



Upgrade ONTAP tools für VMware vSphere

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Inhalt

- Upgrade ONTAP tools für VMware vSphere 1
 - Upgrade von ONTAP tools für VMware vSphere 10.x auf 10.5 1
 - ONTAP tools-Upgrade-Fehlercodes. 3

Upgrade ONTAP tools für VMware vSphere

Upgrade von ONTAP tools für VMware vSphere 10.x auf 10.5

Ein Upgrade von ONTAP tools for VMware vSphere 10.3 oder 10.4 auf 10.5 ist möglich. Für ein Upgrade von ONTAP tools 10.0, 10.1 oder 10.2 auf 10.5 ist zunächst ein Upgrade auf 10.3 oder 10.4 erforderlich, bevor auf 10.5 gewechselt werden kann.



- Bei ASA r2-Systemen müssen Sie ONTAP tools for VMware vSphere auf Version 10.5 und ONTAP auf Version 9.16.1 aktualisieren, bevor Sie weitere Storage Availability Zones (SAZs) einrichten.
- Wenn das Upgrade von ONTAP tools for VMware vSphere 10.3 oder 10.4 auf 10.5 fehlschlägt, ist ein Rollback nicht möglich. Zur Wiederherstellung der Konfiguration kann eine Wiederherstellung mit niedrigem RPO oder per Snapshot erfolgen. Für ONTAP tools for VMware vSphere 10.2 und frühere Versionen kann eine Wiederherstellung mit Zero-RPO erfolgen.

Bevor Sie beginnen

- Alle Knoten müssen aktiv sein.
- Es ist sicherzustellen, dass das ONTAP Systemzertifikat und die eingebundenen vCenter Zertifikate mindestens 5 Tage gültig sind. Sollten die Zertifikate früher ablaufen, schlägt das Upgrade fehl.
- Stellen Sie sicher, dass auf allen Knoten eine fünfte Festplatte mit einer Kapazität von 100 GB vorhanden ist.
- Es sollte sichergestellt sein, dass die Knotenkonfiguration den Spezifikationen in der folgenden Tabelle entspricht.

Bereitstellungstyp	CPU (Kern) pro Knoten	Speicher (GB) pro Knoten	Speicherplatz (GB) pro Knoten	Gesamt-CPU (Core)	Arbeitsspeicher (GB)	Gesamtspeicherplatz (GB)
Nicht-HA Small	9	18	350	9	18	350
Nicht-HA Medium	13	26	350	13	26	350
HA Small	9	18	350	27	54	1050
HA Medium	13	26	350	39	78	1050
HA Large	17	34	350	51	102	1050

- Sichergestellt ist, dass Hot-Plug-in für CPU und RAM aktiviert ist.
- Eine Sicherung mit niedrigem RPO aktivieren und sicherstellen, dass eine Sicherung in der vCenter Client-Oberfläche sichtbar ist. Der Sicherungsordner sollte vor dem Upgrade heruntergeladen werden.
- Ein Backup mit niedrigem RPO wird empfohlen. In einer Bereitstellung ohne Hochverfügbarkeit (HA) kann vor dem Upgrade ein konsistenter Snapshot der virtuellen Maschine der ONTAP tools erstellt werden.

Weitere Informationen zu Backup und Recovery finden Sie unter ["Backup-Einstellungen bearbeiten"](#) und ["Wiederherstellung der ONTAP tools Konfiguration"](#).

Schritte

1. ONTAP tools für VMware vSphere Upgrade-ISO in die Inhaltsbibliothek hochladen.
2. Auf der primären VM-Seite **Aktionen > Einstellungen bearbeiten** auswählen. Zur Identifizierung des Namens der primären VM:
 - a. Die Diagnose-Shell auf einem beliebigen Knoten aktivieren
 - b. Führen Sie folgenden Befehl aus: `grep sourceHost /opt/netapp/meta/ansible_vars.yaml`
3. Im Bearbeitungsfenster unter dem Feld **CD/DVD-Laufwerk** die **content library ISO-Datei** auswählen.
4. Die ISO-Datei auswählen, das Kontrollkästchen **Verbunden** für das Feld **CD/DVD-Laufwerk** aktivieren und auf **OK** klicken.
5. Vom vCenter Server aus eine Konsole zu ONTAP tools öffnen.
6. Melden Sie sich als Wartungsbenutzer an.
7. Geben Sie **2** ein, um das Menü **System Configuration** auszuwählen.
8. **6** eingeben, um die Option **Upgrade** auszuwählen.
9. Geben Sie die vCenter-Anmeldeinformationen ein, wenn Sie dazu aufgefordert werden. Dies ist die vCenter-Instanz, auf der die ONTAP tools gehostet werden.

