



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

Upgrade controllers

NetApp  
February 22, 2024

# Sommario

Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller con ONTAP 9.8 o versione successiva . . . . .	1
Panoramica . . . . .	1
Automatizzare il processo di aggiornamento del controller . . . . .	2
Decidere se utilizzare la procedura di trasferimento degli aggregati . . . . .	2
Strumenti e documentazione richiesti . . . . .	4
Linee guida per l'aggiornamento dei controller con ARL . . . . .	4
Verificare lo stato della configurazione MetroCluster . . . . .	6
Verificare la presenza di errori di configurazione MetroCluster . . . . .	7
Verificare lo switchover, la riparazione e lo switchback . . . . .	7
Panoramica dell'aggiornamento ARL . . . . .	7
Fase 1. Preparatevi per l'aggiornamento . . . . .	9
Fase 2. Spostare e dismettere il node1 . . . . .	15
Fase 3. Installazione e boot node3 . . . . .	19
Fase 4. Spostare e dismettere il node2 . . . . .	48
Fase 5. Installazione e boot node4 . . . . .	50
Fase 6. Completare l'aggiornamento . . . . .	80
Risolvere i problemi . . . . .	86
Riferimenti . . . . .	93

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

## Panoramica

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

Metodo	Versione di ONTAP	Sistemi supportati
Utilizzo di <code>system controller replace</code> comandi	9.8 o versione successiva	<a href="#">"Link alla matrice dei sistemi supportati"</a>

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.

In queste informazioni, il termine "sistemi con software di virtualizzazione FlexArray" si riferisce ai sistemi che appartengono a queste nuove piattaforme. Il termine "sistema V-Series" si riferisce ai sistemi hardware separati che possono essere collegati agli array di storage.

### Informazioni importanti:

- Questa procedura è complessa e presuppone che si disponga di competenze di amministrazione avanzate di ONTAP. È inoltre necessario leggere e comprendere ["Linee guida per l'aggiornamento dei controller con ARL"](#) e a. ["Panoramica dell'aggiornamento ARL"](#) prima di iniziare l'aggiornamento.
- Questa procedura presuppone che l'hardware del controller sostitutivo sia nuovo e non sia stato utilizzato. I passaggi necessari per preparare i controller usati con `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, V-Series, AFF e ai sistemi con software di virtualizzazione FlexArray. I sistemi FAS rilasciati dopo ONTAP 9.5 possono essere collegati agli array di storage se viene installata la licenza richiesta. Per ulteriori informazioni sui modelli di storage array e V-Series, fare riferimento a. "[Riferimenti](#)" Per collegarsi a *Hardware Universe* e accedere alla matrice di supporto V-Series.
- 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 la procedura di trasferimento degli aggregati

Questo contenuto descrive come aggiornare i controller di storage in una coppia ha con nuovi controller mantenendo i dati e i dischi esistenti. Si tratta di una procedura complessa che deve essere utilizzata solo da amministratori esperti.

È possibile utilizzare questo contenuto nei seguenti casi:

- Si utilizza ONTAP 9.8 o versione successiva.
- Non si desidera 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.

- Se si sta aggiornando una configurazione MetroCluster, si tratta di una configurazione FC a quattro nodi o superiore e tutti i nodi eseguono ONTAP 9.8 o versione successiva.

Per l'aggiornamento delle configurazioni MetroCluster IP, fare riferimento a ["Riferimenti"](#) Per collegarsi al contenuto *aggiornamento ed espansione MetroCluster*.



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

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

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



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

<sup>1</sup>per ulteriori passaggi necessari per i sistemi AFF A800, passare alla fase che fa riferimento a A800 nella sezione ["Controllare e configurare le porte UTA/UTA2 sul nodo 3, passaggio 23"](#), o ["Controllare e configurare le porte UTA/UTA2 sul nodo 4, passaggio 23"](#).

<sup>2</sup>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.

<sup>3</sup>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.

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
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.

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

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

## Strumenti e documentazione richiesti

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

Per eseguire l'aggiornamento sono necessari i seguenti strumenti:

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

Accedere alla ["Riferimenti"](#) per accedere all'elenco dei documenti di riferimento e dei siti di riferimento necessari per questo aggiornamento

## Linee guida per l'aggiornamento dei controller con ARL

Per capire se è possibile utilizzare ARL per aggiornare una coppia di controller 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*.

## Risoluzione dei problemi

In caso di problemi durante l'aggiornamento dei controller, consultare la sezione ["Risolvere i problemi"](#) sezione

alla fine della procedura per ulteriori informazioni e possibili soluzioni.

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.

## Panoramica dell'aggiornamento ARL

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

### Aggiornare la coppia di nodi

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

### Panoramica della sequenza di aggiornamento ARL

Durante la procedura, si aggiorna l'hardware del controller originale con l'hardware del controller sostitutivo, un controller alla volta, sfruttando la configurazione della coppia ha per trasferire la proprietà degli aggregati non root. Tutti gli aggregati non root devono essere sottoposti a due rilocalizzazioni 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"	<p>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.</p> <p>Proprietà aggregata alla fine della fase 1:</p> <ul style="list-style-type: none"> <li>• Node1 è il proprietario della casa e l'attuale proprietario degli aggregati node1.</li> <li>• Node2 è il proprietario domestico e proprietario corrente degli aggregati node2.</li> </ul>
"Fase 2. Spostare e dismettere il node1"	<p>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.</p> <p>Proprietà aggregata alla fine della fase 2:</p> <ul style="list-style-type: none"> <li>• Node2 è l'attuale proprietario degli aggregati node1.</li> <li>• Node2 è il proprietario domestico e proprietario corrente degli aggregati node2.</li> </ul>
"Fase 3. Installazione e boot node3"	<p>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. 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.</p> <p>Proprietà aggregata alla fine della fase 3:</p> <ul style="list-style-type: none"> <li>• Node3 è il proprietario della casa e il proprietario corrente degli aggregati node1.</li> <li>• Node2 è il proprietario domestico e proprietario corrente degli aggregati node2.</li> </ul>

