



ONTAP Mediator Dokumentation

ONTAP Mediator

NetApp
October 19, 2026

This PDF was generated from <https://docs.netapp.com/de-de/ontap-mediator/index.html> on October 19, 2026. Always check docs.netapp.com for the latest.

Inhalt

ONTAP Mediator Dokumentation	1
Versionshinweise	2
Was ist neu in ONTAP Mediator?	2
ONTAP Mediator Unterstützungsmatrix	5
OS Support-Matrix	5
SCST Support-Matrix	8
Los geht's	9
Erfahren Sie mehr über ONTAP Mediator	9
Funktionsweise des ONTAP Mediator	9
ONTAP Mediator Services	9
Für den Systemadministrator bereitgestellte Tools	9
SCST- und Kernel-Updates	10
Unterstützung für HTTPS und iSCSI	10
Schnellstart für ONTAP Mediator	10
Was kommt als Nächstes?	11
Installation und Einrichtung	12
Zusammenfassung des Installationsablaufs von ONTAP Mediator	12
Vorbereitung der Installation des ONTAP Mediators	12
Installationsanforderungen	13
Host-Anforderungen	14
Firewall- und Netzwerkanforderungen	14
OS-Anforderungen	15
ONTAP Mediator installieren, wenn UEFI Secure Boot aktiviert ist	16
Repository-Zugriff für die ONTAP Mediator Installation bereitstellen	17
Das Installationspaket für ONTAP Mediator herunterladen	25
Die Code-Signatur des ONTAP Mediators überprüfen	26
Das ONTAP Mediator Installationspaket installieren	28
Den Sicherheitsschlüssel für UEFI Secure Boot registrieren	46
Signieren von SCST Kernelmodulen	47
ONTAP Mediator Installationsstatus überprüfen	48
ONTAP Mediator verwenden	51
Einsatz von ONTAP Mediator für SnapMirror active sync und MetroCluster IP	51
Aktive Synchronisierungsbeziehungen von SnapMirror überwachen	51
Überwachung von MetroCluster IP Konfigurationen	51
ONTAP Mediator verwalten	53
Upgrade von ONTAP Mediator	53
Upgrade von ONTAP Mediator	53
Aktualisieren Sie das Host-Betriebssystem und installieren oder aktualisieren Sie ONTAP Mediator neu.	61
Konfigurieren der ONTAP Mediator Attribute	66
Konfigurierbare Einstellungen für ONTAP Mediator	66
Installation von SSL-Zertifikaten von Drittanbietern	67
Schutz vor Passwortangriffen konfigurieren	69

Konfiguration von Regeln zur Passwortkomplexität	70
Konfiguration der Freispeicherschwelle	70
Konfiguration des reservierten Protokollspeicherplatzes	70
Änderung von Benutzername und Passwort des ONTAP Mediator	71
Benutzernamen ändern	71
Passwort ändern	72
ONTAP Mediator starten und stoppen	73
ONTAP Mediator stoppen	73
Starten von ONTAP Mediator	73
Überprüfung des ONTAP Mediator Systemstatus	74
Überprüfung des Service-Status	74
Bestätigung der Listening-Ports	75
Zertifikate verwalten	75
Erneutes Generieren eines temporären selbstsignierten Zertifikats für den ONTAP Mediator Host	75
Ersetzen der selbstsignierten Zertifikate von ONTAP Mediator durch vertrauenswürdige Zertifikate von Drittanbietern	77
Fehlerbehebung bei ONTAP Mediator Problemen im Zusammenhang mit Zertifikaten	91
Das Host-Betriebssystem für ONTAP Mediator warten	96
Den Host neu starten	96
Host Paketaktualisierungen	97
Der Kernel des Host-Betriebssystems wird aktualisiert.	97
Hostwartung durchführen	98
Änderungen am Hostnamen oder an der IP	100
ONTAP Mediator deinstallieren	101
Rechtliche Hinweise	103
Copyright	103
Marken	103
Patente	103
Datenschutzrichtlinie	103
Open Source	103
ONTAP Mediator für MetroCluster IP und SnapMirror active sync	103

ONTAP Mediator Dokumentation

Versionshinweise

Was ist neu in ONTAP Mediator?

Mit jeder neuen Version von ONTAP Mediator werden neue Verbesserungen bereitgestellt.



Informationen zur OS- und SCST-Version sind unter ["Supportmatrix"](#) verfügbar.

ONTAP Mediator Version	Verbesserungen
1.12.1	• Unterstützung für RHEL: ◦ Kompatibel: 10.1 und 9.7. ◦ Empfohlen: 10.2, 10.0, 9.8, 9.6, 9.4 und 8.10. • Unterstützung für Rocky Linux 10.2, 9.8 und 8.10. • Unterstützung für Oracle Linux 10.1 und 9.8 mit sowohl rhck- als auch uek-Kernen. • Ab ONTAP Mediator 1.12.1 und ONTAP 9.19.1 kann eine einzelne, mit HTTPS konfigurierte ONTAP Mediator Instanz die folgenden Konfigurationen gleichzeitig überwachen: ◦ Maximal zehn Vier-Knoten- oder fünf Acht-Knoten MetroCluster IP-Konfigurationen bei Installation auf einem Host mit 8-Kern-CPU und mindestens 16GB RAM. Weitere Informationen unter "ONTAP Mediator zur Überwachung mehrerer MetroCluster IP Konfigurationen verwenden". ◦ Eine MetroCluster IP Konfiguration mit vier Knoten und eine SnapMirror active sync Peer-Beziehung, wenn sie auf einem Host mit einer 2-Kern-CPU installiert ist. Weitere Informationen unter "Den ONTAP Mediator für SnapMirror Active Sync konfigurieren". • Enthält ein neues Tool zur Reparatur einer beschädigten SCST-Installation. Nach der Installation von ONTAP Mediator befindet sich das Tool unter <code>/usr/local/bin/mediator_repair_scst</code>. Das Tool kann nach einem Betriebssystem-Upgrade verwendet werden, wenn das aktualisierte Betriebssystem einen SCST-Patch benötigt, der im Standard-SCST-Paket nicht verfügbar ist.

1,12	• Unterstützung für RHEL: ◦ Kompatibel: 10.1 und 9.7. ◦ Empfohlen: 10.2, 10.0, 9.8, 9.6, 9.4 und 8.10. • Unterstützung für Rocky Linux 10.2, 9.8 und 8.10. • Unterstützung für Oracle Linux 10.1 und 9.7 mit sowohl rhck- als auch uek-Kernen. • Ab ONTAP 9.19.1 und ONTAP Mediator 1.12 kann ein ONTAP Mediator konfiguriert werden, der HTTPS für die Kommunikation in MetroCluster IP-Konfigurationen verwendet. HTTPS bietet erhöhte Sicherheit, indem gesamte Sitzungen mit SSL/TLS verschlüsselt werden. Es besteht die Möglichkeit, ONTAP Mediator ausschließlich mit Unterstützung für HTTPS zu installieren. Das SCST-Paket wird bei Verwendung dieser Installationsmethode nicht installiert. "Erfahren Sie mehr über die HTTPS- und iSCSI-Installationsoptionen für ONTAP Mediator".
1,11	• Unterstützung für RHEL 10.1, 10.0, 9.7, 9.6, 9.4 und 8.10. • Unterstützung für Rocky Linux 10.1, 9.7 und 8.10. • Unterstützung für Oracle Linux 10.0 und 9.6 mit sowohl rhck- als auch uek-Kernen. • Fügt Unterstützung für IPv6 für MetroCluster IP-Konfigurationen hinzu. • Unterstützung für fapolicyd wurde hinzugefügt.
1,10	• Unterstützung für RHEL 10.0, 9.6, 9.4 und 8.10. • Unterstützung für Rocky Linux 10.0, 9.6 und 8.10. • Die Basis-Python-Version wird von Python 3.9 auf Python 3.12 aktualisiert.
1.9.1	• Unterstützung für RHEL: ◦ Kompatibel: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 und 8.4. ◦ Empfohlen: 9.5, 9.4, 9.2, 9.0, 8.10 und 8.8. • Unterstützung für Rocky Linux 9.5 und 8.10. • Fügt neue Zertifikate zur Überprüfung von Codesignaturen hinzu. • Unterstützung für das Überspringen von Codesignaturprüfungen mit dem <code>-skip-code-signature-check</code> Flag hinzugefügt. • Das Installationsprogramm zeigt Warnungen an, wenn es abgelaufene Codesignaturzertifikate erkennt.
1,9	• Unterstützung für RHEL: ◦ Kompatibel: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 und 8.4. ◦ Empfohlen: 9.5, 9.4, 9.2, 9.0, 8.10 und 8.8. • Unterstützung für Rocky Linux 9.5 und 8.10. • FIPS-Unterstützung für RHEL und Rocky Linux. • Zusätzliche Leistungsverbesserungen für größere Skalierbarkeit. • Verbesserte Dateinamen zur Vereinfachung der Einrichtung von PKI-signierten Zertifikaten.

1,8	• Unterstützung für RHEL: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4. ◦ Empfohlen: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 und 8.8. • Unterstützung für Rocky Linux 9.4 und 8.10.
1,7	• Unterstützung für RHEL: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4. ◦ Empfohlen: 9.3, 9.2, 9.1, 9.0, 8.9 und 8.8. • Unterstützung für Rocky Linux 9.3 und 8.9. • Unterstützung für SAN (Subject Alternative Name) Daten in selbstsignierten Zertifikaten und von Drittanbietern signierten Zertifikaten.
1,6	• Python 3.9 Updates. • Unterstützung für RHEL: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4. ◦ Empfohlen: 9.2, 9.1, 9.0 und 8.8. • Unterstützung für Rocky Linux 9.2 und 8.8. • Die Unterstützung für RHEL 7.x / CentOS alle Versionen wurde eingestellt.
1,5	• Unterstützung für RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6. • Unterstützung für CentOS 7.9, 7.8, 7.7 und 7.6. • Enthält Warnungen zur Einstellung des Supports für RHEL 7.x / CentOS 7.x. • Optimiert die Geschwindigkeit für größere SnapMirror active sync Systeme. • Dem Installationsprogramm wurde eine kryptografische Codesignatur hinzugefügt.
1,4	• Unterstützung für RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6. • Unterstützung für CentOS 7.9, 7.8, 7.7 und 7.6. • Unterstützung für Secure Boot (SB) von UEFI-basierter Firmware wurde hinzugefügt.
1,3	• Unterstützung für RHEL 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6. • Unterstützung für CentOS 7.9, 7.8, 7.7 und 7.6.
1,2	• Unterstützung für RHEL 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6. • Unterstützung für CentOS 7.9, 7.8, 7.7 und 7.6. • Unterstützung für HTTPS-Mailboxen. • Zur Verwendung mit ONTAP 9.8+ MCC-IP AUSO und SnapMirror active sync ZRTO.
1,1	• Unterstützung für RHEL 8.0 und 7.6. • Unterstützung für CentOS 7.6. • Entfernt Perl-Abhängigkeiten.

1,0	• Unterstützung für iSCSI Mailboxen. • Zur Verwendung mit ONTAP 9.7+ MCC-IP AUSO. • Unterstützung für RHEL/CentOS 7.6.
-----	--

ONTAP Mediator Unterstützungsmatrix

Die Supportmatrix für ONTAP Mediator enthält Informationen zur Unterstützung von Betriebssystemen und SCST Versionen.

OS Support-Matrix

Die folgende Tabelle führt die unterstützten Betriebssysteme für jede Version von ONTAP Mediator auf.

Betriebssystem für ONTAP Mediator	1.12.1	1,12	1,11	1,10	1.9.1	1,9	1,8	1,7	1,6	1,5	1,4	1,3	1,2	1,1	1,0
RHEL 10,2	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 10,1	Kompatibel	Kompatibel	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 10,0	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,8	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,7	Kompatibel	Kompatibel	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,6	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,5	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,4	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,3	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,2	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein

RHE L 9,1	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
RHE L 9,0	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
RHE L 8,10	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHE L 8,9	Nein	Nein	Nein	Nein	Kompatibel	Kompatibel	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHE L 8,8	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
RHE L 8,7	Nein	Nein	Nein	Nein	Kompatibel	Kompatibel	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
RHE L 8,6	Nein	Nein	Nein	Nein	Kompatibel	Kompatibel	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
RHE L 8,5	Nein	Nein	Nein	Nein	Kompatibel	Kompatibel	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
RHE L 8,4	Nein	Nein	Nein	Nein	Kompatibel	Kompatibel	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
RHE L 8,3	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja	Ja	Ja	Nein	Nein	Nein
RHE L 8,2	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja	Ja	Ja	Nein	Nein	Nein
RHE L 8,1	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja	Ja	Ja	Ja	Nein	Nein
RHE L 8,0	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja	Ja	Ja	Ja	Ja	Nein
RHE L und Cent OS 7.9	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja	Ja	Ja	Kompatibel	Nein	Nein
RHE L und Cent OS 7.8	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja	Ja	Ja	Ja	Nein	Nein

RHEL und CentOS 7.7	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja	Ja	Ja	Ja	Nein	Nein
RHEL und CentOS 7.6	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja	Ja	Ja	Ja	Ja	Ja (nur RHEL)
CentOS 8 und Stream	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	k. A.	k. A.
Rocky Linux 10	Ja (10.2)	Ja (10.2)	Ja (10.0 und 10.1)	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Rocky Linux 9	Ja (9.8)	Ja (9.8)	Ja (9.7)	Ja (9.6 und 9.4)	Ja (9.5)	Ja (9.5)	Ja (9.4)	Ja (9.3)	Ja (9.2)	k. A.	k. A.	k. A.	k. A.	k. A.	k. A.
Rocky Linux 8	Ja (8.10)	Ja (8.10)	Ja (8.10)	Ja (8.10)	Ja (8.10)	Ja (8.10)	Ja (8.10)	Ja (8.9)	Ja (8.8)	k. A.	k. A.	k. A.	k. A.	k. A.	k. A.
Oracle Linux 10	Ja (10.1)	Ja (10.1)	Ja (10.0)	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Oracle Linux 9	Ja (9.8)	Ja (9.7)	Ja (9.6)	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein

- „Ja“ bedeutet, dass das Betriebssystem für die Installation von ONTAP Mediator empfohlen wird und vollständig kompatibel sowie unterstützt ist.
- „Nein“ bedeutet, dass das Betriebssystem und der ONTAP Mediator nicht kompatibel sind.
- „Kompatibel“ bedeutet, dass Red Hat diese RHEL-Versionen nicht mehr unterstützt, ONTAP Mediator aber weiterhin darauf installiert werden kann.
- ONTAP Mediator 1.6 bietet Unterstützung für Rocky Linux 9 und 8.
- ONTAP Mediator 1.5 war die letzte unterstützte Version für Betriebssysteme der RHEL 7.x Reihe.
- CentOS 8 wurde aufgrund der Neustrukturierung für alle Releases entfernt. CentOS Stream wurde als ungeeignetes Zielbetriebssystem für den Produktiveinsatz eingestuft. Kein Support ist geplant.

SCST Support-Matrix

Die folgende Tabelle zeigt die unterstützte SCST-Version für jede Version von ONTAP Mediator.

ONTAP Mediator Version	Unterstützte SCST Version
ONTAP Mediator 1.12.1	scst-3.10.tar.gz
ONTAP Mediator 1.12	scst-3.10.tar.gz
ONTAP Mediator 1.11	scst-3.9.tar.gz
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAP Mediator 1.9.1	scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	scst-3.5.0.tar.bz2
ONTAP Mediator 1.2	scst-3.4.0.tar.bz2
ONTAP Mediator 1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	scst-3.3.0.tar.bz2

Los geht's

Erfahren Sie mehr über ONTAP Mediator

ONTAP Mediator unterstützt ONTAP Funktionen durch die Bereitstellung eines persistenten und abgegrenzten Speichers für Hochverfügbarkeitsmetadaten (HA), durch eine synchrone Funktion zur Abfrage des Node-Systemstatus zur Unterstützung der Quorumbestimmung sowie als Ping-Proxy für die Controller-Erreichbarkeit.



Diese Dokumentation bezieht sich auf die On-Premise-Version von ONTAP Mediator. Informationen zu ONTAP Cloud Mediator, verfügbar ab ONTAP 9.17.1, sind in der "[SnapMirror active sync Dokumentation](#)" zu finden.

Funktionsweise des ONTAP Mediator

ONTAP Mediator läuft auf einem Linux-Host in einer dritten Ausfalldomäne, getrennt von Ihren ONTAP Clustern, und stellt dort einen persistenten, geschützten Speicher für HA-Metadaten bereit. ONTAP nutzt diesen Speicher zusammen mit der Systemstatusabfrage des Mediators und den Ping-Proxy-Funktionen, um SnapMirror active sync Beziehungen und MetroCluster IP Konfigurationen zu überwachen.

- ONTAP Mediator nutzt die Knotenverwaltungs-LIF und die Clusterverwaltungs-LIF, um über mehrere redundante Pfade mit jedem Cluster zu kommunizieren. Dadurch kann ONTAP zwischen einem vollständigen Standortausfall und dem Ausfall einer einzelnen InterSwitch Link (ISL) unterscheiden.
- Bei SnapMirror active sync behandelt ONTAP den Peer als nicht erreichbar, wenn ein Cluster die Verbindung sowohl zu seinem Peer als auch zu ONTAP Mediator verliert, und kann automatisch auf die verbleibende Kopie umschalten.
- In MetroCluster IP-Konfigurationen unterstützt ONTAP Mediator einen Mediator-gestützten automatischen ungeplanten Switchover (MAUSO), indem er Statusinformationen über die MetroCluster Knoten speichert und dabei hilft, im Fehlerfall die geeignete Vorgehensweise zu bestimmen.

ONTAP Mediator Services

ONTAP Mediator bietet zwei zusätzliche systemctl Dienste:

- **ontap_mediator.service**

Wartet den REST API Server zur Verwaltung der ONTAP Beziehungen.

- **mediator-scst.service**

Steuert das Starten und Herunterfahren des iSCSI-Moduls (SCST).

Für den Systemadministrator bereitgestellte Tools

Für den Systemadministrator bereitgestellte Tools:

- **/usr/local/bin/mediator_change_password**

Legt ein neues API-Passwort fest, wenn der aktuelle API-Benutzername und das aktuelle API-Passwort angegeben sind.

- **/usr/local/bin/mediator_change_user**

Legt einen neuen API-Benutzernamen fest, wenn der aktuelle API-Benutzername und das aktuelle Passwort angegeben werden.

- **/usr/local/bin/mediator_generate_support_bundle**

Erzeugt eine lokale tgz-Datei mit allen relevanten Supportinformationen, die für die Kommunikation mit dem NetApp Kundensupport benötigt werden. Dies umfasst Anwendungskonfiguration, Protokolle und einige Systeminformationen. Die Bundles werden auf der lokalen Festplatte erstellt und können bei Bedarf manuell übertragen werden. Speicherort: /opt/netapp/data/support_bundles/

- **/usr/local/bin/uninstall_ontap_mediator**

Entfernt das ONTAP Mediator Paket und das SCST Kernelmodul. Dies umfasst alle Konfigurations-, Protokoll- und Mailbox-Daten.

