



# **Procedure di aggiornamento del sistema HCI**

NetApp  
October 22, 2024

This PDF was generated from [https://docs.netapp.com/it-it/hci/docs/task\\_hcc\\_update\\_management\\_services.html](https://docs.netapp.com/it-it/hci/docs/task_hcc_update_management_services.html) on October 22, 2024. Always check docs.netapp.com for the latest.

# Sommario

- Procedure di aggiornamento del sistema . . . . . 1
  - Servizi di gestione degli aggiornamenti . . . . . 1
  - Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage . . . . . 4
  - Aggiornare il software Element . . . . . 9
  - Aggiornare il firmware dello storage. . . . . 20
  - Aggiornare un nodo di gestione . . . . . 30
  - Aggiornare il plug-in Element per vCenter Server . . . . . 33
  - Eseguire i controlli dello stato dei nodi di calcolo prima di aggiornare il firmware di calcolo . . . . . 40
  - Aggiornare i driver dei nodi di calcolo . . . . . 48
  - Aggiornare il firmware del nodo di calcolo . . . . . 49
  - Automatizza gli aggiornamenti del firmware dei nodi di calcolo con Ansible . . . . . 63

# Procedure di aggiornamento del sistema

## Servizi di gestione degli aggiornamenti

È possibile aggiornare i servizi di gestione alla versione più recente del bundle dopo aver installato il nodo di gestione 11.3 o successivo.

A partire dalla release del nodo di gestione Element 11.3, la progettazione del nodo di gestione è stata modificata in base a una nuova architettura modulare che fornisce servizi individuali. Questi servizi modulari offrono funzionalità di gestione centralizzata ed estesa per i sistemi NetApp HCI. I servizi di gestione includono servizi di telemetria, registrazione e aggiornamento del sistema, il servizio QoSSIOC per Element Plug-in per vCenter Server, NetApp Hybrid Cloud Control e molto altro ancora.

### A proposito di questa attività

- Prima di aggiornare il software Element, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente.



- Management Services 2.22.7 include Element Plug-in per vCenter Server 5.0 che contiene il plug-in remoto. Se si utilizza il plug-in Element, è necessario eseguire l'aggiornamento ai servizi di gestione 2.22.7 o versioni successive per rispettare la direttiva VMware che rimuove il supporto per i plug-in locali. ["Scopri di più"](#).
- Per le ultime note di rilascio dei servizi di gestione che descrivono i principali servizi, le nuove funzionalità, le correzioni dei bug e le soluzioni alternative per ciascun bundle di servizi, vedere ["note di rilascio dei servizi di gestione"](#)

### Di cosa hai bisogno

A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare il Contratto di licenza con l'utente finale (EULA) prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare i servizi di gestione:

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

### Opzioni di aggiornamento

Puoi aggiornare i servizi di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control o l'API REST del nodo di gestione:

- [Servizi di gestione degli aggiornamenti con Hybrid Cloud Control](#) (Metodo consigliato)
- [Aggiornare i servizi di gestione utilizzando l'API del nodo di gestione](#)

## Servizi di gestione degli aggiornamenti con Hybrid Cloud Control

Puoi aggiornare i tuoi servizi di gestione NetApp utilizzando NetApp Hybrid Cloud Control.

I bundle di servizi di gestione offrono funzionalità e correzioni avanzate per l'installazione al di fuori delle release principali.

### Prima di iniziare

- Si sta eseguendo il nodo di gestione 11.3 o versione successiva.
- Se si aggiornano i servizi di gestione alla versione 2.16 o successiva e si esegue un nodo di gestione da 11.3 a 11.8, sarà necessario aumentare la RAM della VM del nodo di gestione prima di aggiornare i servizi di gestione:
  - a. Spegnerne la VM del nodo di gestione.
  - b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.
  - c. Accendere la VM del nodo di gestione.
- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.1.326. Gli aggiornamenti di NetApp Hybrid Cloud Control non sono disponibili nei pacchetti di servizi precedenti.



Per un elenco dei servizi disponibili per ciascuna versione del bundle di servizi, vedere ["Note sulla versione di Management Services"](#).

### Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina Upgrades (aggiornamenti), selezionare la scheda **Management Services** (servizi di gestione).
5. Seguire le istruzioni riportate nella pagina per scaricare e salvare un pacchetto di aggiornamento dei servizi di gestione sul computer.
6. Selezionare Browse (Sfoglia) per individuare il pacchetto salvato e caricarlo.

Dopo aver caricato il pacchetto, l'aggiornamento viene avviato automaticamente.

Una volta avviato l'aggiornamento, lo stato dell'aggiornamento viene visualizzato in questa pagina. Durante l'aggiornamento, potresti perdere la connessione con NetApp Hybrid Cloud Control e devi effettuare nuovamente l'accesso per visualizzare i risultati dell'aggiornamento.

## Aggiornare i servizi di gestione utilizzando l'API del nodo di gestione

Gli utenti dovrebbero idealmente eseguire aggiornamenti dei servizi di gestione da NetApp Hybrid Cloud Control. Tuttavia, è possibile caricare, estrarre e distribuire manualmente un aggiornamento del bundle di servizi per i servizi di gestione nel nodo di gestione utilizzando l'API REST. È possibile eseguire ciascun comando dall'interfaccia utente API REST per il nodo di gestione.

## Prima di iniziare

- È stato implementato un nodo di gestione software NetApp Element 11.3 o successivo.
- Se si aggiornano i servizi di gestione alla versione 2.16 o successiva e si esegue un nodo di gestione da 11.3 a 11.8, sarà necessario aumentare la RAM della VM del nodo di gestione prima di aggiornare i servizi di gestione:
  - a. Spegnerne la VM del nodo di gestione.
  - b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.
  - c. Accendere la VM del nodo di gestione.
- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.1.326. Gli aggiornamenti di NetApp Hybrid Cloud Control non sono disponibili nei pacchetti di servizi precedenti.



Per un elenco dei servizi disponibili per ciascuna versione del bundle di servizi, vedere ["Note sulla versione di Management Services"](#).

## Fasi

1. Aprire l'interfaccia utente API REST sul nodo di gestione:

`https://<ManagementNodeIP>/mnode`

2. Selezionare **autorizzare** e completare le seguenti operazioni:
  - a. Inserire il nome utente e la password del cluster.
  - b. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
  - c. Selezionare **autorizzare** per avviare una sessione.
  - d. Chiudere la finestra.
3. Caricare ed estrarre il bundle di servizi sul nodo di gestione utilizzando questo comando: `PUT /services/upload`
4. Implementare i servizi di gestione sul nodo di gestione: `PUT /services/deploy`
5. Monitorare lo stato dell'aggiornamento: `GET /services/update/status`

Un aggiornamento riuscito restituisce un risultato simile al seguente esempio:

```
{
  "current_version": "2.10.29",
  "details": "Updated to version 2.17.52",
  "status": "success"
}
```

## Trova ulteriori informazioni

- ["Plug-in NetApp Element per server vCenter"](#)
- ["Pagina delle risorse NetApp HCI"](#)

# Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

Prima di aggiornare lo storage Element, è necessario eseguire controlli di integrità per assicurarsi che tutti i nodi di storage nel cluster siano pronti per l'upgrade dello storage Element successivo.

## Di cosa hai bisogno

- **Servizi di gestione:** È stato eseguito l'aggiornamento al bundle di servizi di gestione più recente (2.10.27 o versione successiva).



Prima di aggiornare il software Element, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente.

- **Nodo di gestione:** Si sta eseguendo il nodo di gestione 11.3 o successivo.
- **Software Element:** La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- **Contratto di licenza con l'utente finale (EULA):** A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per eseguire i controlli dello stato dello storage Element:
  - a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

- b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
- c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
- d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

## Opzioni di controllo dello stato di salute

È possibile eseguire i controlli dello stato di salute utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control o l'API di NetApp Hybrid Cloud Control:

- [Utilizza NetApp Hybrid Cloud Control per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage](#) (Metodo preferito)
- [Utilizzare l'API per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage](#)

Per ulteriori informazioni sui controlli dello stato dello storage eseguiti dal servizio, consultare:

- [Controlli dello stato dello storage eseguiti dal servizio](#)

## Utilizza NetApp Hybrid Cloud Control per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

Utilizzando NetApp Hybrid Cloud Control (HCC), è possibile verificare che un cluster di storage sia pronto per l'aggiornamento.

## Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare la scheda **Storage**.
5. Selezionare il controllo dello stato di salute  per il cluster che si desidera controllare per verificare la disponibilità all'aggiornamento.
6. Nella pagina **Storage Health Check**, selezionare **Run Health Check**.
7. In caso di problemi, procedere come segue:
  - a. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata.
  - b. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.
  - c. Una volta risolti i problemi del cluster, selezionare **Riesegui controllo stato di salute**.

Una volta completato il controllo dello stato di salute senza errori, il cluster di storage è pronto per l'aggiornamento. Vedere aggiornamento del nodo di storage ["istruzioni"](#) per procedere.

## Utilizzare l'API per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

È possibile utilizzare REST API per verificare che un cluster di storage sia pronto per l'aggiornamento. Il controllo dello stato di salute verifica che non vi siano ostacoli all'aggiornamento, ad esempio nodi in sospeso, problemi di spazio su disco e guasti del cluster.

## Fasi

1. Individuare l'ID del cluster di storage:
  - a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/mnode
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:
  - i. Inserire il nome utente e la password del cluster.
  - ii. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
  - iii. Selezionare **autorizzare** per avviare una sessione.
  - iv. Chiudere la finestra di autorizzazione.
- c. Dall'interfaccia utente API REST, selezionare `GET /assets`.
- d. Selezionare **Provalo**.

e. Selezionare **Esegui**.

f. Dalla risposta, copiare "id" dal "storage" sezione del cluster che si intende controllare per verificare la disponibilità all'aggiornamento.



Non utilizzare "parent" Valore in questa sezione perché si tratta dell'ID del nodo di gestione, non dell'ID del cluster di storage.

```
"config": {},  
"credentialid": "12bbb2b2-f1be-123b-1234-12c3d4bc123e",  
"host_name": "SF_DEMO",  
"id": "12cc3a45-e6e7-8d91-a2bb-0bdb3456b789",  
"ip": "10.123.12.12",  
"parent": "d123ec42-456e-8912-ad3e-4bd56f4a789a",  
"sshcredentialid": null,  
"ssl_certificate": null
```

2. Eseguire i controlli di integrità sul cluster di storage:

a. Aprire l'interfaccia utente dell'API REST dello storage sul nodo di gestione:

```
https://<ManagementNodeIP>/storage/1/
```

b. Selezionare **autorizzare** e completare le seguenti operazioni:

- i. Inserire il nome utente e la password del cluster.
- ii. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
- iii. Selezionare **autorizzare** per avviare una sessione.
- iv. Chiudere la finestra di autorizzazione.

c. Selezionare **POST /Health-checks**.

d. Selezionare **Provalo**.

e. Nel campo Parameter (parametro), inserire l'ID del cluster di storage ottenuto nella fase 1.

```
{  
  "config": {},  
  "storageId": "123a45b6-1a2b-12a3-1234-1a2b34c567d8"  
}
```

f. Selezionare **Esegui** per eseguire un controllo dello stato di salute sul cluster di storage specificato.

La risposta deve indicare lo stato come `initializing`:



```
{
  "_links": {
    "collection": "https://10.117.149.231/storage/1/health-checks",
    "log": "https://10.117.149.231/storage/1/health-checks/358f073f-896e-4751-ab7b-ccbb5f61f9fc/log",
    "self": "https://10.117.149.231/storage/1/health-checks/358f073f-896e-4751-ab7b-ccbb5f61f9fc"
  },
  "config": {},
  "dateCompleted": null,
  "dateCreated": "2020-02-21T22:11:15.476937+00:00",
  "healthCheckId": "358f073f-896e-4751-ab7b-ccbb5f61f9fc",
  "state": "initializing",
  "status": null,
  "storageId": "c6d124b2-396a-4417-8a47-df10d647f4ab",
  "taskId": "73f4df64-bda5-42c1-9074-b4e7843dbb77"
}
```

a. Copiare il `healthCheckId` ciò fa parte della risposta.

3. Verificare i risultati dei controlli di stato:

- a. Selezionare **GET /Health-checks/{healthCheckId}**.
- b. Selezionare **Provalo**.
- c. Inserire l'ID del controllo di salute nel campo dei parametri.
- d. Selezionare **Esegui**.
- e. Scorrere fino alla parte inferiore del corpo della risposta.

Se tutti i controlli di integrità hanno esito positivo, il reso è simile al seguente esempio:

```
"message": "All checks completed successfully.",
"percent": 100,
"timestamp": "2020-03-06T00:03:16.321621Z"
```

4. Se il message la restituzione indica la presenza di problemi relativi allo stato del cluster, procedere come segue:

- a. Selezionare **GET /Health-checks/{healthCheckId}/log**
- b. Selezionare **Provalo**.
- c. Inserire l'ID del controllo di salute nel campo dei parametri.
- d. Selezionare **Esegui**.
- e. Esaminare eventuali errori specifici e ottenere i relativi collegamenti agli articoli della Knowledge base.
- f. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata.

- g. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.
- h. Dopo aver risolto i problemi del cluster, eseguire di nuovo **GET /Health-checks/{healthCheckId}/log**.

## Controlli dello stato dello storage eseguiti dal servizio

I controlli dello stato dello storage effettuano i seguenti controlli per cluster.

Selezionare Nome	Nodo/cluster	Descrizione
check_async_results	Cluster	Verifica che il numero di risultati asincroni nel database sia inferiore a un numero di soglia.
check_cluster_faults	Cluster	Verifica che non vi siano errori del cluster che bloccano l'aggiornamento (come definito nell'origine dell'elemento).
check_upload_speed	Nodo	Misura la velocità di caricamento tra il nodo di storage e il nodo di gestione.
connection_speed_check	Nodo	Verifica che i nodi dispongano di connettività al nodo di gestione che fornisce pacchetti di aggiornamento e stima la velocità di connessione.
check_core	Nodo	Verifica la presenza di un crash dump del kernel e dei file core sul nodo. Il controllo non riesce per eventuali crash in un periodo di tempo recente (soglia 7 giorni).
check_root_disk_space	Nodo	Verifica che il file system root disponga di spazio libero sufficiente per eseguire un aggiornamento.
check_var_log_disk_space	Nodo	Lo verifica /var/log lo spazio libero soddisfa una certa soglia percentuale di spazio libero. In caso contrario, il controllo ruota e elimina i registri meno recenti per scendere sotto la soglia. Il controllo non riesce se non riesce a creare spazio libero sufficiente.
check_pending_nodes	Cluster	Verifica che non vi siano nodi in sospeso nel cluster.

## Trova ulteriori informazioni

- ["Plug-in NetApp Element per server vCenter"](#)
- ["Pagina delle risorse NetApp HCI"](#)

# Aggiornare il software Element

Per aggiornare il software NetApp Element, è possibile utilizzare l'interfaccia utente di controllo del cloud ibrido NetApp o l'API REST. Alcune operazioni vengono soppresse durante l'aggiornamento di un software Element, ad esempio l'aggiunta e la rimozione di nodi, l'aggiunta e la rimozione di dischi e i comandi associati a iniziatori, gruppi di accesso ai volumi e reti virtuali.



A partire da Element 12.5, NetApp HealthTools non è più supportato per gli aggiornamenti del software Element. Se si esegue Element 11.0 o 11.1, è necessario prima ["Eseguire l'aggiornamento a Element 12.3 utilizzando HealthTools"](#) E quindi eseguire l'aggiornamento a Element 12.5 o versioni successive utilizzando NetApp Hybrid Cloud Control.

