



Upgrade Health Checker Dokumentation

Upgrade Health Checker

NetApp

March 16, 2026

This PDF was generated from <https://docs.netapp.com/de-de/upgrade-health-checker/index.html> on March 16, 2026. Always check docs.netapp.com for the latest.

Inhalt

Upgrade Health Checker Dokumentation	1
Versionshinweise	2
Was ist neu im Upgrade Health Checker	2
13. Februar 2026	2
Los geht's	3
Erfahren Sie mehr über den Upgrade Health Checker	3
Upgrade Health Checker herunterladen und einrichten	3
Upgrade Health Checker verwenden	7
Upgrade-Plan mit Upgrade Health Checker generieren	7
Automatisieren Sie die Erstellung von Upgrade-Plänen mit Upgrade Health Checker	9
Erfahren Sie mehr über die Eingabeparameter für Upgrade Health Checker	11
Priorität der Eingabemethoden	11
Eingabeparameter	11
Cluster-IP	11
Cluster-Benutzername	12
Clusterpasswort	12
Zielversion von ONTAP	13
EULA akzeptieren	14
Pfad der Konfigurationsdatei	15
Ausgabepfad ausführen	15
Kompatibilitätsprüfung überspringen	16
Telemetrie deaktivieren	16
Automatische Updates deaktivieren	16
Beispiele für die Verwendung jeder Eingabemethode	16
Kombinierte CLI-Argumente	17
Config.yaml-Datei	17
Interaktivmodus	17
Zusätzliche Befehle	17
FAQ für Upgrade Health Checker	19
Worin unterscheidet sich der Upgrade Health Checker vom Upgrade Advisor?	19
Welche Informationen enthält ein Upgrade Health Checker-Bericht?	19
Kann Upgrade Health Checker ohne Internetverbindung verwendet werden?	19
Welche Versionen von ONTAP werden vom Upgrade Health Checker unterstützt?	19
Rechtliche Hinweise	20
Copyright	20
Marken	20
Patente	20
Datenschutzrichtlinie	20
Open Source	20

Upgrade Health Checker Dokumentation

Versionshinweise

Was ist neu im Upgrade Health Checker

Erfahren Sie, was es Neues im Upgrade Health Checker gibt. Zusätzliche Informationen zu Verbesserungen finden Sie, indem Sie zur Upgrade Health Checker-Kachel in der ["NetApp Console Automation Hub"](#) navigieren und die neuesten Upgrade Health Checker-Download-Dateien ansehen.

13. Februar 2026

Upgrade Health Checker bietet eine neue Lösung zur Erstellung umfassender Vor-Ort-Berichte, damit Sie ein erfolgreiches ONTAP-Upgrade durchführen können. Es kann mit bestehenden Automatisierungs- und Orchestrierungsframeworks verwendet werden, um die Effizienz beim Upgrade einzelner oder mehrerer Cluster zu steigern. Upgrade Health Checker unterstützt Upgrades auf ONTAP 9.11.1 und höher.

["Erfahren Sie mehr über Upgrade Health Checker"](#).

Los geht's

Erfahren Sie mehr über den Upgrade Health Checker

Upgrade Health Checker ist ein Upgrade-Beratungsdienst, der detaillierte Informationen und Empfehlungen bereitstellt, um Ihnen zu helfen, ein erfolgreiches ONTAP Upgrade durchzuführen. Er führt umfassende Systemprüfungen vor Ort durch, die Blocker und Warnungen identifizieren, die Sie vor der Durchführung eines Upgrades beheben müssen.

Upgrade Health Checker lässt sich in Ihre bestehenden Automatisierungs- und Orchestrierungs-Frameworks integrieren, um Sie bei der Aktualisierung einzelner oder mehrerer Cluster zu unterstützen. Es verwendet Ihre aktuellsten AutoSupport-Daten, um einen detaillierten, präzisen Bericht über die mit Ihren Clustern verbundenen Risiken, Informationen zu neuen Funktionen und Verbesserungen in der ONTAP-Version, auf die Sie aktualisieren, sowie über alle Maßnahmen zu erstellen, die vor dem Versuch eines ONTAP-Upgrades zu ergreifen sind.