- **/usr/local/bin/mediator_unlock_user**

Die Sperre des API-Benutzerkontos wird aufgehoben, wenn das Authentifizierungs-Limit für Wiederholungsversuche erreicht wurde. Diese Funktion wird verwendet, um Brute-Force-Passwortableitungen zu verhindern. Der Benutzer wird zur Eingabe des korrekten Benutzernamens und Passworts aufgefordert.

- **/usr/local/bin/mediator_add_user**

(Nur für Supportzwecke) Wird verwendet, um den API-Benutzer bei der Installation hinzuzufügen.

SCST- und Kernel-Updates

ONTAP Mediator verwendet SCST, um iSCSI für die Kommunikation in MetroCluster IP-Konfigurationen bereitzustellen. Das SCST-Paket ist ein Kernelmodul, das während der Installation kompiliert wird. Sie müssen SCST möglicherweise nach Updates des Kernels neu installieren. Alternativ deinstallieren Sie ONTAP Mediator, installieren es dann erneut und konfigurieren die ONTAP-Beziehung neu. Weitere Informationen zu SCST finden Sie unter "[SCST: Ein generisches SCSI-Zielsubsystem für Linux](#)".



Sie sollten alle Aktualisierungen des Server-OS-Kernels mit einem Wartungsfenster in ONTAP koordinieren.

Unterstützung für HTTPS und iSCSI

Ab ONTAP 9.19.1 und ONTAP Mediator 1.12 kann ein ONTAP Mediator konfiguriert werden, der HTTPS oder iSCSI zur Überwachung einer MetroCluster IP-Konfiguration verwendet. Es besteht die Möglichkeit, ONTAP Mediator mit Unterstützung für sowohl iSCSI als auch HTTPS oder nur für HTTPS zu installieren. Wenn ONTAP Mediator ausschließlich mit Unterstützung für HTTPS installiert wird, wird das SCST-Paket nicht installiert. Weitere Informationen finden Sie unter "[HTTPS- und iSCSI-Installationsoptionen für ONTAP Mediator](#)".

Schnellstart für ONTAP Mediator

Für den Einstieg in ONTAP Mediator wird die Software installiert und für die Verwendung mit Ihrer ONTAP Umgebung konfiguriert.

1

Installation von ONTAP Mediator

"[Installieren Sie ONTAP Mediator](#)" auf Ihrem System und stellen Sie sicher, dass alle erforderlichen Abhängigkeiten erfüllt sind.

2

Überprüfung der ONTAP Mediator Installation

"[Überprüfung der erfolgreichen Installation von ONTAP Mediator](#)" durch Überprüfung des Servicestatus und Durchsicht der Protokolle auf Fehler oder Warnungen.

3

ONTAP Mediator für Ihre ONTAP Umgebung konfigurieren

Je nachdem, ob Sie "[Verwendung von ONTAP Mediator für MetroCluster IP, SnapMirror active sync oder beides](#)" möchten, sind die entsprechenden Konfigurationsschritte erforderlich, damit alle notwendigen Einstellungen korrekt angewendet werden.

Was kommt als Nächstes?

Mit ONTAP Mediator können Sie nun MetroCluster IP Konfigurationen, SnapMirror active sync Konfigurationen oder beides überwachen. Weitere Informationen finden Sie unter "[SnapMirror active sync Dokumentation](#)" und "[MetroCluster Dokumentation](#)".

Installation und Einrichtung

Zusammenfassung des Installationsablaufs von ONTAP Mediator

Die Installation von ONTAP Mediator umfasst die Vorbereitung der Installation, die Bereitstellung des Zugriffs auf die Repositories, das Herunterladen des Installationspakets, die Überprüfung der Codesignatur und die Installation des ONTAP Mediator Pakets.

1

"Vorbereitung der Installation des ONTAP Mediators"

Für die Installation von ONTAP Mediator muss sichergestellt sein, dass alle Voraussetzungen erfüllt sind.

2

"Repository-Zugriff bereitstellen"

Der Zugriff auf die Repositories sollte aktiviert werden, damit ONTAP Mediator während des Installationsprozesses auf die benötigten Pakete zugreifen kann.

3

"Das Installationspaket für ONTAP Mediator herunterladen"

Das ONTAP Mediator Installationspaket steht auf der ONTAP Mediator Downloadseite zum Herunterladen bereit.

4

"Die Codesignatur des ONTAP Mediator Installationspakets überprüfen"

NetApp empfiehlt, die ONTAP Mediator-Code-Signatur vor der Installation des ONTAP Mediator Installationspakets zu überprüfen.

5

"Das ONTAP Mediator Installationspaket installieren"

Das Installationspaket wird heruntergeladen und das Installationsprogramm auf dem Host ausgeführt.

6

"Die Installation des ONTAP Mediators überprüfen"

Nach der Installation von ONTAP Mediator sollte überprüft werden, ob dieser erfolgreich ausgeführt wird.

Vorbereitung der Installation des ONTAP Mediators

Für die Installation von ONTAP Mediator müssen alle Voraussetzungen erfüllt sein, das Installationspaket heruntergeladen und das Installationsprogramm auf dem Host ausgeführt werden.



- Informationen zum Upgrade von ONTAP Mediator auf eine neue Version finden Sie unter

"Upgrade von ONTAP Mediator".

- Falls Sie das Host-Betriebssystem aktualisieren und ONTAP Mediator in diesem Zuge neu installieren oder aktualisieren müssen, finden sich weitere Informationen unter ["Aktualisieren Sie das Host-Betriebssystem und ONTAP Mediator"](#).

Installationsanforderungen

Vor der Installation von ONTAP Mediator ist eine Prüfung der folgenden Anforderungen erforderlich.



- ONTAP Mediator 1.8 und frühere Versionen sind nicht mit dem FIPS-Modus von Red Hat Enterprise Linux (RHEL) kompatibel und verhindern eine erfolgreiche Installation. Ob der FIPS-Modus aktiviert ist, lässt sich mit dem `fips-mode-setup --check` Befehl überprüfen. Der FIPS-Modus kann mit dem `fips-mode-setup --disable` Befehl deaktiviert werden. Nach der Deaktivierung des FIPS-Modus ist ein Neustart erforderlich, damit ONTAP Mediator 1.8 oder eine frühere Version erfolgreich installiert werden kann.
- Falls die Installation fehlschlägt, müssen Sie es möglicherweise mit einer neueren Version von ONTAP Mediator versuchen.
- Ab dem 15. Juni 2025 können ONTAP Mediator 1.9 und 1.8 nicht mehr installiert oder aktualisiert werden, da deren Code-Signing-Zertifikate abgelaufen sind. Falls die Installation fehlschlägt, kann stattdessen die Patch-Version ONTAP Mediator 1.9.1 verwendet werden.

- Wenn Sie das `yum-utils` Paket installieren, können Sie den `needs-restarting` Befehl verwenden.
- Ab ONTAP Mediator 1.11 wird IPv6 für MetroCluster IP-Konfigurationen unterstützt.

HTTPS- und iSCSI-Installationsoptionen für ONTAP Mediator

Vor der Installation von ONTAP Mediator sind die folgenden Informationen zu beachten:

- Im ONTAP Mediator wird das SCST-Paket verwendet, um iSCSI für die Kommunikation in MetroCluster IP Konfigurationen bereitzustellen. Das SCST-Paket ist ein Kernelmodul, das während der Installation kompiliert wird. Ab ONTAP 9.19.1 und Mediator 1.12 lässt sich ein ONTAP Mediator konfigurieren, der HTTPS anstelle von iSCSI zur Überwachung einer MetroCluster IP Konfiguration verwendet.
- Ab ONTAP 9.19.1 und ONTAP Mediator 1.12 besteht die Möglichkeit, ONTAP Mediator mit iSCSI und HTTPS-Unterstützung oder nur mit HTTPS-Unterstützung zu installieren. Wenn ONTAP Mediator nur mit HTTPS-Unterstützung installiert wird, wird das SCST-Paket nicht installiert.
- Wenn Sie von ONTAP Mediator 1.11 oder einer früheren Version mit installiertem SCST aktualisieren und während des Upgrades die Option „Nur HTTPS“ auswählen, wird das SCST-Paket deinstalliert und die neue ONTAP Mediator Version enthält das SCST-Paket nicht.
- Wenn die Überwachung mehrerer MetroCluster IP-Konfigurationen mit ONTAP Mediator vorgesehen ist, hängt die Unterstützung vom Mediator-Typ, der ONTAP Version und dem Betriebssystem ab. Weitere Informationen finden Sie unter ["ONTAP Mediator zur Überwachung mehrerer MetroCluster IP Konfigurationen verwenden"](#).
- Die Installation des ONTAP Mediators mit ausschließlicher HTTPS-Unterstützung wird für die folgenden Anwendungsfälle unterstützt:
 - Sie planen, ONTAP Mediator ausschließlich zur Überwachung Ihrer SnapMirror active sync Cluster zu verwenden.
 - Es ist vorgesehen, ONTAP Mediator mit HTTPS zu konfigurieren, um eine oder mehrere MetroCluster IP-Konfigurationen zu überwachen.

- ONTAP Mediator muss mit Unterstützung für iSCSI und HTTPS im folgenden Szenario installiert werden:
 - Sie planen, ONTAP Mediator mit iSCSI zu konfigurieren, um eine oder mehrere MetroCluster IP-Konfigurationen zu überwachen.

Host-Anforderungen

Diese Anforderungen sind bei der Installation von RHEL oder Rocky Linux und der Konfiguration der zugehörigen Repositories zu berücksichtigen.



Wenn Sie den Installations- oder Konfigurationsprozess ändern, könnten zusätzliche Schritte erforderlich sein.

Anforderungen an Linux-Distributionen

- RHEL oder Rocky Linux gemäß den Best Practices von Red Hat installieren. Da CentOS 8.x das Ende seines Lebenszyklus erreicht hat, werden kompatible Versionen von CentOS 8.x nicht empfohlen.
- Bei der Installation von ONTAP Mediator ist sicherzustellen, dass das System Zugriff auf das erforderliche Repository hat, damit das Installationsprogramm alle erforderlichen Softwareabhängigkeiten abrufen und installieren kann.
- Damit der yum Installer abhängige Software in den RHEL-Repositories finden kann, wird das System während der Installation oder anschließend mit einem gültigen Red Hat Abonnement registriert.



Weitere Informationen enthält die Dokumentation zum Red Hat Subscription Manager.

Firewall- und Netzwerkanforderungen

ONTAP Mediator nutzt eine Reihe von Ports zur Kommunikation mit bestimmten Diensten.

- Wenn Sie eine Firewall eines Drittanbieters verwenden:
 - Der HTTPS-Zugriff muss aktiviert sein.
 - Es muss so konfiguriert werden, dass der Zugriff auf den Ports 31784 und 3260 erlaubt ist.

Bei Verwendung der standardmäßigen Red Hat- oder CentOS-Firewall wird die Firewall während der Mediator-Installation automatisch konfiguriert.

- Für Linux-Hosts ohne Internetzugang sollte sichergestellt sein, dass die benötigten Pakete in einem lokalen Repository verfügbar sind.

Wenn das Link Aggregation Control Protocol (LACP) in einer Linux-Umgebung verwendet wird, sollten der Kernel konfiguriert und die `sysctl net.ipv4.conf.all.arp_ignore` auf 2 gesetzt werden.

Die folgende Tabelle listet die Ports auf, die Sie in Ihrer Firewall zulassen müssen:



- Der iSCSI-Anschluss wird nur in einer MetroCluster IP-Konfiguration benötigt.
- Der 22/tcp-Port wird für den normalen Betrieb nicht benötigt, kann aber für Wartungszwecke vorübergehend aktiviert und nach Abschluss der Wartungssitzung wieder deaktiviert werden.

Port/Dienste	Quelle	Richtung	Ziel	Zweck
--------------	--------	----------	------	-------

22/tcp	Management Host	Eingehend	ONTAP Mediator	(Optional) SSH / ONTAP Mediator Verwaltung
31784/tcp	Cluster-mgmt- und node-mgmt-LIFs	Eingehend	ONTAP Mediator Webserver	(Erforderlich) REST API (HTTPS)
3260/tcp	Node-Management- LIFs	Eingehend	ONTAP Mediator iSCSI-Ziele	(Für MetroCluster IP-Konfigurationen erforderlich) iSCSI- Datenverbindung für Mailboxen



Für einen SnapMirror active sync oder MetroCluster IP ONTAP Mediator, der HTTPS für die Kommunikation verwendet, ist es in ONTAP nicht erforderlich, dass Port 3260 aktiviert oder verbunden ist.

OS-Anforderungen

Ihr Betriebssystem muss die folgenden Anforderungen erfüllen:

- 64-Bit-physische Installation oder virtuelle Maschine
- 8 GB RAM
- 1 GB Festplattenspeicher (für die Installation von Anwendungen, Serverprotokolle und die Datenbank)
- Benutzer: Root Zugriff

In der "[OS Support-Matrix](#)" finden Sie die unterstützten Betriebssysteme für jede Version von ONTAP Mediator.

Für das Betriebssystem erforderliche Pakete

Für ONTAP Mediator sind die folgenden Pakete erforderlich:



Die Pakete sind entweder vorinstalliert oder werden automatisch vom ONTAP Mediator Installationsprogramm installiert.

Alle RHEL/CentOS Versionen	Zusätzliche Pakete für RHEL 10.x / Rocky Linux 10	Zusätzliche Pakete für RHEL 9.x / Rocky Linux 9	Zusätzliche Pakete für RHEL 8.x / Rocky Linux 8
-------------------------------	---	--	--

• openssl • openssl-devel • kernel-devel-\$ (uname -r) • gcc • machen • libselinux-utils • Patch • bzip2 • perl-Data-Dumper • perl-ExtUtils- MakeMaker • efibootmgr • mokutil	• python3.12 • python3.12-devel	• elfutils-libelf-devel • policycoreutils-python- utils • python3 • python3-devel	• elfutils-libelf-devel • policycoreutils-python- utils • redhat-lsb-core • python39 • python39-devel
--	--	--	---

Das Mediator-Installationspaket ist eine selbstextrahierende, komprimierte TAR-Datei, die Folgendes enthält:

- Eine RPM-Datei, die alle Abhängigkeiten enthält, die nicht aus dem Repository der unterstützten Version bezogen werden können.
- Ein Installationsskript.

Ein gültiges SSL-Zertifikat wird empfohlen.



- Die Kernel-Version muss mit der Betriebssystemversion übereinstimmen.
- Aktualisieren Sie den Kernel nicht über die für Ihre ONTAP Mediator-Version unterstützte Betriebssystemversion hinaus, da das getestete SCST-Modul möglicherweise nicht funktioniert.

ONTAP Mediator installieren, wenn UEFI Secure Boot aktiviert ist

ONTAP Mediator kann auf einem System mit oder ohne aktiviertem UEFI Secure Boot installiert werden.

Über diese Aufgabe

- Sie können UEFI Secure Boot vor der Installation von ONTAP Mediator deaktivieren, falls es nicht benötigt wird oder wenn Sie Installationsprobleme mit ONTAP Mediator beheben. Die Option UEFI Secure Boot kann in den Systemeinstellungen deaktiviert werden.
- Wenn Sie ONTAP Mediator 1.12 oder höher mit Unterstützung nur für HTTPS installiert haben, wird das SCST-Paket nicht installiert und Sie können diese Aufgabe überspringen.



Detaillierte Anweisungen zum Deaktivieren von UEFI Secure Boot sind in der Dokumentation Ihres Host-Betriebssystems enthalten.

Um ONTAP Mediator mit aktiviertem UEFI Secure Boot zu installieren, muss ein Sicherheitsschlüssel registriert werden, bevor der Dienst gestartet werden kann. Der Schlüssel wird während des Kompilierungsschritts der SCST-Installation generiert und als privates/öffentliches Schlüsselpaar auf Ihrem Rechner gespeichert. Mit dem `mokutil` Dienstprogramm wird der öffentliche Schlüssel als Machine Owner

Key (MOK) zur UEFI-Firmware hinzugefügt, sodass das System dem signierten Modul vertrauen und es laden kann. Die `mokutil` Passphrase sollte an einem sicheren Ort gespeichert werden, da sie beim Neustart des Systems zur Aktivierung des MOK erforderlich ist.

Schritte

1. Prüfen, ob UEFI Secure Boot auf Ihrem System aktiviert ist:

```
mokutil --sb-state
```

Die Ergebnisse geben Aufschluss darüber, ob UEFI Secure Boot auf diesem System aktiviert ist.

Wenn...	Wechseln zu...
UEFI Secure Boot ist aktiviert	
UEFI Secure Boot ist deaktiviert	"Repository-Zugriff für die ONTAP Mediator Installation bereitstellen"



- Sie werden aufgefordert, eine Passphrase zu erstellen, die Sie an einem sicheren Ort aufbewahren müssen. Sie benötigen diese Passphrase, um den Schlüssel im UEFI Boot Manager zu aktivieren.
- ONTAP Mediator 1.2.0 und frühere Versionen unterstützen diesen Modus nicht.

2. Falls das ``mokutil`` Dienstprogramm nicht installiert ist, kann folgender Befehl ausgeführt werden:

```
yum install mokutil
```

Was kommt als Nächstes?

["Repository-Zugriff für die ONTAP Mediator Installation bereitstellen"](#)

Repository-Zugriff für die ONTAP Mediator Installation bereitstellen

Der Zugriff auf die Repositories sollte aktiviert werden, damit ONTAP Mediator während des Installationsprozesses auf die benötigten Pakete zugreifen kann.

Schritte

1. Es wird ermittelt, auf welche Repositories zugegriffen werden muss, wie in der folgenden Tabelle dargestellt:

Wenn Ihr Betriebssystem...	Sie müssen Zugriff auf diese Repositories gewähren...
Oracle Linux 10.x	• ol-10-for-x86_64-baseos-rpms • ol-10-for-x86_64-appstream-rpms
Oracle Linux 9.x	• ol-9-for-x86_64-baseos-rpms • ol-9-for-x86_64-appstream-rpms

RHEL 10.x	• rhel-10-for-x86_64-baseos-rpms • rhel-10-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-for-x86_64-baseos-rpms • rhel-9-for-x86_64-appstream-rpms
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-rpms
RHEL 7.x	• rhel-7-server-optional-rpms
CentOS 7.x	• C7.6.1810 - Basis Repository
Rocky Linux 10	• appstream • baseos
Rocky Linux 9	• appstream • baseos
Rocky Linux 8	• appstream • baseos

2. Verwenden Sie eines der folgenden Verfahren, um den Zugriff auf die oben aufgeführten Repositories zu ermöglichen, damit ONTAP Mediator während des Installationsprozesses auf die erforderlichen Pakete zugreifen kann.



