



Usa Upgrade Health Checker

Upgrade Health Checker

NetApp

September 11, 2026

This PDF was generated from <https://docs.netapp.com/it-it/upgrade-health-checker/generate-report-upgrade-health-checker.html> on September 11, 2026. Always check docs.netapp.com for the latest.

Sommario

- Usa Upgrade Health Checker 1
 - Genera un piano di upgrade con Upgrade Health Checker..... 1
 - Aggiorna la dashboard di Health Checker 3
 - Automatizza la generazione di piani di upgrade con Upgrade Health Checker..... 5
 - Ricevi i report di verifica dello stato di aggiornamento via e-mail 7
 - Configura tramite il file config.yaml 7
 - Configura tramite argomenti della riga di comando 8

Usa Upgrade Health Checker

Genera un piano di upgrade con Upgrade Health Checker

È possibile utilizzare Upgrade Health Checker per generare un piano di aggiornamento per uno o più cluster ONTAP.

Puoi anche ["automatizzare la generazione di report di aggiornamento"](#) per fornire assistenza nel mantenere aggiornati i piani di aggiornamento se hai un ambiente ampio e complesso con più cluster.

Informazioni su questa attività

Upgrade Health Checker supporta gli aggiornamenti per le versioni ONTAP on-premises 9.11.1 e successive. Se si utilizza Cloud Volumes ONTAP, consultare ["Aggiorna Cloud Volumes ONTAP"](#) per informazioni sull'aggiornamento del sistema.

Prima di iniziare

Per saperne di più su un parametro specifico di Upgrade Health Checker e sull'ordine di priorità con cui lo strumento accetta l'input, fare riferimento a ["Scopri i parametri di input per Upgrade Health Checker"](#).

Passaggi

1. Imposta l'autorizzazione di esecuzione sul binario prima di eseguirlo per la prima volta:

```
chmod +x uhc
```



Upgrade Health Checker è un pacchetto autonomo e dovrà essere decompresso prima di essere eseguito. Questo può richiedere alcuni secondi.

2. Prima di completare un'esecuzione completa di Upgrade Health Checker, esegui un controllo completo per assicurarti che lo strumento possa connettersi al cluster e agli endpoint richiesti:

```
--test all
```

Il controllo completo garantisce che la macchina virtuale che ospita Upgrade Health Checker abbia:

- Connettività all'indirizzo IP del cluster ONTAP tramite HTTPS
 - Connettività all'endpoint di telemetria (<https://support.netapp.com/> e <https://api.activeiq.netapp.com>) tramite HTTPS
 - Connettività agli endpoint di aggiornamento automatico (<https://api.uhc.netapp.com>, <https://gql.aiq.netapp.com>, e <https://api.activeiq.netapp.com>) tramite HTTPS (443)
 - Almeno 4 GB di spazio /tmp disponibile
3. (Facoltativo) Se si desidera utilizzare un file di configurazione per memorizzare i parametri, rinominare il `config.yaml.example` file che si trova nella stessa posizione in cui è stato scaricato il file binario in `config.yaml`.

Ecco un esempio di file `config.yaml`:

```
# Application Configuration
APP:
  RUNS_PATH: "/opt/uhc/runs"

# Cluster Credentials
CLUSTER:
  IP: "x.x.x.x"
  USERNAME: "admin"
  PASSWORD: "xyz"
  TARGET_ONTAP_VERSION: "" # Optional: Specify target ONTAP version
  (e.g., "9.16.1" or "current" to keep existing version). Leave empty to
  prompt user.
  ACCEPT_EULA: false # Optional: Set to true to accept EULA through
  config. If false/empty, user will be prompted interactively.
```

4. Esegui Upgrade Health Checker inserendo la versione di ONTAP a cui vuoi eseguire l'aggiornamento e accettando l'EULA, inclusi eventuali parametri aggiuntivi necessari.



L'EULA è un documento composto da più pagine. Inserisci `all` per visualizzare l'intero documento in una sola volta e inserisci `y` per accettarlo.