## Di cosa hai bisogno

- **Privilegi di amministratore:** Si dispone delle autorizzazioni di amministratore del cluster di storage per eseguire l'aggiornamento.
- **Percorso di aggiornamento valido:** Sono state verificate le informazioni sul percorso di aggiornamento per la versione dell'elemento a cui si sta eseguendo l'aggiornamento e il percorso di aggiornamento è valido. Vedere ["KB di NetApp: Matrice di aggiornamento per cluster di storage che eseguono il software NetApp Element"](#)
- **System Time Sync:** Hai garantito che l'ora di sistema su tutti i nodi sia sincronizzata e che NTP sia configurato correttamente per il cluster di storage e i nodi. Ciascun nodo deve essere configurato con un server dei nomi DNS nell'interfaccia utente Web per nodo (`https://[IP address]:442`) senza errori del cluster irrisolti correlati all'inclinazione temporale.
- **Porte di sistema:** Se si utilizza NetApp Hybrid Cloud Control per gli aggiornamenti, si è assicurati che le porte necessarie siano aperte. Vedere ["Porte di rete"](#) per ulteriori informazioni.
- **Nodo di gestione:** Per l'interfaccia utente e l'API di NetApp Hybrid Cloud Control, il nodo di gestione nel tuo ambiente esegue la versione 11.3.
- **Servizi di gestione:** Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente.



È necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente prima di aggiornare il software Element alla versione 12.5 o successiva. Se si sta aggiornando il software Element alla versione 12.5 o successiva, per procedere sono necessari i servizi di gestione 2.21.61 o successiva.

- **Cluster Health:** Hai verificato che il cluster è pronto per l'aggiornamento. Vedere ["Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage"](#).
- **Baseboard Management Controller (BMC) aggiornato per i nodi H610S:** È stata aggiornata la versione BMC per i nodi H610S. Vedere ["note di rilascio e istruzioni per l'aggiornamento"](#).
- **Upgrade Process Time** (tempo di aggiornamento): È stato pianificato un tempo sufficiente per eseguire l'aggiornamento. Quando si esegue l'aggiornamento al software Element 12.5 o versione successiva, il tempo di aggiornamento varia in base alla versione corrente del software Element e agli aggiornamenti del firmware.

Nodo di storage	Versione corrente del software Element	Tempo approssimativo di installazione di software e firmware per nodo <sup>1</sup>	Tempo approssimativo di sincronizzazione dei dati per nodo <sup>2</sup>	Tempo di aggiornamento totale approssimativo per nodo
Tutti i nodi SolidFire e NetApp serie H con firmware aggiornato	12.x	15 minuti	da 10 a 15 minuti	da 20 a 30 minuti
H610S e H410S	12.x e 11.8	60 minuti	da 30 a 60 minuti	da 90 a 120 minuti
H610S	11.7 e versioni precedenti	90 minuti	da 40 a 70 minuti	Da 130 a 160 minuti "eseguire uno spegnimento completo del nodo e lo scollegamento dell'alimentazione" Per ogni nodo H610S.

<sup>1</sup>per una matrice completa di firmware e firmware del driver per l'hardware, vedere "[Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI](#)".

<sup>2</sup>se si combina un cluster con un carico IOPS in scrittura pesante con un tempo di aggiornamento del firmware più lungo, il tempo di sincronizzazione dei dati aumenterà.

- **Contratto di licenza con l'utente finale (EULA):** A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare il software Element:

- a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

- b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
- c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
- d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

### Opzioni di upgrade

Scegliere una delle seguenti opzioni di aggiornamento del software Element:

- [Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare lo storage Element](#)
- [Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare lo storage degli elementi](#)



Se si sta aggiornando un nodo della serie H610S a Element 12.5 o versione successiva e il nodo esegue una versione del software Element precedente alla 11.8, sarà necessario eseguire le procedure di aggiornamento aggiuntive descritte in questo documento ["Articolo della Knowledge base"](#) per ciascun nodo di storage. Se si esegue Element 11.8 o versioni successive, non sono necessarie ulteriori procedure di aggiornamento.

## Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare lo storage Element

Utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control, è possibile aggiornare un cluster di storage.



Per i potenziali problemi durante l'aggiornamento dei cluster di storage utilizzando NetApp Hybrid Cloud Control e le relative soluzioni alternative, consulta questo articolo ["Articolo della Knowledge base"](#).

### Fasi




1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare **Storage**.

La scheda **Storage** elenca i cluster di storage che fanno parte dell'installazione. Se un cluster non è accessibile da NetApp Hybrid Cloud Control, non verrà visualizzato nella pagina **Upgrade**.

5. Scegliere una delle seguenti opzioni ed eseguire la serie di passaggi applicabili al cluster:

Opzione	Fasi
Tutti i cluster che eseguono Element 11.8 e versioni successive	<p>a. Selezionare <b>Sfoglia</b> per caricare il pacchetto di aggiornamento scaricato.</p> <p>b. Attendere il completamento del caricamento. Una barra di avanzamento mostra lo stato del caricamento.</p> <div data-bbox="922 415 976 468">  </div> <div data-bbox="1036 390 1414 489"> <p>Se ci si allontana dalla finestra del browser, il caricamento del file viene perso.</p> </div> <p>Una volta caricato e validato il file, viene visualizzato un messaggio sullo schermo. La convalida potrebbe richiedere alcuni minuti. Se in questa fase ci si allontana dalla finestra del browser, il caricamento del file viene preservato.</p> <p>c. Selezionare <b>Avvia aggiornamento</b>.</p> <div data-bbox="922 961 976 1014">  </div> <div data-bbox="1036 814 1442 1155"> <p>Lo stato dell'aggiornamento viene modificato durante l'aggiornamento per riflettere lo stato del processo. Cambia anche in risposta alle azioni intraprese, come la sospensione dell'aggiornamento o se l'aggiornamento restituisce un errore. Vedere <a href="#">Lo stato dell'aggiornamento cambia</a>.</p> </div> <div data-bbox="922 1388 976 1440">  </div> <div data-bbox="1036 1209 1458 1619"> <p>Mentre l'aggiornamento è in corso, è possibile uscire dalla pagina e tornare ad essa in un secondo momento per continuare a monitorare i progressi. La pagina non aggiorna dinamicamente lo stato e la versione corrente se la riga del cluster viene compressa. La riga del cluster deve essere espansa per aggiornare la tabella oppure è possibile aggiornare la pagina.</p> </div> <p>Una volta completato l'aggiornamento, è possibile scaricare i registri.</p>

Opzione	Fasi
Si sta eseguendo l'aggiornamento di un cluster H610S con una versione di Element precedente alla 11.8.	<p>a. Selezionare la freccia verso il basso accanto al cluster che si sta aggiornando e scegliere una delle versioni di aggiornamento disponibili.</p> <p>b. Selezionare <b>Avvia aggiornamento</b>. Una volta completato l'aggiornamento, l'interfaccia utente richiede di eseguire ulteriori passaggi di aggiornamento.</p> <p>c. Completare i passaggi aggiuntivi richiesti in <a href="#">"Articolo della Knowledge base"</a> e riconoscere nell'interfaccia utente che sono stati completati.</p> <p>Una volta completato l'aggiornamento, è possibile scaricare i registri. Per informazioni sulle varie modifiche dello stato dell'aggiornamento, vedere <a href="#">Lo stato dell'aggiornamento cambia</a>.</p>

## Lo stato dell'aggiornamento cambia

Di seguito sono riportati i diversi stati visualizzati nella colonna **Upgrade Status** (Stato aggiornamento) dell'interfaccia utente prima, durante e dopo il processo di aggiornamento:

Stato di aggiornamento	Descrizione
Aggiornato	Il cluster è stato aggiornato alla versione più recente di Element disponibile.
Versioni disponibili	Le versioni più recenti del firmware per elementi e/o storage sono disponibili per l'aggiornamento.
In corso	L'aggiornamento è in corso. Una barra di avanzamento mostra lo stato dell'aggiornamento. I messaggi a schermo mostrano anche gli errori a livello di nodo e visualizzano l'ID di ogni nodo nel cluster durante l'aggiornamento. È possibile monitorare lo stato di ciascun nodo utilizzando l'interfaccia utente Element o il plug-in NetApp Element per l'interfaccia utente del server vCenter.
Aggiornamento in pausa	È possibile scegliere di sospendere l'aggiornamento. A seconda dello stato del processo di aggiornamento, l'operazione di pausa può avere esito positivo o negativo. Viene visualizzato un prompt dell'interfaccia utente che richiede di confermare l'operazione di pausa. Per garantire che il cluster si trovi in una posizione sicura prima di mettere in pausa un aggiornamento, l'operazione di aggiornamento può richiedere fino a due ore. Per riprendere l'aggiornamento, selezionare <b>Riprendi</b> .
In pausa	L'aggiornamento è stato sospeso. Selezionare <b>Riprendi</b> per riprendere il processo.

Stato di aggiornamento	Descrizione
Errore	Si è verificato un errore durante l'aggiornamento. È possibile scaricare il registro degli errori e inviarlo al supporto NetApp. Dopo aver risolto l'errore, tornare alla pagina e selezionare <b>Riprendi</b> . Quando si riprende l'aggiornamento, la barra di avanzamento si sposta indietro per alcuni minuti mentre il sistema esegue il controllo dello stato di salute e verifica lo stato corrente dell'aggiornamento.
Completo di follow-up	Solo per l'aggiornamento dei nodi H610S dalla versione Element precedente alla 11.8. Una volta completata la fase 1 del processo di aggiornamento, questo stato richiede di eseguire ulteriori passaggi di aggiornamento (vedere la " <a href="#">Articolo della Knowledge base</a> "). Dopo aver completato questi passaggi aggiuntivi e aver accettato di averlo completato, lo stato diventa <b>aggiornato</b> .

## Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare lo storage degli elementi

È possibile utilizzare le API per aggiornare i nodi di storage in un cluster alla versione più recente del software Element. È possibile utilizzare uno strumento di automazione a scelta per eseguire le API. Il flusso di lavoro API qui documentato utilizza l'interfaccia utente REST API disponibile sul nodo di gestione come esempio.

### Fasi

1. Scaricare il pacchetto di aggiornamento dello storage su un dispositivo accessibile al nodo di gestione; accedere al software NetApp HCI "[pagina download](#)" e scaricare l'immagine più recente del nodo di storage.
2. Caricare il pacchetto di aggiornamento dello storage nel nodo di gestione:
  - a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/package-repository/1/
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:
  - i. Inserire il nome utente e la password del cluster.
  - ii. Immettere l'ID client come `mnode-client`.
  - iii. Selezionare **autorizzare** per avviare una sessione.
  - iv. Chiudere la finestra di autorizzazione.
- c. Dall'interfaccia utente API REST, selezionare **POST /packages**.
- d. Selezionare **Provalo**.
- e. Selezionare **Sfoglia** e selezionare il pacchetto di aggiornamento.
- f. Selezionare **Esegui** per avviare il caricamento.
- g. Dalla risposta, copiare e salvare l'ID del pacchetto ("`id`") da utilizzare in un passaggio successivo.



3. Verificare lo stato del caricamento.

- a. Dall'interfaccia utente API REST, selezionare **GET /packages/{id}/status**.
- b. Selezionare **Provalo**.
- c. Inserire l'ID del pacchetto copiato nel passaggio precedente in **id**.
- d. Selezionare **Esegui** per avviare la richiesta di stato.

La risposta indica `state` come `SUCCESS` al termine dell'operazione.

4. Individuare l'ID del cluster di storage:

- a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:
  - i. Inserire il nome utente e la password del cluster.
  - ii. Immettere l'ID client come `mnode-client`.
  - iii. Selezionare **autorizzare** per avviare una sessione.
  - iv. Chiudere la finestra di autorizzazione.
- c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
- d. Selezionare **Provalo**.
- e. Selezionare **Esegui**.
- f. Dalla risposta, copiare l'ID della risorsa di installazione ("`id`").
- g. Dall'interfaccia utente API REST, selezionare **GET /Installations/{id}**.
- h. Selezionare **Provalo**.
  - i. Incollare l'ID della risorsa di installazione nel campo **id**.
  - j. Selezionare **Esegui**.
- k. Dalla risposta, copiare e salvare l'ID del cluster di storage ("`id`") del cluster che si intende aggiornare per utilizzarlo in un secondo momento.

5. Eseguire l'aggiornamento dello storage:

- a. Aprire l'interfaccia utente dell'API REST dello storage sul nodo di gestione:

```
https://<ManagementNodeIP>/storage/1/
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:
  - i. Inserire il nome utente e la password del cluster.
  - ii. Immettere l'ID client come `mnode-client`.
  - iii. Selezionare **autorizzare** per avviare una sessione.
  - iv. Chiudere la finestra di autorizzazione.

- c. Selezionare **POST /upgrade**.
- d. Selezionare **Provalo**.
- e. Inserire l'ID del pacchetto di aggiornamento nel campo dei parametri.
- f. Inserire l'ID del cluster di storage nel campo dei parametri.

Il payload dovrebbe essere simile al seguente esempio:

```
{
  "config": {},
  "packageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4",
  "storageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4"
}
```

- g. Selezionare **Esegui** per avviare l'aggiornamento.

La risposta deve indicare lo stato come initializing:

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-b3fc-2c963f66abc1",
    "log": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-b3fc-2c963f66abc1/log"
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055`-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
    "percent": 0,
    "step": "ClusterPreStart",
  }
}
```

```
"timestamp": "2020-04-21T22:10:57.057Z",
"failedHealthChecks": [
  {
    "checkID": 0,
    "name": "string",
    "displayName": "string",
    "passed": true,
    "kb": "string",
    "description": "string",
    "remedy": "string",
    "severity": "string",
    "data": {},
    "nodeID": 0
  }
],
"taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
"dateCompleted": "2020-04-21T22:10:57.057Z",
"dateCreated": "2020-04-21T22:10:57.057Z"
}
```

- a. Copiare l'ID dell'aggiornamento ("upgradeId") che fa parte della risposta.
6. Verificare l'avanzamento e i risultati dell'aggiornamento:
- a. Selezionare **GET /upgrades/{upgradeld}**.
  - b. Selezionare **Provalo**.
  - c. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeld**.
  - d. Selezionare **Esegui**.
  - e. In caso di problemi o requisiti speciali durante l'aggiornamento, eseguire una delle seguenti operazioni:

Opzione	Fasi
È necessario correggere i problemi di integrità del cluster dovuti a. <code>failedHealthChecks</code> messaggio nel corpo della risposta.	<p>i. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata.</p> <p>ii. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.</p> <p>iii. Una volta risolti i problemi del cluster, eseguire nuovamente l'autenticazione, se necessario, e selezionare <b>PUT /upgrades/{upgradeld}</b>.</p> <p>iv. Selezionare <b>Provalo</b>.</p> <p>v. Inserire l'ID dell'aggiornamento del passaggio precedente in <b>upgradeld</b>.</p> <p>vi. Invio <code>"action": "resume"</code> nel corpo della richiesta.</p> <pre>{   "action": "resume" }</pre> <p>vii. Selezionare <b>Esegui</b>.</p>
È necessario sospendere l'aggiornamento perché la finestra di manutenzione si sta chiudendo o per un altro motivo.	<p>i. Se necessario, eseguire nuovamente l'autenticazione e selezionare <b>PUT /upgrades/{upgradeld}</b>.</p> <p>ii. Selezionare <b>Provalo</b>.</p> <p>iii. Inserire l'ID dell'aggiornamento del passaggio precedente in <b>upgradeld</b>.</p> <p>iv. Invio <code>"action": "pause"</code> nel corpo della richiesta.</p> <pre>{   "action": "pause" }</pre> <p>v. Selezionare <b>Esegui</b>.</p>

Opzione	Fasi
Se si sta aggiornando un cluster H610S con una versione di Element precedente alla 11.8, viene visualizzato lo stato <code>finishedNeedsAck</code> nel corpo di risposta. È necessario eseguire ulteriori passaggi di aggiornamento per ciascun nodo di storage H610S.	<p>i. Completare i passaggi aggiuntivi di aggiornamento descritti in questo documento <a href="#">"Articolo della Knowledge base"</a> per ogni nodo.</p> <p>ii. Se necessario, eseguire nuovamente l'autenticazione e selezionare <b>PUT /upgrades/{upgradeld}</b>.</p> <p>iii. Selezionare <b>Provalo</b>.</p> <p>iv. Inserire l'ID dell'aggiornamento del passaggio precedente in <code>upgradeld</code>.</p> <p>v. Invio <code>"action": "acknowledge"</code> nel corpo della richiesta.</p> <pre>{   "action": "acknowledge" }</pre> <p>vi. Selezionare <b>Esegui</b>.</p>

- f. Eseguire l'API **GET /upgrades/{upgradeld}** più volte, in base alle necessità, fino al completamento del processo.