Falls ONTAP Mediator Abhängigkeiten von Python-Modulen hat, die in den Repositories „extras“ und „optional“ vorhanden sind, könnte ein Zugriff auf die `rhel-X-for-x86_64-extras-rpms` und `rhel-X-for-x86_64-optional-rpms` Dateien erforderlich sein.

▼ Vorgehensweise für das Oracle Linux 10.x Betriebssystem

Führen Sie dieses Verfahren durch, wenn Ihr Betriebssystem **Oracle Linux 10.x** ist, um den Zugriff auf Repositories zu aktivieren:

Schritte

- a. Das benötigte Repository abonnieren:

```
subscription-manager repos --enable ol-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable ol-10-for-x86_64-appstream-rpms
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls:

```
[root@localhost ~]# subscription-manager repos --enable ol-10-for-x86_64-baseos-rpms
Repository 'ol-10-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable ol-10-for-x86_64-appstream-rpms
```

```
Repository 'ol-10-for-x86_64-appstream-rpms' is enabled for this system.
```

- b. Mit dem folgenden Befehl lassen sich die aktivierten Repositories auflisten:

```
yum repolist
```

Die neu abonnierten Repositories sollten in der Liste erscheinen.

▼ Vorgehensweise für das Oracle Linux 9.x Betriebssystem

Führen Sie dieses Verfahren durch, wenn Ihr Betriebssystem **Oracle Linux 9.x** ist, um den Zugriff auf Repositories zu aktivieren:

Schritte

- a. Das benötigte Repository abonnieren:

```
subscription-manager repos --enable ol-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable ol-9-for-x86_64-appstream-rpms
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls:

```
[root@localhost ~]# subscription-manager repos --enable ol-9-for-x86_64-baseos-rpms
Repository 'ol-9-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable ol-9-for-x86_64-appstream-rpms
Repository 'ol-9-for-x86_64-appstream-rpms' is enabled for this system.
```

- b. Mit dem folgenden Befehl lassen sich die aktivierten Repositories auflisten:

```
yum repolist
```

Die neu abonnierten Repositories sollten in der Liste erscheinen.

▼ Vorgehensweise für das Betriebssystem RHEL 10.x

Dieses Verfahren gilt, wenn Ihr Betriebssystem **RHEL 10.x** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

a. Das benötigte Repository abonnieren:

```
subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls:

```
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
Repository 'rhel-10-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
Repository 'rhel-10-for-x86_64-appstream-rpms' is enabled for this system.
```

b. Mit dem folgenden Befehl lassen sich die aktivierten Repositories auflisten:

```
yum repolist
```

Die neu abonnierten Repositories sollten in der Liste erscheinen.

▼ **Vorgehensweise für das Betriebssystem RHEL 9.x**

Dieses Verfahren gilt, wenn Ihr Betriebssystem **RHEL 9.x** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

a. Das benötigte Repository abonnieren:

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls:

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
```

```
system.  
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-  
x86_64-appstream-rpms  
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this  
system.
```

b. Mit dem folgenden Befehl lassen sich die aktivierten Repositories auflisten:

```
yum repolist
```

Die neu abonnierten Repositories sollten in der Liste erscheinen.

▼ Vorgehensweise für das Betriebssystem RHEL 8.x

Dieses Verfahren gilt, wenn Ihr Betriebssystem **RHEL 8.x** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

a. Das benötigte Repository abonnieren:

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-  
rpms
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls:

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-  
x86_64-baseos-rpms  
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this  
system.  
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-  
x86_64-appstream-rpms  
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this  
system.
```

b. Mit dem folgenden Befehl lassen sich die aktivierten Repositories auflisten:

```
yum repolist
```

Die neu abonnierten Repositories sollten in der Liste erscheinen.

▼ Vorgehensweise für das Betriebssystem RHEL 7.x

Dieses Verfahren gilt, wenn Ihr Betriebssystem **RHEL 7.x** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

- a. Das benötigte Repository abonnieren:

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls:

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-  
server-optional-rpms  
Repository 'rhel-7-server-optional-rpms' is enabled for this  
system.
```

- b. Mit dem folgenden Befehl lassen sich die aktivierten Repositories auflisten:

```
yum repolist
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls. Das Repository „rhel-7-server-optional-rpms“ sollte in der Liste erscheinen.

```
[root@localhost ~]# yum repolist  
Loaded plugins: product-id, search-disabled-repos, subscription-  
manager  
rhel-7-server-optional-rpms | 3.2 kB  00:00:00  
rhel-7-server-rpms | 3.5 kB  00:00:00  
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group |  
26 kB  00:00:00  
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo |  
2.5 MB  00:00:00  
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db |  
8.3 MB  00:00:01  
repo id                                repo name  
status  
rhel-7-server-optional-rpms/7Server/x86_64  Red Hat Enterprise Linux  
7 Server - Optional (RPMs)  19,447  
rhel-7-server-rpms/7Server/x86_64          Red Hat Enterprise Linux  
7 Server (RPMs)  26,758  
repolist: 46,205  
[root@localhost ~]#
```

▼ Vorgehensweise für das Betriebssystem CentOS 7.x

Verwenden Sie dieses Verfahren, wenn Ihr Betriebssystem **CentOS 7.x** ist, um den Zugriff auf Repositories zu ermöglichen:



Die folgenden Beispiele zeigen ein Repository für CentOS 7.6 und funktionieren möglicherweise nicht mit anderen CentOS Versionen. Das Basis-Repository für Ihre Version von CentOS ist zu verwenden.

Schritte

- Das C7.6.1810 - Base Repository hinzufügen. Das C7.6.1810 - Base Vault Repository enthält das Paket „kernel-devel“, das für ONTAP Mediator benötigt wird.
- Fügen Sie die folgenden Zeilen zu `/etc/yum.repos.d/CentOS-Vault.repo` hinzu.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

- Mit dem folgenden Befehl lassen sich die aktivierten Repositories auflisten:

```
yum repolist
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls. Das Repository "CentOS-7.6.1810 - Base" sollte in der Liste erscheinen.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: distro.ibiblio.org
* extras: distro.ibiblio.org
* updates: ewr.edge.kernel.org
C7.6.1810-base | 3.6 kB 00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz | 166 kB 00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db | 6.0 MB 00:00:04
repo id repo name status
C7.6.1810-base/x86_64 CentOS-7.6.1810 - Base 10,019
base/7/x86_64 CentOS-7 - Base 10,097
extras/7/x86_64 CentOS-7 - Extras 307
updates/7/x86_64 CentOS-7 - Updates 1,010
repolist: 21,433
[root@localhost ~]#
```

▼ Vorgehensweise für Rocky Linux 10, 9 oder 8 Betriebssysteme

Dieses Verfahren ist anzuwenden, wenn Ihr Betriebssystem **Rocky Linux 10, Rocky Linux 9** oder

Rocky Linux 8 ist, um den Zugriff auf die Repositories zu ermöglichen:

Schritte

a. Erforderliche Repositories abonnieren:

```
dnf config-manager --set-enabled baseos
```

```
dnf config-manager --set-enabled appstream
```

b. Eine clean-Operation ausführen:

```
dnf clean all
```

c. Die Liste der Repositories überprüfen:

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                                repo name
appstream                              Rocky Linux 10 - AppStream
baseos                                 Rocky Linux 10 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                                repo name
appstream                              Rocky Linux 9 - AppStream
baseos                                 Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
```

repo id	repo name
appstream	Rocky Linux 8 - AppStream
baseos	Rocky Linux 8 - BaseOS

```
[root@localhost ~]#
```

Was kommt als Nächstes?

"[Das Installationspaket für ONTAP Mediator herunterladen](#)"

Das Installationspaket für ONTAP Mediator herunterladen

Laden Sie das ONTAP Mediator Installationspaket herunter und installieren Sie es.

Schritte

1. Das ONTAP Mediator Installationspaket steht auf der ONTAP Mediator Downloadseite zum Herunterladen bereit.

"[ONTAP Mediator Downloadseite](#)"

2. Platzieren Sie das Mediator-Installationspaket im aktuellen Arbeitsverzeichnis:

```
ls ontap-mediator-1.12.1.tgz
```

```
ontap-mediator-1.12.1.tgz
```



Für ONTAP Mediator Versionen 1.4 und früher heißt das Installationsprogramm `ontap-mediator`.

Falls Ihr System keinen Internetzugang hat, muss das Installationsprogramm auf die erforderlichen Pakete zugreifen können.

3. Verschieben Sie das Mediator Installationspaket gegebenenfalls in das Installationsverzeichnis.
4. Das Installationspaket entpacken:

```
tar xvfz ontap-mediator-1.12.1.tgz
```

```
ontap-mediator-1.12.1/
ontap-mediator-1.12.1/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.12.1/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.12.1/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.12.1/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.12.1/ONTAP-Mediator-production.pub
ontap-mediator-1.12.1/ontap-mediator-1.12.1
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig.tsr
```

```
ontap-mediator-1.12.1/ontap-mediator-1.12.1.tsr
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig
```

Was kommt als Nächstes?

["Die Code-Signatur des ONTAP Mediators überprüfen"](#)

Die Code-Signatur des ONTAP Mediators überprüfen

NetApp empfiehlt, die ONTAP Mediator-Code-Signatur vor der Installation zu überprüfen. Dieser Schritt ist optional.

Bevor Sie beginnen

Vor der Überprüfung der ONTAP Mediator-Code-Signatur sollte sichergestellt sein, dass Ihr System diese Anforderungen erfüllt.



- Ab dem 15. Juni 2025 ist die Installation oder das Upgrade auf ONTAP Mediator 1.9 und 1.8 nicht mehr möglich, da die Zertifikate zur Überprüfung der Codesignatur abgelaufen sind. Installieren oder aktualisieren Sie stattdessen auf ONTAP Mediator 1.10 oder später.
- Wenn das System die folgenden Anforderungen nicht erfüllt, ist der Verifizierungsprozess nicht erforderlich und es kann direkt zu ["Das ONTAP Mediator Installationspaket installieren"](#) gewechselt werden.

- OpenSSL Versionen 1.0.2 bis 3.0 für die grundlegende Überprüfung
- OpenSSL Version 1.1.0 oder höher für Time Stamping Authority (TSA) Operationen
- Öffentlicher Internetzugang zur OCSP-Verifizierung

Das Downloadpaket enthält die folgenden Dateien:

Datei	Beschreibung
ONTAP-Mediator-production.pub	Der öffentliche Schlüssel zur Überprüfung der Signatur
csc-prod-chain-ONTAP-Mediator.pem	Die öffentliche Zertifizierungs-CA-Vertrauenskette
csc-prod-ONTAP-Mediator.pem	Das Zertifikat, das zur Generierung des Schlüssels verwendet wurde
ontap-mediator-1.12.1	Die ausführbare Installationsdatei für Version 1.12
ontap-mediator-1.12.1.sig	Die mit SHA-256 gehashte und anschließend mit dem csc-prod Schlüssel RSA-signierte Signatur für das Installationsprogramm
ontap-mediator-1.12.1.sig.tsr	Der Widerrufs Antrag zur Verwendung durch OCSP für die Signatur des Installers
ontap-mediator-1.12.1.tsr	Die Datei mit der Zeitstempel-Signaturanfrage
tsa-prod-ONTAP-Mediator.pem	Das öffentliche Zertifikat für die TSR
tsa-prod-chain-ONTAP-Mediator.pem	Die öffentliche Zertifikats-CA-Kette für die TSR

Schritte

1. Die Widerrufsprüfung auf `csc-prod-ONTAP-Mediator.pem` mithilfe des Online Certificate Status Protocol (OCSP) durchführen.
 - a. Die OCSP-URL für das Zertifikat kann ermittelt werden. Entwicklerzertifikate enthalten möglicherweise keine URI:

```
openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
```

- b. Eine OCSP-Anfrage für das Zertifikat generieren.

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout req.der
```

- c. Mit dem OCSP Manager verbinden, um die OCSP-Anfrage zu senden:

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-chain-ONTAP-Mediator.pem
```

2. Die Vertrauenskette des CSC und die Ablaufdaten werden mit dem lokalen Host abgeglichen:

```
openssl verify
```



Die openssl-Version aus dem PATH muss eine gültige `cert.pem` (nicht selbstsignierte) Signatur haben.

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath ${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath ${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem
```

Der Befehl schlägt fehl, wenn das Zertifikat für die Code-Signaturprüfung oder das Zeitstempelzertifikat abgelaufen oder ungültig ist. Der Download einer neueren Version von ONTAP Mediator ist erforderlich.

3. Überprüfen Sie die `ontap-mediator-1.12.1.sig.tsr` und `ontap-mediator-1.12.1.tsr` Dateien mithilfe der zugehörigen Zertifikate:

OpenSSL 3.x

```
openssl ts -verify -data ontap-mediator-1.12.1.sig -in ontap-
```

```
mediator-1.12.1.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem  
-untrusted tsa-prod-ONTAP-Mediator.pem
```

OpenSSL 1.x

```
openssl ts -verify -data ontap-mediator-1.12.1 -in ontap-mediator-  
1.12.1.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -partial_chain
```



.tsr Dateien enthalten den Zeitstempel der Antwort, der mit dem Installationsprogramm und der Codesignatur verknüpft ist. Die Verarbeitung bestätigt, dass der Zeitstempel eine gültige Signatur von TSA aufweist und dass Ihre Eingabedatei nicht verändert wurde. Die Überprüfung wird lokal auf Ihrem Rechner durchgeführt. Ein Zugriff auf die TSA-Server ist nicht erforderlich.

4. Signaturen mit dem Schlüssel verifizieren:

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature  
ontap-mediator-1.12.1.sig ontap-mediator-1.12.1
```

Was kommt als Nächstes?

["Das ONTAP Mediator Installationspaket installieren"](#)

Das ONTAP Mediator Installationspaket installieren

Um ONTAP Mediator zu installieren, müssen Sie das Installationspaket erhalten und das Installationsprogramm auf dem Host ausführen.



Informationen zum Upgrade einer bestehenden ONTAP Mediator Installation finden Sie stattdessen unter ["Upgrade von ONTAP Mediator"](#).

Über diese Aufgabe

- Ab ONTAP 9.19.1 und ONTAP Mediator 1.12 besteht die Möglichkeit, ONTAP Mediator mit iSCSI und HTTPS-Unterstützung oder nur mit HTTPS-Unterstützung zu installieren. Wenn ONTAP Mediator nur mit HTTPS-Unterstützung installiert wird, wird das SCST-Paket nicht installiert.
- Wenn Sie von ONTAP Mediator 1.11 oder einer früheren Version mit installiertem SCST aktualisieren und während des Upgrades die Option „Nur HTTPS“ auswählen, wird das SCST-Paket deinstalliert und die neue ONTAP Mediator Version enthält das SCST-Paket nicht.
- Wenn die Überwachung mehrerer MetroCluster IP-Konfigurationen mit ONTAP Mediator vorgesehen ist, hängt die Unterstützung vom Mediator-Typ, der ONTAP Version und dem Betriebssystem ab. Weitere Informationen finden Sie unter ["ONTAP Mediator zur Überwachung mehrerer MetroCluster IP Konfigurationen verwenden"](#).

- Die Installation des ONTAP Mediators mit ausschließlicher HTTPS-Unterstützung wird für die folgenden Anwendungsfälle unterstützt:
 - Sie planen, ONTAP Mediator ausschließlich zur Überwachung Ihrer SnapMirror active sync Cluster zu verwenden.
 - Es ist vorgesehen, ONTAP Mediator mit HTTPS zu konfigurieren, um eine oder mehrere MetroCluster IP-Konfigurationen zu überwachen.
- ONTAP Mediator muss mit Unterstützung für iSCSI und HTTPS im folgenden Szenario installiert werden:
 - Sie planen, ONTAP Mediator mit iSCSI zu konfigurieren, um eine oder mehrere MetroCluster IP-Konfigurationen zu überwachen.
- Während der Installation oder des Upgrades auf ONTAP Mediator 1.12 oder höher werden Sie vom Installationsprogramm aufgefordert, auf Folgendes zu antworten:

ONTAP Mediator can be installed with iSCSI and HTTPS support, or HTTPS support only.

Do you wish to install ONTAP Mediator with iSCSI and HTTPS support?

Y(es)/n(o) :

- Antworten Sie **Yes**, wenn Sie planen, ONTAP Mediator mit iSCSI zu verwenden, um eine oder mehrere MetroCluster IP-Konfigurationen zu überwachen.
- Antworten Sie **No**, wenn geplant ist, ONTAP Mediator ausschließlich für SnapMirror active sync zu verwenden oder wenn ONTAP Mediator mit HTTPS konfiguriert werden soll, um eine oder mehrere MetroCluster IP-Konfigurationen zu überwachen.

Alternativ können Sie die `--https-only` Option im `./ontap-mediator-1.12.1/ontap-mediator-1.12.1` Befehl verwenden, um nur HTTPS anzugeben.

- Für Automatisierungsanwendungen kann der `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 -y` Befehl verwendet werden, um die Installationsabfragen zu überspringen.

Schritte

1. Führen Sie das Installationsprogramm aus und beantworten Sie die Eingabeaufforderungen wie erforderlich:

```
./ontap-mediator-1.12.1/ontap-mediator-1.12.1
```

```
[root@mediator_host ~]# ./ontap-mediator-1.12.1/ontap-mediator-1.12.1
```



Zum Überspringen der Signaturprüfung während der Installation dient der `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 --skip-code-signature -check` Befehl

Das Installationsprogramm erstellt die erforderlichen Konten und installiert die erforderlichen Pakete. Falls ONTAP Mediator bereits installiert ist, fordert das Installationsprogramm stattdessen zu einem Upgrade auf; upgrade-spezifische Schritte und Beispiele finden Sie unter "[Upgrade von ONTAP Mediator](#)".