Fase	Descrizione
"Fase 4. Spostare e dismettere il node2"	<p>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.</p> <p>Proprietà aggregata alla fine della fase 4:</p> <ul style="list-style-type: none"> <li>• Node3 è il proprietario della casa e l'attuale proprietario di aggregati che originariamente appartenevano al node1.</li> <li>• Node2 è il proprietario domestico degli aggregati node2.</li> <li>• Node3 è l'attuale proprietario degli aggregati node2.</li> </ul>
"Fase 5. Installazione e boot node4"	<p>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. 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.</p> <p>Proprietà aggregata alla fine della fase 5:</p> <ul style="list-style-type: none"> <li>• Node3 è il proprietario di casa e l'attuale proprietario degli aggregati che originariamente appartenevano al node1.</li> <li>• Node4 è il proprietario della casa e l'attuale proprietario di aggregati che originariamente appartenevano al node2.</li> </ul>
"Fase 6. Completare l'aggiornamento"	<p>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.</p>

## Fase 1. Preparatevi per l'aggiornamento

### Panoramica

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

### Fasi

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

## Preparare i nodi per l'aggiornamento

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

### Fasi

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

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



- 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
```

- Il `system controller replace start` il comando può essere eseguito 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.
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.

Eeguire un controllo preliminare	Descrizione
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 <a href="#">"Riferimenti"</a> Collegamento a <i>Upgrade ONTAP</i> .
Verifica dello stato HA	Controlla se entrambi i nodi da sostituire sono in una configurazione di coppia ad alta disponibilità (ha). Se il failover dello storage non è abilitato per i controller, l'operazione non riesce.
Verifica dello stato dell'aggregato	Se i nodi che vengono sostituiti possiedono aggregati per i quali non sono proprietari di casa, l'attività non riesce. I nodi non devono possedere aggregati non locali.
Verifica dello stato del disco	Se i nodi da sostituire presentano dischi mancanti o guasti, l'attività non riesce. In caso di dischi mancanti, fare riferimento a <a href="#">"Riferimenti"</a> Per collegarsi a <i>Disk and aggregate management con CLI, Logical storage management con CLI e High Availability management</i> 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.

- 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:

```
° vservice 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

### Panoramica

Durante la fase 2, è possibile spostare gli aggregati non root node1 e le LIF dei dati NAS

in node2. Questo processo è in gran parte automatizzato; l'operazione viene interrotta per consentirti di controllarne lo stato. È necessario riprendere manualmente l'operazione. Se necessario, spostare gli aggregati non riusciti o vetoed. Inoltre, registrare le informazioni necessarie sul node1, dismettere il node1 e prepararsi al netboot node3 e node4 più avanti nella procedura.

#### Fasi

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

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

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

#### Prima di iniziare

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

#### A proposito di questa attività

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



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

#### Fasi

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

```
system controller replace resume
```

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

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

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

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

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

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

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

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

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID Status
aggr_1	744.9GB	744.8GB	0%	online	5	node2	
raid_dp,normal							
aggr_2	825.0GB	825.0GB	0%	online	1	node2	
raid_dp,normal							

2 entries were displayed.

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

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

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

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

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

```
volume online -vserver vservice_name -volume volume_name
```

Il *vservice\_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 vservice_name -lif LIF_name -home-node  
nodename -status-admin up
```

## Spostare gli aggregati non riusciti o vetoed

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

### A proposito di questa attività

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

### Fasi

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

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

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

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

Opzione	Descrizione
Ignorare i controlli di veto	Utilizzare il seguente comando: storage aggregate relocation start -node node1 -destination node2 -aggregate-list <i>aggr_list</i> -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 <i>aggr_list</i> -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	<div>Estrarre il contenuto di &lt;ontap_version&gt;_image.tgz file nella directory di destinazione: tar -zxvf &lt;ontap_version&gt;_image.tgz</div> <div><div></div><div>Se si sta estraendo il contenuto su Windows, utilizzare 7-zip o WinRAR per estrarre l'immagine di netboot.</div></div> <div>L'elenco delle directory deve contenere una cartella netboot con un file kernel: netboot/kernel</div>
Tutti gli altri sistemi	<div>L'elenco delle directory deve contenere il seguente file: &lt;ontap_version&gt;_image.tgz</div> <div><div></div><div>Non è necessario estrarre il contenuto di &lt;ontap_version&gt;_image.tgz file.</div></div>

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

**Fase 3. Installazione e boot node3**

**Panoramica**

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. 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.

**Fasi**

- 1. "Installazione e boot node3"

2. ["Impostare la configurazione FC o UTA/UTA2 su node3"](#)
3. ["Verificare l'installazione di node3"](#)
4. ["Ripristinare la configurazione del gestore delle chiavi sul node3"](#)
5. ["Spostare gli aggregati non root e le LIF di dati NAS di proprietà del node1 da node2 a 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"](#).

### Importante:

- Se stai aggiornando un sistema V-Series connesso a storage array o un sistema con software di virtualizzazione FlexArray connesso a storage array, devi completare la procedura [Fase 1](#) attraverso [Fase 21](#), quindi uscire da questa sezione e seguire le istruzioni in ["Configurare le porte FC sul nodo 3"](#) e ["Controllare e configurare le porte UTA/UTA2 sul nodo 3"](#) Sezioni secondo necessità, immissione dei comandi in modalità manutenzione. Quindi, tornare a questa sezione e riprendere con [Fase 23](#).
- 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 nello chassis e node3. In caso contrario, quando si avvia node3, il nodo si comporta come se fosse in una configurazione a doppio chassis e quando si avvia node4, l'interconnessione tra i nodi non si verificherà.

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

Collegare i seguenti collegamenti utilizzando le *istruzioni di installazione e configurazione* o i *requisiti e riferimenti per l'installazione della virtualizzazione FlexArray* per la piattaforma node3, il documento relativo allo shelf di dischi e la *gestione dell'alta disponibilità*.

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

- Console (porta di gestione remota)
- Porte 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.



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



Fare riferimento a. "[Preparatevi per il netboot](#)".

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



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

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

7. Esegui netboot al nodo3:

Per...	Quindi...
Sistemi della serie FAS/AFF8000	<code>netboot http://&lt;web_server_ip/path_to_web-accessible_directory&gt;/netboot/kernel</code>
Tutti gli altri sistemi	<code>netboot http://&lt;web_server_ip/path_to_web-accessible_directory&gt;/&lt;ontap_version&gt;_image.tgz</code>

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

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
```