Wenn Sie ONTAP tools in einer Zwei-vCenter-Server-Topologie verwenden – wobei die Appliance auf einer vCenter-Instanz gehostet wird und eine andere verwaltet –, können Sie der vCenter-Instanz, die die ONTAP tools hostet, eine eingeschränkte Rolle zuweisen. Sie können einen dedizierten vCenter-Benutzer und eine Rolle erstellen, die nur die für die OVF-Vorlagenbereitstellung erforderlichen Berechtigungen besitzt. Weitere Informationen finden Sie in der Liste der Rollen "[Mit ONTAP tools for VMware vSphere 10 enthaltene Rollen](#)".

Für die vCenter Instanz, die von ONTAP tools verwaltet wird, muss das vCenter Benutzerkonto über Administratorrechte verfügen.

Während des Upgrades erhalten Sie eine Benachrichtigung, falls bei integrierten Storage-Backend-Zertifikaten Einträge für Subject Alternative Name (SAN) fehlen. Wenn Sie sich entscheiden, ohne Validierung des SAN fortzufahren, wird das Upgrade fortgesetzt, was jedoch aufgrund potenzieller Sicherheitsrisiken nicht empfohlen wird.

10. Beim Upgrade werden die folgenden Aktionen automatisch ausgeführt:
 - a. Das Gateway-Zertifikat wird mit einer Gültigkeitsdauer von einem Jahr erneuert. Beim Entfernen des vorherigen SRA-Adapters und Hochladen des neuen 10.5-Adapters ändert sich die Gültigkeitsdauer des SRA-Zertifikats von 10 Jahren auf 1 Jahr.
 - b. Das Remote Plug-in ist aktualisiert.
 - c. ONTAP und vCenter Server-Zertifikate werden validiert und zu ONTAP tools hinzugefügt
 - d. Backup ist aktiviert.

Was kommt als Nächstes

Nach dem Upgrade auf ONTAP tools für VMware vSphere 10.5:

- Systemwarnungen werden überwacht und es empfiehlt sich, die Erneuerung des Gateway-Zertifikats vor Ablauf der einjährigen Gültigkeitsdauer einzuplanen.
- Den ONTAP tools 10.4 oder 10.3 SRA Adapter entfernen und die 10.5 SRA Adapter tar-Datei hochladen.
- Nach dem Hochladen des SRA-Adapter-Tar-Archivs wird der Installationsbefehl ausgeführt. Anschließend erfolgt ein erneuter Scan der SRA-Adapter, wodurch die Seite „VMware Site Recovery Storage Replication

Adapters“ aktualisiert wird.

Nach dem Upgrade können Sie:

- Die Dienste können über die Manager-Benutzeroberfläche deaktiviert werden.
- Wechsel von einer Non-HA-Konfiguration zu einer HA-Konfiguration
- Eine nicht-HA-Kleinkonfiguration kann auf eine nicht-HA-Mittlere oder auf eine HA-Mittlere oder HA-Großkonfiguration skaliert werden.

Verwandte Informationen

["Migration von ONTAP tools für VMware vSphere 9.xx auf 10.5"](#)

ONTAP tools-Upgrade-Fehlercodes

Während des Upgrades der ONTAP tools for VMware vSphere können Fehlercodes auftreten. Die Fehlercodes sind fünfstellig, wobei die ersten beiden Ziffern das Skript kennzeichnen, bei dem das Problem aufgetreten ist, und die letzten drei Ziffern den spezifischen Workflow innerhalb dieses Skripts darstellen.

Alle Fehlerprotokolle werden in der Datei `ansible-perl-errors.log` gespeichert, um die Nachverfolgung und Behebung von Problemen zu vereinfachen. Diese Protokolldatei enthält den Fehlercode und die fehlgeschlagene Ansible-Aufgabe.



Die auf dieser Seite angegebenen Fehlercodes dienen nur als Referenz. Wenden Sie sich an das Support-Team, falls der Fehler weiterhin besteht oder keine Lösung genannt wird.