Um mehr über Upgrade Health Checker zu erfahren, können Sie auf die ["FAQ für Upgrade Health Checker"](#) verweisen oder sich das folgende Einführungsvideo ansehen.

 | <https://img.youtube.com/vi/5mwmigXAB9c/maxresdefault.jpg>

Upgrade Health Checker herunterladen und einrichten

Sie können den Upgrade Health Checker herunterladen, um vor dem Upgrade auf eine neuere Version von ONTAP umfassende Vor-Ort-Berichte zu erstellen.

Über diese Aufgabe

Upgrade Health Checker unterstützt Upgrades für lokale ONTAP Versionen ab 9.11.1. Wenn Sie Cloud Volumes ONTAP verwenden, finden Sie unter ["Upgrade von Cloud Volumes ONTAP"](#) Informationen zum Upgrade Ihres Systems.

Bevor Sie beginnen

Richten Sie eine virtuelle Maschine für Upgrade Health Checker mit den folgenden Spezifikationen ein:

- Verarbeitung und Speicher: m5.large VM oder gleichwertig mit 2 vCPUs und 8 GiB RAM.
- Empfohlenes Betriebssystem: Jedes Linux-Betriebssystem mit glibc Bibliothek Version 2.28 oder höher für optimale Kompatibilität. Dies umfasst:
 - Ubuntu 22.04
 - RHEL8
 - RHEL9
- Speicher: Stellen Sie ein Root-Volume mit mindestens 100 GB und ein zusätzliches NFS-Volume mit mindestens 100 GB bereit, um die Datenaufbewahrung sicherzustellen, falls die virtuelle Maschine kompromittiert wird.
- Hosting-Anforderungen: Platzieren Sie die VM an einem Standort mit Clusteranbindung und Internetzugang, um automatische Tool-Updates zu ermöglichen. Die Maschine sollte über HTTPS auf die folgenden Endpunkte zugreifen können, um automatische Updates durchzuführen:

- <https://api.uhc.netapp.com>
- <https://gql.aiq.netapp.com>

Falls kein Internetzugang verfügbar ist, wenden Sie sich an NetApp für Anweisungen.

- Empfohlene Pakete: Installieren Sie einen Webserver, um den Zugriff zu erleichtern.

Stellen Sie außerdem sicher, dass die virtuelle Maschine über HTTPS eine Verbindung zum Telemetrie-Endpunkt (<https://support.netapp.com/>) herstellen kann, um NetApp AutoSupport-Informationen über Ihre Upgrade-Pläne zu erhalten.

Schritte

1. Laden Sie die Binärdatei „Upgrade Health Checker“ herunter, indem Sie "[Navigieren zum NetApp Console Automation Hub](#)" die Kachel „Upgrade Health Checker“ suchen.
2. Richten Sie die virtuelle Maschine Upgrade Health Checker ein und verwenden Sie SSH, um die Binärdatei an einem Ort Ihrer Wahl abzulegen.
3. Überprüfen Sie die digitale Signatur von Upgrade Health Checker.

Upgrade Health Checker verfügt über ein öffentliches Codesignaturzertifikat (UHC-Linux-codesigning-certificate-public.pem) und eine Zertifikatskette mit Zwischen- und Stammzertifikaten (UHC-Linux-chain-certificates-public.pem).

- a. (Optional) Überprüfen Sie das Codesignaturzertifikat anhand der Kette:

```
openssl verify -CAfile UHC-Linux-chain-certificates-public.pem UHC-
Linux-codesigning-certificate-public.pem
```

Eine Ausgabe von `OK` bestätigt eine gültige Vertrauenskette.