Durante l'aggiornamento, il `status` indica `running` se non si riscontrano errori. Man mano che ogni nodo viene aggiornato, il `step` il valore cambia in `NodeFinished`.

L'aggiornamento è stato completato correttamente quando `percent` il valore è 100 e `a. state` indica `finished`.

## Cosa succede se un aggiornamento non riesce utilizzando NetApp Hybrid Cloud Control

In caso di guasto di un disco o di un nodo durante un aggiornamento, l'interfaccia utente dell'elemento visualizza gli errori del cluster. Il processo di aggiornamento non passa al nodo successivo e attende la risoluzione dei guasti del cluster. La barra di avanzamento nell'interfaccia utente mostra che l'aggiornamento è in attesa della risoluzione degli errori del cluster. In questa fase, la selezione di **Pausa** nell'interfaccia utente non funzionerà, perché l'aggiornamento attende che il cluster sia integro. Sarà necessario contattare il supporto NetApp per fornire assistenza durante l'indagine sul guasto.

NetApp Hybrid Cloud Control dispone di un periodo di attesa di tre ore preimpostato, durante il quale può verificarsi uno dei seguenti scenari:

- Gli errori del cluster vengono risolti entro tre ore e l'aggiornamento riprende. In questo scenario non è necessario eseguire alcuna azione.
- Il problema persiste dopo tre ore e lo stato dell'aggiornamento visualizza **Error** (errore) con un banner rosso. Una volta risolto il problema, è possibile riprendere l'aggiornamento selezionando **Riprendi**.

- Il supporto NetApp ha stabilito che l'aggiornamento deve essere temporaneamente interrotto per intraprendere un'azione correttiva prima della finestra di tre ore. Il supporto utilizzerà l'API per interrompere l'aggiornamento.



L'interruzione dell'aggiornamento del cluster durante l'aggiornamento di un nodo potrebbe causare la rimozione dei dischi dal nodo. Se i dischi vengono rimossi in modo non corretto, l'aggiunta dei dischi durante un aggiornamento richiederà l'intervento manuale del supporto NetApp. Il nodo potrebbe richiedere più tempo per eseguire gli aggiornamenti del firmware o le attività di sincronizzazione post-aggiornamento. Se l'aggiornamento sembra bloccato, contattare il supporto NetApp per assistenza.

## Trova ulteriori informazioni

- ["Plug-in NetApp Element per server vCenter"](#)
- ["Pagina delle risorse NetApp HCI"](#)

## Aggiornare il firmware dello storage

A partire da Element 12.0 e dalla versione 2.14 dei servizi di gestione, è possibile eseguire aggiornamenti solo firmware sui nodi di storage utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control e l'API REST. Questa procedura non aggiorna il software Element e consente di aggiornare il firmware dello storage al di fuori di una release elemento principale.

### Di cosa hai bisogno

- **Privilegi di amministratore:** Si dispone delle autorizzazioni di amministratore del cluster di storage per eseguire l'aggiornamento.
- **System Time Sync:** Hai garantito che l'ora di sistema su tutti i nodi sia sincronizzata e che NTP sia configurato correttamente per il cluster di storage e i nodi. Ciascun nodo deve essere configurato con un server dei nomi DNS nell'interfaccia utente Web per nodo (`https://[IP address]:442`) senza errori del cluster irrisolti correlati all'inclinazione temporale.
- **Porte di sistema:** Se si utilizza NetApp Hybrid Cloud Control per gli aggiornamenti, si è assicurati che le porte necessarie siano aperte. Vedere ["Porte di rete"](#) per ulteriori informazioni.
- **Nodo di gestione:** Per l'interfaccia utente e l'API di NetApp Hybrid Cloud Control, il nodo di gestione nel tuo ambiente esegue la versione 11.3.
- **Servizi di gestione:** Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente.



Per i nodi di storage H610S che eseguono il software Element versione 12.0, applicare D-patch SUST-909 prima di eseguire l'aggiornamento al bundle firmware di storage 2.27. Contattare il supporto NetApp per ottenere la D-patch prima di eseguire l'aggiornamento. Vedere ["Note sulla versione di Storage firmware Bundle 2.27"](#).



Prima di aggiornare il firmware sui nodi di storage, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente. Se si sta aggiornando il software Element alla versione 12.2 o successiva, per procedere sono necessari i servizi di gestione 2.14.60 o successiva.



Per aggiornare il firmware iDRAC/BIOS, contattare il supporto NetApp. Per ulteriori informazioni, consultare questa sezione ["Articolo della Knowledge base"](#).

- **Cluster Health:** Sono stati eseguiti controlli di integrità. Vedere ["Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage"](#).
- **Baseboard Management Controller (BMC) aggiornato per i nodi H610S:** È stata aggiornata la versione BMC per i nodi H610S. Vedere ["note di rilascio e istruzioni per l'aggiornamento"](#).



Per una matrice completa di firmware e firmware del driver per l'hardware, vedere ["Versioni firmware supportate per i nodi di storage NetApp HCI"](#).

- **Upgrade Process Time** (tempo di aggiornamento): È stato pianificato un tempo sufficiente per eseguire l'aggiornamento. Quando si esegue l'aggiornamento al software Element 12.5 o versione successiva, il tempo di aggiornamento varia in base alla versione corrente del software Element e agli aggiornamenti del firmware.

Nodo di storage	Versione corrente del software Element	Tempo approssimativo di installazione di software e firmware per nodo <sup>1</sup>	Tempo approssimativo di sincronizzazione dei dati per nodo <sup>2</sup>	Tempo di aggiornamento totale approssimativo per nodo
Tutti i nodi SolidFire e NetApp serie H con firmware aggiornato	12.x	15 minuti	da 10 a 15 minuti	da 20 a 30 minuti
H610S e H410S	12.x e 11.8	60 minuti	da 30 a 60 minuti	da 90 a 120 minuti
H610S	11.7 e versioni precedenti	90 minuti	da 40 a 70 minuti	Da 130 a 160 minuti <a href="#">"eseguire uno spegnimento completo del nodo e lo scollegamento dell'alimentazione"</a> Per ogni nodo H610S.

<sup>1</sup>per una matrice completa di firmware e firmware del driver per l'hardware, vedere ["Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"](#).

<sup>2</sup>se si combina un cluster con un carico IOPS in scrittura pesante con un tempo di aggiornamento del firmware più lungo, il tempo di sincronizzazione dei dati aumenterà.

- **Contratto di licenza con l'utente finale (EULA):** A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare il firmware dello storage:
  - a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

`https://<ManagementNodeIP>`

- b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
- c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
- d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

### Opzioni di upgrade

Scegliere una delle seguenti opzioni di aggiornamento del firmware dello storage:

- [Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware dello storage](#)
- [Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare il firmware dello storage](#)

## Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware dello storage

È possibile utilizzare l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware dei nodi di storage nel cluster.

### Di cosa hai bisogno

Se il nodo di gestione non è connesso a Internet "[Scaricato il pacchetto firmware dello storage per i cluster di storage NetApp HCI](#)".



Per i potenziali problemi durante l'aggiornamento dei cluster di storage utilizzando NetApp Hybrid Cloud Control e le relative soluzioni alternative, consulta questo articolo "[Articolo della Knowledge base](#)".



Il processo di aggiornamento richiede circa 30 minuti per nodo di storage. Se si sta aggiornando un cluster di storage Element a un firmware di storage più recente della versione 2.76, i singoli nodi di storage si riavvieranno durante l'aggiornamento solo se è stato scritto un nuovo firmware nel nodo.

### Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare **Storage**.





La scheda **Storage** elenca i cluster di storage che fanno parte dell'installazione. Se un cluster non è accessibile da NetApp Hybrid Cloud Control, non verrà visualizzato nella pagina **Upgrade**. Se si utilizzano cluster con Element 12.0 o versioni successive, viene visualizzata la versione corrente del bundle firmware per questi cluster. Se i nodi di un singolo cluster dispongono di versioni firmware diverse o durante il processo di aggiornamento, nella colonna **versione corrente del bundle del firmware** verrà visualizzato **multiplo**. È possibile selezionare **multipli** per accedere alla pagina **nodi** e confrontare le versioni del firmware. Se tutti i cluster eseguono versioni di Element precedenti alla 12.0, non verranno visualizzate informazioni relative ai numeri di versione del bundle del firmware. Queste informazioni sono disponibili anche nella pagina **nodi**. Vedere ["Visualizza l'inventario"](#).

Se il cluster è aggiornato e/o non sono disponibili pacchetti di aggiornamento, le schede **Element** e **firmware only** non vengono visualizzate. Queste schede non vengono visualizzate anche quando è in corso un aggiornamento. Se viene visualizzata la scheda **Element**, ma non la scheda **firmware only**, non sono disponibili pacchetti firmware.

5. Selezionare la freccia verso il basso accanto al cluster che si sta aggiornando.
6. Selezionare **Sfoglia** per caricare il pacchetto di aggiornamento scaricato.
7. Attendere il completamento del caricamento. Una barra di avanzamento mostra lo stato del caricamento.



Se ci si allontana dalla finestra del browser, il caricamento del file viene perso.

Una volta caricato e validato il file, viene visualizzato un messaggio sullo schermo. La convalida potrebbe richiedere alcuni minuti. Se in questa fase ci si allontana dalla finestra del browser, il caricamento del file viene preservato.

8. Selezionare **solo firmware** e scegliere una delle versioni di aggiornamento disponibili.
9. Selezionare **Avvia aggiornamento**.



Lo stato dell'aggiornamento viene modificato durante l'aggiornamento per riflettere lo stato del processo. Cambia anche in risposta alle azioni intraprese, come la sospensione dell'aggiornamento o se l'aggiornamento restituisce un errore. Vedere [Lo stato dell'aggiornamento cambia](#).



Mentre l'aggiornamento è in corso, è possibile uscire dalla pagina e tornare ad essa in un secondo momento per continuare a monitorare i progressi. La pagina non aggiorna dinamicamente lo stato e la versione corrente se la riga del cluster viene compressa. La riga del cluster deve essere espansa per aggiornare la tabella oppure è possibile aggiornare la pagina.

Una volta completato l'aggiornamento, è possibile scaricare i registri.

## Lo stato dell'aggiornamento cambia

Di seguito sono riportati i diversi stati visualizzati nella colonna **Upgrade Status** (Stato aggiornamento) dell'interfaccia utente prima, durante e dopo il processo di aggiornamento:

Stato di aggiornamento	Descrizione
Aggiornato	Il cluster è stato aggiornato alla versione più recente disponibile di Element o il firmware è stato aggiornato alla versione più recente.
Impossibile rilevare	Questo stato viene visualizzato quando l'API del servizio di storage restituisce uno stato di aggiornamento non presente nell'elenco degli stati di aggiornamento possibili.
Versioni disponibili	Le versioni più recenti del firmware per elementi e/o storage sono disponibili per l'aggiornamento.
In corso	L'aggiornamento è in corso. Una barra di avanzamento mostra lo stato dell'aggiornamento. I messaggi a schermo mostrano anche gli errori a livello di nodo e visualizzano l'ID di ogni nodo nel cluster durante l'aggiornamento. È possibile monitorare lo stato di ciascun nodo utilizzando l'interfaccia utente Element o il plug-in NetApp Element per l'interfaccia utente del server vCenter.
Aggiornamento in pausa	È possibile scegliere di sospendere l'aggiornamento. A seconda dello stato del processo di aggiornamento, l'operazione di pausa può avere esito positivo o negativo. Viene visualizzato un prompt dell'interfaccia utente che richiede di confermare l'operazione di pausa. Per garantire che il cluster si trovi in una posizione sicura prima di mettere in pausa un aggiornamento, l'operazione di aggiornamento può richiedere fino a due ore. Per riprendere l'aggiornamento, selezionare <b>Riprendi</b> .
In pausa	L'aggiornamento è stato sospeso. Selezionare <b>Riprendi</b> per riprendere il processo.
Errore	Si è verificato un errore durante l'aggiornamento. È possibile scaricare il registro degli errori e inviarlo al supporto NetApp. Dopo aver risolto l'errore, tornare alla pagina e selezionare <b>Riprendi</b> . Quando si riprende l'aggiornamento, la barra di avanzamento si sposta indietro per alcuni minuti mentre il sistema esegue il controllo dello stato di salute e verifica lo stato corrente dell'aggiornamento.

## Cosa succede se un aggiornamento non riesce utilizzando NetApp Hybrid Cloud Control

In caso di guasto di un disco o di un nodo durante un aggiornamento, l'interfaccia utente dell'elemento visualizza gli errori del cluster. Il processo di aggiornamento non passa al nodo successivo e attende la risoluzione dei guasti del cluster. La barra di avanzamento nell'interfaccia utente mostra che l'aggiornamento è in attesa della risoluzione degli errori del cluster. In questa fase, la selezione di **Pausa** nell'interfaccia utente non funzionerà, perché l'aggiornamento attende che il cluster sia integro. Sarà necessario contattare il supporto NetApp per fornire assistenza durante l'indagine sul guasto.

NetApp Hybrid Cloud Control dispone di un periodo di attesa di tre ore preimpostato, durante il quale può verificarsi uno dei seguenti scenari:

- Gli errori del cluster vengono risolti entro tre ore e l'aggiornamento riprende. In questo scenario non è necessario eseguire alcuna azione.
- Il problema persiste dopo tre ore e lo stato dell'aggiornamento visualizza **Error** (errore) con un banner rosso. Una volta risolto il problema, è possibile riprendere l'aggiornamento selezionando **Riprendi**.
- Il supporto NetApp ha stabilito che l'aggiornamento deve essere temporaneamente interrotto per intraprendere un'azione correttiva prima della finestra di tre ore. Il supporto utilizzerà l'API per interrompere l'aggiornamento.



L'interruzione dell'aggiornamento del cluster durante l'aggiornamento di un nodo potrebbe causare la rimozione dei dischi dal nodo. Se i dischi vengono rimossi in modo non corretto, l'aggiunta dei dischi durante un aggiornamento richiederà l'intervento manuale del supporto NetApp. Il nodo potrebbe richiedere più tempo per eseguire gli aggiornamenti del firmware o le attività di sincronizzazione post-aggiornamento. Se l'aggiornamento sembra bloccato, contattare il supporto NetApp per assistenza.

## Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare il firmware dello storage

È possibile utilizzare le API per aggiornare i nodi di storage in un cluster alla versione più recente del software Element. È possibile utilizzare uno strumento di automazione a scelta per eseguire le API. Il flusso di lavoro API qui documentato utilizza l'interfaccia utente REST API disponibile sul nodo di gestione come esempio.

### Fasi

1. Scaricare il pacchetto di aggiornamento del firmware dello storage più recente su un dispositivo accessibile al nodo di gestione; accedere a ["Pagina bundle firmware storage software Element"](#) e scaricare l'immagine più recente del firmware dello storage.
2. Caricare il pacchetto di aggiornamento del firmware dello storage nel nodo di gestione:
  - a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/package-repository/1/
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:
    - i. Inserire il nome utente e la password del cluster.
    - ii. Immettere l>ID client come `mnode-client`.
    - iii. Selezionare **autorizzare** per avviare una sessione.
    - iv. Chiudere la finestra di autorizzazione.
  - c. Dall'interfaccia utente API REST, selezionare **POST /packages**.
  - d. Selezionare **Provalo**.
  - e. Selezionare **Sfoglia** e selezionare il pacchetto di aggiornamento.
  - f. Selezionare **Esegui** per avviare il caricamento.
  - g. Dalla risposta, copiare e salvare l>ID del pacchetto ("`id`") da utilizzare in un passaggio successivo.
3. Verificare lo stato del caricamento.

- a. Dall'interfaccia utente API REST, selezionare **GET /packages/{id}/status**.
- b. Selezionare **Provalo**.
- c. Inserire l'ID del pacchetto firmware copiato nella fase precedente in **id**.
- d. Selezionare **Esegui** per avviare la richiesta di stato.

La risposta indica `state` come `SUCCESS` al termine dell'operazione.

