시작하기
Upgrade Health Checker

NetApp
September 24, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/upgrade-health-checker/learn-about-upgrade-health-checker.html on September 24, 2026. Always check docs.netapp.com for the latest.

목차

시작하기 1
업그레이드 상태 점검 도구에 대해 알아보십시오 1
Upgrade Health Checker를 다운로드하고 설정합니다 1
업그레이드 상태 검사기의 입력 매개변수 4
입력 방법 우선순위 4
입력 매개변수 5
각 입력 방법을 사용하는 예 10
추가 명령 11

시작하기

업그레이드 상태 점검 도구에 대해 알아보십시오

Upgrade Health Checker는 ONTAP 업그레이드를 성공적으로 완료하는 데 도움이 되는 자세한 정보와 권장 사항을 제공하는 업그레이드 자문 서비스 도구입니다. 현장에서 포괄적인 상태 점검을 수행하여 업그레이드를 수행하기 전에 해결해야 하는 차단 요소와 경고를 식별합니다.

Upgrade Health Checker는 기존 자동화 및 오케스트레이션 프레임워크에 통합되어 단일 또는 여러 클러스터 업그레이드를 지원합니다. 최신 AutoSupport 데이터를 사용하여 클러스터 관련 위험 요소, 업그레이드할 ONTAP 버전의 새로운 기능 및 개선 사항, ONTAP 업그레이드를 시도하기 전에 수행해야 할 조치에 대한 상세하고 정확한 보고서를 생성합니다.

Upgrade Health Checker에 대해 더 자세히 알아보려면 "업그레이드 상태 점검 도구 FAQ"를 참조하거나 다음 소개 영상을 시청하세요.

[] | *https://img.youtube.com/vi/5mwmigXAB9c/maxresdefault.jpg*

Upgrade Health Checker를 다운로드하고 설정합니다

Upgrade Health Checker를 다운로드하여 최신 버전의 ONTAP로 업그레이드하기 전에 현장에서 포괄적인 보고서를 생성할 수 있습니다.

이 작업 정보

업그레이드 상태 검사기는 온프레미스 ONTAP 버전 9.11.1 이상에 대한 업그레이드를 지원합니다. Cloud Volumes ONTAP를 사용하는 경우 시스템 업그레이드에 대한 자세한 내용은 "Cloud Volumes ONTAP 업그레이드"를 참조하십시오.

시작하기 전에

다음 사양으로 Upgrade Health Checker용 가상 머신을 설정하십시오.

구성 요소	사양
VM	2개의 vCPU와 8GiB RAM을 갖춘 m5.large VM 또는 이와 동등한 사양
운영 체제	glibc 라이브러리 버전 2.28 이상이 설치된 모든 Linux 운영 체제(Ubuntu 22.04, RHEL8 또는 RHEL9)
디스크 공간	최소 4GB(8GB 권장)의 여유 공간 `/tmp` 및 실행 권한
네트워크	ONTAP 클러스터 관리 LIF에 대한 HTTPS 연결
ONTAP 버전	ONTAP 9.11.1 이상을 실행하는 클러스터

구성 요소	사양
호스팅 요구 사항	자동 툴 업데이트를 위해 VM을 클러스터 연결 및 인터넷 액세스가 가능한 위치에 배치하십시오. 자동 업데이트를 수행하고 NetApp이 업그레이드 계획에 대한 AutoSupport 정보를 수신할 수 있도록 VM은 HTTPS(443)를 통해 다음 엔드포인트에 액세스할 수 있어야 합니다: https://support.netapp.com/ https://api.uhc.netapp.com https://gql.aiq.netapp.com https://api.activeiq.netapp.com
권장 패키지	액세스를 용이하게 하기 위해 웹 서버를 설치하십시오

> 가상 머신이 HTTPS(443)를 통해 자동 업데이트 및 원격 측정 엔드포인트(https://support.netapp.com/ 및 https://api.activeiq.netapp.com)에 연결할 수 있는지 확인하여 NetApp이 업그레이드 계획에 대한 AutoSupport 정보를 수신할 수 있도록 하십시오. 인터넷에 액세스할 수 없는 경우 업그레이드 상태 검사기의 최신 버전을 수동으로 다운로드해야 합니다.