- b. Extrahieren Sie den öffentlichen Schlüssel aus dem Codesignaturzertifikat:

```
openssl x509 -in UHC-Linux-codesigning-certificate-public.pem -pubkey
-noout -out UHC-Linux-public.pub
```

- c. Überprüfen Sie die Signaturdatei (uhc.sig) anhand der Binärdatei des Upgrade Health Checker mithilfe des öffentlichen Schlüssels:

```
openssl dgst -sha256 -verify UHC-Linux-public.pub -signature uhc.sig
uhc
```

Eine Ausgabe von `Verified OK` bestätigt, dass die Signatur gültig ist.

4. Konfigurieren Sie ein Dienstkonto und eine Rolle für den Zugriff auf das ONTAP Cluster. Für den Zugriff auf das Cluster über den Upgrade Health Checker erstellen Sie die Dienstrolle als REST-Rolle.



Sie können ein Ansible-Playbook erstellen, um die Bereitstellung der Rolle und des Benutzers auf allen ONTAP Clustern zu automatisieren.

Sie müssen das Dienstkonto für die http-Anwendung erstellen. Verwenden Sie die folgenden CLI-Befehle, um die erforderlichen Berechtigungen zu konfigurieren:

```
security login rest-role create -role uhctool -api /api -access readonly -vserver

security login rest-role create -role uhctool -api
/api/support/autosupport -access read_create_modify -vserver

security login rest-role create -role uhctool -api
/api/support/autosupport/messages -access read_create_modify -vserver

vserver services web access create -name spi -role uhctool -vserver

security login create -user-or-group-name uhctool -role uhctool
-application http -authentication-method password

security login create -user-or-group-name uhctool -role uhctool
-application ssh -authentication-method password
```

5. (Optional) Richten Sie das Anmeldeinformationsmanagement ein, um den Zugriff auf die Anwendung zu sichern.

Wenn Sie beispielsweise CyberArk und Conjur verwenden, können Sie Ihre Umgebung so konfigurieren, dass Sie Anmeldeinformationen nicht über eine yaml-Datei oder die Befehlszeile übergeben müssen.

- a. Erstellen Sie die erforderlichen CyberArk Safes:

- i. Erstellen Sie einen Safe (Main-Conjur-Safe), der die Anmeldeinformationen und Geheimnisse der Anwendung enthält
- ii. Erstellen Sie einen Safe (API-Credentials-Safe), der die Conjur Host ID und den API Key enthält
- iii. Erstellen Sie einen Safe (Conjur-SSL-Certificate), der das erforderliche Zertifikat enthält

- b. Erstellen Sie die Konfigurationsdatei (Conjur.conf) und die Identitätsdatei (Conjur.identity) für diese Anwendung:

- i. Conjur.conf

```
account:
plugins:[]
appliance_url: https://FQDN
cert_file: /etc/conjur.pem
```

- ii. Conjur.identity

```
machine https://FQDN/authn
login host /prodvault/devops/<Main-Conjur-Safe>/host1
password XXXXXX
```

Hier ist ein Beispiel dafür, wie CyberArk und Conjur in einem Ansible-Playbook verwendet werden:

- c. Installieren Sie die Conjur Ansible Collection, die das Conjur Ansible Lookup Plugin enthält, auf dem Ansible Host:

```
ansible-galaxy collection install cyberark.conjur
```

- d. Erstellen Sie eine Aufgabe in einer YAML-Datei, um den Benutzernamen und das Passwort von CyberArk abzurufen:

```
conjur_username: "{{ lookup('cyberark.conjur.conjur_variable',
'prodvault/devops/<Main-Conjur-Safe>/<Account name>/username',
validate_certs=false) }}"
conjur_password: "{{ lookup('cyberark.conjur.conjur_variable',
'prodvault/devops/<Main-Conjur-Safe>/<Account name>/password',
validate_certs=false) }}"
```

Was kommt als Nächstes?

Sie können den Upgrade Health Checker verwenden, um Ihnen bei der Planung eines ONTAP Upgrades zu helfen, indem Sie ["einen Upgrade-Bericht generieren"](#).