4. Individuare l'ID della risorsa di installazione:

- a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:
  - i. Inserire il nome utente e la password del cluster.
  - ii. Immettere l'ID client come `mnode-client`.
  - iii. Selezionare **autorizzare** per avviare una sessione.
  - iv. Chiudere la finestra di autorizzazione.
- c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
- d. Selezionare **Provalo**.
- e. Selezionare **Esegui**.
- f. Dalla risposta, copiare l'ID della risorsa di installazione (`id`).

```
"id": "abcd01e2-xx00-4ccf-11ee-11f111xx9a0b",
"management": {
  "errors": [],
  "inventory": {
    "authoritativeClusterMvip": "10.111.111.111",
    "bundleVersion": "2.14.19",
    "managementIp": "10.111.111.111",
    "version": "1.4.12"
```

- g. Dall'interfaccia utente API REST, selezionare **GET /Installations/{id}**.
- h. Selezionare **Provalo**.
  - i. Incollare l'ID della risorsa di installazione nel campo **id**.
  - j. Selezionare **Esegui**.
- k. Dalla risposta, copiare e salvare l'ID del cluster di storage ("`id`") del cluster che si intende aggiornare per utilizzarlo in un secondo momento.

```
"storage": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterUuid": "a1bd1111-4f1e-46zz-ab6f-0a1111b1111x",
        "id": "a1bd1111-4f1e-46zz-ab6f-a1a1a111b012",
```

5. Eseguire l'aggiornamento del firmware dello storage:

- a. Aprire l'interfaccia utente dell'API REST dello storage sul nodo di gestione:

```
https://<ManagementNodeIP>/storage/1/
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:

- i. Inserire il nome utente e la password del cluster.
- ii. Immettere l'ID client come `mnode-client`.
- iii. Selezionare **autorizzare** per avviare una sessione.
- iv. Chiudere la finestra.

- c. Selezionare **POST /upgrade**.

- d. Selezionare **Provalo**.

- e. Inserire l'ID del pacchetto di aggiornamento nel campo dei parametri.

- f. Inserire l'ID del cluster di storage nel campo dei parametri.

- g. Selezionare **Esegui** per avviare l'aggiornamento.

La risposta deve indicare lo stato come `initializing`:

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-b3fc-2c963f66abc1",
    "log": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-b3fc-2c963f66abc1/log"
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
```

```

    "string"
  ],
  "message": "string",
  "nodeDetails": [
    {
      "message": "string",
      "step": "NodePreStart",
      "nodeID": 0,
      "numAttempt": 0
    }
  ],
  "percent": 0,
  "step": "ClusterPreStart",
  "timestamp": "2020-04-21T22:10:57.057Z",
  "failedHealthChecks": [
    {
      "checkID": 0,
      "name": "string",
      "displayName": "string",
      "passed": true,
      "kb": "string",
      "description": "string",
      "remedy": "string",
      "severity": "string",
      "data": {},
      "nodeID": 0
    }
  ]
},
"taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
"dateCompleted": "2020-04-21T22:10:57.057Z",
"dateCreated": "2020-04-21T22:10:57.057Z"
}

```

- a. Copiare l'ID dell'aggiornamento ("upgradeId") che fa parte della risposta.
6. Verificare l'avanzamento e i risultati dell'aggiornamento:
- a. Selezionare **GET /upgrades/{upgradeld}**.
  - b. Selezionare **Provalo**.
  - c. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeld**.
  - d. Selezionare **Esegui**.
  - e. In caso di problemi o requisiti speciali durante l'aggiornamento, eseguire una delle seguenti operazioni:

Opzione	Fasi
È necessario correggere i problemi di integrità del cluster dovuti a. <code>failedHealthChecks</code> messaggio nel corpo della risposta.	<ul style="list-style-type: none"> <li>i. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata.</li> <li>ii. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.</li> <li>iii. Una volta risolti i problemi del cluster, eseguire nuovamente l'autenticazione, se necessario, e selezionare <b>PUT /upgrades/{upgradeld}</b>.</li> <li>iv. Selezionare <b>Provalo</b>.</li> <li>v. Inserire l'ID dell'aggiornamento del passaggio precedente in <b>upgradeld</b>.</li> <li>vi. Invio <code>"action": "resume"</code> nel corpo della richiesta. <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <pre>{   "action": "resume" }</pre> </div> </li> <li>vii. Selezionare <b>Esegui</b>.</li> </ul>
È necessario sospendere l'aggiornamento perché la finestra di manutenzione si sta chiudendo o per un altro motivo.	<ul style="list-style-type: none"> <li>i. Se necessario, eseguire nuovamente l'autenticazione e selezionare <b>PUT /upgrades/{upgradeld}</b>.</li> <li>ii. Selezionare <b>Provalo</b>.</li> <li>iii. Inserire l'ID dell'aggiornamento del passaggio precedente in <b>upgradeld</b>.</li> <li>iv. Invio <code>"action": "pause"</code> nel corpo della richiesta. <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <pre>{   "action": "pause" }</pre> </div> </li> <li>v. Selezionare <b>Esegui</b>.</li> </ul>

f. Eseguire l'API **GET /upgrades/{upgradeld}** più volte, in base alle necessità, fino al completamento del processo.

Durante l'aggiornamento, il `status` indica `running` se non si riscontrano errori. Man mano che ogni nodo viene aggiornato, il `step` il valore cambia in `NodeFinished`.

L'aggiornamento è stato completato correttamente quando percent il valore è 100 e a. state indica finished.

## Trova ulteriori informazioni

- ["Plug-in NetApp Element per server vCenter"](#)
- ["Pagina delle risorse NetApp HCI"](#)

## Aggiornare un nodo di gestione

È possibile aggiornare il nodo di gestione al nodo di gestione 12.5 o successivo dalla versione 12.3.x o successiva.

L'aggiornamento del sistema operativo del nodo di gestione non è più necessario per aggiornare il software Element sul cluster di storage. Puoi semplicemente aggiornare i servizi di gestione alla versione più recente per eseguire gli aggiornamenti degli elementi utilizzando NetApp Hybrid Cloud Control. Se si desidera aggiornare il sistema operativo del nodo di gestione per altri motivi, ad esempio la risoluzione dei problemi di protezione, seguire la procedura di aggiornamento del nodo di gestione per lo scenario in uso.



Per informazioni sull'aggiornamento dei nodi di gestione 12.2 o versioni precedenti, consultare ["Documentazione sull'aggiornamento del nodo di gestione di NetApp HCI 1.9"](#).

### Opzioni di upgrade

Scegliere una delle seguenti opzioni:

- [Aggiornare un nodo di gestione alla versione 12.5 o successiva dalla versione 12.3.x o successiva](#)
- [Riconfigurare l'autenticazione utilizzando l'API REST del nodo di gestione](#)

Scegli questa opzione se hai aggiornato in modo **sequenziale** (1) la versione dei servizi di gestione e (2) la versione dello storage Element e vuoi mantenere \* il nodo di gestione esistente:



Se non si aggiornano in sequenza i servizi di gestione seguiti dallo storage degli elementi, non è possibile riconfigurare la riautenticazione utilizzando questa procedura. Seguire invece la procedura di aggiornamento appropriata.

## Aggiornare un nodo di gestione alla versione 12.5 o successiva dalla versione 12.3.x o successiva

È possibile eseguire un aggiornamento in-place del nodo di gestione dalla versione 12.3.x o successiva alla versione 12.5 o successiva senza dover eseguire il provisioning di una nuova macchina virtuale con nodo di gestione.



Il nodo di gestione Element 12.5 o versione successiva è un aggiornamento opzionale. Non è richiesto per le implementazioni esistenti.

### Di cosa hai bisogno

- La RAM della VM del nodo di gestione è di 24 GB.
- Il nodo di gestione che si intende aggiornare è la versione 12.0 e utilizza la rete IPv4. Il nodo di gestione versione 12.5 o successiva non supporta IPv6.





Per verificare la versione del nodo di gestione, accedere al nodo di gestione e visualizzare il numero di versione dell'elemento nel banner di accesso.

- Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente utilizzando NetApp Hybrid Cloud Control. È possibile accedere a NetApp Hybrid Cloud Control dal seguente indirizzo IP:  
`https://<ManagementNodeIP>`
- Se si sta aggiornando il nodo di gestione alla versione 12.5 o successiva, per procedere sono necessari i servizi di gestione 2.21.61 o successiva.
- È stato configurato un adattatore di rete aggiuntivo (se necessario) seguendo le istruzioni per ["Configurazione di una scheda di rete storage aggiuntiva"](#).



I volumi persistenti potrebbero richiedere un adattatore di rete aggiuntivo se eth0 non è in grado di essere instradato a SVIP. Configurare un nuovo adattatore di rete sulla rete di storage iSCSI per consentire la configurazione di volumi persistenti.

- I nodi di storage eseguono Element 12.3.x o versioni successive.

## Fasi

1. Accedere alla macchina virtuale del nodo di gestione utilizzando l'accesso a SSH o alla console.
2. Scaricare il ["Nodo di gestione ISO"](#) Per il software Element dal sito di supporto NetApp alla macchina virtuale del nodo di gestione.



Il nome dell'ISO è simile a `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Verificare l'integrità del download eseguendo md5sum sul file scaricato e confrontare l'output con quello disponibile sul NetApp Support Site per il software Element, come nell'esempio seguente:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

4. Montare l'immagine ISO del nodo di gestione e copiare il contenuto nel file system utilizzando i seguenti comandi:

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

5. Passare alla home directory e smontare il file ISO da /mnt:

```
sudo umount /mnt
```

6. Eliminare l'ISO per risparmiare spazio sul nodo di gestione:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-  
XX.X.X.XXXX.iso
```

7. Sul nodo di gestione che si sta aggiornando, eseguire il comando seguente per aggiornare la versione del sistema operativo del nodo di gestione. Lo script conserva tutti i file di configurazione necessari dopo l'aggiornamento, ad esempio le impostazioni di Active IQ Collector e proxy.

```
sudo /sf/rftfi/bin/sfrtfti_inplace  
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

Al termine del processo di aggiornamento, il nodo di gestione viene riavviato con un nuovo sistema operativo.



Dopo aver eseguito il comando sudo descritto in questo passaggio, la sessione SSH viene terminata. L'accesso alla console è necessario per il monitoraggio continuo. Se non è disponibile alcun accesso alla console durante l'aggiornamento, riprovare a eseguire l'accesso SSH e verificare la connettività dopo 15 - 30 minuti. Una volta effettuato l'accesso, è possibile confermare la nuova versione del sistema operativo nel banner SSH che indica che l'aggiornamento è stato eseguito correttamente.

8. Sul nodo di gestione, eseguire `redeploy-mnode` script per conservare le impostazioni di configurazione dei servizi di gestione precedenti:



Lo script conserva la precedente configurazione dei servizi di gestione, inclusa la configurazione dal servizio di raccolta Active IQ, dai controller (vCenter) o dal proxy, a seconda delle impostazioni.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```



Se in precedenza era stata disattivata la funzionalità SSH sul nodo di gestione, è necessario ["Disattivare nuovamente SSH"](#) sul nodo di gestione ripristinato. Funzionalità SSH che offre ["Accesso alla sessione del NetApp Support Remote Support Tunnel \(RST\)"](#) è attivato sul nodo di gestione per impostazione predefinita.

## Riconfigurare l'autenticazione utilizzando l'API REST del nodo di gestione

È possibile mantenere il nodo di gestione esistente se sono stati aggiornati in sequenza (1) servizi di gestione e (2) storage di elementi. Se si è seguito un ordine di aggiornamento diverso, consultare le procedure per gli aggiornamenti dei nodi di gestione in-place.

### Prima di iniziare

- I servizi di gestione sono stati aggiornati alla versione 2.20.69 o successiva.
- Il cluster di storage esegue Element 12.3 o versione successiva.
- I servizi di gestione sono stati aggiornati in sequenza, seguito dall'aggiornamento dello storage Element. Non è possibile riconfigurare l'autenticazione utilizzando questa procedura a meno che non siano stati completati gli aggiornamenti nella sequenza descritta.

