



Preparatevi all'aggiornamento

ONTAP MetroCluster

NetApp
February 28, 2025

Sommario

Preparatevi all'aggiornamento	1
Requisiti per l'utilizzo di questa procedura di aggiornamento dell'IP di MetroCluster	1
Piattaforme supportate da questa procedura	1
Requisiti	1
Attivare la registrazione della console prima dell'aggiornamento del controller IP MetroCluster	2
Impostare il bootarg richiesto (per gli aggiornamenti MetroCluster IP ai sistemi introdotti in ONTAP 9.15.1 o versioni successive)	3
Passo 1: Determinare il bootarg da impostare sui vecchi controller	3
Fase 2: Impostare il bootarg richiesto sui vecchi controller	3
Preparare il sistema IP MetroCluster per l'aggiornamento	4
Aggiornare gli RCF degli switch MetroCluster prima di aggiornare i controller	4
Mappare le porte dai vecchi nodi ai nuovi nodi	6
NetBoot i nuovi controller	7
Cancellare la configurazione su un modulo controller	9
Verificare lo stato di salute di MetroCluster prima dell'aggiornamento del sito	9
Raccogliere informazioni prima dell'aggiornamento	11
Rimuovere il monitoraggio di Mediator o Tiebreaker	13
Inviare un messaggio AutoSupport personalizzato prima della manutenzione	14

Preparatevi all'aggiornamento

Requisiti per l'utilizzo di questa procedura di aggiornamento dell'IP di MetroCluster

Verifica che il tuo sistema soddisfi tutti i requisiti prima di eseguire l'upgrade del controller.

Piattaforme supportate da questa procedura

- Sulle piattaforme deve essere in esecuzione ONTAP 9.8 o versione successiva.
 - La piattaforma di destinazione (nuova) deve essere un modello diverso rispetto alla piattaforma originale.
 - È possibile aggiornare solo modelli di piattaforma specifici utilizzando questa procedura in una configurazione MetroCluster IP.
 - Per informazioni sulle combinazioni di aggiornamento della piattaforma supportate, consultare la tabella di aggiornamento IP di MetroCluster in ["Scegliere una procedura di aggiornamento del controller"](#).
- Fare riferimento a ["Scelta di un metodo di aggiornamento o refresh"](#) per ulteriori procedure.

Requisiti

- Questa procedura si applica ai moduli controller in una configurazione MetroCluster IP.
- Tutti i controller della configurazione devono essere aggiornati durante lo stesso periodo di manutenzione.

L'utilizzo della configurazione MetroCluster con diversi tipi di controller non è supportato al di fuori di questa attività di manutenzione.

- I sistemi IP di MetroCluster devono eseguire la stessa versione di ONTAP in entrambi i siti.
- Gli switch IP MetroCluster (tipo di switch, vendor e modello) e la versione del firmware devono essere supportati sui controller nuovi ed esistenti nella configurazione di aggiornamento.

Per informazioni sugli switch supportati e sulle versioni del firmware, fare riferimento alla ["Hardware Universe"](#) o ["IMT"](#) alla .

- Quando si esegue l'aggiornamento da sistemi con più slot o porte rispetto al nuovo sistema, è necessario verificare che siano presenti slot e porte sufficienti sul nuovo sistema.

Prima di iniziare l'aggiornamento, consultare la ["Hardware Universe"](#) per verificare il numero di slot e porte sul nuovo sistema.

- Se è abilitato sul sistema, ["disattiva la crittografia end-to-end"](#) prima di eseguire l'aggiornamento.
- Se la nuova piattaforma ha meno slot rispetto al sistema originale o se ha un numero inferiore o diversi tipi di porte, potrebbe essere necessario aggiungere un adattatore al nuovo sistema.
- Riutilizzate gli indirizzi IP, le netmask e i gateway delle piattaforme originali sulle nuove piattaforme.

In questa procedura vengono utilizzati i seguenti nomi di esempio:

- Cluster_A presso il sito_A.

- Prima dell'aggiornamento:
 - Node_A_1-old
 - Node_A_2-old
- Dopo l'aggiornamento:
 - Node_A_1-new
 - Node_A_2-new
- Cluster_B nel sito_B.
 - Prima dell'aggiornamento:
 - Node_B_1-old
 - Node_B_2-old
 - Dopo l'aggiornamento:
 - Node_B_1-new
 - Node_B_2-new

Quali sono le prossime novità?