단계

1. "NetApp Console 자동화 허브"로 이동하여 Upgrade Health Checker 타일을 찾아 Upgrade Health Checker 바이너리를 다운로드하십시오.
2. Upgrade Health Checker 가상 머신을 설정하고 SSH를 사용하여 원하는 위치에 바이너리를 배치하십시오.
3. Upgrade Health Checker의 디지털 서명을 확인하십시오.

   Upgrade Health Checker는 공개 코드 서명 인증서(`UHC-Linux-codesigning-certificate-public.pem`와 중간 및 루트 인증서 체인(`UHC-Linux-chain-certificates-public.pem`을 보유하고 있습니다.

   a. (선택 사항) 코드 서명 인증서를 체인과 비교하여 확인합니다.

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

   ```
   `OK` 출력은 유효한 신뢰 체인을 확인합니다.
   ```

   b. 코드 서명 인증서에서 공개 키를 추출합니다.

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

   c. 공개 키를 사용하여 Upgrade Health Checker 바이너리에 대해 서명 파일(`uhc.sig`)을 검증하십시오.

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

`Verified OK`의 출력은 서명이 유효함을 확인합니다.

4. ONTAP 클러스터 액세스를 위한 서비스 계정 및 역할을 구성하십시오. Upgrade Health Checker를 통한 클러스터 액세스를 위해서는 서비스 역할을 REST 역할로 생성하십시오.

   Ansible 플레이북을 작성하여 모든 ONTAP 클러스터에 역할과 사용자를 자동으로 배포할 수 있습니다.

   HTTP 애플리케이션용 서비스 계정을 생성해야 합니다. 다음 CLI 명령을 사용하여 필요한 권한을 구성하십시오:

```
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. (선택 사항) 애플리케이션에 대한 액세스를 보호하기 위해 자격 증명 관리를 설정합니다.

   예를 들어 CyberArk와 Conjur를 사용하는 경우 yaml 파일이나 명령줄을 통해 자격 증명을 전달하지 않도록 환경을 구성할 수 있습니다.

   a. 필요한 CyberArk 금고를 생성하세요:
      i. 애플리케이션 자격 증명과 비밀 키를 저장할 Safe(Main-Conjur-Safe)를 생성합니다
      ii. Conjur 호스트 ID와 API 키를 보유하는 Safe(API-Credentials-Safe)를 생성합니다
      iii. 필요한 인증서를 보유하는 Safe(Conjur-SSL-Certificate)를 생성합니다
   b. 이 애플리케이션에 대한 구성 파일(Conjur.conf)과 ID 파일(Conjur.identity)을 생성합니다.
      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
```

다음은 Ansible 플레이북에서 CyberArk와 Conjur를 사용하는 방법의 예입니다.

c. Conjur Ansible Lookup Plugin이 포함된 Conjur Ansible Collection을 Ansible Host에 설치합니다.

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

d. YAML 파일에서 CyberArk의 사용자 이름과 암호를 가져오는 작업을 생성합니다.

```
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) }}"
```

관련 정보

- "Upgrade Health Checker의 입력 매개변수에 대해 알아보십시오"

다음 단계

업그레이드 상태 검사기를 사용하여 "업그레이드 보고서 생성"으로 ONTAP 업그레이드를 계획할 수 있습니다.

업그레이드 상태 검사기의 입력 매개변수

Upgrade Health Checker의 입력 매개변수와 CLI 인수, 구성 파일 또는 대화형 프롬프트를 통해 이러한 매개변수를 제공하여 ONTAP 클러스터에 대한 업그레이드 보고서 생성을 지원하는 방법에 대해 자세히 알아볼 수 있습니다.