## Fasi

1. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/mnode
```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
  - a. Inserire il nome utente e la password del cluster.
  - b. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
  - c. Selezionare **autorizzare** per avviare una sessione.
3. Dall'interfaccia utente API REST, selezionare **POST /Services/reconfigure-auth**.
4. Selezionare **Provalo**.
5. Per il parametro **load\_images**, selezionare `true`.
6. Selezionare **Esegui**.

Il corpo della risposta indica che la riconfigurazione è stata eseguita correttamente.

## Trova ulteriori informazioni

- ["Plug-in NetApp Element per server vCenter"](#)
- ["Pagina delle risorse NetApp HCI"](#)

## Aggiornare il plug-in Element per vCenter Server

Per gli ambienti vSphere esistenti con un plug-in NetApp Element registrato per VMware vCenter Server, è possibile aggiornare la registrazione del plug-in dopo il primo aggiornamento del pacchetto di servizi di gestione che contiene il servizio plug-in.

È possibile aggiornare la registrazione del plug-in su vCenter Server Virtual Appliance (vCSA) o Windows utilizzando l'utility di registrazione. È necessario modificare la registrazione per il plug-in vCenter su ogni vCenter Server in cui è necessario utilizzare il plug-in.



Management Services 2.22.7 include Element Plug-in per vCenter Server 5.0 che contiene il plug-in remoto. Se si utilizza il plug-in Element, è necessario eseguire l'aggiornamento ai servizi di gestione 2.22.7 o versioni successive per rispettare la direttiva VMware che rimuove il supporto per i plug-in locali. ["Scopri di più"](#).

### Plug-in Element per vCenter 5.0 e versioni successive

Questa procedura di aggiornamento riguarda i seguenti scenari di aggiornamento:

- Stai effettuando l'aggiornamento a Element Plug-in per vCenter Server 5,3, 5,2, 5,1 o 5,0.
- Si sta eseguendo l'aggiornamento a 8.0 o 7.0 HTML5 vSphere Web Client.



Il plug-in Element per vCenter 5,0 o versioni successive non è compatibile con vCenter Server 6,7 e 6,5.



Quando si esegue l'aggiornamento da Element Plug-in per vCenter Server 4.x a 5.x, i cluster già configurati con il plug-in vengono persi perché i dati non possono essere copiati da un'istanza di vCenter a un plug-in remoto. È necessario aggiungere nuovamente i cluster al plug-in remoto. Si tratta di un'attività singola durante l'aggiornamento da un plug-in locale a un plug-in remoto.

### Plug-in Element per vCenter 4.10 e versioni precedenti

Questa procedura di aggiornamento riguarda i seguenti scenari di aggiornamento:

- Si sta eseguendo l'aggiornamento a Element Plug-in per vCenter Server 4.10, 4.9, 4.8, 4.7, 4.6, 4.5 o 4.4.
- Si sta eseguendo l'aggiornamento a un client Web 7.0, 6.7 o 6.5 HTML5 vSphere.

- Il plug-in non è compatibile con VMware vCenter Server 8.0 per Element Plug-in per VMware vCenter Server 4.x.
- Il plug-in non è compatibile con VMware vCenter Server 6.5 per Element Plug-in per VMware vCenter Server 4.6, 4.7 e 4.8.

- Si sta eseguendo l'aggiornamento a 6.7 Flash vSphere Web Client.



Il plug-in non è compatibile con la versione 6.7 U2 build 13007421 del client Web vSphere HTML5 e con altre build 6.7 U2 rilasciate prima dell'aggiornamento 2a (build 13643870). Per ulteriori informazioni sulle versioni di vSphere supportate, consultare le note sulla versione di ["versione del plug-in"](#).

### Di cosa hai bisogno

- **Privilegi di amministratore:** Si dispone dei privilegi di amministratore vCenter per installare un plug-in.
- **Aggiornamenti vSphere:** Sono stati eseguiti tutti gli aggiornamenti vCenter necessari prima di aggiornare il plug-in NetApp Element per vCenter Server. Questa procedura presuppone che gli aggiornamenti di vCenter siano già stati completati.
- **vCenter Server:** Il plug-in vCenter versione 4.x o 5.x è registrato con vCenter Server. Dall'utility di registrazione ([https://\[management node IP\]:9443](https://[management node IP]:9443)), selezionare **Registration Status** (Stato registrazione), completare i campi necessari e selezionare **Check Status** (Controlla stato) per verificare che il plug-in vCenter sia già registrato e che il numero di versione dell'installazione corrente.
- **Aggiornamenti dei servizi di gestione:** È stato aggiornato il ["bundle di servizi di gestione"](#) alla versione più recente. Gli aggiornamenti del plug-in vCenter vengono distribuiti utilizzando gli aggiornamenti dei

servizi di gestione rilasciati al di fuori delle principali release di prodotti per NetApp HCI.

- **Aggiornamenti del nodo di gestione:**

**Plug-in Element per vCenter 5.0 e versioni successive**

Si sta eseguendo un nodo di gestione che è stato "aggiornato" alla versione 12.3.x o successiva.

**Plug-in Element per vCenter 4.10 e versioni precedenti**

Si sta eseguendo un nodo di gestione che è stato "aggiornato" alla versione 11.3 o successiva.

VCenter Plug-in 4.4 o versione successiva richiede un nodo di gestione 11.3 o versione successiva con un'architettura modulare che fornisce singoli servizi. Il nodo di gestione deve essere acceso con il relativo indirizzo IP o DHCP configurato.

- **Upgrade dello storage Element:**

- A partire dal plug-in Element vCenter 5.0, si dispone di un cluster che esegue il software NetApp Element 12.3.x o versione successiva.
- Per il plug-in Element vCenter 4.10 o versione precedente, si dispone di un cluster che esegue il software NetApp Element 11.3 o versione successiva.

- **VSphere Web Client:** Si è disconnessi da vSphere Web Client prima di iniziare qualsiasi aggiornamento del plug-in. Il client Web non riconosce gli aggiornamenti effettuati durante questo processo al plug-in se non si effettua la disconnessione.

## **Fasi**

1. Inserire l'indirizzo IP del nodo di gestione in un browser, inclusa la porta TCP per la registrazione: `https://[management node IP]:9443`` L'interfaccia utente dell'utility di registrazione apre la pagina **Manage QoSSIOC Service Credentials** (Gestisci credenziali servizio QoSSIOC) per il plug-in.

QoSSIOC Management

Manage Credentials
Restart QoSSIOC Service

## Manage QoSSIOC Service Credentials

Old Password

Current password

Current password is required

New Password

New password

Must contain at least 8 characters with at least one lower-case and upper-case alphabet, a number and a special character like #!\$%&'()\*+,-./:;<@^\_`{|}~

Confirm Password

Confirm New Password

New and confirm passwords must match


SUBMIT CHANGES

Contact NetApp Support at <http://mysupport.netapp.com>

## 2. Selezionare vCenter Plug-in Registration.

## Plug-in Element per vCenter 5.0 e versioni successive

Viene visualizzata la pagina di registrazione dei plug-in vCenter:

 Element Plug-in for vCenter Server Management Node

GoSSIOC Service Management vCenter Plug-in Registration

Manage vCenter Plug-in

Register Plug-in  
Update Plug-in  
Unregister Plug-in  
Registration Status

### vCenter Plug-in - Registration

Register version 5.0.0 of the NetApp Element Plug-in for vCenter Server with your vCenter server.  
The Plug-in will not be deployed until a fresh vCenter login after registration.

**vCenter Address**

vCenter Server Address

Enter the IPV4, IPV6 or DNS name of the vCenter server to register plug-in on.

**vCenter User Name**

vCenter Admin User Name

Ensure this user is a vCenter user that has administrative privileges for registration.

**vCenter Password**

vCenter Admin Password

The password for the vCenter user name entered.

☐ Customize URL

Select to customize the Zip file URL.

**Plug-in Zip URL**

https://10.117.227.44:8333/vcp-ui/plugin.json

URL of XML initialization file

REGISTER

Contact NetApp Support at <http://mysupport.netapp.com>

## Plug-in Element per vCenter 4.10 e versioni precedenti

Viene visualizzata la pagina di registrazione dei plug-in vCenter:

Manage vCenter Plug-in

Register Plug-in
Update Plug-in
Unregister Plug-in
Registration Status

### vCenter Plug-in - Registration

Register version  of the NetApp Element Plug-in for vCenter Server with your vCenter server. The Plug-in will not be deployed until a fresh vCenter login after registration.

vCenter Address

vCenter Server Address

Enter the IPV4, IPV6 or DNS name of the vCenter server to register plug-in on.

vCenter User Name

vCenter Admin User Name

Ensure this user is a vCenter user that has administrative privileges for registration.

vCenter Password

vCenter Admin Password

The password for the vCenter user name entered.

☐ Customize URL

Select to customize the Zip file URL.

Plug-in Zip URL

<https://10.117.227.12-9443/solidfire-plugin-4.6.0-bin.zip>

URL of XML initialization file

REGISTER

Contact NetApp Support at <http://mysupport.netapp.com>

3. In **Manage vCenter Plug-in** (Gestisci plug-in vCenter), selezionare **Update Plug-in** (Aggiorna plug-in).

4. Confermare o aggiornare le seguenti informazioni:

- L'indirizzo IPv4 o l'FQDN del servizio vCenter su cui si desidera registrare il plug-in.
- Il nome utente vCenter Administrator.



Il nome utente e la password immessi devono essere assegnati a un utente con privilegi di ruolo vCenter Administrator.

- La password di vCenter Administrator.
- (Per server in-house o siti scuri) a seconda del plug-in Element per la versione vCenter, un URL personalizzato per il file JSON del plug-in o il plug-in ZIP:



#### Plug-in Element per vCenter 5.0 e versioni successive

Un URL personalizzato per il file JSON del plug-in.



È possibile selezionare **Custom URL** (URL personalizzato) per personalizzare l'URL se si utilizza un server HTTP o HTTPS (sito sicuro) o se sono state modificate le impostazioni di rete o il nome del file JSON. Per ulteriori procedure di configurazione se si intende personalizzare un URL, vedere la documentazione di Element Plug-in for vCenter Server sulla modifica delle proprietà di vCenter per un server HTTP interno (sito sicuro).

#### Plug-in Element per vCenter 4.10 e versioni precedenti

Un URL personalizzato per il plug-in ZIP.



È possibile selezionare **Custom URL** (URL personalizzato) per personalizzare l'URL se si utilizza un server HTTP o HTTPS (sito sicuro) o se sono state modificate le impostazioni di rete o il nome del file ZIP. Per ulteriori procedure di configurazione se si intende personalizzare un URL, vedere la documentazione di Element Plug-in for vCenter Server sulla modifica delle proprietà di vCenter per un server HTTP interno (sito sicuro).

#### 5. Selezionare **Aggiorna**.

Una volta completata la registrazione, nell'interfaccia utente dell'utility di registrazione viene visualizzato un banner.

#### 6. Accedere a vSphere Web Client come vCenter Administrator. Se si è già connessi a vSphere Web Client, è necessario prima disconnettersi, attendere due o tre minuti, quindi eseguire nuovamente l'accesso.



Questa azione crea un nuovo database e completa l'installazione in vSphere Web Client.

#### 7. In vSphere Web Client, cercare le seguenti attività completate nel task monitor per assicurarsi che l'installazione sia stata completata: `Download plug-in` e `Deploy plug-in`.

#### 8. Verificare che i punti di estensione del plug-in siano visualizzati nella scheda **Shortcuts** di vSphere Web Client e nel pannello laterale.

#### Plug-in Element per vCenter 5.0 e versioni successive

Viene visualizzato il punto di estensione del plugin remoto di NetApp Element:



#### Plug-in Element per vCenter 4.10 e versioni precedenti

Vengono visualizzati i punti di estensione della configurazione e della gestione di NetApp Element:



Se le icone del plug-in vCenter non sono visibili, vedere ["Plug-in Element per vCenter Server"](#) documentazione sulla risoluzione dei problemi del plug-in.



Dopo aver eseguito l'aggiornamento al plug-in NetApp Element per vCenter Server 4.8 o versioni successive con VMware vCenter Server 6.7U1, se i cluster di storage non sono elencati o viene visualizzato un errore del server nelle sezioni **Clusters** e **QoS SIOC Settings** della configurazione NetApp Element, vedere ["Plug-in Element per vCenter Server"](#) documentazione sulla risoluzione di questi errori.

9. Verificare la modifica della versione nella scheda **About** (informazioni su) nel punto di estensione **NetApp Element Configuration** del plug-in.

Dovrebbero essere visualizzati i seguenti dettagli di versione o dettagli di una versione più recente:

```
NetApp Element Plug-in Version: 5.3
NetApp Element Plug-in Build Number: 9
```



Il plug-in vCenter contiene il contenuto della Guida in linea. Per assicurarsi che la guida contenga i contenuti più recenti, cancellare la cache del browser dopo aver aggiornato il plug-in.

## Trova ulteriori informazioni

- ["Plug-in NetApp Element per server vCenter"](#)
- ["Pagina delle risorse NetApp HCI"](#)

## Eseguire i controlli dello stato dei nodi di calcolo prima di aggiornare il firmware di calcolo

Prima di aggiornare il firmware di calcolo, è necessario eseguire i controlli dello stato di salute per assicurarsi che tutti i nodi di calcolo del cluster siano pronti per l'aggiornamento. I controlli dello stato dei nodi di calcolo possono essere eseguiti solo su cluster di calcolo di uno o più nodi di calcolo NetApp HCI gestiti.

### Di cosa hai bisogno

- **Servizi di gestione:** È stato eseguito l'aggiornamento al bundle di servizi di gestione più recente (2.11 o versione successiva).
- **Nodo di gestione:** Si sta eseguendo il nodo di gestione 11.3 o successivo.
- **Software Element:** Il cluster di storage esegue il software NetApp Element 11.3 o versione successiva.
- **Contratto di licenza con l'utente finale (EULA):** A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per eseguire i controlli dello stato dei nodi di calcolo:
  - a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

- b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
- c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
- d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

### Opzioni di controllo dello stato di salute

Puoi eseguire controlli di integrità utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control o l'API di NetApp Hybrid Cloud Control:

- [Utilizzare NetApp Hybrid Cloud Control per eseguire controlli dello stato dei nodi di calcolo prima di aggiornare il firmware](#) (Metodo preferito)
- [Utilizzare l'API per eseguire i controlli dello stato dei nodi di calcolo prima di aggiornare il firmware](#)

Ulteriori informazioni sui controlli dello stato dei nodi di calcolo eseguiti dal servizio sono disponibili:

- [Verifiche dello stato dei nodi di calcolo effettuate dal servizio](#)

## Utilizzare NetApp Hybrid Cloud Control per eseguire controlli dello stato dei nodi di calcolo prima di aggiornare il firmware

Utilizzando NetApp Hybrid Cloud Control, è possibile verificare che un nodo di calcolo sia pronto per l'aggiornamento del firmware.




Se si dispone di più configurazioni di cluster di storage a due nodi, ciascuna all'interno del proprio vCenter, i controlli di stato dei nodi di controllo potrebbero non generare report accurati. Pertanto, quando si è pronti per aggiornare gli host ESXi, è necessario arrestare solo il nodo di controllo dell'host ESXi da aggiornare. È necessario assicurarsi di avere sempre un nodo di controllo in esecuzione nell'installazione di NetApp HCI spegnendo i nodi di controllo in modo alternativo.

### Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>/hcc
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare la scheda **Compute firmware** (calcolo firmware).
5.  Selezionare il controllo dello stato di salute per il cluster che si desidera controllare per verificare la disponibilità all'aggiornamento.
6. Nella pagina **Compute Health Check**, selezionare **Run Health Check**.
7. In caso di problemi, la pagina fornisce un report. Effettuare le seguenti operazioni:
  - a. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata.

- b. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.
- c. Una volta risolti i problemi del cluster, selezionare **Riesegui controllo stato di salute**.

Una volta completato il controllo dello stato di salute senza errori, i nodi di calcolo nel cluster sono pronti per l'aggiornamento. Vedere ["Aggiornare il firmware del nodo di calcolo"](#) per procedere.

## Utilizzare l'API per eseguire i controlli dello stato dei nodi di calcolo prima di aggiornare il firmware

È possibile utilizzare REST API per verificare che i nodi di calcolo di un cluster siano pronti per l'aggiornamento. Il controllo dello stato di salute verifica che non vi siano ostacoli all'aggiornamento, ad esempio problemi dell'host ESXi o altri problemi di vSphere. Sarà necessario eseguire controlli dello stato dei nodi di calcolo per ciascun cluster di calcolo dell'ambiente.

### Fasi

1. Individuare l'ID del controller e l'ID del cluster:

- a. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:
  - i. Inserire il nome utente e la password del cluster.
  - ii. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
  - iii. Selezionare **autorizzare** per avviare una sessione.
- c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
- d. Selezionare **Provalo**.
- e. Selezionare **Esegui**.
- f. Dal corpo della risposta del codice 200, copiare il "id" per l'installazione che si intende utilizzare per i controlli di integrità.
- g. Dall'interfaccia utente API REST, selezionare **GET /installations/{id}**.
- h. Selezionare **Provalo**.
  - i. Inserire l'ID di installazione.
  - j. Selezionare **Esegui**.
- k. Dal corpo della risposta del codice 200, copiare gli ID per ciascuno dei seguenti elementi:
  - i. L'ID del cluster ("`clusterID`")
  - ii. Un ID del controller ("`controllerId`")

```
{
  "_links": {
    "collection":
      "https://10.117.187.199/inventory/1/installations",
    "self":
      "https://10.117.187.199/inventory/1/installations/xx94f6f0-12a6-412f-8b5e-4cf2z58329x0"
  },
  "compute": {
    "errors": [],
    "inventory": {
      "clusters": [
        {
          "clusterId": "domain-1",
          "controllerId": "abc12c3a-aa87-4e33-9f94-xx588c2cdcf6",
          "datacenterName": "NetApp-HCI-Datacenter-01",
          "installationId": "xx94f6f0-12a6-412f-8b5e-4cf2z58329x0",
          "installationName": "test-nde-mnode",
          "inventoryType": "managed",
          "name": "NetApp-HCI-Cluster-01",
          "summary": {
            "nodeCount": 2,
            "virtualMachineCount": 2
          }
        }
      ]
    }
  },
}
```

2. Eseguire controlli di integrità sui nodi di calcolo nel cluster:

- a. Aprire l'interfaccia utente REST API del servizio di calcolo sul nodo di gestione:

```
https://<ManagementNodeIP>/vcenter/1/
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:
- Inserire il nome utente e la password del cluster.
  - Immettere l'ID client come `mnode-client` se il valore non è già compilato.
  - Selezionare **autorizzare** per avviare una sessione.
- c. Selezionare **POST /compute/{CONTROLLER\_ID}/Health-checks**.
- d. Selezionare **Provalo**.
- e. Inserire il "controllerId" È stata copiata dalla fase precedente nel campo del parametro **Controller\_ID**.

- f. Nel payload, inserire "clusterId" che è stato copiato dal passaggio precedente come "cluster" valutare e rimuovere il valore "nodes" parametro.

```
{
  "cluster": "domain-1"
}
```

- g. Selezionare **Esegui** per eseguire un controllo dello stato di salute sul cluster.

La risposta del codice 200 fornisce un "resourceLink" URL con l'ID attività aggiunto, necessario per confermare i risultati del controllo di integrità.

```
{
  "resourceLink": "https://10.117.150.84/vcenter/1/compute/tasks/[This is the task ID for health check task results]",
  "serviceName": "vcenter-v2-svc",
  "taskId": "ab12c345-06f7-42d7-b87c-7x64x56x321x",
  "taskName": "VCenter service health checks"
}
```

- a. Copiare la parte dell'ID attività di "resourceLink" URL per verificare il risultato dell'attività.

3. Verificare il risultato dei controlli di integrità:

- a. Tornare all'interfaccia utente REST API del servizio di calcolo sul nodo di gestione:

```
https://<ManagementNodeIP>/vcenter/1/
```

- b. Selezionare **GET /compute/tasks/{task\_id}**.

- c. Selezionare **Provalo**.

- d. Inserire l'ID attività di "resourceLink" URL della risposta **POST /compute/{CONTROLLER\_ID} /Health-checks** codice 200 in task\_id campo del parametro.