▼ Beispiel ONTAP Mediator-Installation mit HTTPS- und iSCSI-Unterstützung (Konsolenausgabe)

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.12.1.tgz
ontap-mediator-1.12.1/
ontap-mediator-1.12.1/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.12.1/ONTAP-Mediator-production.pub
ontap-mediator-1.12.1/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.12.1/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.12.1/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.12.1/ontap-mediator-1.12.1
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig
ontap-mediator-1.12.1/ontap-mediator-1.12.1.tsr
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig.tsr
[root@mediator_host ~]# ontap-mediator-1.12.1/ontap-mediator-1.12.1
```

ONTAP Mediator: Self Extracting Installer

```
+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
+ Unpacking the ONTAP Mediator installer
+ ONTAP_MEDIATOR_INSTALL_HTTPS_ONLY is set to '0', args are: ''
+ Starting ONTAP Mediator install/update process: previous
installation_mode is ''
```

ONTAP Mediator can be installed with iSCSI and HTTPS support, or support for HTTPS only.

Do you wish to install ONTAP Mediator with iSCSI and HTTPS support?

Y(es)/n(o): yes

ONTAP Mediator will be installed with mode: ISCSI_HTTPS

+ Selected install package mode: ISCSI_HTTPS

+ Checking that required ports 3260 and 31784 are free

ONTAP Mediator requires two user accounts. One for the service (netapp), and one for use by ONTAP to the mediator API (mediatoradmin).

Would you like to use the default account names: netapp + mediatoradmin? (Y(es)/n(o)): yes

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

```
+ Checking if SELinux is in enforcing mode
SELinux is set to Enforcing. ONTAP Mediator server requires modifying
the SELinux context of the file
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.
This is necessary to start the ONTAP Mediator service while SELinux is
set to Enforcing.
Allow SELinux context change? Y(es)/n(o): yes
The installer will change the SELinux context type of
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.
```

```
+ Checking for default Linux firewall
```

```
+ Installing required packages.
```

```
Last metadata expiration check: 2:16:00 ago on Tue 24 Mar 2026
12:58:28 PM EDT.
Package openssl-1:3.5.1-7.0.1.el9_7.x86_64 is already installed.
Package openssl-devel-1:3.5.1-7.0.1.el9_7.x86_64 is already installed.
Package kernel-uek-devel-6.12.0-109.67.6.el9uek.x86_64 is already
installed.
Package gcc-11.5.0-11.0.2.el9.x86_64 is already installed.
Package make-1:4.3-8.el9.x86_64 is already installed.
Package which-2.21-30.el9_6.x86_64 is already installed.
Package libselinux-utils-3.6-3.el9.x86_64 is already installed.
Package patch-2.7.6-16.el9.x86_64 is already installed.
Package perl-Data-Dumper-2.174-462.el9.x86_64 is already installed.
Package perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch is already
installed.
Package bzip2-1.0.8-10.el9_5.x86_64 is already installed.
Package efibootmgr-16-12.0.1.el9.x86_64 is already installed.
Package mokutil-2:0.7.2-1.el9.x86_64 is already installed.
Package python3-pip-21.3.1-1.el9.noarch is already installed.
Package elfutils-libelf-devel-0.193-1.el9.x86_64 is already installed.
Package policycoreutils-python-utils-3.6-3.el9.noarch is already
installed.
Package python3.12-3.12.12-4.0.1.el9_7.1.x86_64 is already installed.
Package python3.12-devel-3.12.12-4.0.1.el9_7.1.x86_64 is already
installed.
Package gcc-toolset-14-14.0-2.el9.x86_64 is already installed.
Dependencies resolved.
```

```

=====
=====
Package                                Architecture  Version
Repository                            Size
=====
=====
Installing:
  efibootmgr                          x86_64       18-
8.el10                                baseos       47 k
  mokutil                             x86_64
2:0.7.2-1.el10                        baseos       48 k
  patch                               x86_64       2.7.6-
26.el10                               appstream    131 k
  perl-ExtUtils-MakeMaker              noarch       2:7.70-
513.el10                              appstream    295 k
  python3-devel                       x86_64
3.12.12-4.el10_1                     appstream    329 k
  python3-pip                         noarch       23.3.2-
7.el10                               appstream    3.2 M
Upgrading:
  libselinux                         x86_64       3.9-
1.el10                                baseos       97 k
  libselinux-utils                   x86_64       3.9-
1.el10                                baseos       122 k
  libsemanage                       x86_64       3.9-
1.el10                                baseos       122 k
  libsepol                          x86_64       3.9-
1.el10                                baseos       348 k
  policycoreutils                   x86_64       3.9-
1.el10                                baseos       224 k
  policycoreutils-python-utils       noarch       3.9-
1.el10                               appstream    51 k
  python-unversioned-command          noarch
3.12.12-4.el10_1                     appstream    11 k
  python3                           x86_64
3.12.12-4.el10_1                     baseos       28 k
  python3-libs                       x86_64
3.12.12-4.el10_1                     baseos       9.4 M
  python3-libselinux                 x86_64       3.9-
1.el10                               appstream    200 k
  python3-libsemanage                 x86_64       3.9-
1.el10                               appstream    81 k
  python3-policycoreutils            noarch       3.9-
1.el10                               appstream    2.2 M
Installing dependencies:
  annobin-docs                       noarch       12.99-

```

1.el10	appstream	88 k
annobin-plugin-gcc	x86_64	12.99-
1.el10	appstream	998 k
dwz	x86_64	0.16-
1.el10	appstream	139 k
efi-filesystem	noarch	6-
7.el10.rocky.0.1	baseos	7.8 k
efi-srpm-macros	noarch	6-
7.el10.rocky.0.1	appstream	22 k
efivar-libs	x86_64	39-
3.el10	baseos	127 k
fonts-srpm-macros	noarch	
1:2.0.5-18.el10	appstream	26 k
forge-srpm-macros	noarch	0.4.0-
6.el10	appstream	20 k
gcc-plugin-annobin	x86_64	14.3.1-
2.1.el10	appstream	67 k
go-srpm-macros	noarch	3.6.0-
7.el10_1	appstream	27 k
kernel-srpm-macros	noarch	1.0-
26.el10	appstream	9.4 k
lua-srpm-macros	noarch	1-
15.el10	appstream	8.8 k
ocaml-srpm-macros	noarch	10-
4.el10	appstream	9.2 k
openblas-srpm-macros	noarch	2-
19.el10	appstream	7.7 k
package-notes-srpm-macros	noarch	0.5-
13.el10	appstream	9.2 k
perl-AutoSplit	noarch	5.74-
512.2.el10_0	appstream	21 k
perl-Benchmark	noarch	1.25-
512.2.el10_0	appstream	27 k
perl-CPAN-Meta-Requirements	noarch	2.143-
11.el10	appstream	35 k
perl-CPAN-Meta-YAML	noarch	0.018-
512.el10	appstream	26 k
perl-Devel-PPPort	x86_64	3.72-
512.el10	appstream	219 k
perl-ExtUtils-Command	noarch	2:7.70-
513.el10	appstream	14 k
perl-ExtUtils-Constant	noarch	0.25-
512.2.el10_0	appstream	43 k
perl-ExtUtils-Install	noarch	2.22-
511.el10	appstream	43 k
perl-ExtUtils-Manifest	noarch	1:1.75-

511.el10	appstream	34 k
perl-ExtUtils-ParseXS	noarch	1:3.51-
512.el10	appstream	189 k
perl-File-Compare	noarch	
1.100.800-512.2.el10_0	appstream	13 k
perl-File-Copy	noarch	2.41-
512.2.el10_0	appstream	20 k
perl-I18N-Langinfo	x86_64	0.24-
512.2.el10_0	appstream	25 k
perl-JSON-PP	noarch	1:4.16-
512.el10	appstream	66 k
perl-Test-Harness	noarch	1:3.48-
512.el10	appstream	282 k
perl-lib	x86_64	0.65-
512.2.el10_0	appstream	15 k
perl-srpm-macros	noarch	1-
57.el10	appstream	8.5 k
perl-version	x86_64	
8:0.99.32-4.el10	appstream	63 k
pyproject-srpm-macros	noarch	1.16.2-
1.el10	appstream	14 k
python-srpm-macros	noarch	3.12-
10.el10	appstream	23 k
python3-pyparsing	noarch	3.1.1-
7.el10	baseos	271 k
qt6-srpm-macros	noarch	6.9.1-
1.el10	appstream	9.6 k
redhat-rpm-config	noarch	293-
1.el10.rocky.0.2	appstream	78 k
rust-toolset-srpm-macros	noarch	1.88.0-
1.el10	appstream	12 k
systemtap-sdt-devel	x86_64	5.3-
3b.el10	appstream	69 k
systemtap-sdt-dtrace	x86_64	5.3-
3b.el10	appstream	70 k
Installing weak dependencies:		
perl-CPAN-Meta	noarch	
2.150010-511.el10	appstream	197 k
perl-Encode-Locale	noarch	1.05-
31.el10	appstream	18 k
perl-Time-HiRes	x86_64	
4:1.9777-511.el10	appstream	58 k
perl-devel	x86_64	
4:5.40.2-512.2.el10_0	appstream	770 k
perl-doc	noarch	5.40.2-
512.2.el10_0	appstream	4.9 M

Transaction Summary

Install 52 Packages

Upgrade 12 Packages

Total download size: 26 M

Is this ok [y/N]: y

Downloading Packages:

(1/64): efi-filesystem-6-7.el10.rocky.0.1.noarch.rpm

206 kB/s | 7.8 kB 00:00

(2/64): efibootmgr-18-8.el10.x86_64.rpm

1.2 MB/s | 47 kB 00:00

(3/64): efivar-libs-39-3.el10.x86_64.rpm

2.8 MB/s | 127 kB 00:00

(4/64): mokutil-0.7.2-1.el10.x86_64.rpm

6.4 MB/s | 48 kB 00:00

(5/64): annobin-docs-12.99-1.el10.noarch.rpm

11 MB/s | 88 kB 00:00

(6/64): python3-pyparsing-3.1.1-7.el10.noarch.rpm

13 MB/s | 271 kB 00:00

(7/64): dwz-0.16-1.el10.x86_64.rpm

12 MB/s | 139 kB 00:00

(8/64): efi-srpm-macros-6-7.el10.rocky.0.1.noarch.rpm

2.7 MB/s | 22 kB 00:00

(9/64): fonts-srpm-macros-2.0.5-18.el10.noarch.rpm

5.1 MB/s | 26 kB 00:00

(10/64): forge-srpm-macros-0.4.0-6.el10.noarch.rpm

4.3 MB/s | 20 kB 00:00

(11/64): gcc-plugin-annobin-14.3.1-2.1.el10.x86_64.rpm

10 MB/s | 67 kB 00:00

(12/64): go-srpm-macros-3.6.0-7.el10_1.noarch.rpm

4.7 MB/s | 27 kB 00:00

(13/64): kernel-srpm-macros-1.0-26.el10.noarch.rpm

2.0 MB/s | 9.4 kB 00:00

(14/64): lua-srpm-macros-1-15.el10.noarch.rpm

2.0 MB/s | 8.8 kB 00:00

(15/64): ocaml-srpm-macros-10-4.el10.noarch.rpm

2.0 MB/s | 9.2 kB 00:00

(16/64): annobin-plugin-gcc-12.99-1.el10.x86_64.rpm

16 MB/s | 998 kB 00:00

(17/64): openblas-srpm-macros-2-19.el10.noarch.rpm

432 kB/s | 7.7 kB 00:00

(18/64): package-notes-srpm-macros-0.5-13.el10.noarch.rpm

519 kB/s | 9.2 kB 00:00

```
(19/64): perl-AutoSplit-5.74-512.2.el10_0.noarch.rpm
4.5 MB/s | 21 kB      00:00
(20/64): patch-2.7.6-26.el10.x86_64.rpm
14 MB/s | 131 kB      00:00
(21/64): perl-Benchmark-1.25-512.2.el10_0.noarch.rpm
3.5 MB/s | 27 kB      00:00
(22/64): perl-CPAN-Meta-Requirements-2.143-11.el10.noarch.rpm
10 MB/s | 35 kB       00:00
(23/64): perl-CPAN-Meta-YAML-0.018-512.el10.noarch.rpm
5.3 MB/s | 26 kB      00:00
(24/64): perl-CPAN-Meta-2.150010-511.el10.noarch.rpm
12 MB/s | 197 kB      00:00
(25/64): perl-Encode-Locale-1.05-31.el10.noarch.rpm
2.6 MB/s | 18 kB      00:00
(26/64): perl-ExtUtils-Command-7.70-513.el10.noarch.rpm
3.0 MB/s | 14 kB      00:00
(27/64): perl-Devel-PPPort-3.72-512.el10.x86_64.rpm
13 MB/s | 219 kB      00:00
(28/64): perl-ExtUtils-Constant-0.25-512.2.el10_0.noarch.rpm
4.9 MB/s | 43 kB      00:00
(29/64): perl-ExtUtils-Install-2.22-511.el10.noarch.rpm
4.7 MB/s | 43 kB      00:00
(30/64): perl-ExtUtils-Manifest-1.75-511.el10.noarch.rpm
6.2 MB/s | 34 kB      00:00
(31/64): perl-File-Compare-1.100.800-512.2.el10_0.noarch.rpm
4.2 MB/s | 13 kB      00:00
(32/64): perl-ExtUtils-MakeMaker-7.70-513.el10.noarch.rpm
17 MB/s | 295 kB      00:00
(33/64): perl-ExtUtils-ParseXS-3.51-512.el10.noarch.rpm
11 MB/s | 189 kB      00:00
(34/64): perl-File-Copy-2.41-512.2.el10_0.noarch.rpm
1.7 MB/s | 20 kB      00:00
(35/64): perl-I18N-Langinfo-0.24-512.2.el10_0.x86_64.rpm
5.0 MB/s | 25 kB      00:00
(36/64): perl-JSON-PP-4.16-512.el10.noarch.rpm
9.3 MB/s | 66 kB      00:00
(37/64): perl-Time-HiRes-1.9777-511.el10.x86_64.rpm
11 MB/s | 58 kB       00:00
(38/64): perl-Test-Harness-3.48-512.el10.noarch.rpm
13 MB/s | 282 kB      00:00
(39/64): perl-lib-0.65-512.2.el10_0.x86_64.rpm
4.4 MB/s | 15 kB      00:00
(40/64): perl-srpm-macros-1-57.el10.noarch.rpm
2.7 MB/s | 8.5 kB     00:00
(41/64): perl-devel-5.40.2-512.2.el10_0.x86_64.rpm
19 MB/s | 770 kB      00:00
```

```
(42/64): perl-version-0.99.32-4.el10.x86_64.rpm
4.3 MB/s | 63 kB      00:00
(43/64): pyproject-srpm-macros-1.16.2-1.el10.noarch.rpm
4.5 MB/s | 14 kB      00:00
(44/64): python-srpm-macros-3.12-10.el10.noarch.rpm
5.1 MB/s | 23 kB      00:00
(45/64): python3-devel-3.12.12-4.el10_1.x86_64.rpm
20 MB/s | 329 kB      00:00
(46/64): qt6-srpm-macros-6.9.1-1.el10.noarch.rpm
3.0 MB/s | 9.6 kB      00:00
(47/64): redhat-rpm-config-293-1.el10.rocky.0.2.noarch.rpm
16 MB/s | 78 kB      00:00
(48/64): rust-toolset-srpm-macros-1.88.0-1.el10.noarch.rpm
3.6 MB/s | 12 kB      00:00
(49/64): systemtap-sdt-devel-5.3-3b.el10.x86_64.rpm
11 MB/s | 69 kB      00:00
(50/64): systemtap-sdt-dtrace-5.3-3b.el10.x86_64.rpm
16 MB/s | 70 kB      00:00
(51/64): libselinux-3.9-1.el10.x86_64.rpm
10 MB/s | 97 kB      00:00
(52/64): libselinux-utils-3.9-1.el10.x86_64.rpm
14 MB/s | 122 kB      00:00
(53/64): libsemanage-3.9-1.el10.x86_64.rpm
13 MB/s | 122 kB      00:00
(54/64): libsepol-3.9-1.el10.x86_64.rpm
18 MB/s | 348 kB      00:00
(55/64): python3-pip-23.3.2-7.el10.noarch.rpm
21 MB/s | 3.2 MB      00:00
(56/64): policycoreutils-3.9-1.el10.x86_64.rpm
4.3 MB/s | 224 kB      00:00
(57/64): python3-3.12.12-4.el10_1.x86_64.rpm
5.7 MB/s | 28 kB      00:00
(58/64): policycoreutils-python-utils-3.9-1.el10.noarch.rpm
6.7 MB/s | 51 kB      00:00
(59/64): perl-doc-5.40.2-512.2.el10_0.noarch.rpm
17 MB/s | 4.9 MB      00:00
(60/64): python-unversioned-command-3.12.12-4.el10_1.noarch.rpm
175 kB/s | 11 kB      00:00
(61/64): python3-libselinux-3.9-1.el10.x86_64.rpm
16 MB/s | 200 kB      00:00
(62/64): python3-libsemanage-3.9-1.el10.x86_64.rpm
7.0 MB/s | 81 kB      00:00
(63/64): python3-policycoreutils-3.9-1.el10.noarch.rpm
28 MB/s | 2.2 MB      00:00
(64/64): python3-libs-3.12.12-4.el10_1.x86_64.rpm
31 MB/s | 9.4 MB      00:00
```

```

-----
Total
19 MB/s | 26 MB      00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :
1/1
  Upgrading      : python3-libs-3.12.12-4.el10_1.x86_64
1/76
  Upgrading      : python-unversioned-command-3.12.12-
4.el10_1.noarch
2/76
  Upgrading      : python3-3.12.12-4.el10_1.x86_64
3/76
  Upgrading      : libsepol-3.9-1.el10.x86_64
4/76
  Upgrading      : libselinux-3.9-1.el10.x86_64
5/76
  Running scriptlet: libselinux-3.9-1.el10.x86_64
5/76
  Installing      : perl-version-8:0.99.32-4.el10.x86_64
6/76
  Installing      : perl-File-Copy-2.41-512.2.el10_0.noarch
7/76
  Installing      : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
8/76
  Upgrading      : libsemanage-3.9-1.el10.x86_64
9/76
  Upgrading      : python3-libselinux-3.9-1.el10.x86_64
10/76
  Installing      : perl-Time-HiRes-4:1.9777-511.el10.x86_64
11/76
  Installing      : perl-JSON-PP-1:4.16-512.el10.noarch
12/76
  Installing      : perl-File-Compare-1.100.800-512.2.el10_0.noarch
13/76
  Installing      : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
14/76
  Installing      : efivar-libs-39-3.el10.x86_64
15/76
  Upgrading      : python3-libsemanage-3.9-1.el10.x86_64
16/76

```

```

Installing      : perl-ExtUtils-Command-2:7.70-513.el10.noarch
17/76
Installing      : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
18/76
Upgrading       : libselinux-utils-3.9-1.el10.x86_64
19/76
Upgrading       : policycoreutils-3.9-1.el10.x86_64
20/76
Running scriptlet: policycoreutils-3.9-1.el10.x86_64
20/76
Upgrading       : python3-policycoreutils-3.9-1.el10.noarch
21/76
Installing      : python3-pyparsing-3.1.1-7.el10.noarch
22/76
Installing      : systemtap-sdt-dtrace-5.3-3b.el10.x86_64
23/76
Installing      : systemtap-sdt-devel-5.3-3b.el10.x86_64
24/76
Installing      : python3-pip-23.3.2-7.el10.noarch
25/76
Installing      : rust-toolset-srpm-macros-1.88.0-1.el10.noarch
26/76
Installing      : qt6-srpm-macros-6.9.1-1.el10.noarch
27/76
Installing      : pyproject-srpm-macros-1.16.2-1.el10.noarch
28/76
Installing      : perl-srpm-macros-1-57.el10.noarch
29/76
Installing      : perl-lib-0.65-512.2.el10_0.x86_64
30/76
Installing      : perl-doc-5.40.2-512.2.el10_0.noarch
31/76
Installing      : perl-I18N-Langinfo-0.24-512.2.el10_0.x86_64
32/76
Installing      : perl-Encode-Locale-1.05-31.el10.noarch
33/76
Installing      : perl-ExtUtils-Constant-0.25-512.2.el10_0.noarch
34/76
Installing      : perl-Devel-PPPort-3.72-512.el10.x86_64
35/76
Installing      : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
36/76
Installing      : perl-CPAN-Meta-2.150010-511.el10.noarch
37/76
Installing      : perl-Benchmark-1.25-512.2.el10_0.noarch
38/76

```

