto/10000   healthy  false
 e0g   Cluster  Cluster          up   9000  auto/10000   healthy  false
 e0h   Default  Default          up   9000  auto/10000   healthy  false
 9 entries were displayed.
```

6. Registrare le porte e i relativi domini di trasmissione.

   I domini di broadcast dovranno essere mappati alle nuove porte sul nuovo controller più avanti nella procedura.

7. Immettere il seguente comando su node1:

   `network fcp adapter show -node` *`node1`*

   Il sistema visualizza le porte FC sul nodo, come mostrato nell'esempio seguente:

```
 cluster::> fcp adapter show -node <node1>
                      Connection  Host
 Node         Adapter Established Port Address
 ------------ ------- ----------- ------------
 node1
               0a     ptp         11400
 node1
               0c     ptp         11700
 node1
               6a     loop        0
 node1
               6b     loop        0
 4 entries were displayed.
```

8. Registrare le porte.

   Le informazioni di output sono necessarie per mappare le nuove porte FC sul nuovo controller più avanti nella procedura.

9. In caso contrario, controllare se ci sono gruppi di interfacce o VLAN configurati sul nodo 1 immettendo i seguenti comandi:

   ```
   network port ifgrp show

   network port vlan show
   ```

   Verranno utilizzate le informazioni contenute nella sezione "Mappare le porte dal nodo 1 al nodo 3".

10. Eseguire una delle seguenti operazioni:

Se…	Quindi…
Il numero dell'ID del sistema NVRAM è stato registrato nella sezione "Preparare i nodi per l'aggiornamento".	Passare alla sezione successiva, "Ritirare il node1".
Il numero dell'ID del sistema NVRAM non è stato registrato nella sezione "Preparare i nodi per l'aggiornamento"	Completo Fase 11 e. Fase 12 quindi passare a. "Ritirare il node1".

11. immettere il seguente comando su uno dei controller:

    ```
    system node show -instance -node node1
    ```

    Il sistema visualizza le informazioni relative al nodo 1 come mostrato nell'esempio seguente:

    ```
    cluster::> system node show -instance -node <node1>
                                Node: node1
                               Owner:
                            Location: GDl
                               Model: FAS6240
                       Serial Number: 700000484678
                           Asset Tag: -
                              Uptime: 20 days 00:07
                     NVRAM System ID: 1873757983
                           System ID: 1873757983
                              Vendor: NetApp
                              Health: true
                         Eligibility: true
    ```

12. registrare il numero di ID del sistema NVRAM da utilizzare nella sezione "Installazione e boot node3".

Ritirare il node1

Per dismettere il node1, è necessario disattivare la coppia ha con node2, chiudere il node1 correttamente e rimuoverlo dal rack o dallo chassis.

Fasi

1. Verificare il numero di nodi nel cluster:

   `cluster show`

   Il sistema visualizza i nodi nel cluster, come illustrato nell'esempio seguente:

   ```
   cluster::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node1                 true    true
   node2                 true    true
   2 entries were displayed.
   ```

2. Disattiva il failover dello storage, a seconda dei casi:

Se il cluster è…	Quindi…

Un cluster a due nodi	a. Disattivare la disponibilità elevata del cluster immettendo il seguente comando su uno dei nodi:
	`cluster ha modify -configured false`
	a. Disattivare il failover dello storage:
	`storage failover modify -node node1 -enabled false`

Un cluster con più di due nodi	Disattivare il failover dello storage: `storage failover modify -node node1 -enabled false`

   Se non si disattiva il failover dello storage, può verificarsi un errore di upgrade del controller che può interrompere l'accesso ai dati e causare la perdita di dati.

3. Verificare che il failover dello storage sia stato disattivato:

   `storage failover show`

   L'esempio seguente mostra l'output di `storage failover show` comando quando il failover dello storage è stato disattivato per un nodo:

```
 cluster::> storage failover show
                                 Takeover
 Node           Partner         Possible State Description
 -------------- -------------- --------
-------------------------------------
 node1          node2          false    Connected to node2, Takeover
                                        is not possible: Storage
failover is
                                        disabled

 node2          node1          false    Node owns partner's aggregates
as part
                                        of the nondisruptive controller
upgrade
                                        procedure. Takeover is not
possible:
                                        Storage failover is disabled
 2 entries were displayed.
```

4. Verificare lo stato LIF dei dati:

   `network interface show -role data -curr-node node2 -home-node node1`

   Controllare nella colonna **Status Admin/Oper** (Amministrazione stato/Oper*) se le LIF non sono attive. Se uno qualsiasi dei LIF è inattivo, consultare il "Troubleshoot" sezione.

5. Eseguire una delle seguenti operazioni:

Se il cluster è…	Quindi…
Un cluster a due nodi	Passare a. Fase 6.
Un cluster con più di due nodi	Passare a. Fase 8.

6. Accedi al livello di privilegio avanzato su uno dei nodi:

   `set -privilege advanced`

7. verificare che il cluster ha sia stato disattivato:

   `cluster ha show`

   Il sistema visualizza il seguente messaggio:

```
High Availability Configured: false
```

   Se il cluster ha non è stato disattivato, ripetere Fase 2.

8. Controlla se il node1 attualmente contiene epsilon:

   `cluster show`

   Poiché esiste la possibilità di un legame in un cluster con un numero pari di nodi, un nodo ha un peso di voto frazionario aggiuntivo chiamato epsilon. Fare riferimento a. "Riferimenti" Per ulteriori informazioni, fare riferimento a *System Administration Reference*.

   > Se si dispone di un cluster a quattro nodi, epsilon potrebbe trovarsi su un nodo di una coppia ha diversa nel cluster.
   >
   > Se si sta aggiornando una coppia HA in un cluster con più coppie HA, è necessario spostare epsilon sul nodo di una coppia HA che non è in fase di aggiornamento del controller. Ad esempio, se si sta aggiornando NodeA/NodeB in un cluster con la configurazione della coppia ha NodeA/NodeB e NODEC/NODed, è necessario spostare epsilon in NODEC o NODed.

   Il seguente esempio mostra che node1 contiene epsilon:

   ```
   cluster::*> cluster show

   Node                  Health  Eligibility  Epsilon
   --------------------- ------- ------------ ------------
   node1                 true    true         true
   node2                 true    true         false
   ```

9. Se node1 contiene epsilon, contrassegnare epsilon `false` sul nodo in modo che possa essere trasferito al nodo 2:

   `cluster modify -node node1 -epsilon false`

10. Trasferire epsilon al nodo 2 contrassegnando epsilon `true` al nodo 2:

    `cluster modify -node node2 -epsilon true`

11. Verificare che si sia verificata la modifica in node2:

    `cluster show`

    ```
    cluster::*> cluster show
    Node                  Health  Eligibility  Epsilon
    --------------------- ------- ------------ ------------
    node1                 true    true         false
    node2                 true    true         true
    ```

    L'epsilon per il node2 dovrebbe ora essere vero e l'epsilon per il node1 dovrebbe essere falso.

12. Verificare se il setup è un cluster senza switch a due nodi:

```
network options switchless-cluster show
```

```
cluster::*> network options switchless-cluster show

Enable Switchless Cluster: false/true
```

Il valore di questo comando deve corrispondere allo stato fisico del sistema.

13. Tornare al livello di amministrazione:

```
set -privilege admin
```

14. Arrestare il node1 dal prompt node1:

```
system node halt -node node1
```

> Se il nodo 1 si trova nello stesso chassis del nodo 2, non spegnere lo chassis utilizzando l'interruttore di alimentazione o tirando il cavo di alimentazione. In tal caso, il nodo 2, che fornisce i dati, non funzionerà.

15. Quando il sistema richiede di confermare che si desidera arrestare il sistema, immettere `y`.

    Il nodo si arresta al prompt dell'ambiente di boot.

16. Quando node1 visualizza il prompt dell'ambiente di avvio, rimuoverlo dallo chassis o dal rack.

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

Fase 3. Installazione e boot node3

Installazione e boot node3

È necessario installare node3 nel rack, trasferire le connessioni del node1 al node3, fare il boot node3 e installare ONTAP. È inoltre necessario riassegnare i dischi spare di node1, i dischi appartenenti al volume root e gli aggregati non root non ricollocati in node2 in precedenza.

A proposito di questa attività

È necessario eseguire l'avvio di rete del nodo 3 se non ha la stessa versione di ONTAP 9 installata sul nodo 1. 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 avvii del sistema. Vedere "Preparatevi per il netboot".

Tuttavia, non è necessario eseguire l'avvio di rete di node3 se è installata la stessa versione o una versione successiva di ONTAP 9 su node1.

- Per un aggiornamento del controller AFF A800 o AFF C800 , è necessario assicurarsi che tutte le unità nello chassis siano saldamente posizionate contro il midplane prima di rimuovere node1. Per maggiori informazioni, vedere "Sostituire i moduli controller AFF A800 o AFF C800".
- Se si sta aggiornando un sistema con dischi di archiviazione, è necessario completare l'intera sezione e quindi andare a "Configurare le porte FC sul nodo 3" E "Controllare e configurare le porte UTA/UTA2 sul nodo 3" , immettendo comandi al prompt del cluster.

Fasi

1. assicurarsi di disporre di spazio rack per node3.

   Se node1 e node2 si trovano in uno chassis separato, è possibile inserire node3 nella stessa posizione rack del node1. Tuttavia, se il nodo 1 si trovava nello stesso chassis con il nodo 2, è necessario inserire il nodo 3 nel proprio spazio rack, preferibilmente vicino alla posizione del nodo 1.

2. [[fase 2]]installare il nodo 3 nel rack seguendo le *istruzioni di installazione e configurazione* relative al modello di nodo in uso.

   Se si esegue l'aggiornamento a un sistema con entrambi i nodi nello stesso chassis, installare node4 e node3 nello chassis. Se non si installano entrambi i nodi nello stesso chassis, quando si avvia node3, questo si comporta come se fosse in una configurazione a doppio chassis, mentre quando si avvia node4, l'interconnessione tra i nodi non si attiva.

3. cavo node3, spostamento delle connessioni da node1 a node3.

   I seguenti riferimenti consentono di stabilire i collegamenti dei cavi corretti. Passare a. "Riferimenti" per collegarli.

   - *Istruzioni di installazione e configurazione* per la piattaforma node3
   - La procedura di shelf di dischi appropriata
   - La documentazione *ha Pair Management*

     Collegare i seguenti cavi:

   - Console (porta di gestione remota)
   - Porte del cluster
   - Porte dati
   - Porte di gestione di cluster e nodi
   - Storage
   - Configurazioni SAN: Porte switch FC e Ethernet iSCSI

     Potrebbe non essere necessario spostare la scheda di interconnessione o la connessione del cavo di interconnessione del cluster dal nodo 1 al nodo 3, poiché la maggior parte dei modelli di piattaforma dispone di un modello di scheda di interconnessione unico. Per la configurazione MetroCluster, è necessario spostare le connessioni del cavo FC-VI dal nodo 1 al nodo 3. Se il nuovo host non dispone di una scheda FC-VI, potrebbe essere necessario spostare la scheda FC-VI.

4. accendere il computer su node3, quindi interrompere il processo di boot premendo Ctrl-C sul terminale

della console per accedere al prompt dell'ambiente di boot.

Se si sta eseguendo l'aggiornamento a un sistema con entrambi i nodi nello stesso chassis, anche node4 viene riavviato. Tuttavia, è possibile ignorare il node4 boot fino a tardi.

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.

   Non ignorare il ritardo; se non si lascia caricare la batteria, si potrebbe verificare una perdita di dati.

6. Al prompt della modalità di manutenzione, immettere il seguente comando:

   ```
   halt
   ```

   Il sistema si arresta al prompt dell'ambiente di avvio.

7. Eseguire una delle seguenti operazioni:

Se il sistema a cui si esegue l'aggiornamento si trova in una…	Quindi…
Configurazione a doppio chassis (con controller in chassis diversi)	Vai aFase 8 .

Se il sistema a cui si esegue l'aggiornamento si trova in una…	Quindi…
Configurazione a unico chassis (con controller nello stesso chassis)	a. Spostare il cavo della console dal nodo 3 al nodo 4. b. 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 avvio. L'alimentazione dovrebbe essere già attiva se entrambi i controller si trovano nello stesso chassis. Lasciare node4 al prompt dell'ambiente di boot; si tornerà a node4 in "Installazione e boot node4". c. Se viene visualizzato il messaggio di avviso nella Fase 4, seguire le istruzioni in Fase 5 d. Riportare il cavo della console dal nodo 4 al nodo 3. e. Vai aFase 8 .

8. Configura node3 per ONTAP:

```
set-defaults
```

9. Se sono installate unità NetApp Storage Encryption (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`**

Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha.

È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

b. Contattare il supporto NetApp per assistenza nel ripristino delle informazioni di gestione delle chiavi integrate.

10.] se la versione di ONTAP installata su node3 è uguale o successiva alla versione di ONTAP 9 installata su node1, elencare e riassegnare i dischi al nuovo node3:

`boot_ontap`

> Se questo nuovo nodo è stato utilizzato in qualsiasi altro cluster o coppia ha, è necessario eseguire `wipeconfig` prima di procedere. In caso contrario, potrebbero verificarsi interruzioni del servizio o perdita di dati. Contattare il supporto tecnico se il controller sostitutivo è stato utilizzato in precedenza, in particolare se i controller eseguivano ONTAP in 7-Mode.

11. Premere CTRL-C per visualizzare il menu di avvio.
12. eseguire una delle seguenti operazioni:

Se il sistema che si sta aggiornando…	**Quindi…**
Non ha la versione ONTAP corretta o corrente sul nodo 3	Vai aFase 13 .
Ha la versione corretta o attuale di ONTAP al nodo 3	Vai aFase 18 .

13. Configurare la connessione netboot scegliendo una delle seguenti azioni.

> 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 immettendo 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 (Domain Name Service). Se si utilizza questo parametro opzionale, non è necessario un nome di dominio completo nell'URL del server netboot; è necessario solo il nome host del server. Potrebbero essere necessari altri parametri per l'interfaccia. Invio `help ifconfig` al prompt del firmware per ulteriori informazioni.

14. Eseguire netboot sul nodo 3:

Per…	Quindi…
Sistemi della serie FAS/AFF8000	`netboot http://<web_server_ip>/<path_to_webaccessible_directory>/netboot/kernel`
Tutti gli altri sistemi	`netboot http://<web_server_ip>/<path_to_webaccessible_directory>/<ontap_version>_image.tgz`

Il `<path_to_the_web-accessible_directory>` consente di accedere alla posizione in cui è stato scaricato `<ontap_version>_image.tgz` poll "Fase 1" Nella sezione *Prepare for netboot*.

Non interrompere l'avvio.

15. Dal menu di avvio, seleziona prima l'opzione **(7) Installa nuovo software**.

    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 essere errata. 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 ONTAP su entrambe le partizioni dell'immagine.

16. Se ti viene chiesto di continuare la procedura, inserisci `y` e quando ti viene richiesto il pacchetto, inserisci il seguente URL:

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

17. Completare i seguenti passaggi secondari:

    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.

18. Seleziona **(5) Avvio in modalità di manutenzione** inserendo `5` , e poi inserisci `y` quando viene richiesto di continuare con l'avvio.
19. prima di continuare, visitare il sito "Impostare la configurazione FC o UTA/UTA2 su node3" Apportare le modifiche necessarie alle porte FC o UTA/UTA2 del nodo.

    Apportare le modifiche consigliate in queste sezioni, riavviare il nodo e passare alla modalità di manutenzione.

20. Trova l'ID di sistema del nodo 3:

    `disk show -a`

    Il sistema visualizza l'ID di sistema del nodo e le informazioni relative ai dischi, come mostrato nell'esempio seguente:

```
 *> disk show -a
 Local System ID: 536881109
 DISK     OWNER                    POOL   SERIAL    HOME          DR
 HOME                                     NUMBER
 -------- -------------            -----  -------- -------------
-------------
 0b.02.23 nst-fas2520-2(536880939) Pool0  KPG2RK6F nst-fas2520-
2(536880939)
 0b.02.13 nst-fas2520-2(536880939) Pool0  KPG3DE4F nst-fas2520-
2(536880939)
 0b.01.13 nst-fas2520-2(536880939) Pool0  PPG4KLAA nst-fas2520-
2(536880939)
 ......
 0a.00.0               (536881109) Pool0  YFKSX6JG
(536881109)
 ......
```

> Potrebbe essere visualizzato il messaggio `disk show: No disks match option -a.` dopo aver immesso il comando. Non si tratta di un messaggio di errore, pertanto è possibile continuare con la procedura.

21. Riassegnare i dischi di riserva del nodo 1, tutti i dischi appartenenti alla radice e tutti gli aggregati non radice che non sono stati trasferiti in precedenza al nodo 2 in"Spostare gli aggregati non root dal nodo 1 al nodo 2" .

    Inserire il modulo appropriato di `disk reassign` comando basato sulla presenza di dischi condivisi nel sistema:

> Se nel sistema sono presenti dischi condivisi, aggregati ibridi o entrambi, è necessario utilizzare il corretto `disk reassign` dalla seguente tabella.

Se il tipo di disco è…	Quindi eseguire il comando…
Con dischi condivisi	`disk reassign -s node1_sysid -d node3_sysid -p node2_sysid`
Senza dischi condivisi	`disk reassign -s node1_sysid -d node3_sysid`

Per *node1_sysid* utilizzare le informazioni acquisite in "Registrare le informazioni del nodo 1". Per ottenere il valore per *node3_sysid*, utilizzare `sysconfig` comando.

Il `-p` l'opzione è richiesta solo in modalità di manutenzione quando sono presenti dischi condivisi.

Il `disk reassign` il comando riassegna solo i dischi per i quali *node1_sysid* è il proprietario corrente.

Il sistema visualizza il seguente messaggio:

```
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)?
```

22. Invio `n`.

Il sistema visualizza il seguente messaggio:

```
After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)?
```

23. Invio `y`

Il sistema visualizza il seguente messaggio:

```
Disk ownership will be updated on all disks previously belonging to
Filer with sysid <sysid>.
Do you want to continue (y/n)?
```

24. Invio `y`.

25. se si esegue l'aggiornamento da un sistema con dischi esterni a un sistema che supporta dischi interni ed esterni (ad esempio, sistemi AFF A800), impostare l'aggregato node1 come root per confermare che node3 si avvia dall'aggregato root di node1.

Attenzione: È necessario eseguire le seguenti fasi secondarie nell'ordine esatto indicato; in caso contrario, si potrebbe verificare un'interruzione o addirittura la perdita di dati.

La seguente procedura imposta node3 per l'avvio dall'aggregato root di node1:

a. Controllare le informazioni su RAID, plex e checksum per l'aggregato node1:

```
aggr status -r
```

b. Controllare lo stato dell'aggregato node1:

```
aggr status
```

c. Se necessario, portare online l'aggregato node1:

```
aggr_online root_aggr_from_node1
```

d. Impedire al node3 di avviarsi dal proprio aggregato root originale:
`aggr offline root_aggr_on_node3`

e. Impostare l'aggregato root node1 come nuovo aggregato root per node3:

```
aggr options aggr_from_node1 root
```

f. Verificare che l'aggregato root di node3 sia offline e che l'aggregato root per i dischi portati da node1 sia online e impostato su root:

```
aggr status
```

La mancata esecuzione del passaggio secondario precedente potrebbe causare l'avvio di node3 dall'aggregato root interno, oppure il sistema potrebbe presumere l'esistenza di una nuova configurazione del cluster o richiedere di identificarne una.

Di seguito viene riportato un esempio dell'output del comando:

```
------------------------------------------------------------------
     Aggr State               Status          Options
aggr0_nst_fas8080_15 online   raid_dp, aggr   root, nosnap=on
                              fast zeroed
                              64-bit

  aggr0 offline               raid_dp, aggr   diskroot
                              fast zeroed
                              64-bit
------------------------------------------------------------------
```

26. verificare che il controller e lo chassis siano configurati come `ha`:

```
ha-config show
```

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

```
*> ha-config show
   Chassis HA configuration: ha
   Controller HA configuration: ha
```

I sistemi registrano in una ROM programmabile (PROM) se si trovano in una configurazione a coppia ha o standalone. Lo stato deve essere lo stesso su tutti i componenti all'interno del sistema standalone o della coppia ha.

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
```

Se si dispone di una configurazione MetroCluster, utilizzare i seguenti comandi per modificare il controller e lo chassis:

```
ha-config modify controller mcc

ha-config modify chassis mcc
```

27. distruggere le caselle di posta sul node3:

```
mailbox destroy local
```

La console visualizza il seguente messaggio:

```
Destroying mailboxes forces a node to create new empty mailboxes, which
clears any takeover state, removes all knowledge of out-of-date plexes
of mirrored volumes, and will prevent management services from going
online in 2-node cluster HA configurations. Are you sure you want to
destroy the local mailboxes?
```

28. Invio `y` quando viene richiesto di confermare che si desidera distruggere le caselle postali locali.
29. Esci dalla modalità di manutenzione:

```
halt
```

Il sistema si arresta al prompt dell'ambiente di avvio.

30. al node2, controllare la data, l'ora e il fuso orario del sistema:

```
date
```

31. al node3, controllare la data al prompt dell'ambiente di boot:

```
show date
```

32. se necessario, impostare la data su node3:

```
set date mm/dd/yyyy
```

33. al node3, controllare l'ora al prompt dell'ambiente di boot:

```
show time
```

34. se necessario, impostare l'ora su node3:

```
set time hh:mm:ss
```

35. Verificare che l'ID del sistema partner sia impostato correttamente come indicato inFase 21 con l'opzione -p:

```
printenv partner-sysid
```

36. se necessario, impostare l'ID di sistema del partner su node3:

```
setenv partner-sysid node2_sysid
```

Salvare le impostazioni:

```
saveenv
```

37. accedere al menu di boot al prompt dell'ambiente di boot:

```
boot_ontap menu
```

38. dal menu di avvio, selezionare l'opzione **(6) Aggiorna flash dalla configurazione di backup** immettendo `6` quando richiesto.

Il sistema visualizza il seguente messaggio:

```
This will replace all flash-based configuration with the last backup to
disks. Are you sure you want to continue?:
```

39. Invio `y` quando richiesto.

L'avvio procede normalmente e il sistema chiede di confermare la mancata corrispondenza dell'ID di sistema.

> Il sistema potrebbe riavviarsi due volte prima di visualizzare l'avviso di mancata corrispondenza.

40. confermare la mancata corrispondenza come mostrato nell'esempio seguente:

```
WARNING: System id mismatch. This usually occurs when replacing CF or
NVRAM cards!
Override system id (y|n) ? [n] y
```

Il nodo potrebbe essere sottoposto a un ciclo di riavvio prima dell'avvio normale.

41. Accedi a node3.

Impostare la configurazione FC o UTA/UTA2 su node3

Se node3 dispone di porte FC integrate, porte UTA/UTA2 (onboard Unified target adapter) o una scheda UTA/UTA2, è necessario configurare le impostazioni prima di completare il resto della procedura.

A proposito di questa attività

Potrebbe essere necessario completareConfigurare le porte FC sul nodo 3 OControllare e configurare le porte UTA/UTA2 sul nodo 3 o entrambe le sezioni.

> I materiali di marketing NetApp potrebbero utilizzare il termine "UTA2" per fare riferimento agli adattatori e alle porte CNA. Tuttavia, la CLI utilizza il termine "CNA".

Se node3 non dispone di porte FC integrate, porte UTA/UTA2 integrate o una scheda UTA/UTA2 e si sta aggiornando un sistema con dischi di archiviazione, è possibile passare a"Mappare le porte dal nodo 1 al nodo 3" .

Configurare le porte FC sul nodo 3

Se il nodo 3 dispone di porte FC, integrate o su un adattatore FC aggiuntivo, è necessario impostare le configurazioni delle porte sul nodo prima di metterlo in servizio, poiché le porte non sono preconfigurate al momento della spedizione dei sistemi. Se non si configurano le porte, si potrebbe verificare un'interruzione del servizio.

Prima di iniziare

È necessario disporre dei valori delle impostazioni della porta FC da node1 salvati in "Preparare i nodi per l'aggiornamento".

A proposito di questa attività

È possibile saltare questa sezione se il sistema non dispone di configurazioni FC. Se il sistema dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2, configurarle in Controllare e configurare le porte UTA/UTA2 sul nodo 3.

> Immettere i comandi in questa sezione al prompt del cluster.

Fasi

1. Visualizza informazioni su tutti gli adattatori di rete FC e convergenti presenti sul sistema.

   ```
   system node hardware unified-connect show
   ```

2. Confronta le impostazioni FC del nodo 3 con le impostazioni acquisite in precedenza dal nodo 1.

3. Esegui una delle seguenti azioni:

Se le impostazioni FC predefinite sui nuovi nodi sono…	Quindi…
Le stesse di quelle che hai catturato sul node1	Vai aFase 9 .
Diverso da quelli che avete catturato sul node1	Vai aFase 4 .

4. Modificare le porte FC sul nodo 3 secondo necessità immettendo uno dei seguenti comandi:
   - Per programmare le porte di destinazione:

     ```
     system node hardware unified-connect modify -type \| -t target -adapter port_name
     ```

   - Per programmare le porte initiator:

     ```
     system node hardware unified-connect modify -type \| -t initiator -adapter port_name
     ```

   `-t` È il tipo FC4: Destinazione o iniziatore.

5. Verificare le nuove impostazioni immettendo il seguente comando ed esaminando l'output:

   ```
   system node hardware unified-connect show
   ```

6. Uscire dalla modalità di manutenzione:

   ```
   halt
   ```

7. Dopo aver immesso il comando, attendere che il sistema si arresti al prompt dell'ambiente di avvio.
8. Avviare node3 al prompt dell'ambiente di avvio:

   ```
   boot_ontap
   ```

9. Esegui una delle seguenti azioni:
   - Se node3 ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate, passare a. Controllare e configurare le porte UTA/UTA2 sul nodo 3.
   - Se node3 non dispone di una scheda UTA/UTA2 o di porte UTA/UTA2 integrate, saltare Controllare e configurare le porte UTA/UTA2 sul nodo 3 e passare a. "Mappare le porte dal nodo 1 al nodo 3".

Controllare e configurare le porte UTA/UTA2 sul nodo 3

Se node3 dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2, è necessario controllare la configurazione delle porte ed eventualmente riconfigurarle, a seconda di come si desidera utilizzare il sistema aggiornato.

Prima di iniziare

È necessario disporre dei moduli SFP+ corretti per le porte UTA/UTA2.

A proposito di questa attività

Se si desidera utilizzare una porta UTA/UTA2 (Unified Target Adapter) per FC, è necessario prima verificare la configurazione della porta.

> I materiali di marketing NetApp potrebbero utilizzare il termine UTA2 per fare riferimento agli adattatori e alle porte CNA. Tuttavia, la CLI utilizza il termine CNA.

È possibile utilizzare `ucadmin show` comando per verificare la configurazione corrente della porta:

```
*> ucadmin show
          Current  Current    Pending  Pending    Admin
 Adapter  Mode     Type       Mode     Type       Status
 -------  -------  ---------  -------  ---------  -----------
 0e       fc       target     -        initiator  offline
 0f       fc       target     -        initiator  offline
 0g       fc       target     -        initiator  offline
 0h       fc       target     -        initiator  offline
 1a       fc       target     -        -          online
 1b       fc       target     -        -          online
6 entries were displayed.
```

Le porte UTA/UTA2 possono essere configurate in modalità FC nativa o UTA/UTA2. La modalità FC supporta l'iniziatore FC e la destinazione FC; la modalità UTA/UTA2 consente la condivisione simultanea del traffico NIC e FCoE con la stessa interfaccia SFP+ 10 GbE e supporta le destinazioni FC.

Le porte UTA/UTA2 potrebbero essere presenti su un adattatore o sul controller e presentano le seguenti configurazioni, ma è necessario controllare la configurazione delle porte UTA/UTA2 sul nodo 3 e modificarla, se necessario:

- Le schede UTA/UTA2 ordinate al momento dell'ordine del controller vengono configurate prima della spedizione per avere la personalità richiesta.
- Le schede UTA/UTA2 ordinate separatamente dal controller vengono fornite con il linguaggio di destinazione FC predefinito.
- Le porte UTA/UTA2 integrate sui nuovi controller vengono configurate prima della spedizione in modo da avere la personalità richiesta.

> Immettere i comandi in questa sezione al prompt del cluster, a meno che non venga richiesto di entrare in modalità Manutenzione.

Fasi

1. Verificare la configurazione attuale della porta immettendo il seguente comando sul nodo 3:

   `system node hardware unified-connect show`

   Il sistema visualizza un output simile al seguente esempio:

```
cluster1::> system node hardware unified-connect show

                 Current  Current    Pending  Pending  Admin
Node  Adapter  Mode     Type       Mode     Type     Status
----  -------  -------  ---------  -------  -------  ------
f-a   0e       fc       initiator  -        -        online
f-a   0f       fc       initiator  -        -        online
f-a   0g       cna      target     -        -        online
f-a   0h       cna      target     -        -        online
f-b   0e       fc       initiator  -        -        online
f-b   0f       fc       initiator  -        -        online
f-b   0g       cna      target     -        -        online
f-b   0h       cna      target     -        -        online
12 entries were displayed.
```

2. [[fase 2]]se il modulo SFP+ corrente non corrisponde all'utilizzo desiderato, sostituirlo con il modulo SFP+ corretto.

   Contattare il rappresentante NetApp per ottenere il modulo SFP+ corretto.

3. esaminare l'output di `system node hardware unified-connect show` oppure `ucadmin show` Per determinare se le porte UTA/UTA2 hanno la personalità desiderata.
4. eseguire una delle seguenti operazioni:

Se le porte UTA/UTA2…	**Quindi…**
Non avere la personalità che si desidera	Passare a. Fase 5.
Avere la personalità che si desidera	Salta il passaggio 5 al passaggio 13 e vai aFase 14 .

5. Se il sistema dispone di dischi di archiviazione ed esegue Data ONTAP 8.3 in cluster, avviare node3 ed entrare in modalità di manutenzione:

   ```
   boot_ontap maint
   ```

6. Verificare le impostazioni:

   ```
   ucadmin show
   ```

7. Eseguire una delle seguenti operazioni:

Se si sta configurando…	**Quindi…**
Porte su una scheda UTA/UTA2	Vai aFase 8 .
Porte UTA/UTA2 integrate	Salta il passaggio 8 e vai aFase 9 .

8. Se l'adattatore è in modalità iniziatore e la porta UTA/UTA2 è online, metti offline la porta UTA/UTA2:

   ```
   storage disable adapter adapter_name
   ```

Gli adattatori in modalità di destinazione sono automaticamente offline in modalità di manutenzione.

9. Se la configurazione corrente non corrisponde all'uso desiderato, modificare la configurazione secondo necessità:

   `ucadmin modify -m fc|cna -t initiator|target adapter_name`

   - `-m` è la modalità personality, `fc` oppure `cna`.
   - `-t` È di tipo FC4, `target` oppure `initiator`.

   > È necessario utilizzare l'iniziatore FC per le unità nastro e le configurazioni MetroCluster . Per i client SAN è necessario utilizzare la destinazione FC.

10. Arrestare il sistema:

    `halt`

    Il sistema si arresta al prompt dell'ambiente di avvio.

11. Immettere il seguente comando:

    `boot_ontap`

12. verificare le impostazioni:

    `system node hardware unified-connect show`

    L'output degli esempi seguenti mostra che il tipo di adattatore FC4 "1b" sta cambiando in `initiator` e che la modalità degli adattatori "2a" e "2b" stia cambiando in `cna`:

```
cluster1::> system node hardware unified-connect show

                Current  Current    Pending  Pending      Admin
Node  Adapter  Mode     Type       Mode     Type         Status
----  -------  -------  ---------  -------  -----------  ------
f-a   1a       fc       initiator  -        -            online
f-a   1b       fc       target     -        initiator    online
f-a   2a       fc       target     cna      -            online
f-a   2b       fc       target     cna      -            online

4 entries were displayed.
```

13. Metti online tutte le porte di destinazione immettendo il seguente comando, una volta per ogni porta:

    `network fcp adapter modify -node node_name -adapter adapter_name -state up`

14. Cablare la porta.

Mappare le porte dal nodo 1 al nodo 3

È necessario assicurarsi che le porte fisiche sul nodo 1 siano mappate correttamente alle porte fisiche sul nodo 3, che consentirà al nodo 3 di comunicare con gli altri nodi del cluster e con la rete dopo l'aggiornamento.