- e. Selezionare **Esegui**.

- f. Se il status il messaggio restituito indica che si sono verificati problemi relativi allo stato del nodo di calcolo, procedere come segue:
- Consultare l'articolo specifico della Knowledge base (KbLink) elencati per ciascun problema o eseguire il rimedio specificato.
  - Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.
  - Dopo aver risolto i problemi del cluster, eseguire di nuovo **POST /compute/{CONTROLLER\_ID} /Health-checks** (vedere il passaggio 2).

Se i controlli di integrità vengono completati senza problemi, il codice di risposta 200 indica un risultato positivo.

## Verifiche dello stato dei nodi di calcolo effettuate dal servizio

I controlli di stato del calcolo, eseguiti con i metodi API o con NetApp Hybrid Cloud Control, eseguono i seguenti controlli per nodo. A seconda dell'ambiente in uso, alcuni di questi controlli potrebbero essere ignorati. È necessario eseguire nuovamente i controlli di integrità dopo aver risolto eventuali problemi rilevati.

Controllare la descrizione	Nodo/cluster	Azione necessaria per risolvere il problema	Articolo della Knowledge base con procedura
DRS è abilitato e completamente automatizzato?	Cluster	Attivare DRS e assicurarsi che sia completamente automatizzato.	<a href="#">"Consulta questa KB"</a> . NOTA: Se si dispone di licenze standard, impostare l'host ESXi in modalità di manutenzione e ignorare questo avviso di errore del controllo dello stato di salute.
DPM è disattivato in vSphere?	Cluster	Disattivare Distributed Power Management.	<a href="#">"Consulta questa KB"</a> .
Il controllo di ammissione ha è disattivato in vSphere?	Cluster	Disattivare il controllo di ammissione ha.	<a href="#">"Consulta questa KB"</a> .
FT è abilitato per una macchina virtuale su un host nel cluster?	Nodo	Sospendere Fault Tolerance su tutte le macchine virtuali interessate.	<a href="#">"Consulta questa KB"</a> .
Vi sono allarmi critici in vCenter per il cluster?	Cluster	Avviare vSphere e risolvere e/o riconoscere eventuali avvisi prima di procedere.	Nessun KB necessario per risolvere il problema.
Sono presenti avvisi informativi generici/globali in vCenter?	Cluster	Avviare vSphere e risolvere e/o riconoscere eventuali avvisi prima di procedere.	Nessun KB necessario per risolvere il problema.
I servizi di gestione sono aggiornati?	Sistema HCI	È necessario aggiornare i servizi di gestione prima di eseguire un aggiornamento o un controllo dello stato di salute prima dell'aggiornamento.	Nessun KB necessario per risolvere il problema. Vedere <a href="#">"questo articolo"</a> per ulteriori informazioni.
Ci sono errori sul nodo ESXi corrente in vSphere?	Nodo	Avviare vSphere e risolvere e/o riconoscere eventuali avvisi prima di procedere.	Nessun KB necessario per risolvere il problema.
I supporti virtuali sono montati su una macchina virtuale su un host nel cluster?	Nodo	Smontare tutti i dischi di supporti virtuali (CD/DVD/floppy) dalle macchine virtuali.	Nessun KB necessario per risolvere il problema.

Controllare la descrizione	Nodo/cluster	Azione necessaria per risolvere il problema	Articolo della Knowledge base con procedura
La versione di BMC è la versione minima richiesta con supporto per redfish?	Nodo	Aggiornare manualmente il firmware BMC.	Nessun KB necessario per risolvere il problema.
L'host ESXi è attivo e in esecuzione?	Nodo	Avviare l'host ESXi.	Nessun KB necessario per risolvere il problema.
Alcune macchine virtuali risiedono nello storage ESXi locale?	Nodo/VM	Rimuovere o migrare lo storage locale collegato alle macchine virtuali.	Nessun KB necessario per risolvere il problema.
BMC è attivo?	Nodo	Accendere il BMC e assicurarsi che sia connesso a una rete raggiungibile da questo nodo di gestione.	Nessun KB necessario per risolvere il problema.
Sono disponibili host ESXi partner?	Nodo	Rendere disponibili uno o più host ESXi nel cluster (non in modalità di manutenzione) per la migrazione delle macchine virtuali.	Nessun KB necessario per risolvere il problema.
Sei in grado di connetterti a BMC tramite il protocollo IPMI?	Nodo	Abilitare il protocollo IPMI su Baseboard Management Controller (BMC).	Nessun KB necessario per risolvere il problema.
L'host ESXi è mappato correttamente all'host hardware (BMC)?	Nodo	L'host ESXi non è mappato correttamente al Baseboard Management Controller (BMC). Correggere la mappatura tra host ESXi e host hardware.	Nessun KB necessario per risolvere il problema. Vedere <a href="#">"questo articolo"</a> per ulteriori informazioni.
Qual è lo stato dei nodi di controllo nel cluster? Nessuno dei nodi di controllo identificati è attivo e in esecuzione.	Nodo	Un nodo di controllo non è in esecuzione su un host ESXi alternativo. Accendere il nodo di controllo su un host ESXi alternativo ed eseguire nuovamente il controllo dello stato di salute. <b>Un nodo di controllo deve essere sempre in esecuzione nell'installazione HCI.</b>	<a href="#">"Consulta questa KB"</a>



Controllare la descrizione	Nodo/cluster	Azione necessaria per risolvere il problema	Articolo della Knowledge base con procedura
Qual è lo stato dei nodi di controllo nel cluster? Il nodo testimone è attivo e in esecuzione su questo host ESXi e il nodo testimone alternativo non è attivo e in esecuzione.	Nodo	Un nodo di controllo non è in esecuzione su un host ESXi alternativo. Accendere il nodo di controllo su un host ESXi alternativo. Quando si è pronti ad aggiornare questo host ESXi, arrestare il nodo di controllo in esecuzione su questo host ESXi ed eseguire nuovamente il controllo dello stato di salute. <b>Un nodo di controllo deve essere sempre in esecuzione nell'installazione HCI.</b>	<a href="#">"Consulta questa KB"</a>
Qual è lo stato dei nodi di controllo nel cluster? Il nodo testimone è attivo e in esecuzione su questo host ESXi e il nodo alternativo è attivo ma è in esecuzione sullo stesso host ESXi.	Nodo	Entrambi i nodi di controllo sono in esecuzione su questo host ESXi. Spostare un nodo di controllo su un host ESXi alternativo. Quando si è pronti ad aggiornare questo host ESXi, arrestare il nodo di controllo rimanente su questo host ESXi ed eseguire nuovamente il controllo dello stato di salute. <b>Un nodo di controllo deve essere sempre in esecuzione nell'installazione HCI.</b>	<a href="#">"Consulta questa KB"</a>
Qual è lo stato dei nodi di controllo nel cluster? Il nodo testimone è attivo e in esecuzione su questo host ESXi e il nodo testimone alternativo è attivo e in esecuzione su un altro host ESXi.	Nodo	Un nodo di controllo è in esecuzione localmente su questo host ESXi. Quando si è pronti ad aggiornare questo host ESXi, arrestare il nodo di controllo solo su questo host ESXi ed eseguire nuovamente il controllo dello stato di salute. <b>Un nodo di controllo deve essere sempre in esecuzione nell'installazione HCI.</b>	<a href="#">"Consulta questa KB"</a>

## Trova ulteriori informazioni

- ["Plug-in NetApp Element per server vCenter"](#)
- ["Pagina delle risorse NetApp HCI"](#)

## Aggiornare i driver dei nodi di calcolo

Per qualsiasi nodo di calcolo della serie H, è possibile aggiornare i driver utilizzati sui nodi utilizzando VMware Update Manager.

### Di cosa hai bisogno

Consultare la matrice del firmware e dei driver per l'hardware all'indirizzo ["Versioni del firmware e dei driver ESXi supportate"](#).

### A proposito di questa attività

Eseguire una sola di queste operazioni di aggiornamento alla volta.

Prima di tentare di eseguire gli aggiornamenti del firmware di calcolo, controllare la versione corrente del driver ESXi. Se il driver non è aggiornato, aggiornarlo. Quindi, aggiornare il firmware di calcolo per i nodi di calcolo.

### Fasi

1. Accedere a ["Download del software NetApp HCI"](#) E selezionare il collegamento per scaricare la versione corretta di NetApp HCI.
2. Selezionare **ESXI\_drivers** dall'elenco a discesa.
3. Accettare il Contratto di licenza con l'utente finale.
4. Scarica il pacchetto di driver per il tuo tipo di nodo e la versione di ESXi.
5. Estrarre il pacchetto di driver scaricato sul computer locale.



Il bundle di driver NetApp include uno o più file ZIP VMware Offline Bundle; non estrarre questi file ZIP.

6. Accedere a **VMware Update Manager** in VMware vCenter.
7. Importare il file bundle offline del driver per i nodi di calcolo in **Patch Repository**.

Per VMware ESXi 6.x e da 7.0 a 7.0 U3, attenersi alla seguente procedura per importare il file bundle offline del driver:

- a. Selezionare la scheda **aggiornamenti**.
  - b. SELEZIONARE **UPLOAD FROM FILE** (CARICA DA FILE).
  - c. Individuare il bundle offline scaricato in precedenza e selezionare **IMPORT**.
8. Creare una nuova baseline host per il nodo di calcolo.
  9. Scegliere **host Extension** per Nome e tipo e selezionare tutti i pacchetti di driver importati da includere nella nuova linea di base.
  10. Nel menu **host and Clusters** di vCenter, selezionare il cluster con i nodi di calcolo che si desidera aggiornare e passare alla scheda **Update Manager**.
  11. Selezionare **bonifica** e selezionare la baseline dell'host appena creata. Assicurarsi che siano selezionati i driver inclusi nella linea di base.

12. Passare alla procedura guidata **Opzioni di correzione dell'host** e assicurarsi che l'opzione **Do Not Change VM Power state** (non modificare lo stato di alimentazione della macchina virtuale) sia selezionata per mantenere le macchine virtuali in linea durante l'aggiornamento del driver.



Se VMware Distributed Resource Scheduler (DRS) è attivato sul cluster (impostazione predefinita nelle installazioni NetApp HCI), le macchine virtuali vengono migrate automaticamente in altri nodi del cluster.

13. Passare alla pagina **Pronto per il completamento** della procedura guidata e selezionare **fine**.

I driver per tutti i nodi di calcolo nel cluster vengono aggiornati un nodo alla volta, mentre le macchine virtuali rimangono online.

## Trova ulteriori informazioni

- ["Plug-in NetApp Element per server vCenter"](#)
- ["Pagina delle risorse NetApp HCI"](#)

## Aggiornare il firmware del nodo di calcolo

Per i nodi di calcolo della serie H, è possibile aggiornare il firmware per i componenti hardware come BMC, BIOS e NIC. Per aggiornare il firmware del nodo di calcolo, è possibile utilizzare l'interfaccia utente di NetApp Hybrid Cloud Control, l'API REST, un'unità USB con l'immagine firmware più recente o l'interfaccia utente BMC.

Dopo l'aggiornamento, il nodo di calcolo si avvia in ESXi e funziona come prima, mantenendo la configurazione.

### Di cosa hai bisogno

- **Compute Drivers:** Hai aggiornato i driver dei nodi di calcolo. Se i driver dei nodi di calcolo non sono compatibili con il nuovo firmware, l'aggiornamento non viene avviato. Vedere ["Tool di matrice di interoperabilità \(IMT\)"](#) per informazioni sulla compatibilità di driver e firmware, consultare la versione più recente ["note di rilascio del firmware del nodo di calcolo"](#) per informazioni importanti su firmware e driver all'avanguardia.
- **Privilegi di amministratore:** Si dispone delle autorizzazioni di amministratore del cluster e BMC per eseguire l'aggiornamento.
- **Porte di sistema:** Se si utilizza NetApp Hybrid Cloud Control per gli aggiornamenti, si è assicurati che le porte necessarie siano aperte. Vedere ["Porte di rete"](#) per ulteriori informazioni.
- **Versioni minime di BMC e BIOS:** Il nodo che intendi aggiornare utilizzando NetApp Hybrid Cloud Control soddisfa i seguenti requisiti minimi:

Modello	Versione minima di BMC	Versione minima del BIOS
H300E/H500E/H700E	6.84.00	NA2.1
H410C	Tutte le versioni supportate (non è richiesto alcun aggiornamento)	Tutte le versioni supportate (non è richiesto alcun aggiornamento)
H610C	3.96.07	3B01
H615C	4.68.07	3B08.CO



I nodi di calcolo H615C devono aggiornare il firmware BMC alla versione 4.68 utilizzando ["bundle firmware di calcolo 2.27"](#) Per consentire a NetApp Hybrid Cloud Control di eseguire futuri aggiornamenti del firmware.



Per una matrice completa di firmware e firmware del driver per l'hardware, vedere ["Versioni del firmware e dei driver ESXi supportate"](#).

- **BIOS boot order** (Ordine di avvio del BIOS): Modificare manualmente l'ordine di avvio nella configurazione del BIOS per ciascun nodo per garantire USB CD/DVD viene visualizzato nell'elenco di avvio. Vedi questo ["articolo"](#) per ulteriori informazioni.
- **Credenziali BMC**: Aggiornare le credenziali utilizzate da NetApp Hybrid Cloud Control per connettersi al nodo di calcolo BMC. Puoi farlo utilizzando il NetApp Hybrid Cloud Control ["INTERFACCIA UTENTE"](#) oppure ["API"](#). L'aggiornamento delle informazioni BMC prima dell'aggiornamento aggiorna l'inventario e garantisce che i servizi dei nodi di gestione siano a conoscenza di tutti i parametri hardware necessari per completare l'aggiornamento.
- **Supporto collegato**: Scollegare qualsiasi USB o ISO fisico prima di avviare un aggiornamento del nodo di calcolo.
- **Console KVM ESXi**: Chiudere tutte le sessioni Serial-over-LAN (Sol) aperte e le sessioni KVM attive nell'interfaccia utente BMC prima di avviare un aggiornamento del nodo di calcolo.
- **Requisiti del nodo di controllo**: In cluster di storage a due e tre nodi, uno ["Nodo di controllo"](#) Deve essere sempre in esecuzione nell'installazione di NetApp HCI.
- **Verifica dello stato del nodo di calcolo**: È stato verificato che il nodo è pronto per l'aggiornamento. Vedere ["Eseguire i controlli dello stato dei nodi di calcolo prima di aggiornare il firmware di calcolo"](#).
- **Contratto di licenza con l'utente finale (EULA)**: A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare il firmware del nodo di calcolo:
  - a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

- b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
- c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
- d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

### A proposito di questa attività

Negli ambienti di produzione, aggiornare il firmware su un nodo di calcolo alla volta.



L'host ESXi deve essere disattivato dalla modalità di blocco prima di eseguire un controllo dello stato di salute e procedere con l'aggiornamento del firmware. Vedere ["Come disattivare la modalità di blocco sull'host ESXi"](#) e ["Comportamento della modalità di blocco VMware"](#) per ulteriori informazioni.

Per gli aggiornamenti API o dell'interfaccia utente di NetApp Hybrid Cloud Control, l'host ESXi verrà automaticamente impostato in modalità di manutenzione durante il processo di aggiornamento, se si dispone della funzione DRS e delle licenze richieste. Il nodo verrà riavviato e, una volta completato il processo di

aggiornamento, l'host ESXi verrà disattivato dalla modalità di manutenzione. Per le opzioni dell'interfaccia utente di USB e BMC, è necessario impostare manualmente l'host ESXi in modalità di manutenzione, come descritto in ciascuna procedura.



Prima di eseguire l'aggiornamento, verificare la versione corrente del driver ESXi. Se il driver non è aggiornato, aggiornarlo. Quindi, aggiornare il firmware di calcolo per i nodi di calcolo.