```

Installing      : perl-Test-Harness-1:3.48-512.el10.noarch
39/76
Installing      : perl-AutoSplit-5.74-512.2.el10_0.noarch
40/76
Installing      : package-notes-srpm-macros-0.5-13.el10.noarch
41/76
Installing      : openblas-srpm-macros-2-19.el10.noarch
42/76
Installing      : ocaml-srpm-macros-10-4.el10.noarch
43/76
Installing      : lua-srpm-macros-1-15.el10.noarch
44/76
Installing      : kernel-srpm-macros-1.0-26.el10.noarch
45/76
Installing      : gcc-plugin-annobin-14.3.1-2.1.el10.x86_64
46/76
Installing      : efi-srpm-macros-6-7.el10.rocky.0.1.noarch
47/76
Installing      : dwz-0.16-1.el10.x86_64
48/76
Installing      : annobin-docs-12.99-1.el10.noarch
49/76
Installing      : annobin-plugin-gcc-12.99-1.el10.x86_64
50/76
Installing      : fonts-srpm-macros-1:2.0.5-18.el10.noarch
51/76
Installing      : forge-srpm-macros-0.4.0-6.el10.noarch
52/76
Installing      : go-srpm-macros-3.6.0-7.el10_1.noarch
53/76
Installing      : python-srpm-macros-3.12-10.el10.noarch
54/76
Installing      : redhat-rpm-config-293-1.el10.rocky.0.2.noarch
55/76
Running scriptlet: redhat-rpm-config-293-1.el10.rocky.0.2.noarch
55/76
Installing      : perl-ExtUtils-Install-2.22-511.el10.noarch
56/76
Installing      : perl-devel-4:5.40.2-512.2.el10_0.x86_64
57/76
Installing      : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
58/76
Installing      : efi-filesystem-6-7.el10.rocky.0.1.noarch
59/76
Installing      : efibootmgr-18-8.el10.x86_64
60/76

```

```

Installing      : python3-devel-3.12.12-4.el10_1.x86_64
61/76
Upgrading       : policycoreutils-python-utils-3.9-1.el10.noarch
62/76
Installing      : mokutil-2:0.7.2-1.el10.x86_64
63/76
Installing      : patch-2.7.6-26.el10.x86_64
64/76
Cleanup         : policycoreutils-python-utils-3.8-1.el10.noarch
65/76
Cleanup         : python3-policycoreutils-3.8-1.el10.noarch
66/76
Running scriptlet: policycoreutils-3.8-1.el10.x86_64
67/76
Cleanup         : policycoreutils-3.8-1.el10.x86_64
67/76
Cleanup         : python3-libsemanage-3.8.1-1.el10_0.x86_64
68/76
Cleanup         : libsemanage-3.8.1-1.el10_0.x86_64
69/76
Cleanup         : python3-libselinux-3.8-2.el10_0.x86_64
70/76
Cleanup         : libselinux-utils-3.8-2.el10_0.x86_64
71/76
Cleanup         : python3-3.12.9-2.el10_0.2.x86_64
72/76
Cleanup         : libselinux-3.8-2.el10_0.x86_64
73/76
Cleanup         : python-unversioned-command-3.12.9-
2.el10_0.2.noarch
74/76
Cleanup         : libsepol-3.8-1.el10.x86_64
75/76
Cleanup         : python3-libs-3.12.9-2.el10_0.2.x86_64
76/76
Running scriptlet: python3-libs-3.12.9-2.el10_0.2.x86_64
76/76

Upgraded:
libselinux-3.9-1.el10.x86_64
libselinux-utils-3.9-1.el10.x86_64
libsemanage-3.9-1.el10.x86_64
libsepol-3.9-1.el10.x86_64
policycoreutils-3.9-1.el10.x86_64
policycoreutils-python-utils-3.9-1.el10.noarch
python-unversioned-command-3.12.12-4.el10_1.noarch

```

```

python3-3.12.12-4.el10_1.x86_64
python3-libs-3.12.12-4.el10_1.x86_64
python3-libseltlinux-3.9-1.el10.x86_64
python3-libsemanage-3.9-1.el10.x86_64
python3-policycoreutils-3.9-1.el10.noarch
Installed:
annobin-docs-12.99-1.el10.noarch
annobin-plugin-gcc-12.99-1.el10.x86_64
dwz-0.16-1.el10.x86_64
efi-
filesystem-6-7.el10.rocky.0.1.noarch
efi-srpm-macros-6-7.el10.rocky.0.1.noarch
efibootmgr-18-8.el10.x86_64
efivar-libs-39-3.el10.x86_64
fonts-srpm-macros-1:2.0.5-18.el10.noarch
forge-srpm-macros-0.4.0-6.el10.noarch
gcc-
plugin-annobin-14.3.1-2.1.el10.x86_64
go-srpm-macros-3.6.0-7.el10_1.noarch
kernel-srpm-macros-1.0-26.el10.noarch
lua-srpm-macros-1-15.el10.noarch
mokutil-2:0.7.2-1.el10.x86_64
ocaml-srpm-macros-10-4.el10.noarch
openblas-srpm-macros-2-19.el10.noarch
package-notes-srpm-macros-0.5-13.el10.noarch
patch-2.7.6-26.el10.x86_64
perl-AutoSplit-5.74-512.2.el10_0.noarch
perl-Benchmark-1.25-512.2.el10_0.noarch
perl-CPAN-Meta-2.150010-511.el10.noarch
perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
perl-CPAN-Meta-YAML-0.018-512.el10.noarch
perl-Devel-PPPort-3.72-512.el10.x86_64
perl-Encode-Locale-1.05-31.el10.noarch
perl-ExtUtils-Command-2:7.70-513.el10.noarch
perl-ExtUtils-Constant-0.25-512.2.el10_0.noarch
perl-ExtUtils-Install-2.22-511.el10.noarch
perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
perl-File-Compare-1.100.800-512.2.el10_0.noarch
perl-File-Copy-2.41-512.2.el10_0.noarch
perl-I18N-Langinfo-0.24-512.2.el10_0.x86_64
perl-JSON-PP-1:4.16-512.el10.noarch
perl-Test-Harness-1:3.48-512.el10.noarch
perl-Time-HiRes-4:1.9777-511.el10.x86_64
perl-devel-4:5.40.2-512.2.el10_0.x86_64
perl-doc-5.40.2-512.2.el10_0.noarch
perl-lib-0.65-512.2.el10_0.x86_64

```

```

perl-srpm-macros-1-57.el10.noarch
perl-version-8:0.99.32-4.el10.x86_64
pyproject-srpm-macros-1.16.2-1.el10.noarch
python-srpm-macros-3.12-10.el10.noarch
python3-devel-3.12.12-4.el10_1.x86_64
python3-pip-23.3.2-7.el10.noarch
python3-pyparsing-3.1.1-7.el10.noarch
srpm-macros-6.9.1-1.el10.noarch
redhat-rpm-config-293-1.el10.rocky.0.2.noarch
rust-toolset-srpm-macros-1.88.0-1.el10.noarch
systemtap-sdt-devel-5.3-3b.el10.x86_64
systemtap-sdt-dtrace-5.3-3b.el10.x86_64

```

qt6-

Complete!

OS package installations finished

OS package installations finished

+ Installing ONTAP Mediator. (Log:

/root/ontap_mediator.pJBcIv/ontap-mediator-1.12.1/ontap-mediator-1.12.1/install_20260324151410.log)

This step will take several minutes. Use the log file to view progress.

Sudoer config verified

ONTAP Mediator rsyslog and logging rotation enabled

+ Install successful. (Moving log to

/opt/netapp/lib/ontap_mediator/log/install_20260324151410.log)

+ WARNING: This system supports UEFI

Secure Boot (SB) is currently disabled on this system.

If SB is enabled in the future, SCST will not work

unless the following action is taken:

Using the keys in

/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow instructions in

/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing

to sign the SCST kernel module. Note that reboot will be needed.

SCST will not start automatically when Secure Boot is enabled and not configured properly.

+ Note: ONTAP Mediator generated a self-signed server certificate for temporary use on

this host. If the DNS name or IP address for the host is changed, the certificate

will no longer be valid. The default certificates should be replaced with secure

trusted certificates signed by a known certificate authority

prior to use for production.

For more information, see
/opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for the current

OS. Using 'yum update' to upgrade the kernel might cause service interruption.

For more information, see
/opt/netapp/lib/ontap_mediator/README
[root@mediator_host ~]#

▼ Beispiel ONTAP Mediator-Installation mit Unterstützung nur für HTTPS (Konsolenausgabe)

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.12.1.tgz
ontap-mediator-1.12.1/
ontap-mediator-1.12.1/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.12.1/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.12.1/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.12.1/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.12.1/ONTAP-Mediator-production.pub
ontap-mediator-1.12.1/ontap-mediator-1.12.1
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig
ontap-mediator-1.12.1/ontap-mediator-1.12.1.tsr
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig.tsr
[root@mediator_host ~]# ontap-mediator-1.12.1/ontap-mediator-1.12.1
--https-only
```

ONTAP Mediator: Self Extracting Installer

```
+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
40E72F35407F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
data:crypto/http/http_client.c:596:
40E72F35407F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:1045:server=http://ocsp.entrust.net:80
WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate
Continue without code signature checking (only recommended if
integrity has been established manually)? y(es)/N(o): yes
```

SKIPPING: Code signature check, manual override due to lack of OCSP response

+ Unpacking the ONTAP Mediator installer

+ ONTAP_MEDIATOR_INSTALL_HTTPS_ONLY is set to '1', args are: ''

+ Starting ONTAP Mediator install/update process: previous installation_mode is ''

+ Selected install package mode: HTTPS_ONLY

+ Checking that required port 31784 is free

ONTAP Mediator requires two user accounts. One for the service (netapp), and one for use by ONTAP to the mediator API (mediatoradmin).

Would you like to use the default account names: netapp + mediatoradmin? (Y(es)/n(o)): yes

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode

+ Checking for default Linux firewall

+ Installing required packages.

Last metadata expiration check: 0:38:52 ago on Mon 20 Apr 2026 11:23:22 AM EDT.

Package openssl-1:3.5.1-7.el9_7.x86_64 is already installed.

Package openssl-devel-1:3.5.1-7.el9_7.x86_64 is already installed.

Package gcc-11.5.0-11.el9.x86_64 is already installed.

Package make-1:4.3-8.el9.x86_64 is already installed.

Package which-2.21-30.el9_6.x86_64 is already installed.

Package libselinux-utils-3.6-3.el9.x86_64 is already installed.

Package patch-2.7.6-16.el9.x86_64 is already installed.

Package perl-Data-Dumper-2.174-462.el9.x86_64 is already installed.

Package perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch is already installed.

Package bzip2-1.0.8-10.el9_5.x86_64 is already installed.

```

Package efibootmgr-16-12.el9.x86_64 is already installed.
Package mokutil-2:0.7.2-1.el9.x86_64 is already installed.
Package python3-pip-21.3.1-1.el9.noarch is already installed.
Package elfutils-libelf-devel-0.193-1.el9.x86_64 is already installed.
Package polycoreutils-python-utils-3.6-3.el9.noarch is already
installed.
Package python3.12-3.12.12-4.el9_7.2.x86_64 is already installed.
Package python3.12-devel-3.12.12-4.el9_7.2.x86_64 is already
installed.
Dependencies resolved.
Nothing to do.
Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.CJqNqu/ontap-
mediator-1.12.1/ontap-mediator-1.12.1/install_20260420120204.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20260420120204.log)

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README
[root@mediator_host ~]#

```

Den Sicherheitsschlüssel für UEFI Secure Boot registrieren

Ab ONTAP Mediator 1.4 ist der Secure Boot Mechanismus auf UEFI-Systemen aktiviert. Wenn Secure Boot aktiviert ist, sind nach der Installation zusätzliche Schritte zur Registrierung des Sicherheitsschlüssels erforderlich.



Wenn Sie ONTAP Mediator 1.12 oder höher mit Unterstützung nur für HTTPS installiert haben, wird das SCST-Paket nicht installiert und Sie können diese Aufgabe überspringen.

Schritte

1. Befolgen Sie die Anweisungen in der README-Datei, um das SCST Kernelmodul zu signieren:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modul
```

e-signing

2. Die benötigten Schlüssel befinden sich an folgender Stelle:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```



Nach der Installation gibt die Systemausgabe die README-Dateien und den Speicherort der Schlüssel an.

3. Den öffentlichen Schlüssel zur MOK-Liste hinzufügen:

```
mokutil --import  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_  
key.der
```



Sie können den privaten Schlüssel am Standardspeicherort belassen oder ihn an einen sicheren Ort verschieben. Der öffentliche Schlüssel muss am aktuellen Speicherort verbleiben, damit der Boot Manager ihn verwenden kann. Weitere Informationen enthält die Datei README.module-signing:

```
[root@hostname ~]# ls  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/  
README.module-signing scst_module_key.der scst_module_key.priv
```

4. Starten Sie den Host neu und verwenden Sie den UEFI Boot Manager Ihres Geräts, um den neuen MOK zu genehmigen. Sie benötigen die für das mokutil Dienstprogramm bereitgestellte Passphrase in ["ONTAP Mediator installieren, wenn UEFI Secure Boot aktiviert ist"](#).

Signieren von SCST Kernelmodulen

Nach der Installation von ONTAP Mediator, falls der systemctl status mediator-scst als fehlgeschlagen (inaktiv) angezeigt wird, sind die folgenden Schritte zum Signieren des SCST-Kernelmoduls erforderlich.



Wenn Sie ONTAP Mediator 1.12 oder höher mit Unterstützung nur für HTTPS installiert haben, wird das SCST-Paket nicht installiert und Sie können diese Aufgabe überspringen.

Schritte

1. Während des Build-Prozesses wird im `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/` Verzeichnis ein öffentliches/privates Schlüsselpaar generiert. Der folgende Befehl zeigt die generierten Schlüssel an:

```
ls /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
```

```
README.module-signing scst_module_key.der scst_module_key.priv
```

2. Der folgende Befehl startet den Import des öffentlichen Schlüssels in das UEFI-Schlüssel-Repository:

```
mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_
key.der
```

Das `mokutil` Dienstprogramm fordert Sie zweimal zur Passworteingabe auf.

3. Die Software `mokutil` fordert während des Importvorgangs ein temporäres Passwort an, das für diesen Schlüssel verwendet werden soll.
4. Mit dem folgenden Befehl lässt sich prüfen, ob der Importvorgang gestartet wurde; anschließend ist ein Neustart des Systems erforderlich. Der Bootloader startet den EFI MOK manager.

```
mokutil --list-new
```

5. Die Aktivierung des Schlüssels für das SCST-Kernelmodul erfolgt über die Menüs auf dem Bildschirm. Nach dem Hochfahren folgt die Ausführung des folgenden Befehls. Nach dem Start des Dienstes sind die SCST-Kernelmodule signiert.

```
systemctl status mediator-scst
```

Was kommt als Nächstes?

["ONTAP Mediator Installationsstatus überprüfen"](#)

ONTAP Mediator Installationsstatus überprüfen

Nach der Installation von ONTAP Mediator sollte überprüft werden, ob dieser erfolgreich ausgeführt wird.

Schritte

1. Status des ONTAP Mediators:

```
systemctl status ontap_mediator
```

```
ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
```

```
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
└─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
```

2. SCST-Status anzeigen:

```
systemctl status mediator-scst
```



Wenn Sie ONTAP Mediator 1.12 oder höher mit Unterstützung nur für HTTPS installiert haben, wird das SCST-Paket nicht installiert und Sie können diesen Schritt überspringen.

