



Usar o Upgrade Health Checker

Upgrade Health Checker

NetApp

September 11, 2026

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

Índice

Usar o Upgrade Health Checker	1
Gere um plano de atualização com o Upgrade Health Checker	1
Painel de controle do verificador de integridade de upgrade	3
Automatize a geração de planos de atualização com o Upgrade Health Checker	5
Receba relatórios do Verificador de Saúde da Atualização por e-mail	7
Configurar usando o arquivo config.yaml	7
Configurar usando argumentos de linha de comando	8

Usar o Upgrade Health Checker

Gere um plano de atualização com o Upgrade Health Checker

Você pode usar o Upgrade Health Checker para gerar um plano de atualização para um ou vários clusters ONTAP.

Você também pode ["automatizar a geração de relatórios de atualização"](#) para ajudar a manter planos de atualização atualizados, caso possua um ambiente grande e complexo com múltiplos clusters.

Sobre esta tarefa

O Upgrade Health Checker oferece suporte a atualizações para versões do ONTAP local 9.11.1 e posteriores. Se você estiver usando Cloud Volumes ONTAP, consulte ["Atualizar Cloud Volumes ONTAP"](#) para obter informações sobre como atualizar seu sistema.

Antes de começar

Para saber mais sobre um parâmetro específico do Upgrade Health Checker e a ordem de prioridade de como a ferramenta aceita input, consulte ["Saiba mais sobre os parâmetros de entrada para o Upgrade Health Checker"](#).

Passos

1. Defina a permissão de execução no arquivo binário antes de executá-lo pela primeira vez:

```
chmod +x uhc
```



Upgrade Health Checker é um pacote independente e precisará se descompactar antes de ser executado. Isso pode levar alguns segundos.

2. Antes de concluir uma execução completa do Upgrade Health Checker, realize uma verificação abrangente para garantir que a ferramenta consiga se conectar ao cluster e aos endpoints necessários:

```
--test all
```

A verificação completa garante que a máquina virtual que hospeda o Upgrade Health Checker tenha:

- Conectividade com o endereço IP do cluster ONTAP via HTTPS
 - Conectividade com o endpoint de telemetria (<https://support.netapp.com/> e <https://api.activeiq.netapp.com>) por HTTPS
 - Conectividade com os endpoints de atualização automática (<https://api.uhc.netapp.com>, <https://gql.aiq.netapp.com> e <https://api.activeiq.netapp.com>) via HTTPS (443)
 - Pelo menos 4 GB de /tmp espaço disponível
3. (Opcional) Se você quiser usar um arquivo de configuração para armazenar parâmetros, renomeie o `config.yaml.example` arquivo localizado no mesmo local onde você baixou o binário para `config.yaml`.

Aqui está um exemplo de arquivo 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. Execute a ferramenta de verificação de integridade da atualização inserindo a versão do ONTAP para a qual deseja atualizar e aceitando o contrato de licença do usuário final, incluindo parâmetros adicionais conforme necessário.



O contrato de licença do usuário final é um documento de várias páginas. Digite `all` para ver o documento inteiro de uma vez e digite `y` para aceitá-lo.

Após o log do AutoSupport ser baixado para um cluster, o processamento geralmente leva de um a dois minutos, dependendo do número de nós do cluster. Como diferentes versões do ONTAP lidam com a coleta do AutoSupport de forma diferente, cada execução do Upgrade Health Checker depende da carga atual do cluster e da versão do ONTAP.

- a. Familiarize-se com os parâmetros disponíveis do Upgrade Health Checker, a ordem de prioridade de entrada e os valores padrão para determinados parâmetros consultando ["Saiba mais sobre os parâmetros de entrada para o Upgrade Health Checker"](#).

O Guia de Parâmetros de Entrada também fornece informações para especificar um caminho de arquivo de configuração personalizado e um caminho de execução para otimizar seu fluxo de trabalho. A melhor prática é criar um diretório de saída personalizado para cada cluster para organizar seus relatórios e logs de forma eficaz.