Prima di iniziare

È necessario disporre già delle informazioni relative alle porte sui nuovi nodi di *Hardware Universe*. (Passare a. "Riferimenti" Per collegarsi a *Hardware Universe*). Le informazioni vengono utilizzate più avanti in questa sezione e in "Mappare le porte dal nodo 2 al nodo 4".

La configurazione software di node3 deve corrispondere alla connettività fisica di node3 e la connettività di rete deve essere ripristinata prima di continuare con l'aggiornamento.

A proposito di questa attività

Le impostazioni delle porte possono variare a seconda del modello dei nodi.

È necessario rendere la porta e la configurazione LIF del nodo originale compatibili con la configurazione del nuovo nodo. Questo perché il nuovo nodo riproduce la stessa configurazione all'avvio, il che significa che quando si avvia node3, ONTAP tenterà di ospitare le LIF sulle stesse porte utilizzate sul node1.

Pertanto, se le porte fisiche sul nodo 1 non vengono mappate direttamente alle porte fisiche sul nodo 3, saranno necessarie modifiche alla configurazione del software per ripristinare la connettività di cluster, gestione e rete dopo l'avvio. Inoltre, se le porte del cluster sul nodo 1 non vengono mappate direttamente alle porte del cluster sul nodo 3, il nodo 3 potrebbe non ricongiungersi automaticamente al quorum quando viene riavviato fino a quando non viene apportata una modifica alla configurazione software per ospitare le LIF del cluster sulle porte fisiche corrette.

Fasi

1. Registra tutte le informazioni di cablaggio node1 per node1, le porte, i domini di trasmissione e gli spazi IPnella seguente tabella:

LIF	Node1 porte	Node1 IPspaces	Dominio di broadcast node1	Node3 porte	Node3 porte	Node3 domini di broadcast
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Cluster 5						
Cluster 6						
Gestione dei nodi						
Gestione del cluster						
Dati 1						
Dati 2						

LIF	Node1 porte	Node1 IPspaces	Dominio di broadcast node1	Node3 porte	Node3 porte	Node3 domini di broadcast
Dati 3						
Dati 4						
SAN						
Porta intercluster						

Fare riferimento a. "Registrare le informazioni del nodo 1" per ottenere queste informazioni.

2. registrare tutte le informazioni di cablaggio per node3, le porte, i domini di trasmissione e gli spazi IPnella tabella precedente utilizzando la stessa procedura descritta in "Registrare le informazioni del nodo 1".
3. [[fase 3]]seguire questi passaggi per verificare se l'installazione è un cluster senza switch a due nodi:

   a. Impostare il livello di privilegio su Advanced (avanzato):

      ```
      cluster::> set -privilege advanced
      ```

   b. Verificare se il setup è un cluster senza switch a due nodi:

      ```
      network options switchless-cluster show
      ```

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

+
Il valore di questo comando deve corrispondere allo stato fisico del sistema.

   a. Tornare al livello di privilegi di amministrazione:

```
cluster::*> set -privilege admin
cluster::>
```

4. inserire il node3 nel quorum effettuando le seguenti operazioni:

   a. Punto di avvio3. Vedere "Installazione e boot node3" per avviare il nodo, se non è già stato fatto.
   b. Verificare che le nuove porte del cluster si trovino nel dominio di trasmissione del cluster:

      ```
      network port show -node node-name -port port-name -fields broadcast-domain
      ```

      L'esempio seguente mostra che la porta "e0a" si trova nel dominio "Cluster" sul nodo 3:

```
 cluster::> network port show -node node3 -port e0a -fields
broadcast-domain

 node       port broadcast-domain
 ---------- ---- ----------------
 node3      e1a  Cluster
```

c. Aggiungere le porte corrette al dominio di trasmissione del cluster:

`network port modify -node node-name -port port-name -ipspace Cluster -mtu 9000`

Questo esempio aggiunge la porta cluster "e1b" al nodo 3:

```
 network port modify -node node3 -port e1b -ipspace Cluster -mtu 9000
```

Per una configurazione MetroCluster, potrebbe non essere possibile modificare il dominio di trasmissione di una porta perché è associata a una porta che ospita la LIF di una SVM di destinazione di sincronizzazione e visualizzare errori simili, ma non limitati al seguente messaggio`:

```
command failed: This operation is not permitted on a Vserver that is
configured as the destination of a MetroCluster Vserver relationship.
```

Immettere il seguente comando dalla SVM di origine di sincronizzazione corrispondente sul sito remoto per riallocare la LIF di destinazione di sincronizzazione su una porta appropriata:

`metrocluster vserver resync -vserver Vserver-name`

d. Migrare le LIF del cluster alle nuove porte, una volta per ogni LIF:

`network interface migrate -vserver Cluster -lif LIF-name -source-node node3 -destination-node node3 -destination-port port-name`

e. Modificare la porta home delle LIF del cluster:

`network interface modify -vserver Cluster -lif LIF-name –home-port port-name`

f. Se le porte del cluster non si trovano nel dominio di broadcast del cluster, aggiungerle:

`network port broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports node:port`

g. Rimuovere le vecchie porte dal dominio di trasmissione del cluster:

`network port broadcast-domain remove-ports`

Nell'esempio seguente viene rimossa la porta "e0d" sul nodo 3:

```
network port broadcast-domain remove-ports -ipspace Cluster -broadcast
-domain Cluster -ports <node3:e0d>
```

a. Verificare che node3 si sia riUnito al quorum:

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

5. regola i domini di broadcast che ospitano le LIF del cluster e le LIF di gestione dei nodi e/o del cluster. Verificare che ciascun dominio di trasmissione contenga le porte corrette. Una porta non può essere spostata tra domini di broadcast se è in hosting o è la sede di una LIF, quindi potrebbe essere necessario migrare e modificare le LIF come segue:

a. Visualizzare la porta home di una LIF:

```
network interface show -fields home-node,home-port
```

b. Visualizza il dominio di trasmissione contenente questa porta:

```
network port broadcast-domain show -ports node_name:port_name
```

c. Aggiungere o rimuovere le porte dai domini di broadcast:

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

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

a. Modificare la porta home di una LIF:

```
network interface modify -vserver Vserver-name -lif LIF-name –home-port
port-name
```

6. regola i domini di trasmissione tra cluster e migra le LIF tra cluster, se necessario, utilizzando gli stessi comandi mostrati nella Fase 5.
7. regolare qualsiasi altro dominio di broadcast e migrare i dati LIF, se necessario, utilizzando gli stessi comandi illustrati nella Fase 5.
8. se vi sono porte sul node1 che non esistono più sul node3, attenersi alla seguente procedura per eliminarle:

a. Accedere al livello di privilegio avanzato su uno dei nodi:

```
set -privilege advanced
```

b. Eliminare le porte:

```
network port delete -node node-name -port port-name
```

c. Tornare al livello di amministrazione:

```
set -privilege admin
```

9. regola tutti i gruppi di failover LIF:

   `network interface modify -failover-group` *`failover-group`* `-failover-policy` *`failover-policy`*

   Nell'esempio seguente viene impostato il criterio di failover su "broadcast-domain-wide" e vengono utilizzate le porte del gruppo di failover "fg1" come destinazioni di failover per LIF "data1" su "node3":

   ```
   network interface modify -vserver node3 -lif data1 failover-policy
   broadcast-domainwide -failover-group fg1
   ```

   Passare a. "Riferimenti" Per ulteriori informazioni, fare riferimento a *Gestione di rete* o ai comandi di *ONTAP 9: Manuale di riferimento pagina*.

10. Verificare le modifiche al nodo 3:

    `network port show -node node3`

11. Ogni LIF del cluster deve essere in ascolto sulla porta 7700. Verificare che le LIF del cluster siano in ascolto sulla porta 7700:

    `::> network connections listening show -vserver Cluster`

    La porta 7700 in ascolto sulle porte del cluster è il risultato previsto, come mostrato nell'esempio seguente per un cluster a due nodi:

    ```
    Cluster::> network connections listening show -vserver Cluster
    Vserver Name     Interface Name:Local Port     Protocol/Service
    ---------------- ----------------------------  -------------------
    Node: NodeA
    Cluster          NodeA_clus1:7700               TCP/ctlopcp
    Cluster          NodeA_clus2:7700               TCP/ctlopcp
    Node: NodeB
    Cluster          NodeB_clus1:7700               TCP/ctlopcp
    Cluster          NodeB_clus2:7700               TCP/ctlopcp
    4 entries were displayed.
    ```

12. Per ogni cluster LIF che non è in ascolto sulla porta 7700, imposta lo stato amministrativo della LIF su `down` e poi `up`:

    `::> net int modify -vserver Cluster -lif` *`cluster-lif`* `-status-admin down; net int modify -vserver Cluster -lif` *`cluster-lif`* `-status-admin up`

    Ripetere il passaggio 11 per verificare che la LIF del cluster sia in ascolto sulla porta 7700.

Verificare l'installazione di node3

Dopo aver installato e avviato il nodo 3, è necessario verificare che sia installato

correttamente, che faccia parte del cluster e che sia in grado di comunicare con il nodo 2.

Fasi

1. [[fase 1]]al prompt del sistema, accedere a node3. Quindi, verificare che node3 faccia parte dello stesso cluster di node2 e sia integro:

   ```
   cluster show
   ```

2. verifica che node3 possa comunicare con node2 e che tutti i LIF siano in funzione:

   ```
   network interface show -curr-node node3
   ```

3. eseguire una delle seguenti operazioni:

Se il cluster è…	Quindi…
In un ambiente SAN	Completo Fase 4 quindi passare alla sezione "Spostamento delle LIF dei dati NAS di proprietà del node1 da node2 a node3 e verifica delle LIF SAN sul node3".
Non in un ambiente SAN	Saltare la fase 4 e passare a. "Spostamento delle LIF dei dati NAS di proprietà del node1 da node2 a node3 e verifica delle LIF SAN sul node3".

4. [[fase 4]] verificare che node2 e node3 siano in quorum immettendo il seguente comando su uno dei nodi ed esaminandone l'output:

   ```
   event log show -messagename scsiblade.*
   ```

   L'esempio seguente mostra l'output quando i nodi nel cluster sono in quorum:

   ```
   cluster::> event log show -messagename scsiblade.*
   Time                Node   Severity      Event
   ------------------- ------ ------------- -------------------------
   8/13/2012 14:03:51  node1  INFORMATIONAL scsiblade.in.quorum: The scsi-
   blade ...
   8/13/2012 14:03:51  node2  INFORMATIONAL scsiblade.in.quorum: The scsi-
   blade ...
   8/13/2012 14:03:48  node3  INFORMATIONAL scsiblade.in.quorum: The scsi-
   blade ...
   8/13/2012 14:03:43  node4  INFORMATIONAL scsiblade.in.quorum: The scsi-
   blade ...
   ```

Spostare le LIF dei dati NAS di proprietà del node1 da node2 a node3 e verificare le LIF SAN sul node3

Dopo aver verificato l'installazione di node3 e prima di spostare gli aggregati da node2 a node3, è necessario spostare i dati NAS LIF appartenenti a node1 che sono attualmente su node2 da node2 a node3. È inoltre necessario verificare le LIF SAN sul nodo 3.

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. Elenca tutte le LIF dati NAS non possedute da node2 immettendo il seguente comando su entrambi i nodi e catturando l'output:

   `network interface show -role data -curr-node` *`node2`* `-is-home false -home-node` *`node3`*

2. se il cluster è configurato per le LIF SAN, registrare le LIF SAN `adapter` e. `switch-port` informazioni di configurazione in questo "foglio di lavoro" da utilizzare in seguito nella procedura.

   a. Elencare le LIF SAN sul node2 ed esaminare l'output:

      `network interface show -data-protocol fc*`

      Il sistema restituisce un output simile al seguente esempio:

```
cluster1::> net int show -data-protocol fc*
  (network interface show)
            Logical     Status     Network            Current
Current Is
Vserver     Interface   Admin/Oper Address/Mask       Node
Port    Home
----------  ----------  ---------- ------------------ -------------
------- ----
svm2_cluster1
            lif_svm2_cluster1_340
                        up/up      20:02:00:50:56:b0:39:99
                                                      cluster1-01
1b      true
            lif_svm2_cluster1_398
                        up/up      20:03:00:50:56:b0:39:99
                                                      cluster1-02
1a      true
            lif_svm2_cluster1_691
                        up/up      20:01:00:50:56:b0:39:99
                                                      cluster1-01
1a      true
            lif_svm2_cluster1_925
                        up/up      20:04:00:50:56:b0:39:99
                                                      cluster1-02
1b      true
4 entries were displayed.
```

b. Elencare le configurazioni esistenti ed esaminare l'output:

```
fcp adapter show -fields switch-port,fc-wwpn
```

Il sistema restituisce un output simile al seguente esempio:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  ----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

3. eseguire una delle seguenti operazioni:

Se nodo1…	Quindi…
Ha configurato gruppi di interfacce o VLAN	Passare a. Fase 4.
Non sono stati configurati gruppi di interfacce o VLAN	Saltare la fase 4 e passare a. Fase 5.

4. eseguire i seguenti passaggi secondari per migrare qualsiasi LIF di dati NAS ospitata su gruppi di interfacce e VLAN originariamente presenti sul nodo 1 da node2 a node3:

a. Migrate qualsiasi LIF di dati ospitata su node2 che in precedenza apparteneva a node1 su un gruppo di interfacce a una porta sul node3 in grado di ospitare LIF sulla stessa rete immettendo il seguente comando, una volta per ogni LIF:

```
network interface migrate -vserver vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

b. Modificare la porta home e il nodo home di LIF in Sotto-fase A. Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node
node3 -home-port netport|ifgrp
```

c. Migrare tutti i dati LIF ospitati su node2 che in precedenza appartenevano a node1 su una porta VLAN a una porta su node3 in grado di ospitare LIF sulla stessa rete immettendo il seguente comando, una volta per ogni LIF:

```
network interface migrate -vserver vserver_name -lif LIF_name -destination
-node node3 –destination-port netport|ifgrp
```

d. Modificare la porta home e il nodo home dei file LIF in Sotto-fase c Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node
node3 -home-port netport|ifgrp
```

5. eseguire una delle seguenti operazioni:

Se il cluster è configurato per…	**Quindi…**
NAS	Completo Fase 6 e. Fase 7, Saltare il passaggio 8 e completare Fase 9 attraverso Fase 12.
SAN	Disattivare tutte le LIF SAN sul nodo per disattivarle per l'aggiornamento: `network interface modify -vserver *vserver_name* -lif *LIF_name* -home-node *node_to_upgrade* -home-port _netport

6. se si dispone di porte dati non uguali sulle piattaforme, aggiungere le porte al dominio di trasmissione:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt -ports node:port
```

Nell'esempio seguente viene aggiunta la porta "e0a" sul nodo "6280-1" e la porta "e0i" sul nodo "8060-1" al dominio di trasmissione "mgmt" nell'IPSpace "Default":

```
cluster::> network port broadcast-domain add-ports -ipspace Default
-broadcast-domain mgmt -ports 6280-1:e0a, 8060-1:e0i
```

7. Migrare ciascun LIF dati NAS in node3 immettendo il seguente comando, una volta per ogni LIF:

```
network interface migrate -vserver vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

8. assicurarsi che la migrazione dei dati sia persistente:

```
network interface modify -vserver vserver_name -lif LIF_name-home-port
netport|ifgrp -home-node node3
```

9. verificare che le LIF SAN si trovino sulle porte corrette sul nodo 3:

a. Immettere il seguente comando ed esaminarne l'output:

`network interface show -data-protocol iscsi|fcp -home-node node3`

Il sistema restituisce un output simile al seguente esempio:

```
cluster::> net int show -data-protocol iscsi|fcp -home-node node3
              Logical     Status      Network              Current
Current  Is
 Vserver      Interface   Admin/Oper  Address/Mask         Node
Port     Home
 -----------  ----------  ----------  ------------------
-------------  -------  ----
 vs0
              a0a         up/down     10.63.0.53/24        node3
a0a      true
              data1       up/up       10.63.0.50/18        node3
e0c      true
              rads1       up/up       10.63.0.51/18        node3
e1a      true
              rads2       up/down     10.63.0.52/24        node3
e1b      true
 vs1
              lif1        up/up       172.17.176.120/24    node3
e0c      true
              lif2        up/up       172.17.176.121/24    node3
e1a      true
```

b. Verificare che i nuovi e. `adapter` e. `switch-port` le configurazioni sono corrette confrontando l'output di `fcp adapter show` con le informazioni di configurazione registrate nel foglio di lavoro in Fase 2.

Elencare le nuove configurazioni LIF SAN al nodo 3:

`fcp adapter show -fields switch-port,fc-wwpn`

Il sistema restituisce un output simile al seguente esempio:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter fc-wwpn                 switch-port
-----------  ------- ----------------------- -------------
cluster1-01 0a      50:0a:09:82:9c:13:38:00 ACME Switch:0
cluster1-01 0b      50:0a:09:82:9c:13:38:01 ACME Switch:1
cluster1-01 0c      50:0a:09:82:9c:13:38:02 ACME Switch:2
cluster1-01 0d      50:0a:09:82:9c:13:38:03 ACME Switch:3
cluster1-01 0e      50:0a:09:82:9c:13:38:04 ACME Switch:4
cluster1-01 0f      50:0a:09:82:9c:13:38:05 ACME Switch:5
cluster1-01 1a      50:0a:09:82:9c:13:38:06 ACME Switch:6
cluster1-01 1b      50:0a:09:82:9c:13:38:07 ACME Switch:7
cluster1-02 0a      50:0a:09:82:9c:6c:36:00 ACME Switch:0
cluster1-02 0b      50:0a:09:82:9c:6c:36:01 ACME Switch:1
cluster1-02 0c      50:0a:09:82:9c:6c:36:02 ACME Switch:2
cluster1-02 0d      50:0a:09:82:9c:6c:36:03 ACME Switch:3
cluster1-02 0e      50:0a:09:82:9c:6c:36:04 ACME Switch:4
cluster1-02 0f      50:0a:09:82:9c:6c:36:05 ACME Switch:5
cluster1-02 1a      50:0a:09:82:9c:6c:36:06 ACME Switch:6
cluster1-02 1b      50:0a:09:82:9c:6c:36:07 ACME Switch:7
16 entries were displayed
```

Se un LIF SAN nella nuova configurazione non si trova su un adattatore ancora collegato allo stesso `switch-port`, potrebbe causare un'interruzione del sistema quando si riavvia il nodo.

c. Se node3 ha LIF SAN o gruppi DI LIF SAN che si trovano su una porta che non esisteva sul node1 o che devono essere mappati su una porta diversa, spostarli su una porta appropriata sul node3 completando i seguenti passaggi secondari:

   i. Impostare lo stato LIF su "DOWN" (giù):

      `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-status -admin down`

   ii. Rimuovere la LIF dal set di porte:

      `portset remove -vserver` *`vserver_name`* `-portset` *`portset_name`* `-port-name` *`port_name`*

   iii. Immettere uno dei seguenti comandi:

      - Spostare una singola LIF:

        `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home -port` *`new_home_port`*

      - Spostare tutte le LIF su una singola porta inesistente o errata su una nuova porta:

```
network interface modify {-home-port port_on_node1 -home-node node1
-role data} -home-port new_home_port_on_node3
```

- Aggiungere nuovamente i file LIF al set di porte:

```
portset add -vserver vserver_name -portset portset_name -port-name
port_name
```

> È necessario spostare I file LIF SAN su una porta con la stessa velocità di collegamento della porta originale.

10. Modificare lo stato di tutte le LIF su "up" in modo che le LIF possano accettare e inviare traffico sul nodo:

```
network interface modify -home-port port_name -home-node node3 -lif data
-status-admin up
```

11. Immettere il seguente comando su uno dei nodi ed esaminare l'output per verificare che le LIF siano state spostate nelle porte corrette e che le LIF abbiano lo stato di "up" immettendo il seguente comando su uno dei nodi ed esaminando l'output:

```
network interface show -home-node node3 -role data
```

12. se le LIF non sono attive, impostare lo stato amministrativo delle LIF su "up" immettendo il seguente comando, una volta per ciascuna LIF:

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

13. Invia un messaggio AutoSupport post-upgrade a NetApp per il node1:

```
system node autosupport invoke -node node3 -type all -message "node1
successfully upgraded from platform_old to platform_new"
```

Foglio di lavoro: Informazioni da registrare prima di spostare i file LIF dei dati NAS in node3

Per verificare di disporre della configurazione corretta dopo aver spostato LE LIF SAN da node2 a node3, è possibile utilizzare il seguente foglio di lavoro per registrare `adapter` e. `switch-port` Informazioni per ciascun LIF.

Registrare la LIF `adapter` informazioni da `network interface show -data-protocol fc*` output del comando e il `switch-port` informazioni da `fcp adapter show -fields switch-port,fc-wwpn` output del comando per node2.

Dopo aver completato la migrazione al nodo 3, registrare il LIF `adapter` e. `switch-port` Informazioni per i LIF sul node3 e verificare che ciascun LIF sia ancora connesso allo stesso `switch-port`.

Node2			**Node3**		
LIF	`adapter`	`switch-port`	LIF	`adapter`	`switch-port`

Node2			Node3		

Spostare gli aggregati non root dal nodo 2 al nodo 3

Prima di sostituire node2 con node4, è necessario inviare un messaggio AutoSupport per node2 e spostare gli aggregati non root di proprietà di node2 a node3.

> Durante questa procedura, non spostare gli aggregati da node3 a node2. In questo modo, gli aggregati vengono portati offline e si verifica una mancanza di servizio dei dati per gli aggregati che vengono ricollocati.

Fasi

1. Verificare che l'ID del sistema partner sia impostato correttamente sul nodo 3:

   a. Immettere il livello di privilegio avanzato:

      ```
      set -privilege advanced
      ```

   b. Mostra l'ID del sistema del partner su node3:

      ```
      ha interconnect config show -node <node3-node1>
      ```

      Il sistema visualizza un output simile al seguente esempio:

   Mostra esempio

   ```
   cluster::*> ha interconnect config show -node <node>
     (system ha interconnect config show)

                           Node: node3-node1
              Interconnect Type: RoCE
                Local System ID: <node3-system-id>
              Partner System ID: <node2-system-id>
           Connection Initiator: local
                      Interface: external

   Port   IP Address
   ----   -----------------
   e4a-17   0.0.0.0
   e4b-18   0.0.0.0
   ```

2. Se "ID sistema partner" non è corretto per node3:

a. Arresto node3:

```
halt
```

b. Al prompt di Loader, impostare il valore corretto "partner-sysid".

Il node3 "partner-sysid" è l'ID di sistema di node2, che è possibile trovare nell' `ha interconnect config show`output in Fase 1.

c. Salvare le impostazioni:

```
saveenv
```

d. Al prompt di Loader, avviare node3 nel menu di avvio:

```
boot_ontap menu
```

e. Accedere a node3.

3. Manda un messaggio a "AutoSupport" a "NetApp for node2:

```
system node autosupport invoke -node <node2> -type all -message "Upgrading
<node2> from <platform_old> to <platform_new>"
```

4. Verificare che il messaggio AutoSupport sia stato inviato:

```
system node autosupport show -node <node2> -instance
```

I campi "ultimo oggetto inviato:" e "ultimo invio:" contengono il titolo dell'ultimo messaggio inviato e l'ora in cui il messaggio è stato inviato.

5. Riposiziona gli aggregati non radice:

a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

b. Elencare gli aggregati di proprietà di node2:

```
storage aggregate show -owner-name <node2>
```

c. Avviare il trasferimento degli aggregati:

```
storage aggregate relocation start -node <node2> -destination <node3>
-aggregate-list * -ndo-controller-upgrade true
```

Il comando individua solo gli aggregati non root.

a. Quando richiesto, immettere `y`.

Il trasferimento avviene in background. La riposizionamento di un aggregato può richiedere da pochi secondi a un paio di minuti. Il tempo include sia le parti di fuori servizio del client che quelle di non fuori servizio. Il comando non sposta aggregati non in linea o con restrizioni.

b. Tornare al livello di privilegio admin:

```
set -privilege admin
```

6. Verificare lo stato di trasferimento del nodo 2:

```
storage aggregate relocation show -node <node2>
```

L'output visualizza "Done" (eseguito) per un aggregato dopo che è stato spostato.

> Prima di passare alla fase successiva, è necessario attendere che tutti gli aggregati di proprietà di node2 siano stati ricollocati in node3.

7. Eseguire una delle seguenti operazioni:

In caso di trasferimento di…	Quindi…
Tutti gli aggregati hanno avuto successo	Andare a Fase 8.

In caso di trasferimento di…	Quindi…

Qualsiasi aggregato ha avuto esito negativo o è stato vetoato	a. Visualizzare un messaggio di stato dettagliato:
	`storage aggregate show -instance`
	È inoltre possibile controllare i registri EMS per visualizzare l'azione correttiva necessaria.
	Il `event log show` command elenca gli errori che si sono verificati.
	b. Eseguire l'azione correttiva.
	c. Impostare il livello di privilegio su Advanced (avanzato):
	`set -privilege advanced`
	d. Spostare eventuali aggregati guasti o vetoed:
	`storage aggregate relocation start -node <node2> -destination <node3> -aggregate-list * -ndo-controllerupgrade true`
	e. Quando richiesto, immettere `y`.
	f. Tornare al livello di privilegio admin:
	`set -privilege admin`
	Se necessario, è possibile forzare il trasferimento utilizzando uno dei seguenti metodi:
	• Sovrascrivendo i veto check:
	`storage aggregate relocation start -override -vetoes true -ndo-controller-upgrade`
	• Sovrascrivendo i controlli di destinazione:
	`storage aggregate relocation start -override -destination-checks true -ndocontroller-upgrade`
	Per ulteriori informazioni sui comandi di trasferimento degli aggregati di storage, visitare il sito Web all'indirizzo "Riferimenti" Per collegarsi alla gestione di *dischi e aggregati con i comandi CLI* e *ONTAP 9: Manuale riferimento pagina*.

8. verificare che tutti gli aggregati non root siano online su node3:

`storage aggregate show -node <node3> -state offline -root false`

Se alcuni aggregati sono andati offline o sono diventati estranei, è necessario portarli online una volta per

ciascun aggregato:

```
storage aggregate online -aggregate <aggregate_name>
```

9. Verificare che tutti i volumi siano online al nodo3:

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

   Se alcuni volumi sono offline sul node3, è necessario portarli online, una volta per ciascun volume:

   ```
   volume online -vserver <Vserver-name> -volume <volume-name>
   ```

10. Verificare che node2 non disponga di aggregati non root online:

    ```
    storage aggregate show -owner-name <node2> -ha-policy sfo -state online
    ```

    L'output del comando non dovrebbe visualizzare gli aggregati online non root perché tutti gli aggregati online non root sono già stati riallocati in node3.

Spostare le LIF dei dati NAS di proprietà del node2 al node3

Dopo aver spostato gli aggregati da node2 a node3, è necessario spostare i dati NAS LIF di proprietà di 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. LE LIF SAN non vengono spostate a meno che non sia necessario mapparle su nuove porte. È necessario verificare che le LIF siano integre e ubicate sulle porte appropriate dopo aver spostato le LIF da node3 a node4 e aver portato node4 online.

Fasi

1. Elenca tutte le LIF dei dati NAS di proprietà di node2 immettendo il seguente comando su uno dei nodi e acquisendo l'output:

   ```
   network interface show -data-protocol nfs|cifs -home-node node2
   ```

   L'esempio seguente mostra l'output del comando per node2:

```
cluster::> network interface show -data-protocol nfs|cifs -home-node
node2
              Logical     Status      Network             Current
Current  Is
 Vserver      Interface   Admin/Oper  Address/Mask        Node     Port
Home
 -----------  ----------  ----------  ------------------  -------
-------  ----
 vs0
              a0a         up/down     10.63.0.53/24       node2    a0a
true
              data1       up/up       10.63.0.50/18       node2    e0c
true
              rads1       up/up       10.63.0.51/18       node2    e1a
true
              rads2       up/down     10.63.0.52/24       node2    e1b
true
 vs1
              lif1        up/up       172.17.176.120/24   node2    e0c
true
              lif2        up/up       172.17.176.121/24   node2    e1a
true
```

2. eseguire una delle seguenti operazioni:

In caso di node2…	Quindi…
Dispone di gruppi di interfacce o VLAN configurati	Passare a. Fase 3.
Non ha gruppi di interfacce o VLAN configurati	Saltare la fase 3 e passare a. Fase 4.

3. eseguire i seguenti passaggi per migrare i dati NAS LIF ospitati su gruppi di interfacce e VLAN sul nodo 2:

   a. Migrate qualsiasi LIF di dati ospitata su un gruppo di interfacce su node2 a una porta su node3 in grado di ospitare LIF sulla stessa rete immettendo il seguente comando, una volta per ogni LIF:

      `network interface migrate -vserver` *`Vserver_name`* `-lif` *`LIF_name`* `-destination -node` *`node3`* `-destination-port` *`netport|ifgrp`*

   b. Modificare la porta home e il nodo home dei file LIF in Sotto-fase A. Alla porta e al nodo che attualmente ospitano i LIF immettendo il seguente comando, una volta per ogni nodo:

      `network interface modify -vserver` *`Vserver_name`* `-lif` *`LIF_name`* `-home-node` *`node3`* `-homeport` *`netport|ifgrp`*

   c. Migrare le LIF ospitate su VLAN su node2 a una porta su node3 in grado di ospitare LIF sulla stessa rete delle VLAN immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface migrate -vserver Vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

d. Modificare la porta home e il nodo home dei file LIF in Sotto-fase c Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface modify -vserver Vserver_name -lif LIF_name -home-node
node3 -homeport netport|ifgrp
```

4. eseguire una delle seguenti operazioni:

Se il cluster è configurato per…	Quindi…
NAS	Completo Fase 5 attraverso Fase 8.
SAN	Saltare i passaggi da 5 a 8, quindi completare Fase 9.
NAS e SAN	Completo Fase 5 attraverso Fase 9.

5. se si dispone di porte dati non uguali sulle piattaforme, aggiungere le porte al dominio di trasmissione:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt -ports node:port
```

Nell'esempio seguente viene aggiunta la porta "e0a" sul nodo "6280-1" e la porta "e0i" sul nodo "8060-1" al dominio di trasmissione "mgmt" nell'IPSpace "Default":

```
cluster::> network port broadcast-domain add-ports -ipspace Default
           -broadcast-domain mgmt -ports 6280-1:e0a, 8060-1:e0i
```

6. Migrare ciascun LIF dati NAS in node3 immettendo il seguente comando, una volta per ogni LIF:

```
network interface migrate -vserver Vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

7. verificare che le LIF NAS siano state spostate nelle porte corrette e che le LIF abbiano lo stato di up immettendo il seguente comando su entrambi i nodi ed esaminando l'output:

```
network interface show -curr-node node3 -data-protocol cifs|nfs
```

8. se le LIF non sono attive, imposta lo stato amministrativo delle LIF su "up" immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface modify -vserver Vserver_name -lif LIF_name -status-admin up
```

9. se sono configurati gruppi di interfacce o VLAN, completare i seguenti passaggi secondari:

a. Rimuovere le VLAN dai gruppi di interfacce:

```
network port vlan delete -node node_name -port ifgrp -vlan-id VLAN_ID
```

b. Immettere il seguente comando ed esaminarne l'output per determinare se nel nodo sono configurati gruppi di interfacce:

```
network port ifgrp show -node node_name -ifgrp ifgrp_name -instance
```

Il sistema visualizza le informazioni sul gruppo di interfacce per il nodo, come illustrato nell'esempio seguente:

```
cluster::> network port ifgrp show -node node2 -ifgrp a0a -instance
                  Node: node2
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode_lacp
          MAC Address: MAC_address
    ort Participation: partial
        Network Ports: e2c, e2d
             Up Ports: e2c
           Down Ports: e2d
```

a. Se nel nodo sono configurati gruppi di interfacce, registrare i nomi dei gruppi di interfacce e le porte ad essi assegnate, quindi eliminare le porte immettendo il seguente comando, una volta per ciascuna porta:

   ```
   network port ifgrp remove-port -node node_name -ifgrp ifgrp_name -port port_name
   ```

Fase 4. Registrare le informazioni e dismettere il node2

Registrare le informazioni del nodo 2

Prima di spegnere e dismettere il nodo 2, è necessario registrare le informazioni relative alla rete del cluster, alla gestione e alle porte FC, nonché l'ID del sistema NVRAM. Queste informazioni sono necessarie più avanti nella procedura quando si esegue il mapping del nodo 2 al nodo 4 e si riassegnano i dischi.