Die folgende Tabelle listet die Fehlercodes und die zugehörigen Dateinamen auf.

Fehlercode	Skriptname
00	firstboot-network-config.pl, Modus Deploy
01	firstboot-network-config.pl, Modus Upgrade
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, deploy, HA
04	firstboot-deploy-otv-ng.pl, Deploy, Non-HA
05	firstboot-deploy-otv-ng.pl, reboot
06	firstboot-deploy-otv-ng.pl, Upgrade, HA
07	firstboot-deploy-otv-ng.pl, Upgrade, non-HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Die letzten drei Ziffern des Fehlercodes geben den spezifischen Workflow-Fehler innerhalb des Skripts an:

Upgrade Fehlercode	Arbeitsablauf	Auflösung
052	Die ISO könnte mit der aktuellen Version identisch sein oder zwei Versionen über der aktuellen Version liegen.	Eine mit Ihrer aktuellen Version kompatible ISO-Version ermöglicht ein Upgrade.
068	Das Rollback der Debian Pakete ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
069	Fehler beim Wiederherstellen der Dateien	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
070	Fehler beim Löschen der Sicherung	-
071	Kubernetes Cluster war nicht fehlerfrei.	-
074	ISO-Einbindung ist fehlgeschlagen	Die Datei /var/log/upgrade-run.log prüfen und das Upgrade erneut versuchen.
075	Die Vorabprüfungen für das Upgrade sind fehlgeschlagen	Das Upgrade kann erneut versucht werden.
076	Das Registry Upgrade ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
077	Die Registry-Wiederherstellung ist fehlgeschlagen	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
078	Das Upgrade des Operators ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
079	Das Zurücksetzen des Operators ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
080	Das Upgrade der Services ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
081	Das Zurücksetzen der Dienste ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.

Upgrade Fehlercode	Arbeitsablauf	Auflösung
082	Das Löschen alter Images aus dem Container ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
083	Das Löschen der Sicherung ist fehlgeschlagen	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
084	Die Rückumstellung von JobManager auf Produktion ist fehlgeschlagen	Führen Sie die folgenden Schritte aus, um das Upgrade wiederherzustellen/abzuschließen. 1. Diagnose-Shell aktivieren 2. Den Befehl ausführen: <i>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> 3. Überprüfen Sie die Protokolle unter <i>/var/log/post-deploy-upgrade.log</i>
087	Die Schritte nach dem Upgrade sind fehlgeschlagen.	Führen Sie die folgenden Schritte aus, um das Upgrade wiederherzustellen/abzuschließen. 1. Diagnose-Shell aktivieren 2. Den Befehl <i>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> ausführen 3. Überprüfen Sie die Protokolle unter <i>/var/log/post-deploy-upgrade.log</i>
088	Die Konfiguration der Protokollrotation für journald ist fehlgeschlagen.	Prüfen Sie, ob die Netzwerkeinstellungen der VM mit dem Host kompatibel sind, auf dem die VM gehostet wird. Sie können versuchen, die VM auf einen anderen Host zu migrieren und neu zu starten.
089	Die Änderung der Besitzverhältnisse der Konfigurationsdatei für die Rotation des Zusammenfassungsprotokolls ist fehlgeschlagen.	Das Upgrade kann erneut versucht werden.
095	Betriebssystem-Upgrade fehlgeschlagen	Keine Wiederherstellung für OS-Upgrade. ONTAP tools Dienste werden aktualisiert und neue Pods werden ausgeführt.
096	Dynamischen Speicherbereitsteller installieren	Die Upgrade-Protokolle prüfen und das Upgrade erneut versuchen.