Dopo che il log di AutoSupport è stato scaricato per un cluster, l'elaborazione richiede generalmente da uno a due minuti, a seconda del numero di nodi del cluster. Poiché le diverse versioni di ONTAP gestiscono la raccolta di AutoSupport in modo diverso, ogni esecuzione di Upgrade Health Checker dipende dal carico attuale del cluster e dalla versione di ONTAP.

- a. Familiarizza con i parametri disponibili di Upgrade Health Checker, l'ordine di priorità di input e i valori predefiniti per determinati parametri facendo riferimento a ["Scopri i parametri di input per Upgrade Health Checker"](#).

La Guida ai Parametri di Input fornisce anche informazioni su come specificare un percorso personalizzato per il file di configurazione e un percorso di esecuzione per semplificare il flusso di lavoro. La best practice è creare una directory di output personalizzata per ogni cluster per organizzare i report e i log in modo efficace.

- b. Esegui Upgrade Health Checker accettando l'EULA e immettendo la versione di ONTAP di destinazione e tutti gli altri parametri.

```
./uhc
```

5. Dopo che Upgrade Health Checker ha completato i controlli, accedi alla `runs` cartella per visualizzare il piano di aggiornamento e il report del cluster.



Ogni esecuzione del programma è una "esecuzione unica" e avrà tutti i dati, i registri e i risultati associati nella cartella `runs` associata.

6. Elenca i file di report generati:

```
ls -lrt
```

7. Apri il file di report (denominato `uhc_<cluster-name>_<YYYYMMDDHHMMSS>`) in un browser web, Microsoft Excel o un visualizzatore JSON per visualizzare il report. Se lo esegui su un host remoto, scarica prima il file di report su un computer in cui puoi visualizzare il report in un browser web, in Excel o in un visualizzatore JSON.

Il percorso del registro e il percorso del report sono i seguenti:

- Percorso del registro: `<output-path>/<unique-run-dir>/<cluster-name>/logs`
- Percorso del report HTML: `<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`
- Percorso del report Excel: `<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.xlsx`
- Percorso del report JSON: `<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.json`

Cosa c'è dopo

Dopo aver generato il piano di aggiornamento e il report del cluster, è possibile visualizzare il ["Aggiorna la dashboard di Health Checker"](#) per dettagli sullo stato di salute dei cluster valutati durante l'esecuzione.