```
Loaded: loaded (/etc/systemd/system/mediator-scst.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1 weeks 0
days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd
```

3. Bestätigen Sie die vom ONTAP Mediator verwendeten Ports:

```
netstat -anlt | grep -E '3260|31784'
```

```
tcp    0    0 0.0.0.0:31784    0.0.0.0:*        LISTEN
tcp    0    0 0.0.0.0:3260    0.0.0.0:*        LISTEN
tcp6   0    0 :::3260        :::*             LISTEN
```

Was kommt als Nächstes?

Nach der Installation und Verifizierung von ONTAP Mediator können Sie mit den folgenden Konfigurationsaufgaben nach der Installation fortfahren:

- "Einsatz von ONTAP Mediator für SnapMirror active sync und MetroCluster IP"
- "Konfigurieren der ONTAP Mediator Attribute" (Optional)

ONTAP Mediator verwenden

Einsatz von ONTAP Mediator für SnapMirror active sync und MetroCluster IP

ONTAP Mediator läuft auf einem Linux Host in einer dritten Ausfalldomäne, getrennt von Ihren ONTAP Clustern, und stellt dort einen persistenten, abgeschotteten Speicher für Hochverfügbarkeitsmetadaten bereit. ONTAP nutzt diesen Speicher zusammen mit der Systemstatusabfrage und den Ping Proxy Funktionen des Mediators, um SnapMirror Active Sync Beziehungen und MetroCluster IP Konfigurationen zu überwachen.



Diese Dokumentation bezieht sich auf die lokale Version von ONTAP Mediator. Informationen zu ONTAP Cloud Mediator, das ab ONTAP 9.17.1 verfügbar ist, enthält die ["SnapMirror active sync Dokumentation"](#).

Aktive Synchronisierungsbeziehungen von SnapMirror überwachen

SnapMirror active sync nutzt ONTAP Mediator als passiven Zeugen für die primäre und die Spiegelkopie in einer Konsistenzgruppe. Wenn eine Netzwerkpartition auftritt oder eine Kopie nicht mehr verfügbar ist, fragt SnapMirror active sync ONTAP Mediator ab, um zu bestimmen, welche Kopie weiterhin E/A bereitstellt, und stellt E/A auf der anderen Kopie ein.

Ab ONTAP 9.8 können Sie jede Version von ONTAP Mediator verwenden, um eine SnapMirror active sync Beziehung zu überwachen.



Grenzwerte für die Anzahl der SnapMirror Active Sync Cluster-Paare, die von einer einzelnen ONTAP Mediator-Instanz überwacht werden können, sind unter ["Objektbeschränkungen für ONTAP SnapMirror active sync"](#) beschrieben.

["Den ONTAP Mediator für SnapMirror Active Sync konfigurieren"](#)

Überwachung von MetroCluster IP Konfigurationen

In einer MetroCluster IP Konfiguration speichert ONTAP Mediator Statusinformationen über die MetroCluster Knoten in Mailbox-LUNs und unterstützt die Knoten mit einem Mediator-gestützten automatischen ungeplanten Switchover (MAUSO) im Falle einer Katastrophe oder bestimmter Fehlerszenarien.

Ab ONTAP 9.19.1 und ONTAP Mediator 1.12 können Sie einen ONTAP Mediator konfigurieren, der HTTPS zur Kommunikation nutzt, um Ihre MetroCluster IP-Konfiguration zu überwachen. Wenn Sie ONTAP Mediator mit dem iSCSI-Protokoll konfigurieren, können Sie jede Version des ONTAP Mediators zur Überwachung einer MetroCluster IP-Konfiguration verwenden.



Die Beschränkungen für die Anzahl der MetroCluster IP-Konfigurationen, die eine einzelne ONTAP Mediator Instanz überwachen kann, sind unter ["ONTAP Mediator zur Überwachung mehrerer MetroCluster IP Konfigurationen verwenden"](#) beschrieben.

["Konfiguration von ONTAP Mediator für eine MetroCluster IP-Konfiguration"](#)

Verwandte Informationen

- ["ONTAP SnapMirror Active Sync-Architektur"](#)
- ["Informationen zur ONTAP Mediator Unterstützung für die automatische ungeplante Umschaltung in einer MetroCluster IP Konfiguration"](#)

ONTAP Mediator verwalten

Upgrade von ONTAP Mediator

Upgrade von ONTAP Mediator

Zur Aktualisierung von ONTAP Mediator auf eine neuere Version ohne Aktualisierung des Host-Betriebssystems können Sie das Installationspaket für die neue Version herunterladen und das Installationsprogramm auf dem Host ausführen, auf dem ONTAP Mediator bereits installiert ist.



Falls Sie das Host-Betriebssystem auf eine neue Version aktualisieren und im Zuge dieses Prozesses ONTAP Mediator neu installieren oder aktualisieren müssen, finden Sie stattdessen weitere Informationen unter ["Aktualisieren Sie das Host-Betriebssystem und ONTAP Mediator"](#).

Bevor Sie beginnen

- Zu prüfen ist, ob Ihr Host die in ["Vorbereitung der Installation des ONTAP Mediators"](#) beschriebenen Voraussetzungen erfüllt, einschließlich der Anforderungen an Host, Firewall und Betriebssystem.
- Das Installationspaket für die neue Version steht zum Herunterladen bereit. Weitere Informationen finden Sie unter ["Das Installationspaket für ONTAP Mediator herunterladen"](#).
- NetApp empfiehlt, die Codesignatur des neuen Installationspakets zu überprüfen. Weitere Informationen finden Sie unter ["Die Codesignatur des ONTAP Mediator Installationspakets überprüfen"](#).

Über diese Aufgabe

Vor dem Upgrade von ONTAP Mediator sollten die folgenden Informationen geprüft werden.

- Ein Upgrade von ONTAP Mediator auf die neueste Version wird empfohlen. Ältere Versionen funktionieren weiterhin mit allen ONTAP Releases, jedoch enthalten neuere Versionen Sicherheitspatches für Drittanbieterkomponenten.
- Wenn Sie auf eine neue ONTAP Mediator-Version aktualisieren, die das SCST-Paket enthält, aktualisiert das Installationsprogramm automatisch auf die empfohlene SCST-Version, sofern keine höhere Version verfügbar ist. Anweisungen zur manuellen Installation einer höheren SCST-Version finden Sie unter ["Das Host-Betriebssystem für ONTAP Mediator warten"](#). Für unterstützte Versionen siehe die ["SCST Support-Matrix"](#).



- Wenn das Upgrade fehlschlägt, ist möglicherweise eine neuere Version von ONTAP Mediator erforderlich.
- Ab dem 15. Juni 2025 lassen sich ONTAP Mediator 1.9 und 1.8 nicht installieren oder aktualisieren, da ihre Code-Signing-Zertifikate abgelaufen sind. Falls die Aktualisierung fehlschlägt, kommt stattdessen die Patch-Version ONTAP Mediator 1.9.1 zum Einsatz.
- Ab ONTAP 9.19.1 und ONTAP Mediator 1.12 besteht die Möglichkeit, ONTAP Mediator mit iSCSI und HTTPS-Unterstützung oder nur mit HTTPS-Unterstützung zu installieren. Wenn ONTAP Mediator nur mit HTTPS-Unterstützung installiert wird, wird das SCST-Paket nicht installiert.
- Wenn Sie von ONTAP Mediator 1.11 oder einer früheren Version mit installiertem SCST aktualisieren und während des Upgrades die Option „Nur HTTPS“ auswählen, wird das SCST-Paket deinstalliert und die neue ONTAP Mediator Version enthält das SCST-Paket nicht.

- Wenn die Überwachung mehrerer MetroCluster IP-Konfigurationen mit ONTAP Mediator vorgesehen ist, hängt die Unterstützung vom Mediator-Typ, der ONTAP Version und dem Betriebssystem ab. Weitere Informationen finden Sie unter ["ONTAP Mediator zur Überwachung mehrerer MetroCluster IP Konfigurationen verwenden"](#).
- Die Installation des ONTAP Mediators mit ausschließlicher HTTPS-Unterstützung wird für die folgenden Anwendungsfälle unterstützt:
 - Sie planen, ONTAP Mediator ausschließlich zur Überwachung Ihrer SnapMirror active sync Cluster zu verwenden.
 - Es ist vorgesehen, ONTAP Mediator mit HTTPS zu konfigurieren, um eine oder mehrere MetroCluster IP-Konfigurationen zu überwachen.
- ONTAP Mediator muss mit Unterstützung für iSCSI und HTTPS im folgenden Szenario installiert werden:
 - Sie planen, ONTAP Mediator mit iSCSI zu konfigurieren, um eine oder mehrere MetroCluster IP-Konfigurationen zu überwachen.
- Wenn Sie das Installationsprogramm für eine bestehende ONTAP Mediator Installation ausführen, erkennt es die aktuelle Version und fordert Sie auf, das Upgrade zu bestätigen:

```
ONTAP Mediator will be upgraded from version <current-version> to <new-version>.
```

```
Do you wish to continue? Y(es)/n(o) :
```

- Im Rahmen des Upgrades erfasst das Installationsprogramm ein Support Bundle Ihrer Konfiguration vor dem Upgrade und migriert die Datenbank, bevor die ONTAP Mediator software aktualisiert wird.
- Für Automatisierungsanwendungen kann der `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 -y` Befehl verwendet werden, um die Installationsabfragen zu überspringen.

Schritte

1. Beim Ausführen des Installationsprogramms für die neue Version beantworten Sie die Eingabeaufforderungen nach Bedarf:

```
./ontap-mediator-1.12.1/ontap-mediator-1.12.1
```



Zum Überspringen der Signaturprüfung während des Upgrades dient der `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 --skip-code-signature-check` Befehl

Das Installationsprogramm erkennt die bestehende Installation und fordert Sie zum Upgrade auf, installiert dann die erforderlichen Pakete und migriert Ihre Konfiguration.

▼ Beispiel für ONTAP Mediator-Upgrade mit HTTPS- und iSCSI-Unterstützung (Konsolenausgabe)

```
[root@mediator_host ~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
```

CAppath:/etc/pki/tls

+ Unpacking the ONTAP Mediator installer

ONTAP Mediator requires two user accounts. One for the service (netapp), and one for use by ONTAP to the mediator API (mediatoradmin).

Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode

+ Checking for default Linux firewall

+ Installing required packages.

Last metadata expiration check: 0:03:56 ago on Mon 20 Apr 2026 02:49:08 PM EDT.

Package openssl-1:3.5.1-7.el9_7.x86_64 is already installed.

Package openssl-devel-1:3.5.1-7.el9_7.x86_64 is already installed.

Package kernel-devel-5.14.0-611.45.1.el9_7.x86_64 is already installed.

Package kernel-modules-core-5.14.0-611.45.1.el9_7.x86_64 is already installed.

Package gcc-11.5.0-11.el9.x86_64 is already installed.

Package make-1:4.3-8.el9.x86_64 is already installed.

Package which-2.21-30.el9_6.x86_64 is already installed.

Package libselinux-utils-3.6-3.el9.x86_64 is already installed.

Package patch-2.7.6-16.el9.x86_64 is already installed.

Package perl-Data-Dumper-2.174-462.el9.x86_64 is already installed.

Package perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch is already installed.

Package bzip2-1.0.8-10.el9_5.x86_64 is already installed.

Package efibootmgr-16-12.el9.x86_64 is already installed.

Package mokutil-2:0.7.2-1.el9.x86_64 is already installed.

Package python3-pip-21.3.1-1.el9.noarch is already installed.

Package elfutils-libelf-devel-0.193-1.el9.x86_64 is already installed.

Package policycoreutils-python-utils-3.6-3.el9.noarch is already installed.

```

Package python3.12-3.12.12-4.el9_7.2.x86_64 is already installed.
Package python3.12-devel-3.12.12-4.el9_7.2.x86_64 is already
installed.
Dependencies resolved.
Nothing to do.
Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.uigddi/ontap-
mediator-1.11.0/ontap-mediator-1.11.0/install_20260420145003.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20260420145003.log)

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
    OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
[root@mediator_host ~]# ontap-mediator-1.12.1/ontap-mediator-1.12.1

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
    Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
+ Unpacking the ONTAP Mediator installer
+ ONTAP_MEDIATOR_INSTALL_HTTPS_ONLY is set to '0', args are: ''
+ Starting ONTAP Mediator install/update process: previous
installation_mode is ''

ONTAP Mediator can be installed with iSCSI and HTTPS support, or

```

```

support for HTTPS only.
Do you wish to install ONTAP Mediator with iSCSI and HTTPS support?
Y(es)/n(o): yes
ONTAP Mediator will be installed with mode: ISCSI_HTTPS
+ Selected install package mode: ISCSI_HTTPS
ONTAP Mediator will be upgraded from version 1.11.0 to 1.12.1.

Do you wish to continue? Y(es)/n(o): yes
Capturing support_bundle to save pre-upgrade configuration. API
Credentials are required.
    Mediator API User Name: mediatoradmin
        Password: Running plugins, please wait...

Creating tar archive...
Support bundle has been generated at
/opt/netapp/data/support_bundles/scs001097036-1_1776711598_BASIC.tgz
Testing the DB can be upgraded
Cloning database...
Cloning successful.
Verifying database is up-to-date...
Database out-of-date.Migrations are necessary:
Current revision: 0d5dcf349b27, Head revision: 758e4873c40d
Performing database migrations against clone...
Migrations successful.
Database upgrade operation complete.
+ Adding python312 specific packages
+ Upgrading ONTAP Mediator. (Log: /root/ontap_mediator.gwaGmU/ontap-
mediator-1.12.1/ontap-mediator-1.12.1/upgrade_20260420145942.log)

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
    OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README

```

```
[root@mediator_host ~]#
```

▼ Beispiel für ONTAP Mediator-Upgrade mit Unterstützung nur für HTTPS (Konsolenausgabe)

```
[root@mediator_host~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0
```

ONTAP Mediator: Self Extracting Installer

```
+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
```

```
+ Unpacking the ONTAP Mediator installer
```

ONTAP Mediator requires two user accounts. One for the service (netapp), and one for use by ONTAP to the mediator API (mediatoradmin).

Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

```
+ Checking if SELinux is in enforcing mode
```

```
+ Checking for default Linux firewall
```

```
+ Installing required packages.
```

Last metadata expiration check: 0:33:41 ago on Tue 21 Apr 2026 10:48:35 AM EDT.

Package openssl-1:3.5.1-7.el9_7.x86_64 is already installed.

Package openssl-devel-1:3.5.1-7.el9_7.x86_64 is already installed.

Package kernel-devel-5.14.0-611.45.1.el9_7.x86_64 is already installed.

Package kernel-modules-core-5.14.0-611.45.1.el9_7.x86_64 is already installed.

Package gcc-11.5.0-11.el9.x86_64 is already installed.

Package make-1:4.3-8.el9.x86_64 is already installed.

Package which-2.21-30.el9_6.x86_64 is already installed.

```

Package libselinux-utils-3.6-3.el9.x86_64 is already installed.
Package patch-2.7.6-16.el9.x86_64 is already installed.
Package perl-Data-Dumper-2.174-462.el9.x86_64 is already installed.
Package perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch is already
installed.
Package bzip2-1.0.8-10.el9_5.x86_64 is already installed.
Package efibootmgr-16-12.el9.x86_64 is already installed.
Package mokutil-2:0.7.2-1.el9.x86_64 is already installed.
Package python3-pip-21.3.1-1.el9.noarch is already installed.
Package elfutils-libelf-devel-0.193-1.el9.x86_64 is already installed.
Package polycoreutils-python-utils-3.6-3.el9.noarch is already
installed.
Package python3.12-3.12.12-4.el9_7.2.x86_64 is already installed.
Package python3.12-devel-3.12.12-4.el9_7.2.x86_64 is already
installed.
Dependencies resolved.
Nothing to do.
Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.JclgnS/ontap-
mediator-1.11.0/ontap-mediator-1.11.0/install_20260421112205.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20260421112205.log)

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
    OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
[root@mediator_host~]#
[root@mediator_host~]# tar -zxvf ontap-mediator-1.12.1.tgz
ontap-mediator-1.12.1/

```

```
ontap-mediator-1.12.1/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.12.1/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.12.1/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.12.1/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.12.1/ONTAP-Mediator-production.pub
ontap-mediator-1.12.1/ontap-mediator-1.12.1
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig
ontap-mediator-1.12.1/ontap-mediator-1.12.1.tsr
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig.tsr
[root@mediator_host~]#
[root@mediator_host~]# ontap-mediator-1.12.1/ontap-mediator-1.12.1
--https-only
```

ONTAP Mediator: Self Extracting Installer

```
+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
+ Unpacking the ONTAP Mediator installer
+ ONTAP_MEDIATOR_INSTALL_HTTPS_ONLY is set to '1', args are: ''
+ Starting ONTAP Mediator install/update process: previous
installation_mode is ''
+ Selected install package mode: HTTPS_ONLY
ONTAP Mediator will be upgraded from version 1.11.0 to 1.12.1.
```

```
Do you wish to continue? Y(es)/n(o): yes
Capturing support_bundle to save pre-upgrade configuration. API
Credentials are required.
```

```
  Mediator API User Name: mediatoradmin
```

```
    Password: Running plugins, please wait...
```

```
Creating tar archive...
Support bundle has been generated at
/opt/netapp/data/support_bundles/scs001097036-1_1776785423_BASIC.tgz
Testing the DB can be upgraded
Cloning database...
Cloning successful.
Verifying database is up-to-date...
Database out-of-date.Migrations are necessary:
Current revision: 0d5dcf349b27, Head revision: 758e4873c40d
Performing database migrations against clone...
Migrations successful.
Database upgrade operation complete.
```

```

+ Adding python312 specific packages
+ Upgrading ONTAP Mediator. (Log: /root/ontap_mediator.cRy0mN/ontap-
mediator-1.12.1/ontap-mediator-1.12.1/upgrade_20260421113003.log)
fapolicyd not installed or no rules.d directory found, skipping
fapolicyd configuration
    ONTAP Mediator rsyslog and logging rotation enabled
+ Upgrade successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/upgrade_20260421113003.log)\n

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
    OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README

[root@mediator_host ~]#

```

Aktualisieren Sie das Host-Betriebssystem und installieren oder aktualisieren Sie ONTAP Mediator neu.

Um das Host-Betriebssystem für ONTAP Mediator mit installiertem SCST auf eine neuere Version zu aktualisieren, müssen Sie ONTAP Mediator deinstallieren. Nach der Aktualisierung des Betriebssystems können Sie Ihre aktuelle Version von ONTAP Mediator neu installieren oder auf eine neuere Version aktualisieren.

Über diese Aufgabe

- Diese Aufgabe gilt für ONTAP Mediator-Versionen mit installiertem SCST. Wenn Sie ONTAP Mediator 1.12 oder höher mit Unterstützung nur für HTTPS installiert haben, ist das SCST-Paket nicht installiert und Sie können das Host-Betriebssystem aktualisieren, ohne ONTAP Mediator zu beeinträchtigen. Anweisungen zur Aktualisierung des Betriebssystems finden Sie in der Dokumentation des Host-Betriebssystemanbieters.
- Wenn Sie lediglich den Kernel des Host-Betriebssystems auf eine unterstützte Version aktualisieren müssen, ohne auf eine neue Betriebssystemversion umzusteigen, ist stattdessen "[Das Host-Betriebssystem für ONTAP Mediator warten](#)" relevant.
- Vor dem Upgrade des Host-Betriebssystems für ONTAP Mediator mit dem Tool leapp-upgrade "[Deinstallation von ONTAP Mediator](#)". Das Tool prüft, ob in den registrierten Repositories neue RPM-Versionen verfügbar sind.

- Der ONTAP Mediator Installer installiert eine .rpm-Datei, die das Tool leapp-upgrade in die Suche einbezieht. Da der Installer die Datei entpackt, anstatt sie aus einem registrierten Repository herunterzuladen, kann das Tool kein Upgrade finden. Das Tool leapp-upgrade ist für die Deinstallation des Pakets zu verwenden.

Schritte

1. Die Protokolldateien sichern:

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Upgrade mit dem leapp-upgrade Tool durchführen:

```
[rootmediator-host ~]# leapp preupgrade --target 9.8
..<snip upgrade checks>..
..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 9.8
..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. ONTAP Mediator neu installieren:



Die restlichen Schritte sollten unmittelbar nach der Neuinstallation von ONTAP Mediator erfolgen, um einen Verlust von Protokolldateien zu verhindern.

```
[rootmediator-host ~]# ontap-mediator-1.12.1/ontap-mediator-1.12.1

ONTAP Mediator: Self Extracting Installer

..<snip installation>..
```

```
[rootmediator-host ~]#
```

4. ontap_mediator anhalten:

```
[rootmediator-host ~]# systemctl stop ontap_mediator  
[rootmediator-host ~]#
```

5. Die Protokolldateien ersetzen:

```
[rootmediator-host ~]# tar -xf ontap_mediator_file_backup.tgz -C  
/opt/netapp/lib/ontap_mediator  
[rootmediator-host ~]#
```

6. ontap_mediator starten:

```
[rootmediator-host ~]# systemctl start ontap_mediator  
[rootmediator-host ~]#
```

7. Alle ONTAP Cluster werden wieder mit dem aktualisierten ONTAP Mediator verbunden:

MetroCluster über IP

```
siteA::> metrocluster configuration-settings mediator show  
Mediator IP      Port    Node                Configuration  
Connection  
Status           Status  
-----  
-----  
172.31.40.122  
31784    siteA-node2         true      false  
          siteA-node1         true      false  
          siteB-node2         true      false  
          siteB-node2         true      false  
  
siteA::> metrocluster configuration-settings mediator remove  
Removing the mediator and disabling Automatic Unplanned Switchover. It  
may take a few minutes to complete.  
Please enter the username for the mediator: mediatoradmin  
Please enter the password for the mediator:  
Confirm the mediator password:  
Automatic Unplanned Switchover is disabled for all nodes...  
Removing mediator mailboxes...  
Successfully removed the mediator.
```

```

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It may
take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP      Port      Node      Configuration
Connection
-----
-----
172.31.40.122
          31784  siteA-node2      true      true
                  siteA-node1      true      true
                  siteB-node2      true      true
                  siteB-node2      true      true
siteA::>

```

SnapMirror Active Sync

Für SnapMirror active sync ist es nicht erforderlich, die außerhalb von /opt/netapp gespeicherten TLS-Zertifikate neu zu installieren. Die in /opt/netapp gespeicherten Zertifikate sollten gesichert und wiederhergestellt werden.

```

peer1::> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
-----
172.31.49.237  peer2      unreachable      true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
Job ID Name      Owing
Vserver      Node      State
-----
39      mediator remove      peer1      peer1-node1      Success
Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver      Serial Number      Certificate Name      Type
-----
-----
-----
-----

```


peer1

4A790360081F41145E14C5D7CE721DC6C210007F

ONTAPMediatorCA

server-

ca

Certificate Authority: ONTAP Mediator CA

Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer1::> security certificate install -type server-ca -vserver peer1

Please enter Certificate: Press <Enter> when done

....