Upgrade Fehlercode	Arbeitsablauf	Auflösung
097	Die Deinstallation der Dienste für das Upgrade ist fehlgeschlagen	Zero RPO oder snapshotbasierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
098	Das Kopieren des dockercréd-Secrets vom ntv-system in den Namespace des dynamischen Storage Provisioners ist fehlgeschlagen.	Die Upgrade-Protokolle prüfen und das Upgrade erneut versuchen.
099	Die Validierung der neuen HDD-Erweiterung ist fehlgeschlagen.	Die neue Festplatte wird im Fall einer HA-Bereitstellung allen Knoten und im Fall einer Nicht-HA-Bereitstellung nur einem Knoten hinzugefügt.
109	Die Sicherung der persistenten Volume-Daten ist fehlgeschlagen.	Die Upgrade-Protokolle prüfen und das Upgrade erneut versuchen.
110	Die Wiederherstellung der persistenten Volumendaten ist fehlgeschlagen	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
111	Die Aktualisierung der etcd Zeitüberschreitung Parameter für RKE2 ist fehlgeschlagen.	Die Upgrade-Protokolle prüfen und das Upgrade erneut versuchen.
112	Die Deinstallation des dynamischen Speicherbereitstellungsdienstes ist fehlgeschlagen.	-
113	Die Aktualisierung der Ressourcen auf den sekundären Knoten ist fehlgeschlagen	Die Upgrade-Protokolle prüfen und das Upgrade erneut versuchen.
104	Der Neustart des sekundären Knotens ist fehlgeschlagen	Starten Sie die Knoten manuell neu, einen nach dem anderen.
100	Kernel-Rollback ist fehlgeschlagen	-
051	Das Upgrade des dynamischen Speicherbereitstellungsdienstes ist fehlgeschlagen.	Upgrade-Protokolle prüfen und Upgrade erneut versuchen.
056	Das Löschen der Migrationssicherung ist fehlgeschlagen	NA
090	Zertifikatsvalidierung für Storage Backends und vCenter fehlgeschlagen	Upgrade-Protokolle und die Protokolldatei unter /var/log/cert_validation_error.log können geprüft und das Upgrade erneut versucht werden.

Upgrade Fehlercode	Arbeitsablauf	Auflösung
114	Interne Zertifikatsaktualisierung in der MongoDB-Collection fehlgeschlagen	Falls das Upgrade mit dem Fehlercode 114 fehlschlägt, führen Sie die folgenden Schritte aus: 1. Stellen Sie eine Verbindung zum Upgrade-ISO auf dem primären Knoten her und aktivieren Sie die Diagnose-Shell. 2. Mounten Sie die ISO-Datei über die SSH-Sitzung auf dem primären Knoten: <pre> sudo mount /dev/cdrom sudo mount -o loop,ro /dev/cdrom/APPLIANCE_UPGRADE.bin /upgrade </pre> 3. Debian-Pakete installieren: <pre> sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vplatform.deb sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vpupgrader.deb sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vmware-tools.deb </pre> 4. Kopieren Sie die Build-Informationsdatei: <pre> sudo cp /upgrade/APPLIANCE_BUILD / </pre>
		Fügen Sie der Sammlung Zertifikate hinzu, indem Sie die



Ab ONTAP tools for VMware vSphere 10.3 wird Zero RPO nicht ⁵ unterstützt.

Erfahren Sie mehr über ["Wie ONTAP tools for VMware vSphere nach einem fehlgeschlagenen Upgrade von Version 10.0 auf 10.1 wiederhergestellt werden können"](#)

Diagnose-Shell aktivieren und folgenden Befehl ausführen:

```
sudo perl
/home/maint/scripts
/post-deploy-
upgrade.pl
--internal_cert_upd
ate_collection
```

Überprüfen Sie die Protokolle unter

```
/var/log/otvng/post-
deploy-upgrade.log.
```

6. Starten Sie die Knoten neu:

```
sudo bash
/home/maint/scripts
/vault_decrypt.sh
cd
/home/maint/rke2-pb
sudo ansible-
playbook site.yaml
--tags
restart_nodes
--skip-tags
debian_upgrade,kern
el_upgrade,rescan_s
csi_bus,source_iso,
eject_upgrade,mount
Iso,upgradeNodes,re
gistryUpg,deleteOld
Images,wait,checkRe
achability,delete_o
tv_cr,uninstall_tri
dent,del_trident_im
ages,refresh_resour
ces,ntp_configure,n
tpd_uninstall
```

7. Führen Sie die Schritte nach dem Upgrade durch:

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, Aufnahmen 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.

```
upgrade.pl
--postupgrade
```

8. Überprüfen Sie den erfolgreichen Abschluss, indem Sie die Protokolle einsehen:

```
tail -f
/var/log/post-
deployment.log
```

Achten Sie auf die Erfolgsmeldung „Completed post 10.5 upgrade steps.“

9. ISO auswerfen

```
sudo umount -l -f
/upgrade
sudo umount
/dev/cdrom
sudo eject
/dev/cdrom
```

10. Starten Sie den primären Knoten neu.

```
sudo reboot -f
```