- b. Execute a verificação de integridade da atualização aceitando o contrato de licença do usuário final e inserindo a versão do ONTAP de destino e quaisquer parâmetros adicionais.

```
./uhc
```

5. Após a conclusão das verificações do Upgrade Health Checker, navegue até a `runs` pasta para visualizar o plano de atualização e o relatório do cluster.



Cada execução do programa é uma "execução única" e terá todos os dados, registros e

resultados associados na pasta `runs` correspondente.

6. Liste os arquivos de relatório gerados:

```
ls -lrt
```

7. Abra o arquivo de relatório (nomeado `uhc_<cluster-name>_<YYYYMMDDHHMMSS>`) em um navegador da web, no Microsoft Excel ou em um visualizador de JSON para visualizar o relatório. Se estiver executando em um host remoto, primeiro baixe o arquivo de relatório para uma máquina onde você possa visualizar o relatório em um navegador da web, no Excel ou em um visualizador de JSON.

O caminho do log e o caminho do relatório são os seguintes:

- Caminho do log: `<output-path>/<unique-run-dir>/<cluster-name>/logs`
- Caminho do relatório HTML: `<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`
- Caminho do relatório do Excel: `<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.xlsx`
- Caminho do relatório JSON: `<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.json`

O que vem a seguir

Após gerar seu plano de atualização e relatório de cluster, você pode visualizar o ["Painel de controle do verificador de integridade de upgrade"](#) para obter detalhes do status de integridade dos clusters avaliados durante a execução.

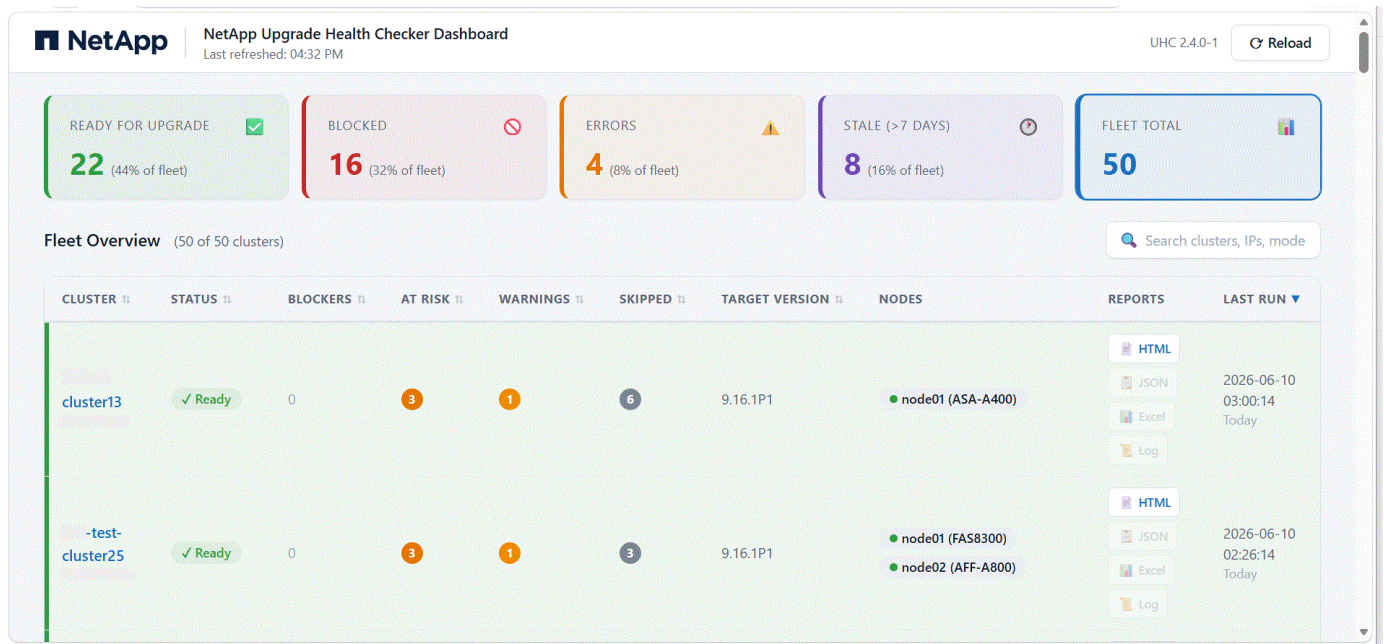
Painel de controle do verificador de integridade de upgrade