22. eseguire una delle seguenti operazioni:

Se il sistema...	Descrizione
Dispone di dischi e non di storage back-end	Passare a. <a href="#">Fase 23</a>

Se il sistema...	Descrizione
È un sistema V-Series o un sistema con software di virtualizzazione FlexArray collegato agli array di storage	<p>a. Vai alla sezione <a href="#">"Impostazione della configurazione FC o UTA/UTA2 su node3"</a> e completare le sottosezioni di questa sezione.</p> <p>b. Tornare a questa sezione e completare i passaggi rimanenti, iniziando da <a href="#">Fase 23</a>.</p> <div>  <p>È necessario riconfigurare le porte FC onboard, le porte CNA onboard e le schede CNA prima di avviare ONTAP su V-Series o sul sistema con il software di virtualizzazione FlexArray.</p> </div>

23. aggiungere le porte FC Initiator del nuovo nodo alle zone di switch.

Se il sistema dispone di UNA SAN a nastro, è necessario eseguire lo zoning per gli iniziatori. Se necessario, modificare le porte integrate in Initiator facendo riferimento a. ["Configurazione delle porte FC sul nodo 3"](#). Per ulteriori informazioni sullo zoning, consultare la documentazione relativa allo storage array e allo zoning.

24. aggiungere le porte FC Initiator all'array di storage come nuovi host, mappando le LUN dell'array ai nuovi host.

Per istruzioni, consultare la documentazione relativa allo storage array e allo zoning.

25. modificare i valori WWPN (Worldwide port name) nei gruppi di host o di volumi associati alle LUN degli array sullo storage array.

L'installazione di un nuovo modulo controller modifica i valori WWPN associati a ciascuna porta FC integrata.

26. se la configurazione utilizza lo zoning basato su switch, regolare lo zoning in modo che rifletta i nuovi valori WWPN.

27. 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	<code>setenv bootarg.storageencryption.support <b>true</b></code>
SED non FIPS di NetApp	<code>setenv bootarg.storageencryption.support <b>false</b></code>



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"](#).

28. Nodo di boot nel menu di boot:

```
boot_ontap menu
```

Se non si dispone di una configurazione FC o UTA/UTA2, eseguire ["Controllare e configurare le porte UTA/UTA2 sul nodo 4, passaggio 15"](#) in modo che node4 possa riconoscere i dischi di node2.

29. per una configurazione MetroCluster, sistemi V-Series e sistemi con software di virtualizzazione FlexArray collegati agli array di storage, è necessario impostare e configurare le porte FC o UTA/UTA2 sul nodo 3 per rilevare i dischi collegati al nodo. Per completare questa attività, passare alla sezione ["Impostare la configurazione FC o UTA/UTA2 su 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 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 eseguendo l'aggiornamento di un sistema con dischi di storage, passare alla sezione ["Verificare l'installazione di node3"](#) sezione.
- Tuttavia, se si dispone di un sistema V-Series o di un sistema con software di virtualizzazione FlexArray con storage array e node3 non dispone di porte FC integrate, porte UTA/UTA integrate o una scheda UTA/UTA2, tornare alla sezione *Installazione e boot node3* e riprendere la sezione all'indirizzo ["Fase 23"](#).

### Scelte

- [Configurare le porte FC sul nodo 3](#)
- [Controllare e configurare le porte UTA/UTA2 sul nodo 3](#)

## Configurare le porte FC sul nodo 3

Se node3 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 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](#).



Se il sistema dispone di dischi di storage, immettere i comandi in questa sezione al prompt del cluster. Se si dispone di un "sistema V-Series" o si dispone del software di virtualizzazione FlexArray e si è connessi agli array di storage, immettere i comandi in questa sezione nella modalità di manutenzione.