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

Please enter Certificate: Press <Enter> when done

....

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer
-cluster peer2 -username mediatoradmin

```
Notice: Enter the mediator password.
```

```
Enter the password:
```

```
Enter the password again:
```

```
Info: [Job: 43] 'mediator add' job queued
```

```
peer1::> job show -id 43
```

Job	ID	Name	Owning Vserver	Node	State
43		mediator add	peer1	peer1-node2	Success
Description: Creating a mediator entry					

```
peer1::> snapmirror mediator show
```

Mediator Address	Peer	Cluster	Connection Status	Quorum Status
172.31.49.237	peer2		connected	true

```
peer1::>
```

Verwandte Informationen

- ["Sicherheitszertifikat löschen"](#)
- ["Sicherheitszertifikat installieren"](#)
- ["Sicherheitszertifikat anzeigen"](#)
- ["snapmirror mediator add"](#)
- ["SnapMirror Mediator entfernen"](#)
- ["storage iscsi-initiator show"](#)

Konfigurieren der ONTAP Mediator Attribute

Sie können hostseitige Attribute von ONTAP Mediator konfigurieren, einschließlich zertifikatsbezogener Einstellungen und Konfigurationsüberschreibungen.

Konfigurierbare Einstellungen für ONTAP Mediator

ONTAP Mediator unterstützt verschiedene konfigurierbare Einstellungen. Die Standardwerte für diese Einstellungen befinden sich in einer `low_space_threshold_mib: 10` schreibgeschützten Datei. Die Datei befindet sich hier:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml
```

Alle Werte, die in das `'ontap_mediator.user_config.yaml'` eingefügt werden, überschreiben die Standardwerte und bleiben bei allen ONTAP Mediator Upgrades erhalten.

Nach der Änderung `ontap_mediator.user_config.yaml` sollte ONTAP Mediator neu gestartet werden:

```
systemctl restart ontap_mediator
```

Die in diesem Abschnitt beschriebenen ONTAP Mediator-Attribute können bei Bedarf angepasst werden.



Andere Standardwerte im `ontap_mediator.config.yaml` sollten nicht geändert werden, da geänderte Werte bei ONTAP Mediator Upgrades nicht beibehalten werden.

Sie ändern die Attribute des ONTAP Mediators, indem Sie die erforderlichen Variablen in die `ontap_mediator.user_config.yaml` Datei kopieren, um die Standardeinstellungen zu überschreiben.

Installation von SSL-Zertifikaten von Drittanbietern

Sie können die standardmäßigen selbstsignierten Zertifikate durch SSL-Zertifikate von Drittanbietern ersetzen, indem Sie die Konfigurationsdateien von ONTAP Mediator ändern.

Zum Ersetzen der standardmäßigen selbstsignierten Zertifikate durch SSL-Zertifikate von Drittanbietern sind bestimmte Attribute in den folgenden Dateien anzupassen:

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`
- `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

Die Variablen in diesen Dateien dienen der Steuerung der von ONTAP Mediator verwendeten Zertifikatsdateien.

ONTAP Mediator 1.9 und höher

Die in der folgenden Tabelle aufgeführten Standardvariablen sind in der `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` Datei enthalten.

Variable	Pfad
<code>cert_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt</code>
<code>key_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key</code>
<code>ca_cert_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt</code>
<code>ca_key_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key</code>
<code>ca_serial_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl</code>

Variable	Pfad
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- cert_valid_days Wird zur Festlegung des Ablaufdatums von Clientzertifikaten verwendet. Der Maximalwert beträgt drei Jahre (1095 Tage).
- x509_passin_pwd ist die Passphrase für das signierte Clientzertifikat.

Die in der folgenden Tabelle aufgeführten Standardvariablen sind in der `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei enthalten.

Variable	Pfad
mediator_cert	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt</code>
mediator_key	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key</code>
ca_cert_path	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt</code>

ONTAP Mediator 1.8 und früher

Die in der folgenden Tabelle aufgeführten Standardvariablen sind in der `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` Datei enthalten.

Variable	Pfad
cert_path	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt</code>
key_path	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key</code>
ca_cert_path	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt</code>
ca_key_path	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key</code>
ca_serial_path	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl</code>
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- cert_valid_days Wird zur Festlegung des Ablaufdatums von Clientzertifikaten verwendet. Der Maximalwert beträgt drei Jahre (1095 Tage).

- x509_passin_pwd ist die Passphrase für das signierte Clientzertifikat.

Die in der folgenden Tabelle aufgeführten Standardvariablen sind in der /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini Datei enthalten.

Variable	Pfad
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt

Wenn diese Attribute geändert werden, muss ONTAP Mediator neu gestartet werden, damit die Änderungen wirksam werden. Ausführliche Anweisungen zum Ersetzen von Standardzertifikaten durch Zertifikate von Drittanbietern finden sich unter ["Selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern ersetzen"](#).

Schutz vor Passwortangriffen konfigurieren

Die folgenden Einstellungen bieten Schutz vor Brute-Force-Passworterraten-Angriffen.

Um die Funktion zu aktivieren, muss ein Wert für die window_seconds und die retry_limit festgelegt werden.

Beispiele:

- Ein Zeitfenster von 5 Minuten für die Versuche wird bereitgestellt, danach wird der Zähler auf null Fehler zurückgesetzt:

```
authentication_lock_window_seconds: 300
```

- Das Konto wird gesperrt, wenn innerhalb des festgelegten Zeitraums fünf Fehler auftreten:

```
authentication_retry_limit: 5
```

- Die Auswirkungen von Brute-Force-Angriffen auf Passwörter lassen sich verringern, indem vor der Ablehnung jedes Versuchs eine Verzögerung eingestellt wird, wodurch die Angriffe verlangsamt werden.

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0    # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null   # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null           # number of retries to allow
before locking API access, null = unlimited
```

Konfiguration von Regeln zur Passwortkomplexität

Die folgenden Felder steuern die Regeln für die Passwortkomplexität des ONTAP Mediator API Benutzerkontos.

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0      # min. uppercase characters

password_lowercase_chars: 1      # min. lowercase character

password_special_chars: 1        # min. non-letter, non-digit

password_nonletter_chars: 2      # min. non-letter characters (digits,
specials, anything)
```

Konfiguration der Festplatten- und Protokollspeicherplatzeinstellungen von ONTAP Mediator, einschließlich des Schwellenwerts für freien Speicherplatz und des reservierten Protokollspeicherplatzes.

Konfiguration der Freispeicherschwelle

Es gibt Einstellungen, die den benötigten freien Speicherplatz auf der `/opt/netapp/lib/ontap_mediator` Festplatte steuern.

Wenn der verfügbare Speicherplatz unter dem festgelegten Schwellenwert liegt, gibt der Dienst ein Warnereignis aus.

```
low_space_threshold_mib: 10
```

Konfiguration des reservierten Protokollspeicherplatzes

Die `RESERVE_LOG_SPACE` Funktion wird durch spezifische Einstellungen gesteuert. Standardmäßig erstellt die ONTAP Mediator Installation einen separaten Speicherplatz für die Protokolle. Das Installationsprogramm erstellt eine neue Datei mit fester Größe und insgesamt 700 MB Speicherplatz, die ausdrücklich für die ONTAP Mediator Protokollierung verwendet wird.

Um diese Funktion zu deaktivieren und den Standardspeicherplatz zu verwenden, sind die folgenden Schritte erforderlich:

1. Den Wert von `RESERVE_LOG_SPACE` in der folgenden Datei von 1 auf 0 ändern:

```
/opt/netapp/lib/ontap_mediator/tools/mediator_env
```

- a. Führen Sie den folgenden Befehl aus:

```
cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep
```

```
"RESERVE_LOG_SPACE"
```

```
RESERVE_LOG_SPACE=0
```

b. ONTAP Mediator neu starten:

```
systemctl restart ontap_mediator
```

Um die Funktion wieder zu aktivieren, den Wert von 0 auf 1 ändern und den Mediator neu starten.



Das Umschalten zwischen verschiedenen Speicherbereichen löscht keine vorhandenen Protokolle. Alle vorherigen Protokolle werden gesichert und nach dem Umschalten sowie dem Neustart des Mediators in den aktuellen Speicherbereich verschoben.

Änderung von Benutzernamen und Passwort des ONTAP Mediator

Der Benutzername oder das Passwort für ONTAP Mediator kann auf dem Linux-Host geändert werden, auf dem ONTAP Mediator installiert ist.

Benutzernamen ändern

Der Benutzername lässt sich mit folgendem Verfahren ändern.

Über diese Aufgabe

Diese Aufgabe ist auf dem Linux-Host auszuführen, auf dem ONTAP Mediator installiert wurde.

Falls Sie diesen Befehl nicht erreichen können, ist es möglicherweise erforderlich, den Befehl mit dem vollständigen Pfad auszuführen, wie im folgenden Beispiel gezeigt:

```
/usr/local/bin/mediator_username
```

Schritte

Der Benutzername kann durch eine der folgenden Optionen geändert werden:

- **Option (a):** Führen Sie den Befehl `mediator_change_user` aus und beantworten Sie die Eingabeaufforderungen wie im folgenden Beispiel gezeigt:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
  Mediator API User Name: mediatoradmin
                        Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
```

```
[root@mediator-host ~]#
```

- **Option (b):** Der folgende Befehl kann ausgeführt werden:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2  
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediator  
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin  
mediator_change_user  
The account username has been modified successfully.  
[root@mediator-host ~]#
```

Passwort ändern

Das Passwort kann mit folgendem Verfahren geändert werden.

Über diese Aufgabe

Diese Aufgabe ist auf dem Linux-Host auszuführen, auf dem ONTAP Mediator installiert wurde.

Falls Sie diesen Befehl nicht erreichen können, ist es möglicherweise erforderlich, den Befehl mit dem vollständigen Pfad auszuführen, wie im folgenden Beispiel gezeigt:

```
/usr/local/bin/mediator_change_password
```

Schritte

Das Passwort kann durch eine der folgenden Optionen geändert werden:

- **Option (a):** Der `mediator_change_password`-Befehl kann ausgeführt und die Eingabeaufforderungen wie im folgenden Beispiel beantwortet werden:

```
[root@mediator-host ~]# mediator_change_password  
Change the Mediator API password by entering the following values:  
Mediator API User Name: mediatoradmin  
Old Password:  
New Password:  
Confirm Password:  
The password has been updated successfully.  
[root@mediator-host ~]#
```

- **Option (b):** Der folgende Befehl kann ausgeführt werden:

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1  
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

Das Beispiel zeigt, dass das Passwort von „mediator1“ auf „mediator2“ geändert wird.

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin  
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2  
mediator_change_password  
The password has been updated successfully.  
[root@mediator-host ~]#
```

ONTAP Mediator starten und stoppen

Zum Warten des Hosts oder zum erneuten Aktivieren des Dienstes können ONTAP Mediator und SCST angehalten oder neu gestartet werden.

ONTAP Mediator stoppen

Um ONTAP Mediator zu beenden, sind die folgenden Schritte erforderlich:

Schritte

1. ONTAP Mediator anhalten:

```
systemctl stop ontap_mediator
```

2. SCST anhalten:

```
systemctl stop mediator-scst
```

3. ONTAP Mediator und SCST deaktivieren:

```
systemctl disable ontap_mediator mediator-scst
```

Starten von ONTAP Mediator

Um ONTAP Mediator wieder zu aktivieren, sind die folgenden Schritte erforderlich:

Schritte

1. ONTAP Mediator und SCST aktivieren:

```
systemctl enable ontap_mediator mediator-scst
```

2. SCST starten:

```
systemctl start mediator-scst
```

3. ONTAP Mediator wird gestartet:

```
systemctl start ontap_mediator
```

Überprüfung des ONTAP Mediator Systemstatus

Der ordnungsgemäße Betrieb von ONTAP Mediator sollte überprüft werden.

Überprüfung des Service-Status

Schritte

1. Status des ONTAP Mediators:

a. Führen Sie den folgenden Befehl aus:

```
systemctl status ontap_mediator
```

```
[root@mediator_host ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@mediator_host ~]#
```

b. Anzeige des Status des SCST Service:



Wenn Sie ONTAP Mediator 1.12 oder höher mit Unterstützung nur für HTTPS installiert haben, wird das SCST-Paket nicht installiert und Sie können diese Aufgabe

überspringen.

```
systemctl status mediator-scst
```

+

```
[root@mediator_host ~]# systemctl status mediator-scst
Loaded: loaded (/etc/systemd/system/mediator-scst.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1 weeks 0
days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@mediator_host ~]#
```

Bestätigung der Listening-Ports

1. Bestätigen Sie die vom ONTAP Mediator verwendeten Ports:

```
netstat -anlt | grep -E '3260|31784'
```

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'
```

tcp	0	0	0.0.0.0:31784	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:3260	0.0.0.0:*	LISTEN
tcp6	0	0	:::3260	:::*	LISTEN

Zertifikate verwalten

Erneutes Generieren eines temporären selbstsignierten Zertifikats für den ONTAP Mediator Host

Wenn eine Änderung des Hostnamens oder der IP-Adresse das vorhandene Zertifikat ungültig macht, wird für den aktuellen Host ein temporäres, selbstsigniertes Zertifikat neu generiert.



Dieses Verfahren wird nur auf Systemen unterstützt, auf denen ONTAP Mediator 1.7 oder höher ausgeführt wird.

Über diese Aufgabe

- Diese Aufgabe ist auf dem Linux-Host auszuführen, auf dem ONTAP Mediator installiert wurde.
- Diese Aufgabe kann nur durchgeführt werden, wenn die generierten selbstsignierten Zertifikate aufgrund von Änderungen des Hostnamens oder der IP-Adresse des Hosts nach der Installation von ONTAP Mediator veraltet sind.
- Nachdem das temporäre selbstsignierte Zertifikat durch ein vertrauenswürdiges Zertifikat eines Drittanbieters ersetzt wurde, wird diese Aufgabe *nicht* verwendet, um ein Zertifikat erneut zu generieren. Das Fehlen eines selbstsignierten Zertifikats führt dazu, dass dieses Verfahren fehlschlägt.

Schritt

Um ein neues temporäres selbstsigniertes Zertifikat für den aktuellen Host zu generieren, ist folgender Schritt erforderlich:

1. ONTAP Mediator neu starten:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

Ersetzen der selbstsignierten Zertifikate von ONTAP Mediator durch vertrauenswürdige Zertifikate von Drittanbietern

Sofern Ihre Umgebung dies zulässt, sollten selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate ersetzt werden, die von einer Zertifizierungsstelle ausgestellt wurden.

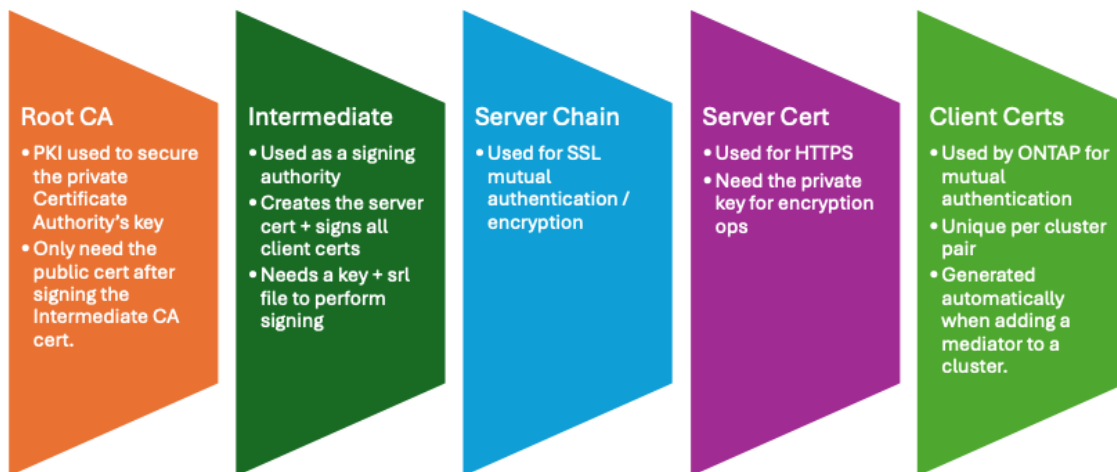


- Zertifikate von Drittanbietern werden erst ab ONTAP 9.16.1 und in einigen früheren ONTAP Patch-Releases unterstützt. Weitere Informationen unter ["NetApp Bugs Online Bug-ID CONTAP-243278"](#).
- Zertifikate von Drittanbietern werden nur auf Systemen unterstützt, auf denen ONTAP Mediator 1.7 oder höher ausgeführt wird.

Über diese Aufgabe

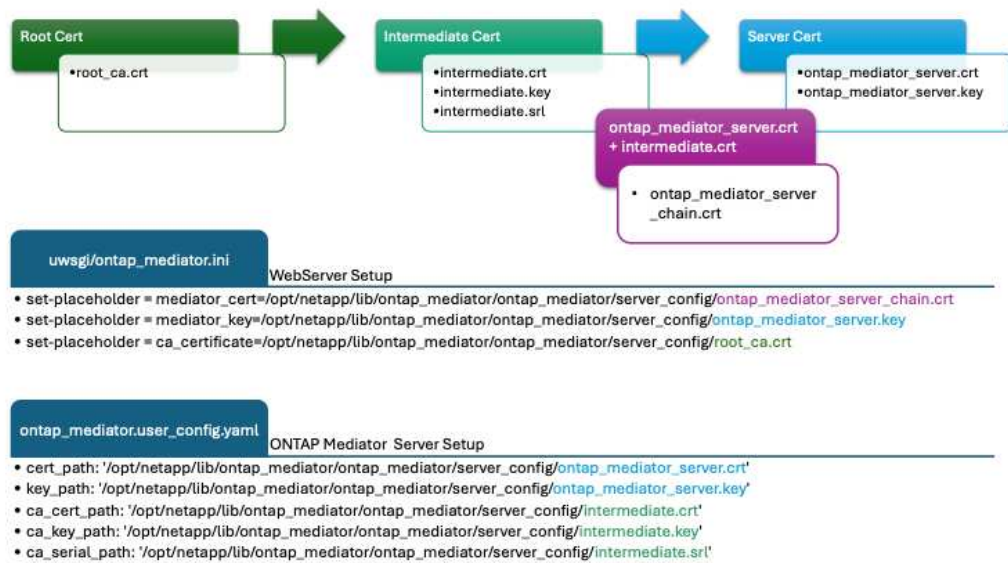
- Diese Aufgabe ist auf dem Linux-Host auszuführen, auf dem ONTAP Mediator installiert wurde.
- Diese Aufgabe können Sie durchführen, wenn die generierten selbstsignierten Zertifikate durch Zertifikate einer vertrauenswürdigen untergeordneten Zertifizierungsstelle (CA) ersetzt werden müssen. Hierfür sollte Zugriff auf eine vertrauenswürdige Public-Key-Infrastruktur (PKI) bestehen.
- Die folgende Abbildung zeigt die Zwecke der einzelnen ONTAP Mediator Zertifikate.

ONTAP Mediator Certificate Purposes



- Das folgende Bild zeigt die Konfiguration für die Webserver-Einrichtung und die ONTAP Mediator-Einrichtung.

ONTAP Mediator Certificates



Schritt 1: Ein Zertifikat von einem Drittanbieter beziehen, der ein CA-Zertifikat ausstellt.

Ein Zertifikat kann von einer PKI-Zertifizierungsstelle mit folgendem Verfahren bezogen werden.

Das folgende Beispiel veranschaulicht den Austausch der selbstsignierten Zertifikatsakteure durch die Zertifikatsakteure von Drittanbietern, die sich unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/` befinden.



Das Beispiel veranschaulicht die notwendigen Kriterien für die für ONTAP Mediator erforderlichen Zertifikate. Die Zertifikate können von einer PKI-Zertifizierungsstelle auf eine von diesem Verfahren abweichende Weise bezogen werden. Das Verfahren kann entsprechend den geschäftlichen Anforderungen angepasst werden.

ONTAP Mediator 1.9 und höher

1. Ein privater Schlüssel `intermediate.key` und eine Konfigurationsdatei `openssl_ca.cnf` werden erstellt, die von der PKI-Behörde zur Erstellung eines Zertifikats verwendet werden.
 - a. Den privaten Schlüssel `intermediate.key` generieren:

Beispiel