Um painel HTML estático é gerado em `runs/dashboard/index.html` ao final de cada execução do Verificador de Integridade da Atualização. O painel fornece uma visão geral de alto nível do status de integridade dos clusters avaliados recentemente, permitindo que você monitore e compare a prontidão para atualização entre os clusters.

Para regenerar o painel de controle posteriormente (sem contatar um cluster), execute:

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

A seguir, apresentamos uma visualização de um painel do Upgrade Health Checker gerado recentemente.



Na parte superior da página, há cinco cartões de resumo com códigos de cores (cada um deles também é um filtro selecionável) que mostram:

- **Pronto para atualização:** Número de clusters cuja última verificação de integridade não encontrou bloqueios, ou seja, pronto para atualização.
- **Bloqueados:** Número de clusters bloqueados e que não podem ser atualizados até que os bloqueadores sejam resolvidos.
- **Erros:** Número de clusters cuja última execução do UHC não foi concluída (por exemplo, falha de conexão, autenticação ou coleta de dados).
- **Desatualizado (>7):** Número de clusters cuja última execução do UHC ocorreu há mais de 7 dias (os dados de verificação de integridade estão desatualizados).
- **Total da frota:** Número total de clusters na frota, (aqueles com uma execução no painel de controle, o padrão são os últimos 30 dias).

A seção Visão geral da frota detalha o estado atual da frota. Para cada cluster, são fornecidas as seguintes informações (a tabela mostra a última execução por cluster):

- **Nome do cluster:** Nome do cluster (com o endereço IP de gerenciamento exibido abaixo do nome).
- **Status:** Status atual do cluster: Pronto, Bloqueado, Erro ou Obsoleto.
- **Bloqueadores:** Número de bloqueadores no cluster. Esses são problemas críticos que devem ser resolvidos antes da atualização.
- **Em risco:** Número de ocorrências de risco no cluster. Esses são riscos identificados durante a verificação pré-atualização.
- **Avisos:** Número de avisos no cluster. A verificação pré-atualização foi concluída com alguns avisos; você pode optar por corrigir esses avisos ou continuar com a atualização.
- **Ignorado:** Número de verificações que foram ignoradas no cluster.
- **Versão de destino:** A versão do ONTAP para a qual o usuário pretende atualizar. (Pode ser a mesma versão atual se você quiser executar uma verificação de integridade na versão em execução.)
- **Nós:** Os nós do cluster, cada um mostrado como nome do nó com seu modelo de hardware (por exemplo, eurbkpcla (FAS8200)).

- **Relatórios:** Formatos de relatório disponíveis para a execução: HTML, JSON, Excel, Log.
- **Última execução:** Data e hora da última execução do Verificador de Saúde da Atualização (com a indicação relativa de "X dias atrás").

Você pode selecionar **Recarregar** para atualizar a página. Use a barra de **Pesquisa** para buscar detalhes de um cluster específico.

Automatize a geração de planos de atualização com o Upgrade Health Checker

Você pode automatizar a geração de relatórios do Upgrade Health Checker para reduzir seu esforço manual ao planejar upgrades do ONTAP em ambientes grandes e complexos.

Sobre esta tarefa

O Upgrade Health Checker oferece suporte a atualizações para versões do ONTAP local 9.11.1 e posteriores. Se você estiver usando Cloud Volumes ONTAP, consulte ["Atualizar Cloud Volumes ONTAP"](#) para obter informações sobre como atualizar seu sistema.