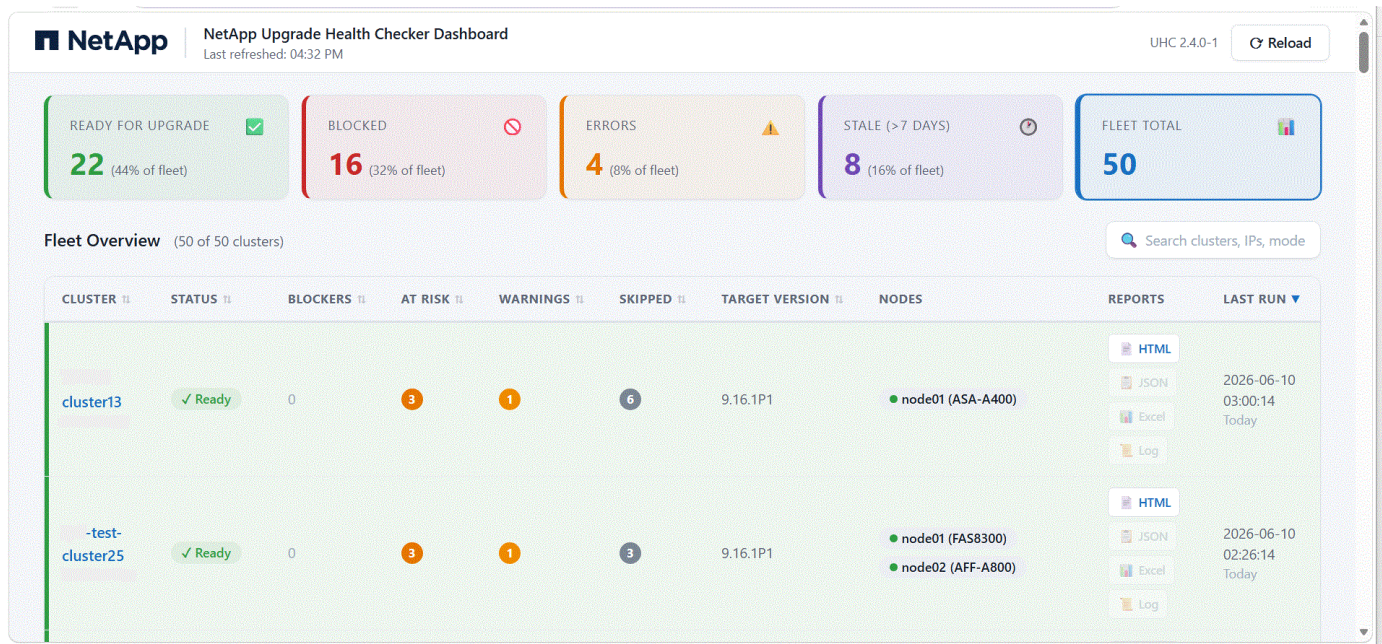
Aggiorna la dashboard di Health Checker

Un dashboard HTML statico viene generato in `runs/dashboard/index.html` al termine di ogni esecuzione di Upgrade Health Checker. Il dashboard fornisce una panoramica high-level dello stato di salute dei cluster valutati di recente, consentendo di monitorare e confrontare la predisposizione all'aggiornamento tra i cluster.

Per rigenerare la dashboard in un secondo momento (senza contattare un cluster), eseguire:

```
./uhc --dashboard
./uhc --dashboard --runs-path /custom/output
./uhc --dashboard --config-path /path/to/custom_config.yaml
```

Di seguito è riportata una schermata di una dashboard di Upgrade Health Checker generata di recente.



Nella parte superiore della pagina sono presenti cinque schede riassuntive con codice colore (ognuna delle quali funge anche da filtro selezionabile) che mostrano:

- **Pronti per l'aggiornamento:** Numero di cluster il cui ultimo controllo di integrità non ha rilevato blocchi, ovvero pronti per l'aggiornamento.
- **Bloccati:** Numero di cluster bloccati e impossibilitati ad eseguire l'aggiornamento fino alla risoluzione dei blocker.
- **Errori:** Numero di cluster la cui ultima esecuzione di UHC non è riuscita a essere completata (ad esempio, errore di connessione, autenticazione o raccolta dati).
- **Obsoleto (>7):** Numero di cluster la cui ultima esecuzione di UHC risale a più di 7 giorni fa (i dati del controllo di integrità sono obsoleti).
- **Totale flotta:** Numero totale di cluster nella flotta (quelli con un'esecuzione nella finestra del dashboard, l'impostazione predefinita è gli ultimi 30 giorni).

La sezione Panoramica della flotta descrive in dettaglio lo stato attuale della flotta. Per ogni cluster vengono fornite le seguenti informazioni (la tabella mostra l'ultima esecuzione per cluster):

- **Nome del cluster:** Nome del cluster (con il relativo indirizzo IP di gestione visualizzato sotto il nome).
- **Stato:** Stato attuale del cluster: Pronto, Bloccato, Errore o Inattivo.
- **Bloccatori:** Numero di bloccanti sul cluster. Si tratta di problemi critici che devono essere risolti prima dell'aggiornamento.
- **A rischio:** Numero di elementi a rischio nel cluster. Si tratta di rischi identificati durante il controllo preliminare all'aggiornamento.
- **Avvisi:** Numero di avvisi sul cluster. Il controllo preliminare all'aggiornamento è stato completato con alcuni avvisi; è possibile scegliere di risolvere questi avvisi o continuare con l'aggiornamento.
- **Saltati:** Numero di controlli che sono stati saltati sul cluster.
- **Versione di destinazione:** La versione di ONTAP a cui l'utente intende eseguire l'aggiornamento. (Può essere la stessa della versione corrente se si desidera eseguire solo un controllo di integrità sulla versione in esecuzione.)