["Attivare la registrazione della console"](#).

Attivare la registrazione della console prima dell'aggiornamento del controller IP MetroCluster

Abilitare la registrazione della console sui dispositivi prima di eseguire l'aggiornamento del controller.

NetApp consiglia vivamente di attivare la registrazione della console sui dispositivi in uso e di eseguire le seguenti operazioni quando si esegue questa procedura:

- Lasciare attivato AutoSupport durante la manutenzione.
- Attivare un messaggio AutoSupport di manutenzione prima e dopo la manutenzione per disattivare la creazione del caso per tutta la durata dell'attività di manutenzione.

Consultare l'articolo della Knowledge base ["Come eliminare la creazione automatica del caso durante le finestre di manutenzione pianificata"](#).

- Abilita la registrazione della sessione per qualsiasi sessione CLI. Per istruzioni su come attivare la registrazione della sessione, consultare la sezione "registrazione dell'output della sessione" nell'articolo della Knowledge base ["Come configurare Putty per una connettività ottimale ai sistemi ONTAP"](#).

Quali sono le prossime novità?

Esaminare le informazioni in ["Impostare il bootarg richiesto \(per gli aggiornamenti ai sistemi introdotti nella versione 9.15.1 o successiva\)"](#) per confermare se è necessario impostare un bootarg richiesto sul sistema esistente.

Impostare il bootarg richiesto (per gli aggiornamenti MetroCluster IP ai sistemi introdotti in ONTAP 9.15.1 o versioni successive)

Gli aggiornamenti dei controller ai sistemi introdotti in ONTAP 9.15.1 o versioni successive richiedono l'impostazione di un bootarg prima di poter avviare l'aggiornamento.

Passo 1: Determinare il bootarg da impostare sui vecchi controller

Tutti gli aggiornamenti supportati ai seguenti sistemi richiedono di impostare un bootarg sui vecchi controller prima di eseguire l'aggiornamento del controller:

- AFF A70, AFF A90, AFF A1K
- FAS70, FAS90
- AFF C80
- AFF A50, AFF A20, AFF A30
- AFF C30, AFF C60



Se si sta eseguendo l'aggiornamento a uno dei sistemi elencati, è **necessario** impostare un bootarg richiesto sul sistema esistente prima di eseguire l'aggiornamento. Per tutti gli altri aggiornamenti, è possibile saltare questa attività e passare direttamente a ["Preparare il sistema per l'aggiornamento"](#).

La maggior parte degli aggiornamenti ai sistemi introdotti in ONTAP 9.15.1 o versioni successive richiedono di impostare il `hw.cxgbe.toe_keepalive_disable` bootarg sui vecchi controller. Tuttavia, alcuni percorsi di aggiornamento richiedono invece di impostare il `bootarg.siw.interop_enabled` bootarg.

Utilizzare la tabella seguente per determinare quale bootarg impostare per la combinazione di aggiornamento specifica.

Per questo aggiornamento...	Impostare il bootarg...
Da AFF A250 a AFF A30	<code>bootarg.siw.interop_enabled</code>
Da AFF C250 a AFF C30	<code>bootarg.siw.interop_enabled</code>
Da AFF A150 a AFF A20	<code>bootarg.siw.interop_enabled</code>
Da AFF A220 a AFF A20	<code>bootarg.siw.interop_enabled</code>
Tutti gli altri aggiornamenti supportati per sistemi AFF A70, AFF A90, AFF A1K, FAS70, FAS90, AFF C80, AFF A50, AFF A20, AFF A30, AFF C30 o AFF C60	<code>hw.cxgbe.toe_keepalive_disable</code>

Fase 2: Impostare il bootarg richiesto sui vecchi controller

Questa attività è **solo** necessaria quando si esegue l'aggiornamento a un sistema AFF A70, AFF A90, AFF A1K, FAS70, FAS90, AFF C80, AFF A50, AFF A20, AFF A30, AFF C30 o AFF C60.