- 1. [[fase 1]]Confronta le impostazioni FC sul nodo 3 con quelle acquisite in precedenza dal nodo 1.
- 2. eseguire una delle seguenti operazioni:

Se il sistema che si sta aggiornando...	Quindi...
Dispone di dischi di storage	<div>In modalità di manutenzione (opzione 5 nel menu di avvio), modificare le porte FC sul nodo 3 in base alle necessità:<ul style="list-style-type: none"><li>• Per programmare le porte di destinazione: <code>ucadmin modify -m fc -t target adapter</code></li><li>• Per programmare le porte initiator: <code>ucadmin modify -m fc -t initiator adapter</code></li></ul><p>-t È il tipo FC4: Destinazione o iniziatore.</p></div>
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	<div>In modalità di manutenzione (opzione 5 nel menu di avvio), modificare le porte FC sul nodo 3 in base alle necessità: <code>ucadmin modify -m fc -t initiator -f adapter_port_name</code> <p>-t È il tipo, la destinazione o l'iniziatore FC4.</p><div> Le porte FC devono essere programmate come iniziatori.</div></div>

- 3. eseguire una delle seguenti operazioni:

Se il sistema che si sta aggiornando...	Quindi...
Dispone di dischi di storage	Verificare le nuove impostazioni utilizzando il seguente comando ed esaminare l'output: <code>ucadmin show</code>
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	Verificare le nuove impostazioni utilizzando il seguente comando ed esaminare l'output: <code>ucadmin show</code>

4. Esci dalla modalità di manutenzione:

```
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 sistema che si sta aggiornando...	Quindi...
Dispone di dischi di storage	<ul style="list-style-type: none"> <li>• Se node3 ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate, passare alla sezione <a href="#">Controllare e configurare le porte UTA/UTA2 sul nodo 3</a>.</li> <li>• Se node3 non dispone di una scheda UTA/UTA2 o di porte UTA/UTA2 integrate, saltare la sezione <a href="#">Controllare e configurare le porte UTA/UTA2 sul nodo 3</a> e andare alla sezione <a href="#">"Verificare l'installazione di node3"</a>.</li> </ul>
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	<ul style="list-style-type: none"> <li>• Se node3 ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate, passare alla sezione <a href="#">Controllare e configurare le porte UTA/UTA2 sul nodo 3</a>.</li> <li>• Se node3 non dispone di una scheda UTA/UTA2 o di porte UTA/UTA2 integrate, saltare la sezione <a href="#">Controllare e configurare le porte UTA/UTA2 sul nodo 3</a> E tornare alla sezione <a href="#">Installazione e boot node3</a> e riprendere da <a href="#">"Fase 23"</a>.</li> </ul>

## 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
```

Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin 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.



**Attenzione:** Se il sistema dispone di dischi di storage, immettere i comandi in questa sezione al prompt del cluster, a meno che non venga richiesto di accedere alla modalità di manutenzione. Se si dispone di un sistema V- Series o del software di virtualizzazione FlexArray e si è connessi agli array di storage, immettere i comandi in questa sezione al prompt della modalità di manutenzione. Per configurare le porte UTA/UTA2, è necessario essere in modalità di manutenzione.

## Fasi

- controllare la configurazione delle porte immettendo il seguente comando sul nodo 3:

Se il sistema...	Quindi...
Dispone di dischi di storage	Non è richiesta alcuna azione.
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	<code>ucadmin show</code>

Il sistema visualizza un output simile al seguente esempio:

```
*> ucadmin show
      Current   Current   Pending   Pending   Admin
Adapter  Mode    Type      Mode      Type      Status
-----  -
0e       fc       initiator -         -         online
0f       fc       initiator -         -         online
0g       cna      target    -         -         online
0h       cna      target    -         -         online
0e       fc       initiator -         -         online
0f       fc       initiator -         -         online
0g       cna      target    -         -         online
0h       cna      target    -         -         online
*>
```

- [[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.

- esaminare l'output di `ucadmin show` Controllare e determinare se le porte UTA/UTA2 hanno la personalità desiderata.
- eseguire una delle seguenti operazioni:

Se le porte UTA/UTA2...	Quindi...
Non avere la personalità che si desidera	Passare a. <a href="#">Fase 5</a> .
Avere la personalità che si desidera	Saltare i passaggi da 5 a 12 e passare a. <a href="#">Fase 13</a> .

- eseguire una delle seguenti operazioni:

Se si sta configurando...	Quindi...
Porte su una scheda UTA/UTA2	Passare a. <a href="#">Fase 7</a>



Se si sta configurando...	Quindi...
Porte UTA/UTA2 integrate	Saltare la fase 7 e passare a. <a href="#">Fase 8</a> .

6. se la scheda di rete è in modalità Initiator e la porta UTA/UTA2 è in linea, portare la porta UTA/UTA2 offline:

```
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 oppure cna.
- -t È di tipo FC4, target oppure initiator.



È necessario utilizzare FC Initiator per unità nastro, sistemi di virtualizzazione FlexArray e configurazioni MetroCluster. È necessario utilizzare la destinazione FC per i client SAN.

8. verificare le impostazioni:

```
ucadmin show
```

9. verificare le impostazioni:

Se il sistema...	Quindi...
Dispone di dischi di storage	ucadmin show
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	ucadmin 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`:

```
*> 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
*>
```

10. posizionare le porte di destinazione online immettendo uno dei seguenti comandi, una volta per ciascuna porta:

Se il sistema...	Quindi...
Dispone di dischi di storage	<code>network fcp adapter modify -node <i>node_name</i> -adapter <i>adapter_name</i> -state up</code>
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	<code>fcp config <i>adapter_name</i> up</code>

11. collegare via cavo la porta.
12. eseguire una delle seguenti operazioni:

Se il sistema...	Quindi...
Dispone di dischi di storage	Passare a. " <a href="#">Verificare l'installazione di node3</a> ".
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	Tornare alla sezione <i>Installazione e boot node3</i> e riprendere il lavoro dal punto " <a href="#">Fase 23</a> ".

13. Esci dalla modalità di manutenzione:

`halt`

14. avviare il nodo nel menu di boot eseguendo `boot_ontap` menu. Se si sta eseguendo l'aggiornamento a un sistema A800, visitare il sito Web all'indirizzo [Fase 23](#).
15. al nodo 3, accedere al menu di boot e selezionare l'opzione nascosta utilizzando `22/7 boot_after_controller_replacement`. Al prompt, immettere `node1` per riassegnare i dischi da `node1` a `node3`, come nell'esempio seguente.

## Espandere l'esempio di output della console

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