Upgrade Health Checker verwenden

Upgrade-Plan mit Upgrade Health Checker generieren

Sie können den Upgrade Health Checker verwenden, um einen Upgrade-Plan für einen oder mehrere ONTAP Cluster zu erstellen.

Sie können auch "[Upgrade-Berichte automatisch generieren](#)" nutzen, um bei der Pflege aktueller Upgrade-Pläne zu unterstützen, wenn Sie eine große, komplexe Umgebung mit mehreren Clustern haben.

Über diese Aufgabe

Upgrade Health Checker unterstützt Upgrades für lokale ONTAP Versionen ab 9.11.1. Wenn Sie Cloud Volumes ONTAP verwenden, finden Sie unter "[Upgrade von Cloud Volumes ONTAP](#)" Informationen zum Upgrade Ihres Systems.

Bevor Sie beginnen

Um mehr über einen bestimmten Parameter des Upgrade Health Checkers und die Prioritätsreihenfolge für die Eingabeverarbeitung durch das Tool zu erfahren, siehe "[Erfahren Sie mehr über die Eingabeparameter für Upgrade Health Checker](#)".

Schritte

1. Setzen Sie die Ausführungsberechtigung für die Binärdatei, bevor Sie sie zum ersten Mal ausführen:

```
chmod +x uhc
```



Upgrade Health Checker ist ein eigenständiges Paket und muss sich vor der Ausführung entpacken. Dies kann einige Sekunden dauern.

2. Bevor Sie einen vollständigen Durchlauf des Upgrade Health Checker durchführen, führen Sie eine umfassende Prüfung durch, um sicherzustellen, dass das Tool eine Verbindung zum Cluster und zu den erforderlichen Endpunkten herstellen kann:

```
--test all
```

Die umfassende Prüfung stellt sicher, dass die virtuelle Maschine, auf der der Upgrade Health Checker gehostet wird, Folgendes aufweist:

- Verbindung zur ONTAP Cluster-IP-Adresse über HTTPS
 - Verbindung zum Telemetrie-Endpunkt (<https://support.netapp.com/>) über HTTPS
 - Verbindung zu den Auto-Update-Endpunkten (<https://api.uhc.netapp.com> und <https://gql.aiq.netapp.com>) über HTTPS
 - Mindestens 4 GB verfügbarer /tmp Speicherplatz
3. (Optional) Wenn Sie eine Konfigurationsdatei zum Speichern von Parametern verwenden möchten, benennen Sie die `config.yaml.example` Datei um, die sich am selben Ort befindet, an den Sie die Binärdatei heruntergeladen haben `config.yaml`.

Hier ist ein Beispiel für eine config.yaml-Datei:

```
# 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. Führen Sie den Upgrade Health Checker aus, indem Sie die ONTAP-Version eingeben, auf die Sie aktualisieren möchten, und die EULA akzeptieren, einschließlich zusätzlicher Parameter nach Bedarf.



Die EULA ist ein mehrseitiges Dokument. Geben Sie `all` ein, um das gesamte Dokument auf einmal anzuzeigen, und geben Sie `y` ein, um es zu akzeptieren.

Nachdem das AutoSupport-Protokoll für einen Cluster heruntergeladen wurde, dauert die Verarbeitung in der Regel ein bis zwei Minuten, abhängig von der Anzahl der Clusterknoten. Da verschiedene ONTAP Softwareversionen die AutoSupport-Erfassung unterschiedlich handhaben, hängt jeder Durchlauf des Upgrade Health Checker von der aktuellen Auslastung des Clusters und der aktuellen ONTAP Version ab.

- a. Machen Sie sich mit den verfügbaren Parametern des Upgrade Health Checkers, der Eingabeprioritätsreihenfolge und den Standardwerten für bestimmte Parameter vertraut, indem Sie auf ["Erfahren Sie mehr über die Eingabeparameter für Upgrade Health Checker"](#) verweisen.

Der Leitfaden zu den Eingabeparametern enthält außerdem Informationen zum Festlegen eines benutzerdefinierten Konfigurationsdateipfads und Ausführungspfads, um Ihren Workflow zu optimieren. Die Best Practice ist es, für jeden Cluster ein benutzerdefiniertes Ausgabeverzeichnis zu erstellen, um Ihre Berichte und Protokolle effektiv zu organisieren.

- b. Führen Sie den Upgrade Health Checker aus, indem Sie die EULA akzeptieren und die Ziel-ONTAP-Version sowie alle zusätzlichen Parameter eingeben.