Fasi

1. Arrestare un nodo in ciascun sito e consentire al partner ha di eseguire un takeover dello storage del nodo:

```
halt -node <node_name>
```

2. Impostare il bootarg richiesto per la combinazione di aggiornamento. È già stato determinato il bootarg che è necessario impostare utilizzando la tabella in [determinare il bootarg da impostare](#).

hw.cxgbe.toe_keepalive_disable

- a. Al LOADER prompt del nodo arrestato, immettere quanto segue:

```
setenv hw.cxgbe.toe_keepalive_disable 1  
  
saveenv  
  
printenv hw.cxgbe.toe_keepalive_disable
```

bootarg.siw.interop_enabled

- a. Al LOADER prompt del nodo arrestato, immettere quanto segue:

```
setenv bootarg.siw.interop_enabled 1  
  
saveenv  
  
printenv bootarg.siw.interop_enabled
```

3. Avviare il nodo:

```
boot_ontap
```

4. All'avvio del nodo, eseguire un giveback per il nodo quando richiesto:

```
storage failover giveback -ofnode <node_name>
```

5. Ripetere la procedura per ciascun nodo del gruppo di DR in fase di aggiornamento.

Quali sono le prossime novità?

["Preparare il sistema per l'aggiornamento"](#).

Preparare il sistema IP MetroCluster per l'aggiornamento

Prima di apportare modifiche alla configurazione MetroCluster esistente, controllare lo stato della configurazione, preparare le nuove piattaforme ed eseguire altre operazioni.

Aggiornare gli RCF degli switch MetroCluster prima di aggiornare i controller

A seconda dei modelli di piattaforma vecchi e nuovi, potrebbe essere necessario aggiornare i file di configurazione di riferimento dello switch MetroCluster (RCF) prima di aggiornare i controller.

A proposito di questa attività

Eeguire questa attività nelle seguenti circostanze:

- La configurazione dell'interruttore RCF non è sulla versione minima.
- È necessario modificare gli ID VLAN utilizzati dalle connessioni MetroCluster back-end.

Prima di iniziare

Stabilire se è necessario aggiornare gli RCF prima di aggiornare i controller:

- Se la configurazione dello switch non è stata configurata con la versione RCF minima supportata, è necessario aggiornare gli RCF prima di aggiornare i controller:

Modello di switch	Versione RCF richiesta
Cisco 3132Q-V.	1.7 o versione successiva
Cisco 3232C	1.7 o versione successiva
Broadcom BES-53248	1.3 o versione successiva
NVIDIA SN2100	2.0 o versione successiva

- Se entrambi i modelli di piattaforma vecchi e nuovi sono elencati di seguito, non è necessario aggiornare l'ID VLAN prima di aggiornare i controller:
 - FAS8200 o AFF A300
 - AFF A320
 - FAS9000 o AFF A700
 - AFF A800, AFF C800, ASA A800 o ASA C800

Se uno dei modelli di piattaforma precedenti o nuovi non è elencato in precedenza, è necessario confermare che le interfacce MetroCluster utilizzano un ID VLAN supportato. Gli ID VLAN supportati per le interfacce MetroCluster sono: 10, 20 o nell'intervallo da 101 a 4096.



- Se l'ID VLAN non è 10, 20 o compreso nell'intervallo da 101 a 4096, è necessario aggiornare lo switch RCF prima di aggiornare i controller.
- Le connessioni del cluster locale possono utilizzare qualsiasi VLAN, non è necessario che rientrino nell'intervallo specificato.
- Il nuovo RCF a cui si sta effettuando l'aggiornamento deve utilizzare le VLAN 10, 20 o essere compreso nell'intervallo da 101 a 4096. Non modificare la VLAN per il cluster locale a meno che non sia necessaria.

Fasi

1. Preparare gli switch IP per l'applicazione dei nuovi RCF.

Seguire la procedura descritta nella sezione relativa al fornitore dello switch:



È necessario aggiornare gli interruttori nel seguente ordine: Switch_A_1, switch_B_1, switch_A_2, switch_B_2.

- "Ripristinare l'interruttore Broadcom IP alle impostazioni predefinite"
- "Ripristinare lo switch IP Cisco alle impostazioni predefinite"
- "Ripristinare le impostazioni predefinite dello switch NVIDIA IP SN2100"

2. Scaricare e installare gli RCF.

Seguire la procedura descritta nella sezione relativa al fornitore dello switch:

- "Scaricare e installare gli RCF Broadcom"
- "Scaricare e installare gli RCF IP Cisco"
- "Scaricare e installare gli RCF IP NVIDIA"

Mappare le porte dai vecchi nodi ai nuovi nodi

È necessario verificare che le porte fisiche su node_A_1-old si mappino correttamente alle porte fisiche su node_A_1-new. Questo consente a node_A_1-new di comunicare con altri nodi nel cluster e con la rete dopo l'aggiornamento.