Fasi

1. Trova le porte di rete cluster, gestione nodi, intercluster e gestione cluster sul nodo 2:

   ```
   network interface show -curr-node node_name -role
   cluster,intercluster,nodemgmt,cluster-mgmt
   ```

   Il sistema visualizza le LIF per quel nodo e per gli altri nodi nel cluster, come mostrato nell'esempio seguente:

```
cluster::> network interface show -curr-node node2 -role
cluster,intercluster,node-mgmt,cluster-mgmt
         Logical     Status     Network            Current     Current
Is
Vserver  Interface   Admin/Oper Address/Mask       Node        Port
Home
-------- ----------  ---------- ------------------ ----------  -------
----
node2
         intercluster up/up     192.168.1.202/24   node2       e0e
true
         clus1        up/up     169.254.xx.xx/24   node2       e0a
true
         clus2        up/up     169.254.xx.xx/24   node2       e0b
true
         mgmt1        up/up     192.168.0.xxx/24   node2       e0c
true
4 entries were displayed.
```

Il sistema potrebbe non disporre di LIF intercluster. Si avrà una LIF di gestione del cluster solo su un nodo di una coppia di nodi. Una LIF di gestione cluster viene visualizzata nell'output di esempio di "Fase 1" In *Record node1 port information*.

2. Acquisire le informazioni nell'output da utilizzare nella sezione "Mappare le porte dal nodo 2 al nodo 4".

   Le informazioni di output sono necessarie per mappare le nuove porte del controller alle vecchie porte del controller.

3. Determinare le porte fisiche sul nodo 2:

   `network port show -node node_name -type physical +`

   `node_name` è il nodo che viene migrato.

   Il sistema visualizza le porte fisiche sul nodo 2, come mostrato nell'esempio seguente:

```
cluster::> network port show -node node2 -type physical

                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- -----------
node2
       e0M       Default      IP_address       up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

4. Registrare le porte e i relativi domini di trasmissione.

   I domini di broadcast dovranno essere mappati alle porte sul nuovo controller più avanti nella procedura.

5. Determinare le porte FC sul nodo 2:

   `network fcp adapter show`

   Il sistema visualizza le porte FC sul nodo 2, come mostrato nell'esempio seguente:

```
cluster::> network fcp adapter show -node node2
                     Connection  Host
Node         Adapter Established Port Address
------------ ------- ----------- ------------
node2
             0a      ptp         11400
node2
             0c      ptp         11700
node2
             6a      loop        0
node2
             6b      loop        0
4 entries were displayed.
```

6. Registrare le porte.

   Le informazioni di output sono necessarie per mappare le nuove porte FC sul nuovo controller più avanti nella procedura.

7. Se non è stato fatto in precedenza, controllare se ci sono gruppi di interfacce o VLAN configurati su node2:

   `ifgrp show`

```
vlan show
```

Verranno utilizzate le informazioni contenute nella sezione "Mappare le porte dal nodo 2 al nodo 4".

8. Eseguire una delle seguenti operazioni:

Se…	Quindi…
Numero ID sistema NVRAM registrato in "Preparare i nodi per l'aggiornamento"	Passare a. "Andare in pensione node2".
Il numero dell'ID del sistema NVRAM non è stato registrato in "Preparare i nodi per l'aggiornamento"	Completo Fase 9 e. Fase 10 quindi passare alla sezione successiva, "Andare in pensione node2".

9. Visualizza gli attributi del node2:

```
system node show -instance -node node2
```

```
cluster::> system node show -instance -node node2
                              ...
                NVRAM System ID: system_ID
                              ...
```

10. registrare l'ID del sistema NVRAM da utilizzare nella sezione "Installazione e boot node4".

Andare in pensione node2

Per dismettere il node2, è necessario chiudere il node2 correttamente e rimuoverlo dal rack o dallo chassis. Se il cluster si trova in un ambiente SAN, è necessario eliminare anche le LIF SAN.

Fasi

1. Eseguire una delle seguenti operazioni:

Se il cluster è…	Quindi…
Un cluster a due nodi	Passare a. Fase 2.
Un cluster con più di due nodi	Passare a. Fase 9.

2. accedere al livello di privilegio avanzato immettendo il seguente comando su uno dei nodi:

```
set -privilege advanced
```

3. Verificare che l'ha del cluster sia stato disattivato immettendo il seguente comando ed esaminandone l'output:

```
cluster ha show
```

Il sistema visualizza il seguente messaggio:

```
High Availability Configured: false
```

4. Verificare se node2 attualmente contiene epsilon immettendo il seguente comando ed esaminandone l'output:

   `cluster show`

   Il seguente esempio mostra che node2 contiene epsilon:

```
cluster*::> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -----------
node1                 true    true          false
node2                 true    true          true

Warning: Cluster HA has not been configured. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

2 entries were displayed.
```

   Se si sta aggiornando una coppia HA in un cluster con più coppie HA, è necessario spostare epsilon sul nodo di una coppia HA che non è in fase di aggiornamento del controller. Ad esempio, se si sta aggiornando NodeA/NodeB in un cluster con la configurazione della coppia ha NodeA/NodeB e NODEC/NODed, è necessario spostare epsilon in NODEC o NODed.

5. Se il node2 contiene epsilon, contrassegnare epsilon come `false` sul nodo in modo che possa essere trasferito al nodo 3:

   `cluster modify -node node2 -epsilon false`

6. Trasferire epsilon al nodo 3 contrassegnando epsilon `true` al nodo 3:

   `cluster modify -node node3 -epsilon true`

7. Verificare se il setup è un cluster senza switch a due nodi:

   `network options switchless-cluster show`

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

Il valore di questo comando deve corrispondere allo stato fisico del sistema.

8. Verificare se il setup è un cluster senza switch a due nodi:

   `network options switchless-cluster show`

   ```
   cluster::*> network options switchless-cluster show
   Enable Switchless Cluster: false/true
   ```

   Il valore di questo comando deve corrispondere allo stato fisico del sistema.

9. Torna al livello di amministrazione:

   `set -privilege admin`

10. Arrestare il node2 immettendo il seguente comando su uno dei controller:
    `system node halt -node node2`
11. Dopo lo spegnimento completo del node2, rimuoverlo dallo chassis o dal rack. È possibile decommissionare il node2 una volta completato l'aggiornamento. Vedere "Decommissionare il vecchio sistema".

Fase 5. Installazione e boot node4

Installazione e boot node4

È necessario installare node4 nel rack, trasferire node2 connessioni al node4 e fare il boot node4. È inoltre necessario riassegnare eventuali spare node2, dischi appartenenti a root e aggregati non root che non sono stati riallocati in precedenza in node3.

A proposito di questa attività

È necessario eseguire l'avvio di rete del nodo 4 se la versione ONTAP sul nodo 4 è diversa dalla versione ONTAP sul nodo 2. Dopo aver installato node4, avviarlo dall'immagine ONTAP 9 memorizzata sul server web. È quindi possibile scaricare i file corretti sul dispositivo di supporto di avvio per i successivi avvii del sistema seguendo le istruzioni in "Preparatevi per il netboot"

Tuttavia, non è necessario eseguire l'avvio di rete del nodo 4 se la versione ONTAP sul nodo 4 è uguale o successiva alla versione ONTAP sul nodo 2.

- Per un aggiornamento del controller AFF A800 o AFF C800 , è necessario assicurarsi che tutte le unità nello chassis siano saldamente posizionate contro il midplane prima di rimuovere node2. Per maggiori informazioni, vedere "Sostituire i moduli controller AFF A800 o AFF C800".
- Se si sta aggiornando un sistema con dischi di archiviazione, è necessario completare l'intera sezione e quindi procedere alla sezione "Impostare la configurazione FC o UTA/UTA2 su node4" , immettendo comandi al prompt del cluster.

Fasi

1. eseguire una delle seguenti operazioni:

Se node4 sarà in …	Quindi…
Uno chassis separato dal node3	Passare a. Fase 2.
Lo stesso chassis con node3	Saltare i passaggi 2 e 3 e passare a. Fase 4.

2. assicurarsi che node4 disponga di spazio rack sufficiente.

   Se il nodo 4 si trova in uno chassis separato dal nodo 3, è possibile inserire il nodo 4 nella stessa posizione del nodo 2. Se node3 e node4 si trovano nello stesso chassis, node4 si trova già nella posizione rack appropriata.

3. Installare il nodo 4 nel rack seguendo le istruzioni contenute nelle *istruzioni di installazione e configurazione* relative al modello di nodo.
4. cavo node4, spostamento delle connessioni da node2 a node4.

   I seguenti riferimenti consentono di stabilire i collegamenti dei cavi corretti. Passare a. "Riferimenti" per collegarli.

   - *Istruzioni di installazione e configurazione* per la piattaforma node4
   - La procedura di shelf di dischi appropriata
   - La documentazione *ha Pair Management*

   Collegare i seguenti cavi:

   - Console (porta di gestione remota)
   - Porte del cluster
   - Porte dati
   - Porte di gestione di cluster e nodi
   - Storage
   - Configurazioni SAN: Porte switch FC e Ethernet iSCSI

   Non è necessario spostare la scheda di interconnessione/scheda FC_VI o la connessione del cavo Interconnect/FC_VI dal nodo 2 al nodo 4, poiché la maggior parte dei modelli di piattaforma dispone di modelli di schede di interconnessione univoci.

5. Eseguire una delle seguenti operazioni:

Se il nodo 4 è in…	Quindi…
Lo stesso chassis del node3	Passare a. Fase 8.
Uno chassis separato dal node3	Passare a. Fase 6.

6. accendere l'alimentazione a node4, quindi interrompere l'avvio premendo Ctrl-C per accedere al prompt dell'ambiente di avvio.

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

```
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'
```

7. se viene visualizzato il messaggio di avviso nella fase 6, 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 sia terminato.

   Non ignorare il ritardo. Se la batteria non viene caricata, si potrebbe verificare una perdita di dati.

8. Al prompt della modalità di manutenzione, immettere il seguente comando:

   `halt`

   Il sistema si arresta al prompt dell'ambiente di avvio.

9. Configurare il nodo 4 per ONTAP:

   `set-defaults`

10. Se sono installate unità NetApp Storage Encryption (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`**

    Non è possibile combinare dischi FIPS con altri tipi di dischi sullo stesso nodo o coppia ha.

    È possibile combinare SED con dischi non crittografanti sullo stesso nodo o coppia ha.

b. Contattare il supporto NetApp per assistenza nel ripristino delle informazioni di gestione delle chiavi integrate.

11. Se la versione di ONTAP installata sul nodo 4 è la stessa o successiva alla versione di ONTAP 9 installata sul nodo 2, immettere il seguente comando:

```
boot_ontap menu
```

12. Eseguire una delle seguenti operazioni:

Se il sistema che si sta aggiornando…	**Quindi…**
Non dispone della versione ONTAP corretta o corrente sul nodo 4	Vai aFase 13 .
Ha la versione corretta o attuale di ONTAP al nodo 4	Vai aFase 18 .

13. Configurare la connessione netboot scegliendo una delle seguenti azioni.

> Come connessione di netboot, è necessario utilizzare la porta di gestione e l'indirizzo IP. Non utilizzare un indirizzo 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 immettendo 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 (Domain Name Service). Se si utilizza questo parametro opzionale, non è necessario un nome di dominio completo nell'URL del server netboot; è necessario solo il nome host del server. Potrebbero essere necessari altri parametri per l'interfaccia. Invio `help ifconfig` al prompt del firmware per ulteriori informazioni.

14. Eseguire il netboot al nodo 4:

Per…	Quindi…
Sistemi della serie FAS/AFF8000	`netboot http://<web_server_ip/path_to_webaccessible_directory> /netboot/kernel`
Tutti gli altri sistemi	`netboot http://<web_server_ip/path_to_webaccessible_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` poll "Fase 1" Nella sezione *Prepare for netboot*.

Non interrompere l'avvio.

15. Dal menu di avvio, selezionare `option (7) Install new software first`.

    Questa opzione di menu consente di scaricare e installare la nuova immagine Data 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 Data 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.

16. se viene richiesto di continuare la procedura, inserire y e, quando richiesto, inserire l'URL:

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

17. Completare i seguenti passaggi secondari:

    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.

18. Seleziona la modalità di manutenzione `5` dal menu di avvio e inserisci `y` quando ti viene chiesto di continuare con l'avvio.
19. Prima di continuare, vai a"Impostare la configurazione FC o UTA/UTA2 su node4" per apportare le modifiche necessarie alle porte FC o UTA/UTA2 sul nodo. Apportare le modifiche consigliate in quelle sezioni, riavviare il nodo e passare alla modalità di manutenzione.
20. Immettere il seguente comando ed esaminare l'output per trovare l'ID di sistema di node4:

    `disk show -a`

    Il sistema visualizza l'ID di sistema del nodo e le informazioni relative ai dischi, come mostrato nell'esempio seguente:

```
*> disk show -a
Local System ID: 536881109
DISK         OWNER                      POOL   SERIAL NUMBER   HOME
------------ -------------              -----  -------------
-------------
0b.02.23     nst-fas2520-2(536880939)    Pool0  KPG2RK6F        nst-
fas2520-2(536880939)
0b.02.13     nst-fas2520-2(536880939)    Pool0  KPG3DE4F        nst-
fas2520-2(536880939)
0b.01.13     nst-fas2520-2(536880939)    Pool0  PPG4KLAA        nst-
fas2520-2(536880939)
......
0a.00.0                   (536881109)    Pool0  YFKSX6JG
(536881109)
......
```

21. Riassegnare le parti di ricambio di node2, i dischi appartenenti alla root e gli aggregati non root che non sono stati ricollocati in node3 precedentemente nella sezione "Spostare gli aggregati non root dal nodo 2 al nodo 3":

    Se nel sistema sono presenti dischi condivisi, aggregati ibridi o entrambi, è necessario utilizzare il corretto `disk reassign` dalla seguente tabella.

Tipo di disco...	Eseguire il comando...
Con dischi condivisi	`disk reassign -s` *`node2_sysid`* `-d` *`node4_sysid`* `-p` *`node3_sysid`*
Senza condivisione	`disks disk reassign -s` *`node2_sysid`* `-d` *`node4_sysid`*

    Per `<node2_sysid>` utilizzare le informazioni acquisite in "Fase 10" Della sezione *Record node2*

information. Per `node4_sysid`, utilizzare le informazioni acquisite in Fase 23.

> Il `-p` l'opzione è richiesta solo in modalità di manutenzione quando sono presenti dischi condivisi.

Il `disk reassign` command riassegna solo i dischi per i quali *`node2_sysid`* è il proprietario corrente.

Il sistema visualizza il seguente messaggio:

```
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n
```

Invio `n` quando viene richiesto di interrompere la riassegnazione del disco.

Quando viene richiesto di interrompere la riassegnazione del disco, è necessario rispondere a una serie di richieste come indicato di seguito:

a. Il sistema visualizza il seguente messaggio:

```
After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
```

b. Invio `y` per continuare.

Il sistema visualizza il seguente messaggio:

```
Disk ownership will be updated on all disks previously belonging to
Filer with sysid <sysid>.
Do you want to continue (y/n)? y
```

a. Invio `y` per consentire l'aggiornamento della proprietà del disco.

22. Se si esegue l'aggiornamento da un sistema con dischi esterni a un sistema che supporta dischi interni ed esterni (ad esempio, sistemi A800), impostare node4 come root per confermare che si avvia dall'aggregato root di node2.

> **Attenzione: È necessario eseguire le seguenti procedure secondarie nell'ordine esatto indicato; in caso contrario, si potrebbe verificare un'interruzione o persino la perdita di dati.**

La seguente procedura imposta node4 per l'avvio dall'aggregato root di node2:

a. Controllare le informazioni su RAID, plex e checksum per l'aggregato node2:

```
aggr status -r
```

b. Controllare lo stato generale dell'aggregato node2:

```
aggr status
```

c. Se necessario, portare online l'aggregato node2:

```
aggr_online root_aggr_from_node2
```

d. Impedire al node4 di avviarsi dal proprio aggregato root originale:

```
aggr offline root_aggr_on_node4
```

e. Impostare l'aggregato root node2 come nuovo aggregato root per node4:

```
aggr options aggr_from_node2 root
```

23. Verificare che il controller e lo chassis siano configurati come `ha` immettendo il seguente comando e osservando l'output:

```
ha-config show
```

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

```
*> ha-config show
   Chassis HA configuration: ha
   Controller HA configuration: ha
```

I sistemi registrano in una PROM se si trovano 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.

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.
```

Se si dispone di una configurazione MetroCluster, utilizzare i seguenti comandi per correggere la configurazione:

```
ha-config modify controller mcc

ha-config modify chassis mcc.
```

24. Distruggere le caselle di posta sul node4:

```
mailbox destroy local
```

25. Uscire dalla modalità di manutenzione:

    `halt`

    Il sistema si arresta al prompt dell'ambiente di avvio.