- **Nodi:** I nodi del cluster, ciascuno mostrato come nome del nodo con il relativo modello hardware (ad esempio eurbkpc1a (FAS8200)).
- **Report:** Formati di report disponibili per l'esecuzione: HTML, JSON, Excel, Log.
- **Ultima esecuzione:** Data e ora dell'ultima esecuzione di Upgrade Health Checker (con un riferimento relativo "X giorni fa").

Puoi selezionare **Ricarica** per aggiornare la pagina. Utilizza la barra **Cerca** per cercare i dettagli di uno specifico cluster.

Automatizza la generazione di piani di upgrade con Upgrade Health Checker

È possibile automatizzare la generazione di report Upgrade Health Checker per ridurre lo sforzo manuale durante la pianificazione degli aggiornamenti ONTAP in ambienti di grandi dimensioni e complessi.

Informazioni su questa attività

Upgrade Health Checker supporta gli aggiornamenti per le versioni ONTAP on-premises 9.11.1 e successive. Se si utilizza Cloud Volumes ONTAP, consultare ["Aggiorna Cloud Volumes ONTAP"](#) per informazioni sull'aggiornamento del sistema.

Passaggi

1. Per garantire la corretta creazione dei report di aggiornamento, completare tutti i passaggi di configurazione necessari e le attività una tantum descritte in ["Genera un report di aggiornamento ONTAP"](#).
2. Crea uno script per eseguire Upgrade Health Checker con i parametri appropriati per il tuo ambiente.

```
./uhc \
  --cluster-ip=<cluster-ip> \
  --cluster-username=<cluster-username> \
  --cluster-password=<cluster-password> \
  --target-ontap-version=<target-ontap-version> \
  --accept-eula=true
```

3. Crea uno script di automazione per le pianificazioni cron per eseguire Upgrade Health Checker. Il seguente script di esempio esegue Upgrade Health Checker per più cluster. I file binario e config.yaml sono stati installati in /opt/uhc/tool/.

```
#!/bin/bash
# /opt/uhc/tool/uhccron.sh
# Automated weekly Upgrade Health Checker run for all managed clusters
# Schedule: Every Monday to Friday at 4am

cd /opt/uhc/tool/

# Cluster1 - keep current version (health check only)
/opt/uhc/tool/uhc --cluster-ip cluster1-mgmt.example.com \ --target
```

```
-ontap-version current

# Cluster2 - target upgrade to 9.16.1
/opt/uhc/tool/uhc --cluster-ip cluster2-mgmt.example.com \ --target
-ontap-version 9.16.1

# Cluster3 - target upgrade to 9.17.1
/opt/uhc/tool/uhc --cluster-ip cluster3-mgmt.example.com \ --target
-ontap-version 9.17.1

# Cluster4 - by IP address
/opt/uhc/tool/uhc --cluster-ip 10.20.30.40 --target-ontap-version 9.16.1

# Add additional clusters as needed

# Make the script executable (one-time setup step)
chmod +x /opt/uhc/tool/uhcron.sh
```

4. Configura il cron job per eseguire lo script dal lunedì al venerdì alle 4:00 del mattino:

```
# Edit the crontab for the uhctool user
crontab -e

# Add the following line to schedule the script to run Monday through
Friday at 4:00 am
0 4 * * 1-5 /opt/uhc/tool/uhcron.sh
```



Per il monitoraggio continuo dello stato di salute, utilizzare `--target-ontap-version current` senza un target di aggiornamento specifico.

1. Dopo che Upgrade Health Checker ha completato i controlli, accedere alla `runs` cartella per visualizzare il piano di aggiornamento e il report del cluster.



Ogni esecuzione del programma è un'esecuzione unica e avrà tutti i dati, i log e i risultati associati nella cartella associata `runs`.

2. Apri il file di report (denominato `uhc_<cluster-name>_<YYYYMMDDHHMMSS>`) in un browser web, Microsoft Excel o un visualizzatore JSON per visualizzare il report. Se esegui Upgrade Health Checker su un host remoto, scarica prima il file di report su un computer in cui puoi visualizzare il report in un browser web, in Excel o in un visualizzatore JSON.