```
./uhc
```

5. Nachdem der Upgrade Health Checker seine Prüfungen abgeschlossen hat, navigieren Sie zum `runs` Ordner, um den Upgrade-Plan und den Clusterbericht anzuzeigen.



Jede Ausführung des Programms ist ein „einzigartiger Lauf“ und hat alle zugehörigen Daten, Protokolle und Ergebnisse im zugehörigen `runs` Ordner.

6. Öffnen Sie die Berichtsdatei (namens `uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`) in einem Webbrowser, um den Bericht anzuzeigen. Wenn Sie sie auf einem Remote-Host ausführen, laden Sie die Berichtsdatei zunächst auf einen Rechner herunter, auf dem Sie den Bericht in einem Webbrowser anzeigen können.

Der Protokollpfad und der Berichtspfad lauten wie folgt:

- Protokollpfad: `<output-path>/<unique-run-dir>/<cluster-name>/logs`
- Berichtspfad: `<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`

Automatisieren Sie die Erstellung von Upgrade-Plänen mit Upgrade Health Checker

Sie können die Generierung von Upgrade Health Checker-Berichten automatisieren, um Ihren manuellen Aufwand bei der Planung von ONTAP-Upgrades in großen, komplexen Umgebungen zu reduzieren.

Über diese Aufgabe

Upgrade Health Checker unterstützt Upgrades für lokale ONTAP Versionen ab 9.11.1. Wenn Sie Cloud Volumes ONTAP verwenden, finden Sie unter ["Upgrade von Cloud Volumes ONTAP"](#) Informationen zum Upgrade Ihres Systems.

Schritte

1. Um die erfolgreiche Erstellung Ihrer Upgrade-Berichte zu gewährleisten, führen Sie alle erforderlichen Einrichtungsschritte und einmaligen Aufgaben aus, die in ["Erstellen Sie einen ONTAP Upgrade-Bericht"](#) beschrieben sind.
2. Erstellen Sie ein Skript, um Upgrade Health Checker mit den für Ihre Umgebung geeigneten Parametern auszuführen.

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

Hier ist ein Beispiel für einen Cronjob, der das Tool von Montag bis Freitag um 4 Uhr morgens ausführt. Die Binärdatei und die config.yaml Dateien wurden in `/opt/uhc/tool/` installiert.

Bash-Skript:

```
#!/bin/bash
cd /opt/uhc/tool
/opt/uhc/tool/uhc --accept-eula true --cluster-ip cluster-
mgmt1.example.com --target-ontap-version current --cluster-username
uhctool --cluster-password passw0rd
/opt/uhc/tool/uhc --accept-eula true --cluster-ip cluster-
mgmt2.example.com --target-ontap-version 9.14.1 --cluster-username
uhctool --cluster-password passw0rd
```

Cron-Job:

```
0 4 * * 1-5 /usr/local/bin/uhcron.sh
```

3. Nachdem der Upgrade Health Checker seine Prüfungen abgeschlossen hat, navigieren Sie zum `runs` Ordner, um den Upgrade-Plan und den Clusterbericht anzuzeigen.



Jede Ausführung des Programms ist ein einzigartiger Durchlauf und hat alle zugehörigen Daten, Protokolle und Ergebnisse im zugehörigen `runs` Ordner.

4. Öffnen Sie die Berichtsdatei (mit dem Namen `uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`) in einem Webbrowser, um den Bericht anzuzeigen. Wenn Sie Upgrade Health Checker auf einem Remote-Host ausführen, laden Sie die Berichtsdatei zunächst auf einen Rechner herunter, auf dem Sie sie in einem Webbrowser anzeigen können.

Der Protokollpfad und der Berichtspfad lauten wie folgt:

- **Protokollpfad:** `<output-path>/<unique-run-dir>/<cluster-name>/logs`
- **Berichtspfad:** `<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`

Erfahren Sie mehr über die Eingabeparameter für Upgrade Health Checker

Sie können mehr über die Eingabeparameter für den Upgrade Health Checker und darüber erfahren, wie Sie diese über CLI-Argumente, Konfigurationsdateien oder interaktive Eingabeaufforderungen bereitstellen, um Sie bei der Erstellung eines Upgrade-Berichts für Ihren ONTAP Cluster zu unterstützen.

Priorität der Eingabemethoden

Upgrade Health Checker bietet mehrere Eingabeoptionen für alle Parameter. Die Prioritätsreihenfolge für die Annahme von Eingaben ist:

1. CLI arguments (höchste Priorität)
2. Konfigurationsdatei (`config.yaml`)
3. Interaktive Eingabeaufforderungen (niedrigste Priorität)

Wenn ein Parameter über mehrere Methoden bereitgestellt wird, verwendet das Tool den Wert aus der Quelle mit der höchsten Priorität.

Eingabeparameter

Cluster-IP

Der `--cluster-ip` Parameter gibt die IP-Adresse oder den Hostnamen des ONTAP Clusters an, zu dem eine Verbindung hergestellt werden soll.

Die Prioritätsreihenfolge für die Bereitstellung dieses Parameters ist:

1. CLI-Argument: `--cluster-ip`
2. Konfigurationsdatei: `CLUSTER.IP`
3. Interaktives Eingabeaufforderungsfenster

Beispiele

- CLI-Argument:

```
./uhc --cluster-ip 192.168.1.100
```

- Config.yaml:

```
CLUSTER:  
  IP: "192.168.1.100"
```

- Interaktiver Modus (wenn nicht oben angegeben):

Das Tool wird Sie auffordern: Enter cluster IP address:

Cluster-Benutzername

Der `--cluster-username` Parameter gibt den Benutzernamen für die Authentifizierung beim ONTAP Cluster an.

Die Prioritätsreihenfolge für die Bereitstellung dieses Parameters ist:

1. CLI-Argument: `--cluster-username`
2. Konfigurationsdatei: `CLUSTER.USERNAME`
3. Interaktives Eingabeaufforderungsfenster

Beispiele

- CLI-Argument:

```
./uhc --cluster-username admin
```

- Config.yaml:

```
CLUSTER:  
  USERNAME: "admin"
```

- Interaktiver Modus (wenn nicht oben angegeben):

Das Tool wird Sie auffordern: Enter cluster username:

Clusterpasswort

Der `--cluster-password` Parameter gibt das Passwort für die Authentifizierung beim ONTAP Cluster an.

Die Prioritätsreihenfolge für die Bereitstellung dieses Parameters ist:

1. CLI-Argument: `--cluster-password`
2. Konfigurationsdatei: `CLUSTER.PASSWORD`
3. Interaktive Eingabeaufforderung (sichere Eingabe)

Beispiele

- CLI argument (aus Sicherheitsgründen nicht empfohlen):

```
./uhc --cluster-password mypassword
```

- Config.yaml (stellen Sie sicher, dass die Dateiberechtigungen eingeschränkt sind):

```
CLUSTER:  
  PASSWORD: "mypassword"
```

- Interaktivmodus (empfohlen – Passwort verborgen):

Das Tool wird Sie auffordern: `Enter cluster password:`

Zielversion von ONTAP

Der `--target-ontap-version` Parameter gibt die ONTAP Version an, auf die Sie für die Analyse aktualisieren möchten. Verwenden Sie "current", um die bestehende ONTAP Version des Clusters beizubehalten.

Die Prioritätsreihenfolge für die Bereitstellung dieses Parameters ist:

1. CLI-Argument: `--target-ontap-version`
2. Konfigurationsdatei: `CLUSTER.TARGET_ONTAP_VERSION`
3. Interaktives Auswahlmenü

Beispiele

- CLI-Argument:

Aktualisierte Version von ONTAP: `./uhc --target-ontap-version 9.15.1`

Behalten Sie die aktuelle Version von ONTAP: `./uhc --target-ontap-version current`

- Config.yaml:

```
CLUSTER:
  TARGET_ONTAP_VERSION: "9.15.1"
```

- Interaktiver Modus (wenn nicht oben angegeben):

Das Tool zeigt die verfügbaren Versionen an und fordert zur Auswahl auf

EULA akzeptieren

Der `--accept-eula` Parameter legt fest, ob die Endbenutzer-Lizenzvereinbarung akzeptiert werden soll. Muss auf `true` gesetzt werden, um fortzufahren.

Die Prioritätsreihenfolge für die Bereitstellung dieses Parameters ist:

1. CLI-Argument: `--accept-eula`
2. Konfigurationsdatei: `CLUSTER.ACCEPT_EULA`
3. Interaktives Eingabeaufforderungsfenster

Beispiele

- CLI-Argument:

`./uhc --accept-eula true`

- Config.yaml:

```
CLUSTER:
  ACCEPT_EULA: true
```

- Interaktiver Modus (wenn nicht oben angegeben):

Das Tool zeigt die EULA an und fordert zur Annahme auf

Pfad der Konfigurationsdatei

Der `--config-path` Parameter gibt den Pfad zu einer benutzerdefinierten YAML-Konfigurationsdatei an.

Die Prioritätsreihenfolge für die Bereitstellung dieses Parameters ist:

1. CLI-Argument: `--config-path`
2. Standard: `config.yaml`

Beispiele

- CLI-Argument:

```
./uhc --config-path /path/to/custom_config.yaml
```

- Standardwert (falls nicht angegeben):

Das Tool sucht im aktuellen Verzeichnis nach der `config.yaml`

Ausgabepfad ausführen

Der `--runs-path` Parameter gibt ein benutzerdefiniertes Verzeichnis zum Speichern von Ausgaben und Berichten an.

Die Prioritätsreihenfolge für die Bereitstellung dieses Parameters ist:

1. CLI-Argument: `--runs-path`
2. Konfigurationsdatei: `APP.RUNS_PATH`
3. Standard: `./runs`

Beispiele

- CLI-Argument:

```
./uhc --runs-path /custom/output/path
```

- Config.yaml:

```
APP:
  RUNS_PATH: "/custom/output/path"
```

- Standardwert (falls nicht angegeben):

Tool verwendet `./runs` Verzeichnis

Kompatibilitätsprüfung überspringen

Der `--skip-compatibility-check` Parameter umgeht die Hardware-Kompatibilitätsprüfungen und verwendet die angegebene Version von ONTAP, auf die Sie aktualisieren möchten.



Nutzen Sie diese Option nur, wenn Sie sicher sind, dass die Ziel-ONTAP-Version mit Ihrer Hardware kompatibel ist.

Die Prioritätsreihenfolge für die Bereitstellung dieses Parameters ist:

1. CLI-Argument: `--skip-compatibility-check`
2. Konfigurationsdatei: `CLUSTER.SKIP_COMPATIBILITY_CHECK`
3. Standard: `false`

Beispiele

- CLI-Argument:

```
./uhc --skip-compatibility-check true
```

- Config.yaml:

```
CLUSTER:  
  SKIP_COMPATIBILITY_CHECK: true
```

Telemetrie deaktivieren

Um die Telemetrie zu deaktivieren, fügen Sie Folgendes zu Ihrer `config.yaml` Datei hinzu:

```
TELEMETRY:  
  ENABLED: false
```

Automatische Updates deaktivieren

Um automatische Updates für Upgrade Health Checker zu deaktivieren, fügen Sie Folgendes zu Ihrer `config.yaml` Datei hinzu:

```
AUTO_UPDATE:  
  ENABLED: false
```

Beispiele für die Verwendung jeder Eingabemethode

Kombinierte CLI-Argumente