26. Al nodo 3, controllare la data, l'ora e il fuso orario del sistema:

    `date`

27. Al nodo 4, controllare la data al prompt dell'ambiente di boot:

    `show date`

28. Se necessario, impostare la data sul node4:

    `set date` *`mm/dd/yyyy`*

29. Al nodo 4, controllare l'ora al prompt dell'ambiente di boot:

    `show time`

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

    `set time` *`hh:mm:ss`*

31. Verificare che l'ID del sistema partner sia impostato correttamente come indicato inFase 19 in opzione.

    `printenv partner-sysid`

32. Se necessario, impostare l'ID di sistema del partner su node4:

    `setenv partner-sysid` *`node3_sysid`*

    a. Salvare le impostazioni:

       `saveenv`

33. Al prompt dell'ambiente di boot, accedere al menu di boot:

    `boot_ontap menu`

34. Nel menu di avvio, selezionare l'opzione **(6) Aggiorna flash dalla configurazione di backup** immettendo `6` quando richiesto.

    Il sistema visualizza il seguente messaggio:

    ```
    This will replace all flash-based configuration with the last backup to
    disks. Are you sure you want to continue?:
    ```

35. Invio `y` quando richiesto.

L'avvio procede normalmente e il sistema richiede di confermare la mancata corrispondenza dell'ID di sistema.

> Il sistema potrebbe riavviarsi due volte prima di visualizzare l'avviso di mancata corrispondenza.

36. Confermare la mancata corrispondenza. Il nodo potrebbe completare un ciclo di riavvio prima di avviarsi normalmente.
37. Accedere a node4.

Impostare la configurazione FC o UTA/UTA2 su node4

Se node4 dispone di porte FC integrate, porte UTA/UTA2 (onboard Unified target adapter) o una scheda UTA/UTA2, è necessario configurare le impostazioni prima di completare il resto della procedura.

A proposito di questa attività

Potrebbe essere necessario completareConfigurare le porte FC sul nodo 4 OControllare e configurare le porte UTA/UTA2 sul nodo 4 o entrambe le sezioni.

Se node4 non dispone di porte FC integrate, porte UTA/UTA2 integrate o una scheda UTA/UTA2 e si sta eseguendo l'aggiornamento di un sistema con dischi di storage, è possibile passare a. "Mappare le porte dal nodo 2 al nodo 4".

Configurare le porte FC sul nodo 4

Se node4 dispone di porte FC, integrate o su un adattatore FC, è necessario impostare le configurazioni delle porte sul nodo prima di metterlo in servizio, perché le porte non sono preconfigurate. Se le porte non sono configurate, si potrebbe verificare un'interruzione del servizio.

Prima di iniziare

È necessario disporre dei valori delle impostazioni della porta FC del nodo 2 salvati nella sezione "Preparare i nodi per l'aggiornamento".

A proposito di questa attività

È possibile saltare questa sezione se il sistema non dispone di configurazioni FC. Se il sistema dispone di porte UTA/UTA2 integrate o di un adattatore UTA/UTA2, configurarle in Controllare e configurare le porte UTA/UTA2 sul nodo 4.

> Immettere i comandi in questa sezione al prompt del cluster.

Fasi

1. Visualizza informazioni su tutti gli adattatori di rete FC e convergenti sul sistema:

   ```
   system node hardware unified-connect show
   ```

2. Confrontare le impostazioni FC sui nuovi nodi con quelle acquisite in precedenza dal nodo originale.
3. Modificare le porte FC sul nodo 4 in base alle necessità:

   - Per programmare le porte di destinazione:

```
system node hardware unified-connect modify -type \| -t target -adapter port_name
```

- Per programmare le porte initiator:

```
system node unified-connect modify type \| -t initiator -adapter port_name
```

`-type` È il tipo, la destinazione o l'iniziatore FC4.

4. Verificare le nuove impostazioni immettendo il seguente comando ed esaminando l'output:

```
system node unified-connect show
```

5. Eseguire una delle seguenti operazioni:

Se le impostazioni FC predefinite sui nuovi nodi sono…	Quindi…
Le stesse di quelle acquisite sui nodi originali	Vai aFase 9 .
Diverso da quelli acquisiti sui nodi originali	Vai aStep6 .

6. Esci dalla modalità di manutenzione:

```
halt
```

7. Dopo aver immesso il comando, attendere che il sistema si arresti al prompt dell'ambiente di avvio.
8. Avviare node4 immettendo il seguente comando al prompt dell'ambiente di avvio:

```
boot_ontap
```

9. Esegui una delle seguenti azioni:
   - Passare a. Controllare e configurare le porte UTA/UTA2 sul nodo 4 Se node4 ha una scheda UTA/UTA2A o porte UTA/UTA2 integrate.
   - Saltare la sezione e passare a. "Mappare le porte dal nodo 2 al nodo 4" Se node4 non dispone di una scheda UTA/UTA2 o di porte UTA/UTA2 integrate.

Controllare e configurare le porte UTA/UTA2 sul nodo 4

Se node4 dispone di porte UTA/UTA2 integrate o di una scheda UTA/UTA2A, è necessario controllare la configurazione delle porte e configurarle, a seconda di come si desidera utilizzare il sistema aggiornato.

Prima di iniziare

È necessario disporre dei moduli SFP+ corretti per le porte UTA/UTA2.

A proposito di questa attività

Le porte UTA/UTA2 possono essere configurate in modalità FC nativa o UTA/UTA2A. La modalità FC supporta l'iniziatore FC e la destinazione FC; la modalità UTA/UTA2 consente al traffico simultaneo di NIC e FCoE di condividere la stessa interfaccia SFP+ 10 GbE e supporta la destinazione FC.

I materiali di marketing NetApp potrebbero utilizzare il termine UTA2 per fare riferimento agli adattatori e alle porte CNA. Tuttavia, la CLI utilizza il termine CNA.

Le porte UTA/UTA2 potrebbero essere su un adattatore o sul controller con le seguenti configurazioni:

- Le schede UTA/UTA2 ordinate contemporaneamente al controller vengono configurate prima della spedizione in modo da avere la personalità richiesta.
- Le schede UTA/UTA2 ordinate separatamente dal controller vengono fornite con il linguaggio di destinazione FC predefinito.
- Le porte UTA/UTA2 integrate sui nuovi controller sono configurate (prima della spedizione) in modo da avere la personalità richiesta.

Tuttavia, è possibile controllare la configurazione delle porte UTA/UTA2 sul nodo 4 e modificarla, se necessario.

Immettere i comandi in questa sezione al prompt del cluster, a meno che non venga richiesto di entrare in modalità Manutenzione. Se si dispone di un sistema MetroCluster FC, è necessario essere in modalità di manutenzione per configurare le porte UTA/UTA2.

Fasi

1. Controlla come sono attualmente configurate le porte sul nodo 4:

   `system node hardware unified-connect show`

2. Se il modulo SFP+ corrente non corrisponde all'utilizzo desiderato, sostituirlo con il modulo SFP+ corretto.

   Contattare il rappresentante NetApp per ottenere il modulo SFP+ corretto.

3. Esaminare l'output di `system node hardware unified-connect show` oppure `ucadmin show` Controllare e determinare se le porte UTA/UTA2 hanno la personalità desiderata.
4. Eseguire una delle seguenti operazioni:

Se la porta CNA…	Quindi…
Non avere la personalità che si desidera	Passare a. Fase 5.
Avere la personalità che si desidera	Saltare i passaggi da 5 a 12 e passare a. Fase 13.

5. Se il sistema dispone di dischi di archiviazione ed esegue Data ONTAP 8.3, avviare node4 ed entrare in modalità di manutenzione:

   `boot_ontap maint`

6. Verificare le impostazioni immettendo il seguente comando ed esaminandone l'output:

   `ucadmin show`

7. Eseguire una delle seguenti operazioni:

Se si sta configurando…	Quindi…
Porte su una scheda UTA/UTA2A	Vai aFase 8 .
Porte UTA/UTA2 integrate	Salta il passaggio 8 e vai aFase 9 .

8. Se l'adattatore è in modalità iniziatore e la porta UTA/UTA2 è online, metti offline la porta UTA/UTA2:

   `storage disable adapter` *`adapter_name`*

   Gli adattatori in modalità di destinazione sono automaticamente offline in modalità di manutenzione.

9. Se la configurazione corrente non corrisponde all'uso desiderato, immettere il seguente comando per modificare la configurazione in base alle esigenze:

   `ucadmin modify -m fc|cna -t initiator|target` *`adapter_name`*

   - `-m` È la modalità Personality: FC o 10GbE UTA.
   - `-t` È il tipo FC4: Destinazione o iniziatore.

   > È necessario utilizzare l'iniziatore FC per le unità nastro e la destinazione FC per i client SAN.

10. Se il sistema dispone di dischi di archiviazione, immettere il seguente comando:

    `halt`

    Il sistema si arresta al prompt dell'ambiente di avvio.

    a. Immettere il seguente comando:

       `boot_ontap`

11. Se il sistema dispone di dischi di archiviazione, immettere il seguente comando:

    `system node hardware unified-connect show`

    L'output degli esempi seguenti mostra che il tipo di adattatore FC4 "1b" sta cambiando in `initiator` e che la modalità degli adattatori "2a" e "2b" stia cambiando in `cna`.

```
cluster1::> system node hardware unified-connect show
               Current  Current    Pending  Pending    Admin
Node  Adapter  Mode     Type       Mode     Type       Status
----  -------  -------  ---------  -------  -------    -----
f-a    1a      fc       initiator  -        -          online
f-a    1b      fc       target     -        initiator  online
f-a    2a      fc       target     cna      -          online
f-a    2b      fc       target     cna      -          online
4 entries were displayed.
```

12. Inserire le porte di destinazione in linea immettendo uno dei seguenti comandi, una volta per ciascuna porta:

    `network fcp adapter modify -node node_name -adapter adapter_name -state up`

13. collegare la porta via cavo.

Mappare le porte dal nodo 2 al nodo 4

È necessario assicurarsi che le porte fisiche sul nodo 2 siano mappate correttamente alle porte fisiche sul nodo 4, in modo che il nodo 4 comunichi con gli altri nodi del cluster e con la rete dopo l'aggiornamento.

Prima di iniziare

È necessario disporre già di informazioni sulle porte dei nuovi nodi; per accedere a queste informazioni, fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe*. Le informazioni vengono utilizzate più avanti in questa sezione.

La configurazione software del nodo 4 deve corrispondere alla connettività fisica del nodo 4 e la connettività IP deve essere ripristinata prima di continuare con l'aggiornamento.

A proposito di questa attività

Le impostazioni delle porte possono variare a seconda del modello dei nodi. È necessario rendere la porta e la configurazione LIF del nodo originale compatibili con la configurazione del nuovo nodo. Questo perché il nuovo nodo riproduce la stessa configurazione all'avvio, il che significa che quando si avvia node4 Data ONTAP tenterà di ospitare le LIF sulle stesse porte utilizzate sul node2.

Pertanto, se le porte fisiche sul nodo 2 non vengono mappate direttamente alle porte fisiche sul nodo 4, saranno necessarie modifiche alla configurazione del software per ripristinare la connettività di cluster, gestione e rete dopo l'avvio. Inoltre, se le porte del cluster sul nodo 2 non vengono mappate direttamente alle porte del cluster sul nodo 4, il nodo 4 potrebbe non ricongiungersi automaticamente al quorum quando viene riavviato fino a quando non viene apportata una modifica alla configurazione software per ospitare le LIF del cluster sulle porte fisiche corrette.

Fasi

1. Annotare tutte le informazioni di cablaggio node2 per node2, le porte, i domini di trasmissione e gli spazi IPnella seguente tabella:

LIF	Node2 porte	Node2 IPspaces	Node2 domini di trasmissione	Node4 porte	Node4 IPspaces	Node4 domini di trasmissione
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Cluster 5						
Cluster 6						
Gestione dei nodi						

LIF	Node2 porte	Node2 IPspaces	Node2 domini di trasmissione	Node4 porte	Node4 IPspaces	Node4 domini di trasmissione
Gestione del cluster						
Dati 1						
Dati 2						
Dati 3						
Dati 4						
SAN						
Porta intercluster						

Consultare la sezione "informazioni sul nodo di registrazione 2" per la procedura da seguire per ottenere queste informazioni.

2. Registrare tutte le informazioni di cablaggio per il nodo 4, le porte, i domini di trasmissione e gli IPspaces, nella tabella precedente, utilizzando la stessa procedura descritta in "Registrare le informazioni del nodo 2" sezione per la procedura per ottenere queste informazioni.
3. Per verificare se il setup è un cluster senza switch a due nodi, procedere come segue:
   a. Impostare il livello di privilegio su Advanced (avanzato):
   b. Verificare se il setup è un cluster senza switch a due nodi:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

   Il valore di questo comando deve corrispondere allo stato fisico del sistema.

   c. Tornare al livello di privilegi di amministrazione:

```
cluster::*> set -privilege admin
cluster::>
```

4. Inserire il node4 nel quorum eseguendo i seguenti passaggi:
   a. Punto di avvio4. Vedere "Installazione e boot node4" per avviare il nodo, se non è già stato fatto.
   b. Verificare che le nuove porte del cluster si trovino nel dominio di trasmissione del cluster:

   `network port show -node *node* -port *port* -fields broadcast-domain`L'esempio seguente mostra che la porta "e0a" si trova nel dominio del cluster sul nodo 4:

```
cluster::> network port show -node node4 -port e0a -fields broadcast-
domain

node       port broadcast-domain
---------- ---- ----------------
node4      e1a  Cluster
```

c. Se le porte del cluster non si trovano nel dominio di broadcast del cluster, aggiungerle con il seguente comando:

```
broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports
node:port
```

d. Aggiungere le porte corrette al dominio di trasmissione del cluster:

```
network port modify -node -port -ipspace Cluster -mtu 9000
```

Questo esempio aggiunge la porta cluster "e1b" al nodo 4:

```
network port modify -node node4 -port e1b -ipspace Cluster -mtu 9000
```

> Per una configurazione MetroCluster, potrebbe non essere possibile modificare il dominio di trasmissione di una porta perché è associata a una porta che ospita la LIF di una SVM di destinazione di sincronizzazione e visualizzare errori simili, ma non limitati, a quanto segue:

```
command failed: This operation is not permitted on a Vserver that is
configured as the destination of a MetroCluster Vserver relationship.
```

Immettere il seguente comando dalla SVM di origine di sincronizzazione corrispondente sul sito remoto per riallocare la LIF di destinazione di sincronizzazione su una porta appropriata:

```
metrocluster vserver resync -vserver vserver_name
```

e. Migrare le LIF del cluster alle nuove porte, una volta per ogni LIF:

```
network interface migrate -vserver Cluster -lif lif_name -source-node node4
- destination-node node4 -destination-port port_name
```

f. Modificare la porta home delle LIF del cluster:

```
network interface modify -vserver Cluster -lif lif_name –home-port port_name
```

g. Rimuovere le vecchie porte dal dominio di trasmissione del cluster:

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

Questo comando rimuove la porta "e0d" sul nodo 4:
`network port broadcast-domain remove-ports -ipspace Cluster -broadcast-domain`

```
Cluster -ports node4:e0d
```

a. Verificare che node4 abbia raggiunto nuovamente il quorum:

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

5. regola i domini di broadcast che ospitano le LIF del cluster e le LIF di gestione dei nodi/cluster. Verificare che ciascun dominio di trasmissione contenga le porte corrette. Una porta non può essere spostata tra domini di broadcast se è in hosting o è la sede di una LIF, quindi potrebbe essere necessario migrare e modificare le LIF come indicato di seguito:

a. Visualizzare la porta home di una LIF:

```
network interface show -fields home-node,home-port
```

b. Visualizza il dominio di trasmissione contenente questa porta:

```
network port broadcast-domain show -ports node_name:port_name
```

c. Aggiungere o rimuovere le porte dai domini di broadcast:

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

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

a. Modificare la porta home di una LIF:

```
network interface modify -vserver vserver_name -lif lif_name –home-port
port_name
```

6. Regolare i domini di broadcast dell'intercluster e migrare le LIF dell'intercluster, se necessario, utilizzando gli stessi comandi illustrati nella Fase 5.
7. Regolare gli altri domini di broadcast e migrare i file LIF dei dati, se necessario, utilizzando gli stessi comandi illustrati nella Fase 5.
8. Se sul nodo 2 sono presenti porte che non esistono più sul nodo 4, attenersi alla seguente procedura per eliminarle:

a. Accedere al livello di privilegio avanzato su uno dei nodi:

```
set -privilege advanced
```

b. Per eliminare le porte:

```
network port delete -node node_name -port port_name
```

c. Tornare al livello di amministrazione:

```
set -privilege admin
```

9. Regolare tutti i gruppi di failover LIF:
`network interface modify -failover-group failover_group -failover-policy failover_policy`

Il seguente comando imposta il criterio di failover su `broadcast-domain-wide` e utilizza le porte nel

gruppo di failover `fg1` Come destinazioni di failover per LIF `data1` acceso `node4`:

```
network interface modify -vserver node4 -lif data1 failover-policy broadcast-
domain-wide -failover-group fg1
```

Per ulteriori informazioni, fare riferimento a. "Riferimenti" Per il collegamento a *Gestione di rete* o ai *comandi di ONTAP 9: Riferimento pagina manuale*, e andare a *Configurazione delle impostazioni di failover su un LIF*.