```

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

```

```

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

```



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

16. Se il sistema entra in un loop di riavvio con il messaggio `no disks found`, Indica che il sistema ha ripristinato le porte FC o UTA/UTA2 alla modalità di destinazione e quindi non è in grado di vedere alcun disco. Per risolvere il problema, continuare con [Fase 17](#) a [Fase 22](#) oppure passare alla sezione ["Verificare l'installazione di node3"](#).
17. premere `Ctrl-C` durante l'autoboot per arrestare il nodo su `LOADER>` prompt.
18. al prompt del caricatore, accedere alla modalità di manutenzione:

```
boot_ontap maint
```

19. 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
```

20. verificare che le porte siano state modificate in modalità initiator:

```
ucadmin show
```

21. 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 Web [Fase 22](#).

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 Web [Fase 23](#).

22. 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 del volume root, il software ONTAP non è in grado di leggere le informazioni del 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
```

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 [Fase 22](#) fino a quando il sistema non si avvia normalmente.

23. 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, accedere al menu di boot 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 fast zeroed 64-bit	root, nosnap=on
aggr0	offline	raid_dp, aggr fast zeroed 64-bit	diskroot

## 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 <a href="#">Fase 5</a> .

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.
```

- 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.

- passare alla modalità privilegi avanzati:

```
set advanced
```

- 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
```

- 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
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-
vls show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement network displaced-vls 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	""	0000000000000000020000000000a008a81976
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 eventuali LIF spostate. Elencare eventuali LIF spostate:

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

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

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

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

### Panoramica

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

### Fasi

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

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

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

#### Prima di iniziare

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

#### A proposito di questa attività

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

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



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

### Fasi

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

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

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

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

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

2 entries were displayed.

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

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

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

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

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

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

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

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

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

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

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

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

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

## Andare in pensione node2

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

### Fasi

1. Riprendere l'operazione:

```
system controller replace resume
```

Il nodo si arresta automaticamente.

### Al termine

È possibile decommissionare il node2 una volta completato l'aggiornamento. Vedere ["Decommissionare il vecchio sistema"](#).

## Fase 5. Installazione e boot node4

### Panoramica

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. 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.

### Fasi

1. ["Installazione e boot node4"](#)
2. ["Impostare la configurazione FC o UTA/UTA2 su node4"](#)
3. ["Verificare l'installazione di node4"](#)
4. ["Ripristinare la configurazione del gestore delle chiavi sul nodo 4"](#)
5. ["Spostare gli aggregati non root e le LIF di dati NAS di proprietà di node2 da node3 a 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 il netboot node4 se non dispone della stessa versione di ONTAP 9 installata sul node2.

Dopo aver installato node4, avviarlo dall'immagine di ONTAP 9 memorizzata sul server Web. È quindi possibile scaricare i file corretti sul dispositivo di avvio per i successivi avviamenti del sistema, seguendo le istruzioni riportate in ["Preparatevi per il netboot"](#).

### Importante:

- Se si sta eseguendo l'upgrade di un sistema V-Series collegato a storage array o a un sistema con software di virtualizzazione FlexArray collegato a storage array, è necessario completare la procedura [Fase 1](#) attraverso [Fase 21](#), quindi uscire da questa sezione e seguire le istruzioni a. ["Configurare le porte FC sul nodo 4"](#) e a. ["Controllare e configurare le porte UTA/UTA2 sul nodo 4"](#), Immissione di comandi in modalità manutenzione. Quindi, tornare a questa sezione e riprendere con [Fase 23](#).
- Tuttavia, se si sta aggiornando un sistema con dischi di storage, è necessario completare l'intera sezione e passare alla sezione ["Impostare la configurazione FC o UTA/UTA2 su node4"](#), immettendo i 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 cavo4, spostamento delle connessioni dal nodo 2 al nodo 4.

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

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

- Console (porta di gestione remota)
- Porte 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 boot.



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

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

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

- a. Verificare la presenza di eventuali messaggi della console che potrebbero indicare un problema diverso da una batteria NVRAM in esaurimento e, se necessario, intraprendere le azioni correttive necessarie.
- b. Attendere che la batteria si ricarichi e che il processo di avvio venga completato.



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




Fare riferimento a. ["Preparatevi per il netboot"](#).

6. configurare la connessione 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: <code>ifconfig e0M -auto</code>

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

#### 7. Eseguire il netboot al nodo 4:

Per...	Quindi...
Sistemi della serie FAS/AFF8000	<code>netboot http://&lt;web_server_ip/path_to_web-accessible_directory&gt;/netboot/kernel</code>
Tutti gli altri sistemi	<code>netboot http://&lt;web_server_ip/path_to_web-accessible_directory&gt;/&lt;ontap_version&gt;_image.tgz</code>

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

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. eseguire una delle seguenti operazioni:

Se il sistema...	Quindi...
Dispone di dischi e non di storage back-end	Passare a. <a href="#">Fase 23</a> .

Se il sistema...	Quindi...
È un sistema V-Series o un sistema con software di virtualizzazione FlexArray collegato agli array di storage	<p>a. Vai alla sezione <a href="#">"Impostare la configurazione FC o UTA/UTA2 su node4"</a> e completare le sottosezioni di questa sezione.</p> <p>b. Tornare a questa sezione e completare i passaggi rimanenti, iniziando da <a href="#">Fase 23</a>.</p> <div>  <p>È necessario riconfigurare le porte FC onboard, le porte CNA onboard e le schede CNA prima di avviare ONTAP su V-Series o sul sistema con il software di virtualizzazione FlexArray.</p> </div>

23. aggiungere le porte FC Initiator del nuovo nodo alle zone di switch.

Se il sistema dispone di UNA SAN a nastro, è necessario eseguire lo zoning per gli iniziatori. Se necessario, modificare le porte integrate in Initiator facendo riferimento a. ["Configurare le porte FC sul nodo 4"](#). Per ulteriori informazioni sullo zoning, consultare la documentazione relativa allo storage array e allo zoning.

24. Aggiungere le porte FC Initiator all'array di storage come nuovi host, mappando le LUN dell'array ai nuovi host.

Per istruzioni, consultare la documentazione relativa allo storage array e allo zoning.

25. Modificare i valori WWPN (Worldwide port name) nei gruppi di host o volumi associati alle LUN degli array sullo storage array.

L'installazione di un nuovo modulo controller modifica i valori WWPN associati a ciascuna porta FC integrata.

26. Se la configurazione utilizza lo zoning basato su switch, regolare lo zoning in modo che rifletta i nuovi valori WWPN.

27. se sono installate unità di crittografia archiviazione 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	<code>setenv bootarg.storageencryption.support <b>true</b></code>
SED non FIPS di NetApp	<code>setenv bootarg.storageencryption.support <b>false</b></code>



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"](#).

28. Nodo di boot nel menu di boot:

```
boot_ontap menu
```

Se non si dispone di una configurazione FC o UTA/UTA2, eseguire ["Controllare e configurare le porte UTA/UTA2 sul nodo 4, passaggio 15"](#) in modo che node4 possa riconoscere i dischi di node2.

29. per la configurazione MetroCluster, i sistemi V-Series e i sistemi con software di virtualizzazione FlexArray collegati agli array di storage, è necessario impostare e configurare le porte FC o UTA/UTA2 sul nodo 4 per rilevare i dischi collegati al nodo. Per completare questa attività, passare alla sezione ["Impostare la configurazione FC o UTA/UT2 su 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 completare il [Configurare le porte FC sul nodo 4](#) sezione, la [Controllare 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 ["Verificare l'installazione di node4"](#). Tuttavia, se si dispone di un sistema V-Series o di un software di virtualizzazione FlexArray e si è connessi a storage array, e node4 non dispone di porte FC integrate, porte UTA/UTA2 integrate o una scheda UTA/UTA2, tornare alla sezione *Installazione e boot node4* e riprendere a ["Fase 22"](#). 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.

### Scelte

- [Configurare le porte FC sul nodo 4](#)
- [Controllare e configurare le porte UTA/UTA2 sul 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](#).



Se il sistema dispone di dischi di storage, è necessario immettere i comandi in questa sezione al prompt del cluster. Se si dispone di un sistema V-Series o di un sistema con software di virtualizzazione FlexArray collegato agli array di storage, immettere i comandi in questa sezione in modalità manutenzione.

## Fasi


1. Eseguire una delle seguenti operazioni:

Se il sistema che si sta aggiornando...	Quindi...
Dispone di dischi di storage	<code>system node hardware unified-connect show</code>
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	<code>ucadmin show</code>

Il sistema visualizza informazioni su tutti gli adattatori di rete FC e convergenti del sistema.

2. Confrontare le impostazioni FC sul nodo 4 con quelle acquisite in precedenza dal nodo 1.
3. Eseguire una delle seguenti operazioni:

Se il sistema che si sta aggiornando...	Quindi...
Dispone di dischi di storage	<p>Modificare le porte FC sul nodo 4 in base alle necessità:</p> <ul style="list-style-type: none"><li>• Per programmare le porte di destinazione: <code>ucadmin modify -m fc -t target adapter</code></li><li>• Per programmare le porte initiator: <code>ucadmin modify -m fc -t initiator adapter</code></li></ul> <p>-t È il tipo FC4: Destinazione o iniziatore.</p>

Se il sistema che si sta aggiornando...	Quindi...
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	<p>Modificare le porte FC sul nodo 4 in base alle necessità:</p> <pre>ucadmin modify -m fc -t initiator -f adapter_port_name</pre> <p>-t È il tipo, la destinazione o l'iniziatore FC4.</p> <p> Le porte FC devono essere programmate come iniziatori.</p>

4. Uscire dalla modalità di manutenzione:

```
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 sistema che si sta aggiornando...	Quindi...
Dispone di dischi di storage	<ul style="list-style-type: none"> <li>• Saltare questa sezione e andare a. <a href="#">"Verificare l'installazione di node4"</a> Se node4 non dispone di una scheda UTA/UTA2 o di porte UTA/UTA2 integrate.</li> </ul>
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	<ul style="list-style-type: none"> <li>• Passare a. <a href="#">Controllare e configurare le porte UTA/UTA2 sul nodo 4</a> Se node4 ha una scheda UTA/UTA2 o porte UTA/UTA2 integrate.</li> <li>• Saltare la sezione <i>controllare e configurare le porte UTA/UTA2 su node4</i> se node4 non dispone di una scheda UTA/UTA2 o di porte integrate UTA/UTA2, tornare alla sezione <i>Installazione e boot node4</i> e riprendere da <a href="#">"Fase 23"</a>.</li> </ul>

## 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.



**Attenzione:** Se il sistema dispone di dischi di storage, immettere i comandi in questa sezione al prompt del cluster, a meno che non venga richiesto di accedere alla modalità di manutenzione. Se si dispone di un sistema MetroCluster FC, V-Series o un sistema con software di virtualizzazione FlexArray collegato agli array di storage, è necessario essere in modalità di manutenzione per configurare le porte UTA/UTA2.