### Opzioni di upgrade

Scegliere l'opzione appropriata per lo scenario di aggiornamento:

- [Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare un nodo di calcolo](#) (Consigliato)
- [Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare un nodo di calcolo](#)
- [Utilizza un'unità USB con l'immagine del più recente bundle di firmware di calcolo](#)
- [Utilizzo dell'interfaccia utente \(UI\) del Baseboard Management Controller \(BMC\)](#)

## Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare un nodo di calcolo

A partire dai servizi di gestione 2.14, è possibile aggiornare un nodo di calcolo utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control. Dall'elenco dei nodi, selezionare il nodo da aggiornare. La scheda **Current Versions** (versioni correnti) mostra le versioni correnti del firmware e la scheda **Proposed Versions** (versioni proposte) mostra le eventuali versioni di aggiornamento disponibili.



Per un aggiornamento corretto, assicurarsi che il controllo dello stato di salute del cluster vSphere sia stato eseguito correttamente.



L'aggiornamento di NIC, BIOS e BMC può richiedere circa 60 minuti per nodo, a seconda della velocità di connettività di rete tra il nodo di gestione e l'host BMC.



L'utilizzo dell'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware di calcolo sui nodi di calcolo H300E/H500E/H700E non è più supportato. Per eseguire l'aggiornamento, utilizzare un [Unità USB](#) o il [INTERFACCIA UTENTE BMC](#) per montare il bundle del firmware di calcolo.

### Di cosa hai bisogno

- Se il nodo di gestione non è connesso a Internet, il bundle del firmware di calcolo è stato scaricato da "[Sito di supporto NetApp](#)".



Estrarre il TAR.GZ file su a. TAR ed estrarre il TAR file nel bundle del firmware di calcolo.

### Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.

3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare **Compute firmware** (calcolo firmware).
5. Selezionare il cluster da aggiornare.

Verranno visualizzati i nodi nel cluster elencati insieme alle versioni del firmware correnti e alle versioni più recenti, se disponibili per l'aggiornamento.

6. Selezionare **Browse** (Sfoglia) per caricare il bundle del firmware di calcolo scaricato da ["Sito di supporto NetApp"](#).
7. Attendere il completamento del caricamento. Una barra di avanzamento mostra lo stato del caricamento.



Il caricamento del file avviene in background se ci si allontana dalla finestra del browser.

Una volta caricato e validato il file, viene visualizzato un messaggio sullo schermo. La convalida potrebbe richiedere alcuni minuti.

8. Selezionare il bundle del firmware di calcolo.
9. Selezionare **Avvia aggiornamento**.

Dopo aver selezionato **Begin Upgrade** (Avvia aggiornamento), nella finestra vengono visualizzati i controlli di integrità non riusciti, se presenti.



L'aggiornamento non può essere messo in pausa dopo l'inizio. Il firmware verrà aggiornato in sequenza nel seguente ordine: NIC, BIOS e BMC. Non accedere all'interfaccia utente BMC durante l'aggiornamento. L'accesso al BMC termina la sessione Sol (Serial-over-LAN) di Hybrid Cloud Control che monitora il processo di aggiornamento.

10. Se i controlli di integrità a livello di cluster o nodo vengono superati con avvisi, ma senza errori critici, viene visualizzato **Ready to be upgrade** (Pronto per l'aggiornamento). Selezionare **Aggiorna nodo**.



Mentre l'aggiornamento è in corso, è possibile uscire dalla pagina e tornare ad essa in un secondo momento per continuare a monitorare i progressi. Durante l'aggiornamento, l'interfaccia utente visualizza diversi messaggi sullo stato dell'aggiornamento.



Durante l'aggiornamento del firmware sui nodi di calcolo H610C e H615C, non aprire la console Serial-over-LAN (Sol) attraverso l'interfaccia utente Web BMC. Questo potrebbe causare un errore nell'aggiornamento.

Al termine dell'aggiornamento, l'interfaccia utente visualizza un messaggio. Una volta completato l'aggiornamento, è possibile scaricare i registri. Per informazioni sulle varie modifiche dello stato dell'aggiornamento, vedere [Lo stato dell'aggiornamento cambia](#).



Se si verifica un errore durante l'aggiornamento, NetApp Hybrid Cloud Control riavvierà il nodo, ne disconetterà la modalità di manutenzione e visualizzerà lo stato di errore con un link al registro degli errori. È possibile scaricare il log degli errori, che contiene istruzioni specifiche o collegamenti agli articoli della Knowledge base, per diagnosticare e correggere qualsiasi problema. Per ulteriori informazioni sui problemi di aggiornamento del firmware del nodo di calcolo con NetApp Hybrid Cloud Control, consulta questo articolo ["KB"](#) articolo.

## Lo stato dell'aggiornamento cambia

Di seguito sono riportati i diversi stati visualizzati dall'interfaccia utente prima, durante e dopo il processo di aggiornamento:

Stato di aggiornamento	Descrizione
Il nodo non ha superato uno o più controlli di integrità. Espandere per visualizzare i dettagli.	Uno o più controlli di integrità non sono riusciti.
Errore	Si è verificato un errore durante l'aggiornamento. È possibile scaricare il registro degli errori e inviarlo al supporto NetApp.
Impossibile rilevare	Questo stato viene visualizzato se NetApp Hybrid Cloud Control non è in grado di eseguire query sul nodo di calcolo quando la risorsa del nodo di calcolo non dispone del tag hardware.
Pronto per l'aggiornamento.	Tutti i controlli di integrità sono stati superati e il nodo è pronto per essere aggiornato.
Si è verificato un errore durante l'aggiornamento.	L'aggiornamento non riesce con questa notifica quando si verifica un errore critico. Scaricare i registri selezionando il collegamento <b>Download Logs</b> per risolvere l'errore. Dopo aver risolto l'errore, riprovare ad eseguire l'aggiornamento.
Aggiornamento del nodo in corso.	L'aggiornamento è in corso. Una barra di avanzamento mostra lo stato dell'aggiornamento.

## Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare un nodo di calcolo

È possibile utilizzare le API per aggiornare ciascun nodo di calcolo di un cluster alla versione più recente del firmware. È possibile utilizzare uno strumento di automazione a scelta per eseguire le API. Il flusso di lavoro API qui documentato utilizza l'interfaccia utente REST API disponibile sul nodo di gestione come esempio.



L'utilizzo dell'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware di calcolo sui nodi di calcolo H300E/H500E/H700E non è più supportato. Per eseguire l'aggiornamento, utilizzare un [Unità USB](#) o il [INTERFACCIA UTENTE BMC](#) per montare il bundle del firmware di calcolo.

### Di cosa hai bisogno

Le risorse dei nodi di calcolo, incluse le risorse vCenter e hardware, devono essere note alle risorse dei nodi di gestione. È possibile utilizzare le API del servizio di inventario per verificare le risorse (<https://<ManagementNodeIP>/inventory/1/>).

### Fasi

1. Accedere al software NetApp HCI "[pagina di download](#)" e scaricare l'ultimo bundle di firmware di calcolo su un dispositivo accessibile al nodo di gestione.
2. Caricare il bundle del firmware di calcolo nel nodo di gestione:
  - a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/package-repository/1/
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:
    - i. Inserire il nome utente e la password del cluster.
    - ii. Immettere l'ID client come `mnode-client`.
    - iii. Selezionare **autorizzare** per avviare una sessione.
    - iv. Chiudere la finestra di autorizzazione.
  - c. Dall'interfaccia utente API REST, selezionare **POST /packages**.
  - d. Selezionare **Provalo**.
  - e. Selezionare **Browse** (Sfoglia) e selezionare il bundle del firmware di calcolo.
  - f. Selezionare **Esegui** per avviare il caricamento.
  - g. Dalla risposta, copiare e salvare l'ID bundle del firmware di calcolo ("`id`") da utilizzare in un passaggio successivo.
3. Verificare lo stato del caricamento.
- a. Dall'interfaccia utente API REST, selezionare **GET /packages/{id}/status**.
  - b. Selezionare **Provalo**.
  - c. Inserire l'ID bundle del firmware di calcolo copiato nella fase precedente in **id**.
  - d. Selezionare **Esegui** per avviare la richiesta di stato.

La risposta indica `state` come `SUCCESS` al termine dell'operazione.

- e. Dalla risposta, copiare e salvare il nome del bundle del firmware di calcolo ("`name`") e la versione ("`version`") da utilizzare in un passaggio successivo.
4. Individuare l'ID del controller di calcolo e l'ID hardware del nodo da aggiornare:
- a. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:
  - i. Inserire il nome utente e la password del cluster.
  - ii. Immettere l'ID client come `mnode-client`.
  - iii. Selezionare **autorizzare** per avviare una sessione.
  - iv. Chiudere la finestra di autorizzazione.
- c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
- d. Selezionare **Provalo**.
- e. Selezionare **Esegui**.
- f. Dalla risposta, copiare l'ID della risorsa di installazione ("`id`").
- g. Dall'interfaccia utente API REST, selezionare **GET /Installations/{id}**.



- h. Selezionare **Provalo**.
- i. Incollare l'ID della risorsa di installazione nel campo **id**.
- j. Selezionare **Esegui**.
- k. Dalla risposta, copiare e salvare l'ID del controller del cluster ("controllerId") E l'ID hardware del nodo ("hardwareId") per l'utilizzo in un passaggio successivo:

```
"compute": {  
  "errors": [],  
  "inventory": {  
    "clusters": [  
      {  
        "clusterId": "Test-1B",  
        "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
```

```
"nodes": [  
  {  
    "bmcDetails": {  
      "bmcAddress": "10.111.0.111",  
      "credentialsAvailable": true,  
      "credentialsValidated": true  
    },  
    "chassisSerialNumber": "111930011231",  
    "chassisSlot": "D",  
    "hardwareId": "123a4567-01b1-1243-a12b-11ab11ab0a15",  
    "hardwareTag": "00000000-0000-0000-0000-ab1c2de34f5g",  
    "id": "e1111d10-1a1a-12d7-1a23-ab1cde23456f",  
    "model": "H410C",
```

5. Eseguire l'aggiornamento del firmware del nodo di calcolo:
- a. Aprire l'interfaccia utente dell'API REST del servizio hardware sul nodo di gestione:

```
https://<ManagementNodeIP>/hardware/2/
```

- b. Selezionare **autorizzare** e completare le seguenti operazioni:
  - i. Inserire il nome utente e la password del cluster.
  - ii. Immettere l'ID client come `mnode-client`.
  - iii. Selezionare **autorizzare** per avviare una sessione.
  - iv. Chiudere la finestra di autorizzazione.
- c. Selezionare **POST /nodi/{hardware\_id}/upgrade**.
- d. Selezionare **Provalo**.

- e. Inserire l'ID della risorsa host hardware ("hardwareId" salvato da un passo precedente) nel campo dei parametri.
- f. Eseguire le seguenti operazioni con i valori del payload:
  - i. Conservare i valori "force": false e "maintenanceMode": true" In modo che i controlli di integrità vengano eseguiti sul nodo e che l'host ESXi sia impostato sulla modalità di manutenzione.
  - ii. Inserire l'ID del controller del cluster ("controllerId" salvato da un passaggio precedente).
  - iii. Inserire il nome e la versione del bundle del firmware di calcolo salvati in un passaggio precedente.

```
{
  "config": {
    "force": false,
    "maintenanceMode": true
  },
  "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
  "packageName": "compute-firmware-12.2.109",
  "packageVersion": "12.2.109"
}
```

- g. Selezionare **Esegui** per avviare l'aggiornamento.



L'aggiornamento non può essere messo in pausa dopo l'inizio. Il firmware verrà aggiornato in sequenza nel seguente ordine: NIC, BIOS e BMC. Non accedere all'interfaccia utente BMC durante l'aggiornamento. L'accesso al BMC termina la sessione Sol (Serial-over-LAN) di Hybrid Cloud Control che monitora il processo di aggiornamento.

- h. Copiare l'ID dell'attività di aggiornamento che fa parte del link delle risorse ("resourceLink") Nella risposta.
6. Verificare l'avanzamento e i risultati dell'aggiornamento:
- a. Selezionare **GET /task/{task\_id}/logs**.
  - b. Selezionare **Provalo**.
  - c. Inserire l'ID attività del passaggio precedente in **task\_id**.
  - d. Selezionare **Esegui**.
  - e. In caso di problemi o requisiti speciali durante l'aggiornamento, eseguire una delle seguenti operazioni:

Opzione	Fasi
È necessario correggere i problemi di integrità del cluster dovuti a. <code>failedHealthChecks</code> messaggio nel corpo della risposta.	<ul style="list-style-type: none"> <li>i. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata.</li> <li>ii. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.</li> <li>iii. Una volta risolti i problemi del cluster, eseguire nuovamente l'autenticazione, se necessario, e selezionare <b>POST</b> <code>/nodes/{hardware_id}/upgrade</code>.</li> <li>iv. Ripetere i passaggi descritti in precedenza nella fase di aggiornamento.</li> </ul>
L'aggiornamento non riesce e i passaggi di mitigazione non sono elencati nel log di aggiornamento.	<ul style="list-style-type: none"> <li>i. Vedi questo <a href="#">"Articolo della Knowledge base"</a> (accesso richiesto).</li> </ul>

f. Eseguire l'API **GET** `/task/{task_id}/logs` più volte, in base alle necessità, fino al completamento del processo.

Durante l'aggiornamento, il `status` indica `running` se non si riscontrano errori. Al termine di ogni fase, il `status` il valore cambia in `completed`.

L'aggiornamento è stato completato correttamente quando lo stato di ogni passaggio è `completed` e a. `percentageCompleted` il valore è 100.

7. (Facoltativo) confermare le versioni del firmware aggiornate per ciascun componente:

a. Aprire l'interfaccia utente dell'API REST del servizio hardware sul nodo di gestione:

```
https://<ManagementNodeIP>/hardware/2/
```

b. Selezionare **autorizzare** e completare le seguenti operazioni:

- i. Inserire il nome utente e la password del cluster.
- ii. Immettere l'ID client come `mnode-client`.
- iii. Selezionare **autorizzare** per avviare una sessione.
- iv. Chiudere la finestra di autorizzazione.

c. Dall'interfaccia utente API REST, selezionare **GET** `/nodes/{hardware_id}/upgrade`.

d. (Facoltativo) inserire i parametri di data e stato per filtrare i risultati.

e. Inserire l'ID della risorsa host hardware ("`hardwareId`" salvato da un passo precedente) nel campo dei parametri.

f. Selezionare **Provalo**.

g. Selezionare **Esegui**.

h. Verificare nella risposta che il firmware per tutti i componenti sia stato aggiornato correttamente dalla

versione precedente alla versione più recente.

## Utilizza un'unità USB con l'immagine del più recente bundle di firmware di calcolo

È possibile inserire un'unità USB con il pacchetto di firmware di calcolo più recente scaricato su una porta USB del nodo di calcolo. In alternativa all'utilizzo del metodo USB thumb drive descritto in questa procedura, è possibile montare il bundle del firmware di calcolo sul nodo di calcolo utilizzando l'opzione **Virtual CD/DVD** nella console virtuale nell'interfaccia Baseboard Management Controller (BMC). Il metodo BMC impiega molto più tempo del metodo USB thumb drive. Assicurarsi che la workstation o il server disponga della larghezza di banda di rete necessaria e che la sessione del browser con BMC non sia in timeout.

### Di cosa hai bisogno

- Se il nodo di gestione non è connesso a Internet, il bundle del firmware di calcolo è stato scaricato da "[Sito di supporto NetApp](#)".



Estrarre il TAR.GZ file su a. TAR ed estrarre il TAR file nel bundle del firmware di calcolo.

### Fasi

1. Utilizzare l'utility etcher per aggiornare il bundle del firmware di calcolo su un'unità USB.
2. Impostare il nodo di calcolo in modalità di manutenzione utilizzando VMware vCenter e svuotare tutte le macchine virtuali dall'host.



Se VMware Distributed Resource Scheduler (DRS) è attivato sul cluster (impostazione predefinita nelle installazioni NetApp HCI), le macchine virtuali vengono migrate automaticamente in altri nodi del cluster.