입력 방법 우선순위

업그레이드 상태 점검 도구는 모든 매개 변수에 대해 여러 입력 옵션을 제공합니다. 입력을 수락하는 우선 순위는 다음과 같습니다.

1. CLI 인수(최우선 순위)
2. 구성 파일 (`config.yaml`)

3. 대화형 프롬프트(최하위 우선 순위)

매개 변수가 여러 방법을 통해 제공되는 경우 도구는 우선 순위가 가장 높은 소스의 값을 사용합니다.

입력 매개변수

클러스터 **IP**

`` `--cluster-ip` 매개변수는 연결할 ONTAP 클러스터의 IP 주소 또는 호스트 이름을 지정합니다. ``

이 매개변수를 제공하는 우선 순위는 다음과 같습니다.

1. CLI 인수: `--cluster-ip`
2. 구성 파일: `CLUSTER.IP`
3. 대화형 프롬프트

▼ 예

- CLI 인수:

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

- Config.yaml:

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

- 대화형 모드(위에 제공되지 않은 경우):

  도구에서 다음과 같은 메시지가 표시됩니다. `Enter cluster IP address:`

클러스터 사용자 이름

`` `--cluster-username` 매개변수는 ONTAP 클러스터 인증에 사용할 사용자 이름을 지정합니다. ``

이 매개변수를 제공하는 우선 순위는 다음과 같습니다.

1. CLI 인수: `--cluster-username`
2. 구성 파일: `CLUSTER.USERNAME`
3. 대화형 프롬프트

▼ 예

- CLI 인수:

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

- Config.yaml:

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

- 대화형 모드(위에 제공되지 않은 경우):

  도구에서 다음과 같은 메시지가 표시됩니다. `Enter cluster username:`

클러스터 암호

`` `--cluster-password` 매개변수는 ONTAP 클러스터 인증에 사용할 암호를 지정합니다. ``

이 매개변수를 제공하는 우선 순위는 다음과 같습니다.

1. CLI 인수: `--cluster-password`
2. 구성 파일: `CLUSTER.PASSWORD`
3. 대화형 프롬프트(보안 입력)

▼ 예

- CLI 인수(보안상 권장하지 않음):

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

- Config.yaml(파일 권한이 제한되어 있는지 확인):

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

- 대화형 모드(권장 - 암호 숨김):

  도구에서 다음과 같은 메시지가 표시됩니다. `Enter cluster password:`

타겟 **ONTAP** 버전

`` `--target-ontap-version` 매개변수는 분석을 위해 업그레이드할 ONTAP 버전을 지정합니다. 기존 클러스터 ONTAP 버전을 유지하려면 "current"를 사용합니다. ``

이 매개변수를 제공하는 우선 순위는 다음과 같습니다.

1. CLI 인수: `--target-ontap-version`

2. 구성 파일: `CLUSTER.TARGET_ONTAP_VERSION`
3. 대화형 선택 메뉴

▼ 예

- CLI 인수:

  업데이트된 ONTAP 버전: `./uhc --target-ontap-version 9.15.1`

  현재 ONTAP 버전 유지: `./uhc --target-ontap-version current`

- Config.yaml:

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

- 대화형 모드(위에 제공되지 않은 경우):

  도구에 사용 가능한 버전이 표시되고 선택하라는 메시지가 표시됩니다

EULA에 동의합니다

```
`--accept-eula` 매개변수는 최종 사용자 라이선스 계약을 수락할지 여부를 지정합니다.
계속하려면 `true`로 설정해야 합니다.
```

이 매개변수를 제공하는 우선 순위는 다음과 같습니다.