## Fasi

1. Verificare la configurazione delle porte utilizzando uno dei seguenti comandi sul nodo 4:

Se il sistema...	Quindi...
Dispone di dischi di storage	<code>system node hardware unified-connect show</code>
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	<code>ucadmin show</code>

Il sistema visualizza un output simile al seguente esempio:

```
*> ucadmin show
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin 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. Esaminare l'output di `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. <a href="#">Fase 5</a> .
Avere la personalità che si desidera	Saltare i passaggi da 5 a 12 e passare a. <a href="#">Fase 13</a> .

5. eseguire una delle seguenti operazioni:

Se si sta configurando...	Quindi...
Porte su una scheda UTA/UTA2	Passare a. <a href="#">Fase 7</a>
Porte UTA/UTA2 integrate	Saltare la fase 7 e passare a. <a href="#">Fase 8</a> .

6. Se l'adattatore è in modalità Initiator e la porta UTA/UTA2 è in linea, portare la porta UTA/UTA2 offline:

```
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 FC Initiator per unità nastro, sistemi di virtualizzazione FlexArray e configurazioni MetroCluster. È necessario utilizzare la destinazione FC per i client SAN.

8. verificare le impostazioni utilizzando il seguente comando ed esaminandone l'output:

```
ucadmin show
```

9. Verificare le impostazioni:

Se il sistema...	Quindi...
Dispone di dischi di storage	<code>ucadmin show</code>

Se il sistema...	Quindi...
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	<code>ucadmin show</code>

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.
*>
```

10. Inserire le porte di destinazione in linea immettendo uno dei seguenti comandi, una volta per ciascuna porta:

Se il sistema...	Quindi...
Dispone di dischi di storage	<code>network fcp adapter modify -node <i>node_name</i> -adapter <i>adapter_name</i> -state up</code>
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	<code>fcp config <i>adapter_name</i> up</code>

11. Collegare la porta.
12. eseguire una delle seguenti operazioni:

Se il sistema...	Quindi...
Dispone di dischi di storage	Passare a. <a href="#">"Verificare l'installazione di node4"</a> .
È un sistema V-Series o dispone di software di virtualizzazione FlexArray ed è collegato agli array di storage	Tornare alla sezione <i>Installazione e boot node4</i> e riprendere il lavoro dal <a href="#">"Fase 23"</a> .



13. Esci dalla modalità di manutenzione:

```
halt
```

14. nodo di boot nel menu di boot:

```
boot_ontap menu.
```

Se si sta eseguendo l'aggiornamento a un sistema A800, visitare il sito Web all'indirizzo [Fase 23](#)

15. al nodo 4, accedere al menu di boot e selezionare l'opzione nascosta utilizzando 22 ore su 24, 7 giorni su 7 `boot_after_controller_replacement`. Al prompt, immettere `node2` per riassegnare i dischi di `node2` a `node4`, come nell'esempio seguente.

## Espandere l'esempio di output della console

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

```

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

```

```

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

```



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

16. Se il sistema entra in un loop di riavvio con il messaggio `no disks found`, Indica che il sistema ha ripristinato le porte FC o UTA/UTA2 alla modalità di destinazione e quindi non è in grado di vedere alcun

disco. Per risolvere il problema, passare alla [Fase 17](#) a. [Fase 22](#) oppure vai alla sezione "[Verificare l'installazione di node4](#)".

17. premere `Ctrl-C` durante l'autoboot per arrestare il nodo su `LOADER>` prompt.

18. Al prompt del caricatore, accedere alla modalità di manutenzione:

```
boot_ontap maint
```

19. 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
```

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

```
ucadmin show
```

21. 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 Web [Fase 22](#).

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 Web [Fase 23](#).

22. 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 del volume root, il software ONTAP non è in grado di leggere le informazioni del 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

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 [Fase 22](#) fino a quando il sistema non si avvia normalmente.

23. 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 root per garantire l'avvio node4 dall'aggregato root di node2. Per impostare l'aggregato root, accedere al menu di boot 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 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. <a href="#">Fase 5</a> .

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	svml	""	0000000000000000020000000000a008a81976
true			2190178f9350e071fbb90f0000000000000000

## 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.



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 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 eventuali LIF spostate. Elencare eventuali LIF spostate:

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

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

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

## 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

### Panoramica

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

#### Fasi

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

#### Per la configurazione MetroCluster FC

Per la configurazione MetroCluster FC, 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 comando `-skip-metrocluster-check true` Opzione per ignorare i controlli MetroCluster quando si sostituiscono i nodi nel secondo sito.

### 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
```

Node	Partner	Takeover 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 vservice_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 ed è stato impostato `kmip.init.maxwait` variabile a. `off` (ad esempio, in ["Installazione e boot node4, passaggio 27"](#)), è necessario annullare l'impostazione della variabile:

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

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

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

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

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

### Al termine

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

## Impostare Storage Encryption sul nuovo modulo controller

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

### A proposito di questa attività

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

### Fasi

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

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