10. Verificare le modifiche al nodo 4:

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

11. Ogni LIF del cluster deve essere in ascolto sulla porta 7700. Verificare che le LIF del cluster siano in ascolto sulla porta 7700:

```
::> network connections listening show -vserver Cluster
```

La porta 7700 in ascolto sulle porte del cluster è il risultato previsto, come mostrato nell'esempio seguente per un cluster a due nodi:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

12. Per ogni cluster LIF che non è in ascolto sulla porta 7700, imposta lo stato amministrativo della LIF su `down` e poi `up`:

```
::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
int modify -vserver Cluster -lif cluster-lif -status-admin up
```

Ripetere il passaggio 11 per verificare che la LIF del cluster sia in ascolto sulla porta 7700.

Verificare l'installazione di node4

Dopo aver installato e avviato il nodo 4, è necessario verificare che sia installato correttamente, che faccia parte del cluster e che sia in grado di comunicare con il nodo 3.

Fasi

1. Al prompt del sistema, accedere a node4.
2. Verificare che node4 faccia parte dello stesso cluster di node3 e che sia integro:

```
cluster show
```

3. Verificare che node4 possa comunicare con node3 e che tutti i LIF siano in funzione:

```
network interface show -curr-node node4
```

4. Eseguire una delle seguenti operazioni:

Se il nodo 4 è…	Quindi…
In uno chassis separato dal node3	Collegare l'interconnessione ha tra i nodi completando la seguente procedura: a. Collegare la porta di interconnessione superiore del nodo 3 alla porta di interconnessione superiore del nodo 4. b. Collegare la porta di interconnessione inferiore del nodo 3 alla porta di interconnessione inferiore del nodo 4. c. Passare a. Fase 5.
Nello stesso chassis del node3	Passare a. Fase 5. Non è necessario collegare manualmente l'interconnessione ha tra i nodi; nelle configurazioni dello stesso chassis, l'interconnessione ha viene connessa automaticamente attraverso la scheda madre.

5. [[fase 5]]eseguire una delle seguenti operazioni:

Se il cluster è…	Quindi…
In un ambiente SAN	Completo Fase 6 e andare alla sezione "Spostare le LIF dei dati NAS di proprietà di node2 da node3 a node4 e verificare le LIF SAN sul node4".
Non in un ambiente SAN	Saltare il passaggio 6 andare alla sezione "Spostare le LIF dei dati NAS di proprietà di node2 da node3 a node4 e verificare le LIF SAN sul node4".

6. verificare che sia node3 che node4 siano in quorum immettendo il seguente comando su uno dei nodi:

```
event log show -messagename scsiblade.*
```

L'esempio seguente mostra l'output quando i nodi nel cluster sono in quorum:

```
cluster::> event log show -messagename scsiblade.*
Time                Node   Severity      Event
------------------- ------ ------------- -------------------------
8/13/2012 14:03:51  node1  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
8/13/2012 14:03:51  node2  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
8/13/2012 14:03:48  node3  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
8/13/2012 14:03:43  node4  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
```

Spostare le LIF dei dati NAS di proprietà di node2 da node3 a node4 e verificare le LIF SAN sul node4

Dopo aver verificato l'installazione di node4 e prima di spostare gli aggregati node2 da node3 a node4, è necessario spostare i dati NAS LIF di proprietà di node2 attualmente su node3 da node3 a node4. È inoltre necessario verificare le LIF SAN sul nodo 4.

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. Verifica che i file LIF siano integri e posizionati sulle porte appropriate dopo aver portato il node4 online.

Fasi

1. Elencare tutte le LIF dei dati NAS che non sono di proprietà di node3 immettendo il seguente comando su entrambi i nodi e acquisendo l'output:

   ```
   network interface show -role data -curr-node node3 -is-home false
   ```

2. se il cluster è configurato per le LIF SAN, registrare le LIF SAN e le informazioni di configurazione esistenti "foglio di lavoro" da utilizzare in seguito nella procedura.

   a. Elencare le LIF SAN sul node3 ed esaminare l'output:

      ```
      network interface show -data-protocol fc*
      ```

      Il sistema restituisce un output simile al seguente esempio:

```
cluster1::> net int show -data-protocol fc*
  (network interface show)
            Logical     Status     Network            Current
Current Is
Vserver     Interface   Admin/Oper Address/Mask       Node
Port    Home
----------  ----------  ---------- ------------------ -------------
------- ----
svm2_cluster1
            lif_svm2_cluster1_340
                        up/up      20:02:00:50:56:b0:39:99
                                                      cluster1-01
1b      true
            lif_svm2_cluster1_398
                        up/up      20:03:00:50:56:b0:39:99
                                                      cluster1-02
1a      true
            lif_svm2_cluster1_691
                        up/up      20:01:00:50:56:b0:39:99
                                                      cluster1-01
1a      true
            lif_svm2_cluster1_925
                        up/up      20:04:00:50:56:b0:39:99
                                                      cluster1-02
1b      true
4 entries were displayed.
```

b. Elencare le configurazioni esistenti ed esaminare l'output:

   `fcp adapter show -fields switch-port,fc-wwpn`

   Il sistema restituisce un output simile al seguente esempio:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  -----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

3. Eseguire una delle seguenti operazioni:

In caso di node2...	Descrizione
Ha configurato gruppi di interfacce o VLAN	Passare a. Fase 4.
Non sono stati configurati gruppi di interfacce o VLAN	Saltare la fase 4 e passare a. Fase 5.

4. eseguire i seguenti passaggi per migrare qualsiasi file LIF dati NAS ospitati su gruppi di interfacce e VLAN che erano originariamente sul nodo 2 dal nodo 3 al nodo 4.

   a. Migrare le LIF ospitate su node3 che in precedenza appartenevano a node2 su un gruppo di interfacce a una porta su node4 in grado di ospitare LIF sulla stessa rete immettendo il seguente comando, una volta per ciascuna LIF:

      ```
      network interface migrate -vserver vserver_name -lif lif_name -destination
      -node node4 -destination-port netport|ifgrp
      ```

   b. Modificare la porta home e il nodo home dei file LIF in Sotto-fase A. Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

      ```
      network interface modify -vserver vserver_name -lif datalif_name -home-node
      node4 home-port netport|ifgrp
      ```

   c. Migrate le LIF ospitate su node3 che in precedenza appartenevano a node2 su una porta VLAN a una porta su node4 in grado di ospitare LIF sulla stessa rete immettendo il seguente comando, una

volta per ciascuna LIF:

```
network interface migrate -vserver vserver_name -lif datalif_name
-destination-node node4 -destination-port netport|ifgrp
```

d. Modificare la porta home e il nodo home dei file LIF in Sotto-fase c Alla porta e al nodo che attualmente ospitano le LIF immettendo il seguente comando, una volta per ciascuna LIF:

```
network interface modify -vserver vserver_name -lif datalif_name -home-node
node4 home-port netport|ifgrp
```

5. eseguire una delle seguenti operazioni:

Se il cluster è configurato per…	Quindi…
NAS	Completo Fase 6 attraverso Fase 9, Saltare il passaggio 10 e completare Fase 11 attraverso Fase 14.
SAN	Saltare i passaggi da 6 a 9 e completare Fase 10 attraverso Fase 14.
NAS e SAN	Completo Fase 6 attraverso Fase 14.

6. se si dispone di porte dati non uguali sulle piattaforme, immettere il seguente comando per aggiungere le porte al dominio di trasmissione:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt ports node:port
```

Nell'esempio seguente viene aggiunta la porta "e0a" sul nodo "6280-1" e la porta "e0i" sul nodo "8060-1" per trasmettere la gestione del dominio in IPSpace Default:

```
cluster::> network port broadcast-domain add-ports -ipspace Default
-broadcast-domain mgmt -ports 6280-1:e0a, 8060-1:e0i
```

7. Migrare ciascun LIF dati NAS in node4 immettendo il seguente comando, una volta per ogni LIF:

```
network interface migrate -vserver vserver-name -lif datalif-name -destination
-node node4 -destination-port netport|ifgrp -home-node node4
```

8. Assicurarsi che la migrazione dei dati sia persistente:

```
network interface modify -vserver vserver_name -lif datalif_name -home-port
netport|ifgrp
```

9. verifica lo stato di tutti i collegamenti come `up` immettendo il seguente comando per elencare tutte le porte di rete ed esaminarne l'output:

```
network port show
```

L'esempio seguente mostra l'output di `network port show` Comando con alcune LIF in alto e altre in basso:

```
cluster::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- -----------
node3
       a0a       Default      -                up       1500  auto/1000
       e0M       Default      172.17.178.19/24 up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0a-1     Default      172.17.178.19/24 up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
node4
       e0M       Default      172.17.178.19/24 up       1500  auto/100
       e0a       Default      172.17.178.19/24 up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
12 entries were displayed.
```

10. se l'output di `network port show` il comando visualizza le porte di rete che non sono disponibili nel nuovo nodo e che sono presenti nei nodi precedenti, eliminare le porte di rete precedenti completando le seguenti operazioni secondarie:

    a. Immettere il livello di privilegio avanzato immettendo il seguente comando:

       `set -privilege advanced`

    b. Immettere il seguente comando, una volta per ogni vecchia porta di rete:

       `network port delete -node` *`node_name`* `-port` *`port_name`*

    c. Tornare al livello admin immettendo il seguente comando:

       `set -privilege admin`

11. verificare che le LIF SAN si trovino sulle porte corrette sul node4 completando i seguenti passaggi secondari:

    a. Immettere il seguente comando ed esaminarne l'output:

       `network interface show -data-protocol iscsi|fcp -home-node node4`

       Il sistema restituisce un output simile al seguente esempio:

```
cluster::> network interface show -data-protocol iscsi|fcp -home-node
node4
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            a0a          up/down  10.63.0.53/24      node4
a0a     true
            data1        up/up    10.63.0.50/18      node4
e0c     true
            rads1        up/up    10.63.0.51/18      node4
e1a     true
            rads2        up/down  10.63.0.52/24      node4
e1b     true
vs1
            lif1         up/up    172.17.176.120/24  node4
e0c     true
            lif2         up/up    172.17.176.121/24  node4
```

b. Verificare che il nuovo `adapter` e. `switch-port` le configurazioni sono corrette confrontando l'output di `fcp adapter show` con le nuove informazioni di configurazione registrate nel foglio di lavoro in Fase 2.

   Elencare le nuove configurazioni LIF SAN al nodo 4:

   `fcp adapter show -fields switch-port,fc-wwpn`

   Il sistema restituisce un output simile al seguente esempio:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  -----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

Se un LIF SAN nella nuova configurazione non si trova su un adattatore ancora collegato allo stesso `switch-port`, potrebbe causare un'interruzione del sistema quando si riavvia il nodo.

c. Se node4 ha LIF SAN o gruppi DI LIF SAN che si trovano su una porta che non esisteva sul node2, spostarli su una porta appropriata sul node4 immettendo uno dei seguenti comandi:

   i. Impostare lo stato LIF su DOWN (giù):

      `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-status -admin down`

   ii. Rimuovere la LIF dal set di porte:

      `portset remove -vserver` *`vserver_name`* `-portset` *`portset_name`* `-port-name` *`port_name`*

   iii. Immettere uno dei seguenti comandi:

      - Spostare una singola LIF:

        `network interface modify -lif` *`lif_name`* `-home-port` *`new_home_port`*

      - Spostare tutte le LIF su una singola porta inesistente o errata su una nuova porta:

        `network interface modify {-home-port` *`port_on_node2`* `-home-node` *`node2`* `-role data} -home-port` *`new_home_port_on_node4`*

- Aggiungere nuovamente i file LIF al set di porte:

  `portset add -vserver vserver_name -portset portset_name -port-name port_name`

> È necessario spostare I file LIF SAN su una porta con la stessa velocità di collegamento della porta originale.

12. Modificare lo stato di tutti i LIF in `up` In questo modo, i LIF possono accettare e inviare traffico sul nodo immettendo il seguente comando:

    `network interface modify -vserver vserver_name -home-port port_name -home-node node4 lif lif_name -status-admin up`

13. Verificare che le LIF SAN siano state spostate nelle porte corrette e che le LIF abbiano lo stato di `up` immettendo il seguente comando su uno dei nodi ed esaminando l'output:

    `network interface show -home-node node4 -role data`

14. 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 -status-admin up`

Foglio di lavoro: Informazioni da registrare prima di spostare i file LIF dei dati NAS in node4

Per verificare di disporre della configurazione corretta dopo aver spostato LE LIF SAN da node3 a node4, è possibile utilizzare il seguente foglio di lavoro per registrare `adapter` e. `switch-port` Informazioni per ciascun LIF.

Registrare la LIF `adapter` informazioni da `network interface show -data-protocol fc*` output del comando e il `switch-port` informazioni da `fcp adapter show -fields switch-port,fc-wwpn` output del comando per node3.

Dopo aver completato la migrazione al nodo 4, registrare il LIF `adapter` e. `switch-port` Informazioni per i LIF sul node4 e verificare che ciascun LIF sia ancora connesso allo stesso `switch-port`.

Node3			**Node4**		
LIF	`adapter`	`switch-port`	LIF	`adapter`	`switch-port`

Spostare gli aggregati non root node2 da node3 a node4

Dopo aver trasferito gli aggregati non root di node2 in node3, è necessario trasferirli da node3 a node4.

Fasi

1. immettere il seguente comando su uno dei controller ed esaminare l'output per identificare gli aggregati non root da spostare:

   `storage aggregate show -owner-name` *`node3`* `-home-id` *`node2_system_id`*

2. Spostare gli aggregati completando le seguenti fasi secondarie:

   a. Accedere al livello di privilegio avanzato immettendo il seguente comando su uno dei nodi:

      `set -privilege advanced`

   b. Immettere il seguente comando:

      `storage aggregate relocation start -node` *`node3`* `-destination` *`node4`* `-aggregate -list` *`aggr_name1, aggr_name2…`* `-ndo-controller-upgrade true`

   L'elenco aggregato è l'elenco degli aggregati di proprietà del node4 ottenuti in Fase 1.

   a. Quando richiesto, immettere `y`.

      Il trasferimento avviene in background. La riposizionamento di un aggregato potrebbe richiedere da pochi secondi a un paio di minuti. Il tempo include sia le parti di fuori servizio del client che quelle di non fuori servizio. Il comando non ricolloca nessun aggregato offline o limitato.

   b. Tornare al livello di amministrazione:

      `set -privilege admin`

3. controllare lo stato del trasferimento:

   `storage aggregate relocation show -node` *`node3`*

   Viene visualizzato l'output `Done` per un aggregato dopo che è stato trasferito.

   Attendere che tutti gli aggregati node2 siano stati riposizionati al node4 prima di passare alla fase successiva.

4. Eseguire una delle seguenti operazioni:

In caso di trasferimento di…	Quindi…
Tutti gli aggregati hanno avuto successo	Passare a. Fase 5.

In caso di trasferimento di…	Quindi…

Qualsiasi aggregato ha avuto esito negativo o è stato vetoato	a. Controllare i registri EMS per l'azione correttiva.
	b. Eseguire l'azione correttiva.
	c. Accedere al livello di privilegio avanzato immettendo il seguente comando su uno dei nodi:
	`set -privilege advanced`
	d. Spostare eventuali aggregati guasti o vetoed:
	`storage aggregate relocation start -node node3 destination node4 -aggregate-list aggr_name1, aggr_name2… ndo-controller-upgrade true`
	L'elenco aggregato è l'elenco degli aggregati non riusciti o vetoati.
	e. Quando richiesto, immettere `y`.
	f. Tornare al livello admin immettendo il seguente comando:
	`set -privilege admin`
	Se necessario, è possibile forzare il trasferimento utilizzando uno dei seguenti metodi:
	• Ignorare i controlli di veto:
	`storage aggregate relocation start -override -vetoes -ndo-controller-upgrade`
	• Esclusione dei controlli di destinazione:
	`storage aggregate relocation start -override -destination-checks -ndocontroller-upgrade`
	Per ulteriori informazioni sui comandi di trasferimento degli aggregati di storage, fare riferimento a. "Riferimenti" Per collegarsi alla gestione di *dischi e aggregati con i comandi CLI* e *ONTAP 9: Manuale riferimento pagina*.

5. verificare che tutti gli aggregati non root node2 siano online e che il loro stato sia su node4:

   `storage aggregate show -node node4 -state offline -root false`

   Gli aggregati node2 sono stati elencati nell'output del comando in Fase 1.

6. Se un aggregato è diventato offline o straniero, portarlo online utilizzando il seguente comando per ogni aggregato:

   `storage aggregate online -aggregate aggr_name`

7. Verificare che tutti i volumi negli aggregati node2 siano online sul node4:

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

8. Se alcuni volumi sono offline al nodo4, portarli online:

   ```
   volume online -vserver vserver-name -volume volume_name
   ```

9. Invia un messaggio AutoSupport post-upgrade a NetApp per il node4:

   ```
   system node autosupport invoke -node node4 -type all -message "node2
   successfully upgraded from platform_old to platform_new"
   ```

Fase 6. Completare l'aggiornamento

Gestire l'autenticazione utilizzando i server KMIP

Con ONTAP 9.5 e versioni successive, è possibile utilizzare i server KMIP (Key Management Interoperability Protocol) per gestire le chiavi di autenticazione.

Fasi

1. Aggiungere un nuovo controller:

   ```
   security key-manager setup -node new_controller_name
   ```

2. Aggiungere il gestore delle chiavi:

   ```
   security key-manager -add 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 show -status
   ```

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

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

Verificare che i nuovi controller siano impostati correttamente

Per confermare la corretta configurazione, attivare la coppia ha. Inoltre, è possibile verificare che node3 e node4 possano accedere reciprocamente allo storage e che nessuno dei due possieda le LIF dei dati appartenenti ad altri nodi del cluster. Inoltre, confermi 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. Abilitare il failover dello storage immettendo il seguente comando su uno dei nodi:

   ```
   storage failover modify -enabled true -node <node3>
   ```

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. Eseguire una delle seguenti operazioni:

Se il cluster è un…	Descrizione
Cluster a due nodi	Abilitare la disponibilità elevata del cluster immettendo il seguente comando su uno dei nodi: `cluster ha modify -configured true`
Cluster con più di due nodi	Passare a. Fase 4.

4. verificare che node3 e node4 appartengano allo stesso cluster immettendo il seguente comando ed esaminando l'output:

   `cluster show`

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

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

6. Verificare che né node3 né node4 detengano le LIF dei dati di proprietà di altri nodi del cluster immettendo il seguente comando ed esaminando l'output:

   `network interface show`

   Se il nodo 3 o il nodo 4 possiede le LIF dei dati di proprietà di altri nodi del cluster, utilizzare il `network interface revert` Comando per ripristinare le LIF dei dati al proprietario di casa.

7. 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>
   ```