Passos

1. Para garantir a criação bem-sucedida de seus relatórios de atualização, conclua todas as etapas de configuração necessárias e as tarefas únicas descritas em ["Gerar um relatório de atualização do ONTAP"](#).
2. Crie um script para executar o Upgrade Health Checker com os parâmetros apropriados para o seu ambiente.

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

3. Crie um script de automação para agendamentos cron para executar o Upgrade Health Checker. O script de exemplo a seguir executa o Upgrade Health Checker em vários clusters. Os arquivos binário e config.yaml foram instalados em /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. Configure o cron para executar o script de segunda a sexta-feira às 4h da manhã:

```
# 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
```



Para monitoramento contínuo da integridade, utilize `--target-ontap-version current` sem uma meta de atualização específica.

1. [[passo 5]] Depois que o Verificador de Saúde da Atualização concluir suas verificações, navegue até a `runs` pasta para visualizar o plano de atualização e o relatório do cluster.



Cada execução do programa é uma execução única e terá todos os dados, logs e resultados associados na pasta `runs` correspondente.

2. Abra o arquivo de relatório (nomeado `uhc_<cluster-name>_<YYYYMMDDHHMMSS>`) em um navegador da web, no Microsoft Excel ou em um visualizador de JSON para visualizar o relatório. Se você estiver executando o Upgrade Health Checker em um host remoto, primeiro baixe o arquivo de relatório para um computador onde você possa visualizar o relatório em um navegador da web, no Excel ou em um visualizador de JSON.

O caminho do log e o caminho do relatório são os seguintes:

- Caminho do log: `<output-path>/<unique-run-dir>/<cluster-name>/logs`
- Caminho do relatório HTML: `<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`

- Caminho do relatório do Excel: <output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.xlsx
- Caminho do relatório JSON: <output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.json

Receba relatórios do Verificador de Saúde da Atualização por e-mail

O Upgrade Health Checker pode enviar relatórios diretamente para sua caixa de entrada. Habilite esse recurso por meio do arquivo config.yaml ou de um argumento de linha de comando. Quando habilitado, o Upgrade Health Checker envia os relatórios gerados (HTML, Excel ou JSON) para um ou mais destinatários por meio de um servidor SMTP. Quando desabilitado, nenhum relatório é enviado. Se a geração do relatório falhar e o envio de e-mails estiver habilitado, o Upgrade Health Checker envia os arquivos de log para os destinatários configurados.

Configurar usando o arquivo config.yaml

Você pode configurar as definições de e-mail no arquivo config.yaml, ativando os relatórios por e-mail, adicionando detalhes do servidor SMTP e especificando os endereços dos destinatários e os formatos dos relatórios.

1. Ative o envio de relatórios por e-mail no arquivo config.yaml.

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

2. Adicione as configurações SMTP, os detalhes do remetente e o assunto:

```
# 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. Adicione os endereços de e-mail dos destinatários e defina quais formatos de relatório o sistema enviará por e-mail, por exemplo, HTML, EXCEL, JSON ou ALL. Você também pode usar autenticação e criptografia:

```
# 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: "*****"
```

Configurar usando argumentos de linha de comando

Você pode configurar as definições básicas de email usando argumentos de linha de comando para ativar relatórios, especificar destinatários e selecionar formatos de relatório.

1. Ativar relatórios por e-mail usando argumentos de linha de comando:

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

2. Forneça os endereços de e-mail dos destinatários:

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

3. Configure quais formatos de relatório são enviados por e-mail, por exemplo, HTML, EXCEL, JSON:

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



Você pode configurar os três atributos a seguir usando argumentos de linha de comando ou o arquivo config.yaml. Você pode configurar todos os demais atributos somente no arquivo config.yaml:

- E-mail ativado
- Destinatários de e-mail
- Formatos de relatório por e-mail

Observe que os argumentos da linha de comando substituem os valores do arquivo `config.yaml`.

Por exemplo:

```
./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]  

```

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.