```
security key-manager onboard show-backup
```

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

- a. Aggiungere il server di gestione delle chiavi:

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

- b. Ripetere il passaggio precedente per ciascun server di gestione delle chiavi elencato. È possibile collegare fino a quattro server di gestione delle chiavi.
- c. Verificare che i server di gestione delle chiavi siano stati aggiunti correttamente:

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

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

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

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

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

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

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

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

## **Impostare NetApp Volume o aggregate Encryption sul nuovo modulo controller**

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

### **A proposito di questa attività**

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

### Gestione delle chiavi integrata

Configurare NVE o NAE utilizzando Onboard Key Manager.

#### Fasi

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

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

### Gestione esterna delle chiavi

Configurare NVE o NAE utilizzando External Key Management.

#### Fasi

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

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

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

- a. Aggiungere il server di gestione delle chiavi:

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

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

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

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

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

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

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

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

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

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

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

Questo comando richiede la passphrase OKM

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

## Al termine

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

## Decommissionare il vecchio sistema

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

### Fasi

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

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

- Numero di serie (situato sul retro dell'unità)
- Numeri di serie per la mia posizione

4. Selezionare **Go!**

Una tabella visualizza le informazioni sul cluster, inclusi i numeri di serie.

5. Individuare il cluster nella tabella e selezionare **Decommissionare questo sistema** dal menu a discesa Product Tool Set (Set strumenti prodotto).

## Riprendere le operazioni di SnapMirror

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

### Fasi

1. Verificare lo stato di SnapMirror sulla destinazione:

```
snapmirror show
```

2. Riprendere la relazione di SnapMirror:

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

## Risolvere i problemi

### Risolvere i problemi

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



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

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

## Errori di trasferimento aggregati

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

### Verificare la presenza di errori di trasferimento degli aggregati

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

#### Fasi

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

```
storage aggregate relocation show
```

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

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

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

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

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

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

#### A proposito di questa attività

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

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

verrà online con node4 come nodo home invece di node3.

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

### Fasi

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

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

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

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

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

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

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

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

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

Gli aggregati che non hanno node3 come proprietario di casa possono essere ricollocati in node3 utilizzando lo stesso comando di rilocalizzazione 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 node1 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
```

Node	Partner	Takeover 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
```

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

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

### Fasi

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

## Errore di migrazione LIF

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

### Fasi

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

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

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

## Riferimenti

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

- [Contenuto di riferimento](#)
- [Siti di riferimento](#)

## Contenuto di riferimento

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

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

Contenuto	Descrizione
" <a href="#">Gestione di dischi e aggregati con CLI</a> "	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.
" <a href="#">Installazione e configurazione di Fabric-Attached MetroCluster</a> "	Descrive come installare e configurare i componenti hardware e software di MetroCluster in una configurazione fabric.
" <a href="#">Requisiti e riferimenti per l'installazione della virtualizzazione FlexArray</a> "	Contiene istruzioni sul cablaggio e altre informazioni per i sistemi di virtualizzazione FlexArray.
" <a href="#">Gestione dell'alta disponibilità</a> "	Descrive come installare e gestire le configurazioni in cluster ad alta disponibilità, tra cui failover dello storage e takeover/giveback.
" <a href="#">Gestione dello storage logico con la CLI</a> "	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.
" <a href="#">Gestione MetroCluster e disaster recovery</a> "	Descrive come eseguire le operazioni di switchover e switchback MetroCluster, sia nelle operazioni di manutenzione pianificate che in caso di disastro.
" <a href="#">Upgrade ed espansione di MetroCluster</a> "	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.
" <a href="#">Gestione della rete</a> "	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.
" <a href="#">Comandi di ONTAP 9.0: Guida alla pagina</a> "	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.0 supportati.
" <a href="#">Comandi di ONTAP 9.1: Guida alla pagina</a> "	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.1 supportati.
" <a href="#">Comandi di ONTAP 9.2: Guida alla pagina</a> "	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.2 supportati.
" <a href="#">Comandi di ONTAP 9.3: Guida alla pagina</a> "	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.3 supportati.
" <a href="#">Comandi di ONTAP 9.4: Guida alla pagina</a> "	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.4 supportati.
" <a href="#">Comandi di ONTAP 9.5: Guida alla pagina</a> "	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.5 supportati.
" <a href="#">Comandi di ONTAP 9.6: Guida alla pagina</a> "	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.6 supportati.



Contenuto	Descrizione
<a href="#">"Comandi di ONTAP 9.7: Guida alla pagina"</a>	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.7 supportati.
<a href="#">"Comandi di ONTAP 9.8: Guida alla pagina"</a>	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.8 supportati.
<a href="#">"Comandi di ONTAP 9.9.1: Guida alla pagina"</a>	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.9.1 supportati.
<a href="#">"Comandi di ONTAP 9.10.1: Guida alla pagina"</a>	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.10.1 supportati.
<a href="#">"Gestione SAN con CLI"</a>	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.
<a href="#">"Riferimento alla configurazione SAN"</a>	Contiene informazioni sulle topologie FC e iSCSI e sugli schemi di cablaggio.
<a href="#">"Eseguire l'upgrade spostando volumi o storage"</a>	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.
<a href="#">"Aggiornare ONTAP"</a>	Contiene le istruzioni per scaricare e aggiornare ONTAP.
<a href="#">"Utilizzare i comandi "System controller replace" per aggiornare i modelli di controller nello stesso chassis"</a>	Descrive le procedure di trasferimento degli aggregati necessarie per aggiornare un sistema senza interruzioni, mantenendo il vecchio chassis e i dischi del sistema.
<a href="#">"Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller con ONTAP 9.8 o versione successiva"</a>	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".
<a href="#">"Utilizzare il trasferimento di aggregati per aggiornare manualmente l'hardware del controller con ONTAP 9.8 o versione successiva"</a>	Descrive le procedure di trasferimento degli aggregati necessarie per eseguire aggiornamenti manuali dei controller senza interruzioni con ONTAP 9.8 o versione successiva.
<a href="#">"Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller che esegue ONTAP 9.5 a ONTAP 9.7"</a>	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".
<a href="#">"Utilizzare il trasferimento di aggregati per aggiornare manualmente l'hardware del controller con ONTAP 9.7 o versione precedente"</a>	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 © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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