8. Determinare se i volumi sono offline:

   ```
   volume show -node <node3> -state offline
   volume show -node <node4> -state offline
   ```

9. Se alcuni volumi non sono in linea, confrontarli con l'elenco dei volumi non in linea in cui sono stati acquisiti "Fase 19 (d)" In *preparare i nodi per l'aggiornamento* e portare online qualsiasi volume offline, come richiesto, immettendo il seguente comando, una volta per ogni volume:

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

10. Installare nuove licenze per i nuovi nodi immettendo 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, ciascuna chiave di licenza separata da una virgola.

11. se nella configurazione vengono utilizzati dischi con crittografia automatica ed è stato impostato `kmip.init.maxwait` variabile a. `off` (ad esempio, in "Fase 16" Of *Install and boot node3*), devi disimpostare la variabile:

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

12. Per rimuovere tutte le vecchie licenze dai nodi originali, immettere uno dei seguenti comandi:

    ```
    system license clean-up -unused -expired
    system license delete -serial-number <node_serial_number> -package
    <licensable_package>
    ```

    - Per eliminare tutte le licenze scadute, immettere:

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

    - Per eliminare tutte le licenze inutilizzate, immettere:

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

    - Per eliminare una licenza specifica da un cluster, immettere 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.

13. Verificare che le licenze siano installate correttamente immettendo il seguente comando ed esaminandone l'output:

```
system license show
```

Puoi confrontare l'output con l'output che hai catturato in"Fase 29" di *Preparare i nodi per l'aggiornamento*.

14. Configurare gli SP eseguendo il seguente comando su entrambi i nodi:

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

Passare a. "Riferimenti" Per informazioni dettagliate su, fare riferimento alla sezione *Guida all'amministrazione del sistema* e ai *comandi di ONTAP 9: Guida di riferimento alla pagina* `system service- processor network modify` comando.

15. Se si desidera configurare un cluster senza switch sui nuovi nodi, visitare il sito Web all'indirizzo "Riferimenti" Per collegarsi al *sito di supporto di rete* 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 procedura descritta in "Impostare Storage Encryption sul nuovo modulo controller". In caso contrario, completare la procedura descritta in "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 show -status

security key-manager query
```

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 -add 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 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 setup -node new_controller_name`

   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 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.

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:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 o 9.7	`security key-manager key query -node node`
ONTAP 9.5 o versioni precedenti	`security key-manager key show`

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 utilizzando il seguente comando:

      `security key-manager -add 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 utilizzando il seguente comando:

      `security key-manager 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 utilizzando il seguente comando:

```
security key-manager setup -node new_controller_name
```

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.

◦ Ripristinare l'autenticazione per il gestore delle chiavi esterno:

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

Questo comando richiede la passphrase di Onboard Key Manager (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".

◦ Ripristinare l'autenticazione per OKM:

Per questa versione di ONTAP…	Utilizzare questo comando…
Tutte le altre versioni di ONTAP	`security key-manager onboard sync`
ONTAP 9.5	`security key-manager setup -node node_name`

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 di gestione delle chiavi esterne. Riportare online quei volumi 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

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: 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 deve 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. Confronta l'output di Fase 1 con l'output acquisito per node1 nella sezione "Preparare i nodi per l'aggiornamento" e annotare eventuali aggregati che non sono stati correttamente ricollocati.
3. ricollocare gli aggregati rimasti al nodo4:

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

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

4. Immettere il seguente comando per 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.

Riavvio, panic o cicli di alimentazione durante la fase 2

Gli arresti anomali possono verificarsi prima, durante o subito dopo la fase 2, durante la quale si spostano gli aggregati da node1 a node2, si spostano le LIF dei dati e LE LIF SAN di proprietà di node1 in node2, si registrano le informazioni node1 e si ritirano node1.

Node1 o node2 si blocca prima della fase 2 con ha ancora attivato

Se node1 o node2 si bloccano prima della fase 2, nessun aggregato è stato ancora trasferito e la configurazione ha è ancora attivata.

A proposito di questa attività

Il takeover e il giveback possono procedere normalmente.

Fasi

1. Verificare la presenza di messaggi EMS emessi dal sistema nella console ed eseguire l'azione correttiva consigliata.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node1 si blocca durante o subito dopo la fase 2 con ha ancora attivato

Alcuni o tutti gli aggregati sono stati riallocati da node1 a node2 e ha è ancora abilitato. Node2 prenderà il controllo del volume root di 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 restituirà tutti gli aggregati non root node1.

Fasi

1. Completare"Fase 1" nella sezione *Spostare gli aggregati non radice dal nodo 1 al nodo 2* di nuovo.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node1 si blocca dopo la fase 2 mentre ha è disattivato

Node2 non prenderà 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.

   È possibile che vengano visualizzate alcune modifiche nell'output di `storage failover show` comando, ma questo è tipico e non influisce sulla procedura. Consultare la sezione relativa alla risoluzione dei problemi "Il failover dello storage non previsto mostra l'output del comando".

Node2 non funziona durante o dopo la fase 2 con ha ancora attivato

Node1 ha trasferito alcuni o tutti i suoi aggregati al node2. HA è attivato.

A proposito di questa attività

Node1 prenderà il controllo di tutti gli aggregati del node2 e di tutti i suoi aggregati che aveva trasferito al

node2. Quando noda2 entra in `Waiting for Giveback` state, node1 restituisce tutti gli aggregati del node2.

Fasi

1. Completare"Fase 1" nella sezione *Spostare gli aggregati non radice dal nodo 1 al nodo 2* di nuovo.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node2 si blocca dopo la fase 2 e dopo la disattivazione di ha

Node1 non prenderà il posto.

Fasi

1. Alzati il node2.

   Durante l'avvio di node2 si verifica un'interruzione del client per tutti gli aggregati.

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

Riavvio, panic o cicli di alimentazione durante la fase 3

Gli errori possono verificarsi durante o subito dopo la fase 3, durante la quale si installa e si avvia node3, si mappano le porte da node1 a node3, si spostano le LIF dei dati e LE LIF SAN appartenenti a node1 e node2 in node3 e si spostano tutti gli aggregati da node2 a node3.

Node2 si blocca durante la fase 3 con ha disattivato e prima di spostare qualsiasi aggregato

Node3 non si prenderà il controllo in seguito a un crash node2, in quanto ha è già disattivato.

Fasi

1. Alzati il node2.

   Durante l'avvio di node2 si verifica un'interruzione del client per tutti gli aggregati.

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

Node2 si blocca durante la fase 3 dopo aver riallocato alcuni o tutti gli aggregati

Node2 ha trasferito alcuni o tutti i suoi aggregati al node3, che servirà i dati degli aggregati che sono stati ricollocati. HA disattivato.

A proposito di questa attività

Si verificherà un'interruzione del client per gli aggregati che non sono stati ricollocati.

Fasi

1. Alzati il node2.
2. Riposizionare gli aggregati rimanenti completando"Fase 1" Attraverso"Fase 5" nella sezione *Spostare gli aggregati non radice dal nodo 2 al nodo 3*.
3. Continuare con la procedura di aggiornamento della coppia di nodi.

Node3 si blocca durante la fase 3 e prima che node2 abbia riallocato gli aggregati

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.

Node3 si blocca durante la fase 3 durante il trasferimento dell'aggregato

Se il nodo 3 si blocca mentre il nodo 2 sta spostando gli aggregati al nodo 3, il nodo 2 interrompe il trasferimento degli aggregati rimanenti.

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. Completare"Fase 5" di nuovo nella sezione *Spostare gli aggregati non radice dal nodo 2 al nodo 3*.
3. Continuare con la procedura di aggiornamento della coppia di nodi.

Node3 non riesce ad avviarsi dopo il blocco nella fase 3

A causa di un guasto catastrofico, il node3 non può essere avviato in seguito a un crash durante la fase 3.

Fase

1. Contattare il supporto tecnico.

Node2 si blocca dopo la fase 3 ma prima della fase 5

Node3 continua a fornire dati per tutti gli aggregati. La coppia ha è disattivata.

Fasi

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

Node3 si blocca dopo la fase 3 ma prima della fase 5

Node3 si blocca dopo la fase 3 ma prima della fase 5. La coppia ha è disattivata.

Fasi

1. Alzati il node3.

   Si verificherà un'interruzione del servizio client per tutti gli aggregati.

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

Riavvio, panic o cicli di alimentazione durante la fase 5

I crash possono verificarsi durante la fase 5, in cui si installa e si avvia node4, si mappano le porte da node2 a node4, si spostano le LIF dei dati e LE LIF SAN appartenenti a node2 da node3 a node4 e si spostano tutti gli aggregati di node2 da node3 a node4.

Node3 si blocca durante la fase 5

Node3 ha trasferito alcuni o tutti gli aggregati del node2 al node4. Node4 non prende il controllo, ma continua a servire aggregati non root che node3 ha già trasferito. La coppia ha è disattivata.

A proposito di questa attività

Si verifica un'interruzione per il resto degli aggregati fino a quando il node3 non viene riavviato.

Fasi

1. Alzati il node3.
2. Riallocare gli aggregati rimanenti che appartenevano al node2 ripetendo "Fase 1" attraverso "Fase 3" Nella sezione *spostare gli aggregati non root di node2 da node3 a node4*.
3. Continuare con la procedura di aggiornamento della coppia di nodi.

Node4 si blocca durante la fase 5

Node3 ha trasferito alcuni o tutti gli aggregati del node2 al node4. Node3 non prende il controllo, ma continua a servire aggregati non root che node3 possiede e quelli che non sono stati ricollocati. HA disattivato.

A proposito di questa attività

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

Fasi

1. Far salire il node4.
2. Riposizionare gli aggregati rimanenti che appartenevano al nodo 2 completando nuovamente"Fase 1" Attraverso"Fase 3" in *Sposta gli aggregati non radice del nodo2 dal nodo3 al nodo4*.
3. 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 "inattivo".

Le LIF si trovano su porte non valide dopo l'aggiornamento

Una volta completato l'aggiornamento, se si dispone di una configurazione MetroCluster, è possibile che le interfacce logiche FC (LIF) vengano lasciate su porte non corrette. È possibile eseguire un'operazione di risincronizzazione per riassegnare i LIF alle porte corrette.

Fase

1. Inserire il `metrocluster vserver resync` Comando per riallocare le LIF alle porte corrette.

```
metrocluster vserver resync -vserver vserver_name fcp-mc.headupgrade.test.vs
```

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

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.
"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.
"Gestione delle coppie HA"	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.
"Gestione MetroCluster e disaster recovery"	Descrive come eseguire le operazioni di switchover e switchback MetroCluster, sia nelle operazioni di manutenzione pianificate che in caso di disastro.
"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 9.0: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.0 supportati.

Contenuto	Descrizione
"Comandi di ONTAP 9.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.1 supportati.
"Comandi di ONTAP 9.2: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.2 supportati.
"Comandi di ONTAP 9.3: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.3 supportati.
"Comandi di ONTAP 9.4: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.4 supportati.
"Comandi di ONTAP 9.5: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.5 supportati.
"Comandi di ONTAP 9.6: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.6 supportati.
"Comandi di ONTAP 9.7: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.7 supportati.
"Comandi di ONTAP 9.8: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.8 supportati.
"Comandi di ONTAP 9.9.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.9.1 supportati.
"Comandi di ONTAP 9.10.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.10.1 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 "sostituzione controller di sistema" per aggiornare l'hardware del controller introdotto in ONTAP 9.15.1 e versioni successive"	Descrive le procedure di trasferimento degli aggregati necessarie per aggiornare senza interruzioni i controller introdotti in ONTAP 9.15.1 e versioni successive utilizzando i comandi "system controller replace".
"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.
"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".

Contenuto	Descrizione
"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.
"Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller che esegue ONTAP 9.5 a ONTAP 9.7"	Vengono descritte le procedure di riposizionamento degli aggregati necessarie per aggiornare senza interruzioni i controller che eseguono ONTAP 9.5 a ONTAP 9.7 utilizzando i comandi "system controller replace".
"Utilizzare il trasferimento di aggregati per aggiornare manualmente l'hardware del controller con ONTAP 9.7 o versione precedente"	Descrive le procedure di trasferimento degli aggregati necessarie per eseguire aggiornamenti manuali dei controller senza interruzioni con ONTAP 9.7 o versione precedente.

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

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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