3. Inserire la chiavetta USB in una porta USB sul nodo di calcolo e riavviare il nodo di calcolo utilizzando VMware vCenter.
4. Durante il ciclo POST del nodo di calcolo, premere **F11** per aprire Boot Manager. Potrebbe essere necessario premere **F11** più volte in rapida successione. È possibile eseguire questa operazione collegando un video/una tastiera o utilizzando la console in BMC.
5. Selezionare **One Shot > USB Flash Drive** dal menu visualizzato. Se la chiavetta USB non viene visualizzata nel menu, verificare che l'unità flash USB faccia parte dell'ordine di avvio precedente nel BIOS del sistema.
6. Premere **Invio** per avviare il sistema dalla chiavetta USB. Viene avviato il processo di aggiornamento del firmware.

Una volta completato il flash del firmware e riavviato il nodo, l'avvio di ESXi potrebbe richiedere alcuni minuti.

7. Una volta completato il riavvio, uscire dalla modalità di manutenzione sul nodo di calcolo aggiornato utilizzando vCenter.
8. Rimuovere l'unità flash USB dal nodo di calcolo aggiornato.
9. Ripetere questa attività per gli altri nodi di calcolo nel cluster ESXi fino a quando tutti i nodi di calcolo non vengono aggiornati.

## Utilizzo dell'interfaccia utente (UI) del Baseboard Management Controller (BMC)

È necessario eseguire le operazioni sequenziali per caricare il bundle del firmware di calcolo e riavviare il nodo nel bundle del firmware di calcolo per garantire che l'aggiornamento sia stato eseguito correttamente. Il bundle del firmware di calcolo deve trovarsi sul sistema o sulla macchina virtuale (VM) che ospita il browser Web. Prima di avviare il processo, verificare di aver scaricato il bundle del firmware di calcolo.



Si consiglia di avere il sistema o la macchina virtuale e il nodo sulla stessa rete.



L'aggiornamento tramite l'interfaccia utente BMC richiede da 25 a 30 minuti circa.

- [Aggiornare il firmware sui nodi H410C e H300E/H500E/H700E](#)
- [Aggiornare il firmware sui nodi H610C/H615C](#)

### Aggiornare il firmware sui nodi H410C e H300E/H500E/H700E

Se il nodo fa parte di un cluster, è necessario impostare il nodo in modalità di manutenzione prima dell'aggiornamento e portarlo fuori dalla modalità di manutenzione dopo l'aggiornamento.



Ignorare il seguente messaggio informativo visualizzato durante il processo: `Untrusty Debug Firmware Key is used, SecureFlash is currently in Debug Mode`

#### Fasi

1. Se il nodo fa parte di un cluster, metterlo in modalità di manutenzione come indicato di seguito. In caso contrario, passare alla fase 2.
  - a. Accedere al client Web di VMware vCenter.
  - b. Fare clic con il pulsante destro del mouse sul nome dell'host (nodo di calcolo) e selezionare **Maintenance Mode (modalità di manutenzione) > Enter Maintenance Mode (attiva modalità di manutenzione)**.
  - c. Selezionare **OK**. Le VM sull'host verranno migrate su un altro host disponibile. La migrazione delle macchine virtuali può richiedere tempo a seconda del numero di macchine virtuali da migrare.



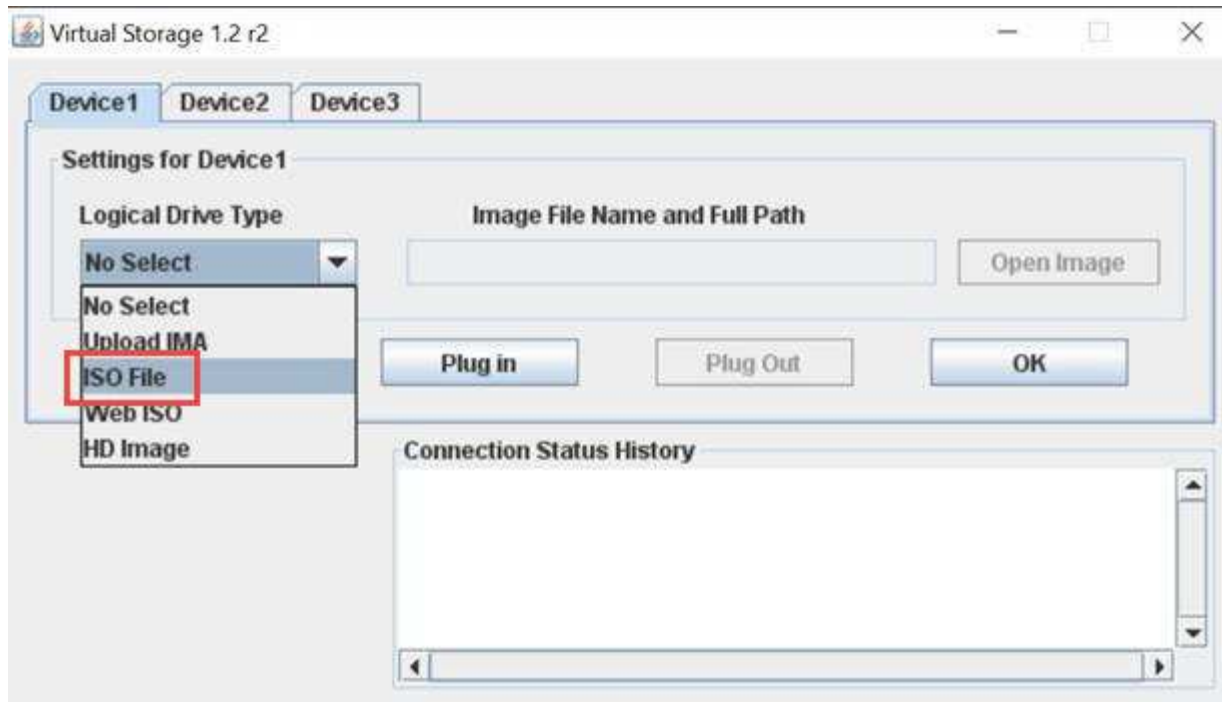
Prima di procedere, assicurarsi che tutte le macchine virtuali dell'host vengano migrate.

2. Accedere all'interfaccia utente BMC, <https://BMCIP/#login>, Dove BMCIP è l'indirizzo IP del BMC.
3. Accedere utilizzando le credenziali.
4. Selezionare **Remote Control > Console Redirection** (controllo remoto > reindirizzamento console).
5. Selezionare **Launch Console** (Avvia console).



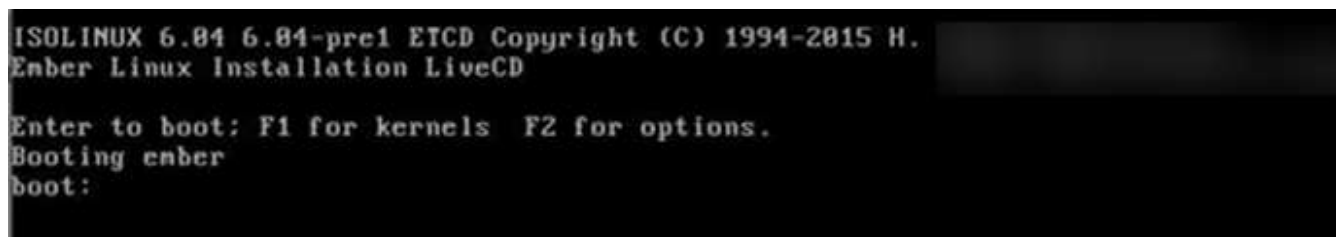
Potrebbe essere necessario installare Java o aggiornarlo.

6. All'apertura della console, selezionare **Virtual Media > Virtual Storage**.
7. Nella schermata **Virtual Storage**, selezionare **Logical Drive Type** (tipo di unità logica) e selezionare **ISO file**.



8. Selezionare **Open Image** (Apri immagine) per accedere alla cartella in cui è stato scaricato il file bundle del firmware di calcolo e selezionare il file bundle del firmware di calcolo.
9. Selezionare **Plug-in**.
10. Quando viene visualizzato lo stato della connessione Device#: VM Plug-in OK!., Selezionare **OK**.
11. Riavviare il nodo premendo **F12** e selezionando **Riavvia** o selezionando **controllo alimentazione > Imposta ripristino alimentazione**.
12. Durante il riavvio, premere **F11** per selezionare le opzioni di avvio e caricare il bundle del firmware di calcolo. Potrebbe essere necessario premere F11 alcune volte prima che venga visualizzato il menu di avvio.

Viene visualizzata la seguente schermata:



13. Nella schermata precedente, premere **Invio**. A seconda della rete in uso, potrebbero essere necessari alcuni minuti dopo aver premuto **Invio** per l'avvio dell'aggiornamento.



Alcuni aggiornamenti del firmware potrebbero causare la disconnessione della console e/o la disconnessione della sessione sul BMC. È possibile accedere nuovamente a BMC, tuttavia alcuni servizi, come la console, potrebbero non essere disponibili a causa degli aggiornamenti del firmware. Una volta completati gli aggiornamenti, il nodo esegue un riavvio a freddo, che può richiedere circa cinque minuti.

14. Accedere nuovamente all'interfaccia utente BMC e selezionare **System** per verificare la versione del BIOS e il tempo di creazione dopo l'avvio del sistema operativo. Se l'aggiornamento è stato completato

correttamente, vengono visualizzate le nuove versioni di BIOS e BMC.



La versione del BIOS non mostrerà la versione aggiornata fino a quando il nodo non avrà completato l'avvio.

15. Se il nodo fa parte di un cluster, completare la procedura riportata di seguito. Se si tratta di un nodo standalone, non sono necessarie ulteriori azioni.
  - a. Accedere al client Web di VMware vCenter.
  - b. Portare l'host fuori dalla modalità di manutenzione. Potrebbe essere visualizzato un segnale d'allarme disconnesso. Attendere che tutti gli stati siano cancellati.
  - c. Accendere tutte le macchine virtuali rimanenti che sono state spente.

### Aggiornare il firmware sui nodi H610C/H615C

I passaggi variano a seconda che il nodo sia standalone o parte di un cluster. La procedura può richiedere circa 25 minuti e comprende lo spegnimento del nodo, il caricamento del bundle del firmware di calcolo, l'aggiornamento dei dispositivi e la riaccensione del nodo dopo l'aggiornamento.

#### Fasi

1. Se il nodo fa parte di un cluster, metterlo in modalità di manutenzione come indicato di seguito. In caso contrario, passare alla fase 2.
  - a. Accedere al client Web di VMware vCenter.
  - b. Fare clic con il pulsante destro del mouse sul nome dell'host (nodo di calcolo) e selezionare **Maintenance Mode (modalità di manutenzione) > Enter Maintenance Mode (attiva modalità di manutenzione)**.
  - c. Selezionare **OK**. Le VM sull'host verranno migrate su un altro host disponibile. La migrazione delle macchine virtuali può richiedere tempo a seconda del numero di macchine virtuali da migrare.



Prima di procedere, assicurarsi che tutte le macchine virtuali dell'host vengano migrate.

2. Accedere all'interfaccia utente BMC, <https://BMCIP/#login>, Dove BMC IP è l'indirizzo IP del BMC.
3. Accedere utilizzando le credenziali.
4. Selezionare **Remote Control > Launch KVM (Java)**.
5. Nella finestra della console, selezionare **Media > Virtual Media Wizard**.



6. Selezionare **Browse** (Sfoglia) e selezionare il firmware di calcolo .iso file.
7. Selezionare **Connect**. Viene visualizzata una finestra a comparsa che indica il successo, insieme al percorso e al dispositivo visualizzati in basso. È possibile chiudere la finestra **Virtual Media**.



8. Riavviare il nodo premendo **F12** e selezionando **Riavvia** o selezionando **controllo alimentazione > Imposta ripristino alimentazione**.
9. Durante il riavvio, premere **F11** per selezionare le opzioni di avvio e caricare il bundle del firmware di calcolo.
10. Selezionare **AMI Virtual CDROM** dall'elenco visualizzato e selezionare **Invio**. Se nell'elenco non viene visualizzato AMI Virtual CDROM, accedere al BIOS e attivarlo nell'elenco di avvio. Il nodo viene riavviato dopo il salvataggio. Durante il riavvio, premere **F11**.



11. Nella schermata visualizzata, selezionare **Invio**.



Alcuni aggiornamenti del firmware potrebbero causare la disconnessione della console e/o la disconnessione della sessione sul BMC. È possibile accedere nuovamente a BMC, tuttavia alcuni servizi, come la console, potrebbero non essere disponibili a causa degli aggiornamenti del firmware. Una volta completati gli aggiornamenti, il nodo esegue un riavvio a freddo, che può richiedere circa cinque minuti.

12. Se ci si disconnette dalla console, selezionare **Remote Control** e selezionare **Launch KVM** or **Launch KVM (Java)** per riconnettersi e verificare quando il nodo ha terminato il backup. Potrebbero essere necessarie più riconnessioni per verificare che il nodo sia stato avviato correttamente.





Durante il processo di accensione, per circa cinque minuti, la console KVM visualizza **Nessun segnale**.

13. Una volta acceso il nodo, selezionare **Dashboard > Device Information > More info** (pannello di controllo > informazioni dispositivo > ulteriori informazioni) per verificare le versioni del BIOS e del BMC. Vengono visualizzate le versioni aggiornate del BIOS e di BMC. La versione aggiornata del BIOS non viene visualizzata fino a quando il nodo non si è avviato completamente.
14. Se il nodo è stato impostato in modalità di manutenzione, dopo l'avvio del nodo in ESXi, fare clic con il pulsante destro del mouse sul nome dell'host (nodo di calcolo) e selezionare **modalità di manutenzione > Esci dalla modalità di manutenzione**, quindi eseguire nuovamente la migrazione delle macchine virtuali nell'host.
15. In vCenter, con il nome host selezionato, configurare e verificare la versione del BIOS.

## Trova ulteriori informazioni

- ["Plug-in NetApp Element per server vCenter"](#)
- ["Pagina delle risorse NetApp HCI"](#)

## Automatizza gli aggiornamenti del firmware dei nodi di calcolo con Ansible

È possibile aggiornare il firmware di sistema sui nodi di calcolo NetApp HCI, incluso il firmware per componenti come BMC, BIOS e NIC, utilizzando i flussi di lavoro in NetApp Hybrid Cloud Control. Per le installazioni con cluster di calcolo di grandi dimensioni, è possibile automatizzare i flussi di lavoro utilizzando Ansible per eseguire un aggiornamento continuo dell'intero cluster.



Mentre il ruolo Ansible per automatizzare gli aggiornamenti del firmware dei nodi di calcolo è reso disponibile da NetApp, l'automazione è un componente ausiliario che richiede una configurazione aggiuntiva e l'esecuzione di componenti software. La modifica dell'automazione Ansible è supportata solo con il massimo sforzo.



Il ruolo Ansible per gli upgrade funziona solo sui nodi di calcolo NetApp HCI serie H. Non è possibile utilizzare questo ruolo per aggiornare i nodi di calcolo di terze parti.

### Di cosa hai bisogno

- **Disponibilità e prerequisiti per gli aggiornamenti del firmware:** L'installazione di NetApp HCI deve essere pronta per l'aggiornamento del firmware, come indicato nelle istruzioni per ["esecuzione degli aggiornamenti del firmware"](#).
- **Possibilità di eseguire l'automazione sul nodo di controllo Ansible:** Un server fisico o virtuale per eseguire l'automazione dell'aggiornamento del firmware in Ansible.

### A proposito di questa attività

In un ambiente di produzione, è necessario aggiornare i nodi di calcolo in un cluster in un'installazione NetApp HCI in modo variabile; un nodo alla volta, uno alla volta. Le API di NetApp Hybrid Cloud Control orchestrano il processo di aggiornamento del firmware del nodo di calcolo complessivo per un singolo nodo di calcolo, tra cui l'esecuzione di controlli dello stato di salute, il posizionamento di ESXi sui nodi di calcolo e il riavvio del nodo di calcolo per applicare gli aggiornamenti del firmware. Il ruolo Ansible consente di orchestrare l'aggiornamento

del firmware per un gruppo di nodi di calcolo o interi cluster.

### **Inizia a utilizzare l'automazione dell'aggiornamento del firmware**

Per iniziare, accedere a. ["Repository NetApp Ansible su GitHub"](#) e scaricare `nar_compute_nodes_firmware_upgrades` ruolo e documentazione.

### **Trova ulteriori informazioni**

- ["Pagina delle risorse NetApp HCI"](#)

## 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.