A proposito di questa attività

Quando il nuovo nodo viene avviato per la prima volta durante il processo di aggiornamento, riproduce la configurazione più recente del vecchio nodo che sta sostituendo. Quando si avvia Node_A_1-new, ONTAP tenta di ospitare le LIF sulle stesse porte utilizzate su Node_A_1-old. Ciò significa che è necessario regolare la porta e la configurazione LIF come parte dell'aggiornamento in modo che sia compatibile con la configurazione del vecchio nodo. Durante la procedura di upgrade, esegui diverse procedure sui nodi vecchi e nuovi per garantire la corretta configurazione del cluster, della gestione e della LIF dati

La seguente tabella mostra esempi di modifiche alla configurazione relative ai requisiti di porta dei nuovi nodi.

Porte fisiche di interconnessione cluster		
Vecchio controller	Nuovo controller	Azione richiesta
e0a, e0b	e3a, e3b	Nessuna porta corrispondente. Dopo l'upgrade, è necessario ricreare le porte del cluster.
e0c, e0d	e0a,e0b,e0c,e0d	e0c e e0d corrispondono alle porte. Non occorre modificare la configurazione, ma dopo l'upgrade puoi suddividere le LIF del cluster nelle porte disponibili.

Fasi

1. Determinare quali porte fisiche sono disponibili sui nuovi controller e quali LIF possono essere ospitate sulle porte.

L'utilizzo della porta del controller dipende dal modulo della piattaforma e dagli switch che verranno utilizzati nella configurazione IP di MetroCluster. È possibile raccogliere l'utilizzo delle porte delle nuove piattaforme da "[Hardware Universe](#)".

2. Pianificare l'utilizzo delle porte e compilare le seguenti tabelle come riferimento per ciascuno dei nuovi nodi.

Durante l'esecuzione della procedura di aggiornamento, fare riferimento alla tabella.

LIF	Node_A_1-old			Node_A_1-new		
	Porte	IPspaces	Domini di broadcast	Porte	IPspaces	Domini di broadcast
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gestione dei nodi						
Gestione del cluster						
Dati 1						
Dati 2						
Dati 3						
Dati 4						
SAN						
Porta intercluster						

NetBoot i nuovi controller

Dopo aver installato i nuovi nodi, è necessario eseguire il netboot per assicurarsi che i nuovi nodi eseguano la stessa versione di ONTAP dei nodi originali. Il termine netboot indica che si sta eseguendo l'avvio da un'immagine ONTAP memorizzata su un server remoto. Durante la preparazione per il netboot, è necessario inserire una copia dell'immagine di boot di ONTAP 9 su un server Web a cui il sistema può accedere.

Fasi

1. NetBoot i nuovi controller:
 - a. Accedere a ["Sito di supporto NetApp"](#) per scaricare i file utilizzati per eseguire il netboot del sistema.
 - b. 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.

c. Passare alla directory accessibile dal Web e verificare che i file necessari siano disponibili.

L'elenco delle directory deve contenere una cartella netboot con un file kernel:

```
_ontap-version_image.tgz
```

Non è necessario estrarre il `_ontap-version_image.tgz` file.

d. Quando `LOADER` richiesto, configurare la connessione netboot per una LIF di gestione:

Se l'indirizzo IP è...	Quindi...
DHCP	Configurare la connessione automatica: <code>ifconfig e0M -auto</code>
Statico	Configurare la connessione manuale: <code>ifconfig e0M -addr=<i>ip_addr</i> - mask=<i>netmask</i> -gw=<i>gateway</i></code>

e. Eseguire il netboot.

```
netboot http://_web_server_ip/path_to_web-accessible_directory/ontap-  
version_image.tgz
```

f. Dal menu di avvio, selezionare l'opzione **(7) installare prima il nuovo software** per scaricare e installare la nuova immagine software sul dispositivo di avvio.