Il percorso del registro e il percorso del report sono i seguenti:

- Percorso del registro: `<output-path>/<unique-run-dir>/<cluster-name>/logs`
- Percorso del report HTML: `<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`

- Percorso del report Excel: <output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.xlsx
- Percorso del report JSON: <output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.json

Ricevi i report di verifica dello stato di aggiornamento via e-mail

Upgrade Health Checker può inviare i report direttamente alla tua casella di posta. Abilita questa funzione tramite il file config.yaml o un argomento della riga di comando. Quando è abilitato, Upgrade Health Checker invia i report generati (HTML, Excel o JSON) a uno o più destinatari tramite un server SMTP. Quando è disabilitato, non viene inviato alcun report. Se la generazione del report non riesce e l'invio tramite email è abilitato, Upgrade Health Checker invia i file di log ai destinatari configurati.

Configura tramite il file config.yaml

Puoi configurare le impostazioni email nel file config.yaml abilitando i report email, aggiungendo i dettagli del server SMTP e specificando gli indirizzi dei destinatari e i formati dei report.

1. Abilita i report via email nel file config.yaml.

```
# Email Report Configuration
EMAIL:
  ENABLED: true
```

2. Aggiungi le impostazioni di configurazione SMTP, i dettagli del mittente e l'oggetto:

```
# SMTP Server Configuration
EMAIL:
  ENABLED: true
  FROM: "uhc-notify@example.com"
  SUBJECT: "UHC Upgrade Health Report"
  REPLY_TO: <email>
  SMTP:
    HOST: "smtp.example.com"
    PORT: [<port-number>]
```

3. Aggiungi gli indirizzi email dei destinatari e imposta i formati dei report che il sistema invia via email, ad esempio HTML, EXCEL, JSON o ALL. Puoi anche usare l'autenticazione e la crittografia:

```
# Recipient Email Addresses, report formats
EMAIL:
  ENABLED: true
```

```
TO: <recipient>
FROM: "uhc-notify@example.com"
SUBJECT: "UHC Upgrade Health Report"
REPLY_TO: <email>
RECIPIENTS: "user1@example.com, user2@example.com"
REPORT_FORMATS: "HTML,EXCEL,JSON"    # valid values: HTML, EXCEL, JSON
or ALL
SMTP:
  HOST: "smtp.example.com"
  PORT: [PORT]
  USE_SMTP_AUTH: true
  USE_TLS: true
  USE_SSL: true
  USERNAME: "user@example.com"
  PASSWORD: "*****"
```

Configura tramite argomenti della riga di comando

Puoi configurare le impostazioni di base dell'email usando gli argomenti della riga di comando per abilitare i report, specificare i destinatari e scegliere i formati dei report.

1. Abilita i report via e-mail tramite argomenti della riga di comando:

```
./uhc --email-enabled=true
```

2. Fornire gli indirizzi e-mail dei destinatari:

```
./uhc --email-recipients="user1@example.com, user2@example.com"
```

3. Configura quali formati di report devono essere inviati via e-mail, ad esempio HTML, EXCEL, JSON:

```
./uhc --email-report-formats=HTML,EXCEL,JSON
```



Puoi configurare i seguenti tre attributi tramite argomenti della riga di comando o il file config.yaml. Puoi configurare tutti gli altri attributi solo nel file config.yaml:

- E-mail abilitata
- Destinatari dell'e-mail
- Formati di report via e-mail

Tieni presente che gli argomenti della riga di comando sovrascrivono i valori del file config.yaml.

Ad esempio:

```
./uhc \  
--email-enabled=true  
--email-recipients="user1@example.com, user2@example.com" \  
--email-report-formats=HTML,EXCEL,JSON \  

```

```
EMAIL:  
FROM: "uhc-notify@example.com"  
SUBJECT: "UHC Upgrade Health Report"  
REPLY_TO: <email>  
SMTP:  
HOST: "smtp.example.com"  
PORT: [PORT]
```

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI 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.