```
./uhc \  
  --cluster-ip 192.168.1.100 \  
  --cluster-username admin \  
  --cluster-password mypassword \  
  --target-ontap-version 9.15.1 \  
  --accept-eula true \  
  --config-path /path/to/custom_config.yaml \  
  --runs-path /custom/output \  
  --skip-compatibility-check false
```

Config.yaml-Datei

```
CLUSTER:  
  IP: "192.168.1.100"  
  USERNAME: "admin"  
  PASSWORD: "mypassword"  
  TARGET_ONTAP_VERSION: "9.15.1"  
  ACCEPT_EULA: true  
  SKIP_COMPATIBILITY_CHECK: false  
  
APP:  
  RUNS_PATH: "/custom/output"
```

Interaktivmodus

Um alle erforderlichen Eingabeparameter interaktiv abzufragen, führen Sie Upgrade Health Checker ohne Argumente aus:

```
./uhc
```

Zusätzliche Befehle

Diese Befehle bieten einige zusätzliche Funktionen über die vollständige Ausführung des Tools hinaus:

- Hilfe anzeigen

```
./uhc --help
```

- Version anzeigen

```
./uhc --version
```

- Testen Sie die Clusterkonnektivität

```
./uhc --test-connectivity cluster
```

- Telemetrie-Konnektivität testen

```
./uhc --test-connectivity telemetry
```

- Testen Sie die Auto-Update-Konnektivität

```
./uhc --test-connectivity autoupdate
```

- Alle Tests ausführen

```
./uhc --test all
```

FAQ für Upgrade Health Checker

Häufig gestellte Fragen (FAQ) für Upgrade Health Checker.

Worin unterscheidet sich der Upgrade Health Checker vom Upgrade Advisor?

Upgrade Health Checker ist ein On-Premise-Tool, das sich für Anwender mit großen oder komplexen Umgebungen, eingeschränktem Internetzugang oder bestehenden Automatisierungs- und Orchestrierungsframeworks eignet. Upgrade Advisor ist für Anwender mit einer kleineren Umgebung geeignet, die eine Cloud-basierte, UI-zentrierte Erfahrung bevorzugen.

Sie können mehr über "[Upgrade Health Checker](#)" und "[Upgrade Advisor](#)" erfahren, um herauszufinden, welches Tool am besten zu Ihren Bedürfnissen passt.

Welche Informationen enthält ein Upgrade Health Checker-Bericht?

Upgrade Health Checker-Berichte liefern detaillierte Informationen zu potenziellen Blockern und Warnungen, die vor dem Upgrade Ihrer ONTAP Cluster behoben werden müssen, zu Risiken im Zusammenhang mit Ihren Clustern sowie zu neuen Funktionen und Verbesserungen in der ONTAP Version, auf die Sie upgraden.

Kann Upgrade Health Checker ohne Internetverbindung verwendet werden?

Sie benötigen keine Internetverbindung, um den Upgrade Health Checker auszuführen. Er erstellt Upgrade-Pläne und Berichte vor Ort anhand der aktuellen Konfigurationsdaten Ihres ONTAP-Clusters.

Für automatische Tool-Updates ist jedoch ein Internetzugang erforderlich. Falls in Ihrer Umgebung keine Internetverbindung besteht, können Sie die neueste Version des Tools manuell von der Kachel „Upgrade Health Checker“ auf dem "[NetApp Console Automation Hub](#)" herunterladen.

Welche Versionen von ONTAP werden vom Upgrade Health Checker unterstützt?

Upgrade Health Checker unterstützt Upgrades für On-Premises ONTAP 9.11.1 und später.

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtsvermerke, Marken, Patente und mehr.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp Trademarks-Seite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patente

Eine aktuelle Liste der NetApp owned patents finden Sie unter:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Datenschutzrichtlinie

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Open Source

Hinweisdateien enthalten Informationen über Urheberrechte und Lizenzen Dritter, die in NetApp Software verwendet werden.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.