Ignorare il seguente messaggio:

"This procedure is not supported for Non-Disruptive Upgrade on an HA pair". Si applica agli aggiornamenti software senza interruzioni e non agli aggiornamenti dei controller.

a. Se viene richiesto di continuare la procedura, immettere ``y`E` quando viene richiesto il pacchetto, inserire l'URL del file immagine:

```
http://web_server_ip/path_to_web-accessible_directory/ontap-  
version_image.tgz
```

b. Immettere il nome utente e la password, se applicabile, oppure premere Invio per continuare.

c. Assicurarsi di entrare `n` per ignorare il ripristino del backup quando viene visualizzato un prompt simile a quanto segue:

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

d. Riavviare immettendo `y` quando viene visualizzato un prompt simile a quanto segue:

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

Cancellare la configurazione su un modulo controller

Prima di utilizzare un nuovo modulo controller nella configurazione MetroCluster, è necessario cancellare la configurazione esistente.

Fasi

1. Se necessario, arrestare il nodo per visualizzare il `LOADER` prompt:

```
halt
```

2. Quando `LOADER` richiesto, impostare le variabili ambientali sui valori predefiniti:

```
set-defaults
```

3. Salvare l'ambiente:

```
saveenv
```

4. Quando `LOADER` richiesto, avviare il menu di avvio:

```
boot_ontap menu
```

5. Al prompt del menu di avvio, cancellare la configurazione:

```
wipeconfig
```

Rispondere `yes` al prompt di conferma.

Il nodo si riavvia e viene visualizzato di nuovo il menu di avvio.

6. Nel menu di avvio, selezionare l'opzione **5** per avviare il sistema in modalità di manutenzione.

Rispondere `yes` al prompt di conferma.

Verificare lo stato di salute di MetroCluster prima dell'aggiornamento del sito

Prima di eseguire l'aggiornamento, è necessario verificare lo stato e la connettività della configurazione di MetroCluster.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:

- a. Controllare se i nodi sono multipercorso:

```
node run -node <node_name> sysconfig -a
```

Immettere questo comando per ogni nodo nella configurazione MetroCluster.

- b. Verificare che non vi siano dischi rotti nella configurazione:

```
storage disk show -broken
```

Emettere questo comando su ciascun nodo nella configurazione MetroCluster.

- c. Verificare la presenza di eventuali avvisi sullo stato di salute:

```
system health alert show
```

Eeguire questo comando su ciascun cluster.

- d. Verificare le licenze sui cluster:

```
system license show
```

Eeguire questo comando su ciascun cluster.

- e. Verificare i dispositivi collegati ai nodi:

```
network device-discovery show
```

Eeguire questo comando su ciascun cluster.

- f. Verificare che il fuso orario e l'ora siano impostati correttamente su entrambi i siti:

```
cluster date show
```

Eeguire questo comando su ciascun cluster. `cluster date` I comandi consentono di configurare l'ora e il fuso orario.

2. Confermare la modalità operativa della configurazione MetroCluster ed eseguire un controllo MetroCluster.

- a. Confermare la configurazione MetroCluster e che la modalità operativa è normal:

```
metrocluster show
```

- b. Verificare che siano visualizzati tutti i nodi previsti:

```
metrocluster node show
```

- c. Immettere il seguente comando:

```
metrocluster check run
```

- d. Visualizzare i risultati del controllo MetroCluster:

```
metrocluster check show
```

3. Controllare il cablaggio MetroCluster con lo strumento Config Advisor.

- a. Scaricare ed eseguire Config Advisor.

["Download NetApp: Config Advisor"](#)

- b. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

Raccogliere informazioni prima dell'aggiornamento

Prima di eseguire l'aggiornamento, è necessario raccogliere informazioni per ciascuno dei nodi e, se necessario, regolare i domini di broadcast di rete, rimuovere eventuali VLAN e gruppi di interfacce e raccogliere informazioni sulla crittografia.

Fasi

1. Registrare il cablaggio fisico di ciascun nodo, etichettando i cavi secondo necessità per consentire il cablaggio corretto dei nuovi nodi.
2. Raccogliete informazioni di interconnessione, porta e LIF per ciascun nodo.