1. CLI 인수: `--accept-eula`
2. 구성 파일: `CLUSTER.ACCEPT_EULA`
3. 대화형 프롬프트

▼ 예

- CLI 인수:

  `./uhc --accept-eula true`

- Config.yaml:

```
CLUSTER:
  ACCEPT_EULA: true
```

- 대화형 모드(위에 제공되지 않은 경우):

  이 도구는 EULA를 표시하고 수락 여부를 묻는 메시지를 표시합니다

구성 파일 경로

`--config-path` 매개변수는 사용자 지정 구성 YAML 파일의 경로를 지정합니다.

이 매개변수를 제공하는 우선 순위는 다음과 같습니다.

1. CLI 인수: `--config-path`
2. 기본값: `config.yaml`

▼ 예

- CLI 인수:

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

- 기본값(제공되지 않은 경우):

  이 도구는 현재 디렉토리에서 config.yaml을 찾습니다

실행 출력 경로

`--runs-path` 매개변수는 실행 출력 및 보고서를 저장하기 위한 사용자 지정 디렉터리를 지정합니다.

이 매개변수를 제공하는 우선 순위는 다음과 같습니다.

1. CLI 인수: `--runs-path`
2. 구성 파일: `APP.RUNS_PATH`
3. 기본값: `./runs`

▼ 예

- CLI 인수:

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

- Config.yaml:

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

- 기본값(제공되지 않은 경우):

  이 도구는 `./runs` 디렉토리를 사용합니다.

호환성 검사 건너뛰기

`--skip-compatibility-check` 매개변수는 하드웨어 호환성 검사를 건너뛰고 업그레이드하려는 지정된 `ONTAP` 버전을 사용합니다.

> ! 대상 ONTAP 버전이 하드웨어와 호환되는지 확실한 경우에만 이 옵션을 사용하십시오.

이 매개변수를 제공하는 우선 순위는 다음과 같습니다.

1. CLI 인수: `--skip-compatibility-check`
2. 구성 파일: `CLUSTER.SKIP_COMPATIBILITY_CHECK`
3. 기본값: `false`

▼ 예

- CLI 인수:

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

- Config.yaml:

  ```
  CLUSTER:
    SKIP_COMPATIBILITY_CHECK: true
  ```

대시보드

`--dashboard` 매개변수는 클러스터에 연결하지 않고 `<runs>/dashboard/index.html`의 기존 실행에서 대시보드를 재생성합니다. 일반 실행 외부에서 플릿 보기를 새로 고치는 데 사용합니다. 대시보드는 최근 평가된 모든 클러스터의 상태에 대한 개괄적인 개요를 제공하므로 한 곳에서 여러 클러스터의 업그레이드 준비 상태를 쉽게 모니터링하고 비교할 수 있습니다. 웹 브라우저에서 대시보드를 열어 각 클러스터의 상태, 잠재적 차단 요소 및 위험을 한눈에 확인할 수 있습니다.

- CLI 인수: `--dashboard`

▼ 예

- CLI 인수:

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

원격 측정을 비활성화합니다

원격 측정 기능을 비활성화하려면 다음 내용을 `config.yaml` 파일에 추가하세요.

```
TELEMETRY:
  ENABLED: false
```

자동 업데이트 비활성화

업그레이드 상태 검사기의 자동 업데이트를 비활성화하려면 다음 내용을 `config.yaml` 파일에 추가하십시오.

```
AUTO_UPDATE:
  ENABLED: false
```

각 입력 방법을 사용하는 예

결합된 **CLI** 인수

```
./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 파일

```
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"
```

대화형 모드

필수 입력 매개변수를 대화형으로 표시하려면 인수 없이 Upgrade Health Checker를 실행하십시오.

```
./uhc
```

추가 명령

이러한 명령은 도구의 전체 실행 외에 몇 가지 추가 기능을 제공합니다.

- 도움말 표시

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

- 버전 표시

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

- 클러스터 연결 테스트

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

- 원격 측정 연결 테스트

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

- 자동 업데이트 연결 테스트

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

- 모든 테스트 실행

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

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.