Raccogliere l'output dei seguenti comandi per ciascun nodo:

- `metrocluster interconnect show`
- `metrocluster configuration-settings connection show`
- `network interface show -role cluster,node-mgmt`
- `network port show -node <node_name> -type physical`
- `network port vlan show -node <node_name>`
- `network port ifgrp show -node <node_name> -instance`
- `network port broadcast-domain show`
- `network port reachability show -detail`
- `network ipspace show`
- `volume show`
- `storage aggregate show`
- `system node run -node <node_name> sysconfig -a`
- `aggr show -r`
- `disk show`
- `system node run <node-name> disk show`
- `vol show -fields type`
- `vol show -fields type , space-guarantee`
- `vserver fcp initiator show`
- `storage disk show`
- `metrocluster configuration-settings interface show`

3. Raccogliere gli UUID per il sito_B (il sito le cui piattaforme sono attualmente in fase di aggiornamento):

```
metrocluster node show -fields node-cluster-uuid, node-uuid
```

Questi valori devono essere configurati con precisione sui nuovi moduli controller Site_B per garantire un aggiornamento corretto. Copiare i valori in un file in modo da poterli copiare nei comandi successivamente nel processo di aggiornamento.

L'esempio seguente mostra l'output del comando con gli UUID:

```

cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
(metrocluster node show)
dr-group-id cluster      node      node-uuid
node-cluster-uuid
-----
1              cluster_A node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1              cluster_A node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1              cluster_B node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1              cluster_B node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::~*

```

NetApp consiglia di registrare gli UUID in una tabella simile alla seguente:

Cluster o nodo	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Node_B_1	f37b240b-9ac1-11e7-9b42-00a098c9e55d
Node_B_2	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A.	ee7db9d5-9a82-11e7-b68b-00a098908039
Node_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039
Node_A_2	aa9a7a7a-9a81-11e7-a4e9-00a098908c35

4. Se i nodi MetroCluster si trovano in una configurazione SAN, raccogliere le informazioni pertinenti.

Raccogliere l'output dei seguenti comandi:

- ° fcp adapter show -instance
- ° fcp interface show -instance
- ° iscsi interface show
- ° ucadm show

5. Se il volume root è crittografato, raccogliere e salvare la passphrase utilizzata per il gestore delle chiavi:

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

6. Se i nodi MetroCluster utilizzano la crittografia per volumi o aggregati, copiare le informazioni relative alle chiavi e alle passphrase.

Per ulteriori informazioni, vedere ["Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate"](#).

- a. Se Onboard Key Manager è configurato:

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

La passphrase è necessaria più avanti nella procedura di aggiornamento.

- b. Se la gestione delle chiavi aziendali (KMIP) è configurata, eseguire i seguenti comandi:

```
security key-manager external show -instance security key-manager key query
```

7. Raccogliere gli ID di sistema dei nodi esistenti:

```
metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
```

Il seguente output mostra i dischi riassegnati.

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
```

dr-group-id	cluster	node	node-systemid	ha-partner-systemid	dr-partner-systemid	dr-auxiliary-systemid
1	cluster_A	node_A_1	537403324	537403323		
537403321		537403322				
1	cluster_A	node_A_2	537403323	537403324		
537403322		537403321				
1	cluster_B	node_B_1	537403322	537403321		
537403323		537403324				
1	cluster_B	node_B_2	537403321	537403322		
537403324		537403323				

4 entries were displayed.

Rimuovere il monitoraggio di Mediator o Tiebreaker

Prima di aggiornare le piattaforme, è necessario rimuovere il monitoraggio se la configurazione MetroCluster viene monitorata con l'utility Tiebreaker o Mediator.

Fasi

1. Raccogliere l'output per il seguente comando:

```
storage iscsi-initiator show
```

2. Rimuovere la configurazione MetroCluster esistente da Tiebreaker, Mediator o altro software in grado di avviare lo switchover.

Se si utilizza...	Utilizzare questa procedura...
Spareggio	"Rimozione delle configurazioni MetroCluster"
Mediatore	Immettere il seguente comando dal prompt di ONTAP: <pre>metrocluster configuration-settings mediator remove</pre>
Applicazioni di terze parti	Consultare la documentazione del prodotto.

Inviare un messaggio AutoSupport personalizzato prima della manutenzione

Prima di eseguire la manutenzione, devi inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Accedere al cluster.
2. Richiamare un messaggio AutoSupport che indica l'inizio della manutenzione:

```
system node autosupport invoke -node * -type all -message MAINT=maintenance-  
window-in-hours
```

Il `maintenance-window-in-hours` parametro specifica la lunghezza della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

3. Ripetere questi passaggi sul sito del partner.

Quali sono le prossime novità?

["Passare alla configurazione MetroCluster"](#).

Informazioni sul copyright

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

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

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

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

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

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

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

Informazioni sul marchio commerciale

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