```
openssl genrsa -aes256 -out intermediate.key 4096
```
 - b. Die Konfigurationsdatei `openssl_ca.cnf` (zu finden unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) definiert die Eigenschaften, die das generierte Zertifikat haben muss.
2. Den privaten Schlüssel und die Konfigurationsdatei verwenden, um eine Zertifikatsignierungsanforderung zu erstellen `intermediate.csr`:

Beispiel:

```
openssl req -key <private_key_name>.key -new -out  
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@mediator_host server_config]# openssl req -key  
intermediate.key -new -config openssl_ca.cnf -out intermediate.csr  
Enter pass phrase for intermediate.key:  
[root@mediator_host server_config]# cat intermediate.csr  
-----BEGIN CERTIFICATE REQUEST-----  
<certificate_value>  
-----END CERTIFICATE REQUEST-----
```

3. Die Zertifikatsignierungsanforderung `intermediate.csr` wird zur Signierung an eine PKI-Zertifizierungsstelle gesendet.

Die PKI-Zertifizierungsstelle prüft die Anfrage und signiert die .csr, wodurch das Zertifikat intermediate.crt generiert wird. Zusätzlich muss das root_ca.crt Zertifikat, das das intermediate.crt Zertifikat von der PKI-Zertifizierungsstelle signiert hat, beschafft werden.



Für SnapMirror active sync Cluster und MetroCluster IP Konfigurationen, die ONTAP Mediator mit HTTPS verwenden, müssen Sie die intermediate.crt und root_ca.crt Zertifikate zu einem ONTAP Cluster hinzufügen. Informationen finden Sie unter ["ONTAP Mediator und Cluster für SnapMirror active sync konfigurieren"](#) und ["Den ONTAP Mediator für eine MetroCluster IP-Konfiguration konfigurieren"](#).

ONTAP Mediator 1.8 und früher

1. Ein privater Schlüssel ca.key und eine Konfigurationsdatei openssl_ca.cnf werden erstellt, die von der PKI-Behörde zur Erstellung eines Zertifikats verwendet werden.

- a. Den privaten Schlüssel ca.key generieren:

Beispiel:

```
openssl genrsa -aes256 -out ca.key 4096
```

- b. Die Konfigurationsdatei openssl_ca.cnf (zu finden unter /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf) definiert die Eigenschaften, die das generierte Zertifikat haben muss.

2. Den privaten Schlüssel und die Konfigurationsdatei verwenden, um eine Zertifikatsignierungsanforderung zu erstellen ca.csr:

Beispiel:

```
openssl req -key <private_key_name>.key -new -out  
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@mediator_host server_config]# openssl req -key ca.key -new  
-config openssl_ca.cnf -out ca.csr  
Enter pass phrase for ca.key:  
[root@mediator_host server_config]# cat ca.csr  
-----BEGIN CERTIFICATE REQUEST-----
```

```
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. Die Zertifikatsignierungsanforderung `ca.csr` wird zur Signierung an eine PKI-Zertifizierungsstelle gesendet.

Die PKI-Zertifizierungsstelle prüft die Anfrage und signiert die `.csr`, wodurch das Zertifikat `ca.crt` generiert wird. Zusätzlich muss das `root_ca.crt` Zertifikat, das das `ca.crt` Zertifikat von der PKI-Zertifizierungsstelle signiert hat, beschafft werden.



Für SnapMirror active sync Cluster müssen die `ca.crt` und `root_ca.crt` Zertifikate zu einem ONTAP Cluster hinzugefügt werden. Weitere Informationen enthält ["ONTAP Mediator und Cluster für SnapMirror active sync konfigurieren"](#).

Schritt 2: Ein Serverzertifikat wird durch Signierung mit einer Drittanbieter-CA-Zertifizierung generiert

ONTAP Mediator 1.9 und höher

Ein Serverzertifikat muss vom privaten Schlüssel `intermediate.key` und dem Drittanbieterzertifikat `intermediate.crt` signiert sein. Zusätzlich enthält die Konfigurationsdatei `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` bestimmte Attribute, die die für von OpenSSL ausgestellte Serverzertifikate erforderlichen Eigenschaften festlegen.

Die folgenden Befehle können ein Serverzertifikat generieren.

Schritte

1. Um eine Serverzertifikatsignierungsanforderung (CSR) zu generieren, wird folgender Befehl aus dem `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` Ordner ausgeführt:

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
ontap_mediator_server.csr
```

2. Um ein Serverzertifikat aus dem CSR zu generieren, wird folgender Befehl aus dem `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` Ordner ausgeführt:



Diese Dateien wurden von einer PKI-Zertifizierungsstelle bezogen. Wenn ein anderer Zertifikatsname verwendet wird, `intermediate.crt` und `intermediate.key` durch die entsprechenden Dateinamen ersetzen.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA
intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095
-req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
```

- Die `-CAcreateserial` Option wird verwendet, um die `intermediate.srl` Dateien zu generieren.

ONTAP Mediator 1.8 und früher

Ein Serverzertifikat muss vom privaten Schlüssel `ca.key` und dem Drittanbieterzertifikat `ca.crt` signiert

sein. Zusätzlich enthält die Konfigurationsdatei

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf bestimmte Attribute, die die für von OpenSSL ausgestellte Serverzertifikate erforderlichen Eigenschaften festlegen.

Die folgenden Befehle können ein Serverzertifikat generieren.

Schritte

1. Um eine Serverzertifikatsignierungsanforderung (CSR) zu generieren, wird folgender Befehl aus dem /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config Ordner ausgeführt:

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey  
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out  
ontap_mediator_server.csr
```

2. Um ein Serverzertifikat aus dem CSR zu generieren, wird folgender Befehl aus dem /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config Ordner ausgeführt:



Diese Dateien wurden von einer PKI-Zertifizierungsstelle bezogen. Wenn ein anderer Zertifikatsname verwendet wird, ca.crt und ca.key durch die entsprechenden Dateinamen ersetzen.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt  
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in  
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

- Die -CAcreateserial Option wird verwendet, um die ca.srl Dateien zu generieren.

Schritt 3: Neues Drittanbieter-CA-Zertifikat und Serverzertifikat in der ONTAP Mediator Konfiguration ersetzen

ONTAP Mediator 1.10 und höher

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei unter

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml bereitgestellt. Die Datei enthält die folgenden Attribute:

```
cert_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi  
ator_server.crt'  
key_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi  
ator_server.key'  
ca_cert_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.crt'  
ca_key_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.key'
```

```
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
te.srl'
```

- cert_path und key_path sind Serverzertifikatvariablen.
- ca_cert_path, ca_key_path und ca_serial_path sind CA-Zertifikatsvariablen.

Schritte

1. Alle intermediate.* Dateien durch die Zertifikate von Drittanbietern ersetzen.
2. Eine Zertifikatskette aus den intermediate.crt- und ontap_mediator_server.crt -Zertifikaten erstellen:

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

3. Die /opt/netapp/lib/ontap_mediator/uvicorn/config.json Datei wird aktualisiert.

Aktualisieren Sie die Werte von ssl_keyfile, ssl_certfile und ssl_ca_certs:

```
ssl_keyfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server.key
```

```
ssl_certfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server_chain.crt
```

```
ssl_ca_certs:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der ssl_keyfile`Wert ist der Schlüsselpfad in der `ontap_mediator_server.crt`Datei, was `ontap_mediator_server.key` ist.
 - Der `ssl\_certfile`Wert ist der Pfad der `ontap\_mediator\_server\_chain.crt`Datei.
 - Der `ssl\_ca\_certs`Wert ist der Pfad der `root\_ca.crt`Datei.
4. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:
 - Linux Gruppeninhaber: netapp:netapp
 - Linux-Berechtigungen: 600

5. ONTAP Mediator neu starten:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 und 1.9

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei unter /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml bereitgestellt. Die Datei enthält die folgenden Attribute:

```

cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
te.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
te.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
te.srl'

```

- cert_path und key_path sind Serverzertifikatvariablen.
- ca_cert_path, ca_key_path und ca_serial_path sind CA-Zertifikatsvariablen.

Schritte

1. Alle intermediate.* Dateien durch die Zertifikate von Drittanbietern ersetzen.
2. Eine Zertifikatskette aus den intermediate.crt- und ontap_mediator_server.crt -Zertifikaten erstellen:

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

3. Die /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini Datei wird aktualisiert.

Aktualisieren Sie die Werte von mediator_cert, mediator_key und ca_certificate:

```

set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server_chain.crt

```

```

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server.key

```

```

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt

```

- Der `mediator\_cert` Wert ist der Pfad der `ontap\_mediator\_server\_chain.crt` Datei.
- Der mediator_key value ist der Schlüsselpfad in der ontap_mediator_server.crt-Datei, der ontap_mediator_server.key ist.
- Der `ca\_certificate` Wert ist der Pfad der `root\_ca.crt` Datei.

4. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:

- Linux Gruppeninhaber: netapp:netapp
- Linux-Berechtigungen: 600

5. ONTAP Mediator neu starten:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 und früher

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` bereitgestellt. Die Datei enthält die folgenden Attribute:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- `cert_path` und `key_path` sind Serverzertifikatsvariablen.
- `ca_cert_path`, `ca_key_path` und `ca_serial_path` sind CA-Zertifikatsvariablen.

Schritte

1. Alle `ca.*` Dateien durch die Zertifikate von Drittanbietern ersetzen.
2. Eine Zertifikatskette aus den `ca.crt`- und `ontap_mediator_server.crt`-Zertifikaten erstellen:

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

3. Die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei wird aktualisiert.

Aktualisieren Sie die Werte von `mediator_cert`, `mediator_key` und `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt
```

```
set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
```

```
set-placeholder = ca_certificate =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der `mediator\_cert` Wert ist der Pfad der `ontap\_mediator\_server\_chain.crt` Datei.
 - Der mediator_key value ist der Schlüsselpfad in der ontap_mediator_server.crt-Datei, der ontap_mediator_server.key ist.
 - Der `ca\_certificate` Wert ist der Pfad der `root\_ca.crt` Datei.
4. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:
- Linux Gruppeninhaber: netapp:netapp
 - Linux-Berechtigungen: 600
5. ONTAP Mediator neu starten:

```
systemctl restart ontap_mediator
```

Schritt 4: Optional kann ein anderer Pfad oder Name für Ihre Drittanbieterzertifikate verwendet werden.

ONTAP Mediator 1.10 und höher

Sie können Zertifikate von Drittanbietern mit einem anderen Namen als `intermediate.*` verwenden oder die Zertifikate von Drittanbietern an einem anderen Ort speichern.

Schritte

1. Die

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`-Datei wird so konfiguriert, dass die Standardwerte der Variablen in der `ontap_mediator.config.yaml`-Datei überschrieben werden.

Wenn Sie `intermediate.crt` von einer PKI-Zertifizierungsstelle erhalten haben und dessen privaten Schlüssel `intermediate.key` am Speicherort `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` ablegen, sollte die `ontap_mediator.user_config.yaml` Datei wie im folgenden Beispiel aussehen:



Wenn `intermediate.crt` zum Signieren des `ontap_mediator_server.crt` Zertifikats verwendet wurde, wird die `intermediate.srl` Datei generiert. Weitere Informationen finden Sie in [Schritt 2: Ein Serverzertifikat wird durch Signierung mit einer Drittanbieter-CA-Zertifizierung generiert](#).

```
[root@mediator_host server_config]# cat  
ontap_mediator.user_config.yaml  
  
# This config file can be used to override the default settings in  
ontap_mediator.config.yaml  
# To override a setting, copy the property key from  
ontap_mediator.config.yaml to this file and  
# set the property to the desired value. e.g.,
```

```
#
# The default value for 'default_mailboxes_per_target' is 4 in
# ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
# following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

- a. Wenn eine Zertifikatsstruktur verwendet wird, bei der das `root_ca.crt` Zertifikat ein `intermediate.crt` Zertifikat bereitstellt, das das `ontap_mediator_server.crt` Zertifikat signiert, wird eine Zertifikatskette aus den `intermediate.crt` und `ontap_mediator_server.crt` Zertifikaten erstellt:



Sie sollten die `intermediate.crt` und `ontap_mediator_server.crt` Zertifikate von einer PKI-Behörde bereits früher im Verfahren erhalten haben.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

- b. Die `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` Datei wird aktualisiert.

Aktualisieren Sie die Werte von `ssl_keyfile`, `ssl_certfile` und `ssl_ca_certs`:

```
ssl_keyfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key

ssl_certfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server_chain.crt
```

```
ssl_ca_certs:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der `ssl_keyfile`-Wert ist der Schlüsselpfad in der `ontap_mediator_server.crt`-Datei, was `ontap_mediator_server.key` ist.
- Der `ssl_certfile`-Wert ist der Pfad der `ontap_mediator_server_chain.crt`-Datei.
- Der `ssl_ca_certs`-Wert ist der Pfad der `root_ca.crt`-Datei.



Für SnapMirror active sync Cluster und MetroCluster IP Konfigurationen, die ONTAP Mediator mit HTTPS verwenden, müssen Sie die `intermediate.crt` und `root_ca.crt` Zertifikate zu einem ONTAP Cluster hinzufügen. Informationen finden Sie unter ["ONTAP Mediator und Cluster für SnapMirror active sync konfigurieren"](#) und ["Den ONTAP Mediator für eine MetroCluster IP-Konfiguration konfigurieren"](#).

c. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:

- Linux Gruppeninhaber: `netapp:netapp`
- Linux-Berechtigungen: `600`

2. ONTAP Mediator wird neu gestartet, wenn die Zertifikate in der Konfigurationsdatei aktualisiert werden:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 und 1.9

Sie können Zertifikate von Drittanbietern mit einem anderen Namen als `intermediate.*` verwenden oder die Zertifikate von Drittanbietern an einem anderen Ort speichern.

Schritte

1. Die

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`-Datei wird so konfiguriert, dass die Standardwerte der Variablen in der `ontap_mediator.config.yaml`-Datei überschrieben werden.

Wenn Sie `intermediate.crt` von einer PKI-Zertifizierungsstelle erhalten haben und dessen privaten Schlüssel `intermediate.key` am Speicherort `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` ablegen, sollte die `ontap_mediator.user_config.yaml` Datei wie im folgenden Beispiel aussehen:



Wenn `intermediate.crt` zum Signieren des `ontap_mediator_server.crt` Zertifikats verwendet wurde, wird die `intermediate.srl` Datei generiert. Weitere Informationen finden Sie in [Schritt 2: Ein Serverzertifikat wird durch Signierung mit einer Drittanbieter-CA-Zertifizierung generiert](#).

```
[root@mediator_host server_config]# cat  
ontap_mediator.user_config.yaml
```

```
# This config file can be used to override the default settings in
```

```

ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'

```

- a. Wenn eine Zertifikatsstruktur verwendet wird, bei der das `root_ca.crt` Zertifikat ein `intermediate.crt` Zertifikat bereitstellt, das das `ontap_mediator_server.crt` Zertifikat signiert, wird eine Zertifikatskette aus den `intermediate.crt` und `ontap_mediator_server.crt` Zertifikaten erstellt:



Sie sollten die `intermediate.crt` und `ontap_mediator_server.crt` Zertifikate von einer PKI-Behörde bereits früher im Verfahren erhalten haben.

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

- b. Die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei wird aktualisiert.

Aktualisieren Sie die Werte von `mediator_cert`, `mediator_key` und `ca_certificate`:

```

set-placeholder = mediator_cert =

```

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt
```

```
set-placeholder = mediator_key =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
```

```
set-placeholder = ca_certificate =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der `mediator_cert`-Wert ist der Pfad der `ontap_mediator_server_chain.crt`-Datei.
- Der `mediator_key`-Wert ist der Schlüsselpfad in der `ontap_mediator_server.crt`-Datei, was `ontap_mediator_server.key` ist.
- Der `ca_certificate`-Wert ist der Pfad der `root_ca.crt`-Datei.



Für SnapMirror Business Continuity (SM-BC) Cluster müssen die `intermediate.crt` und `root_ca.crt` Zertifikate zu einem ONTAP Cluster hinzugefügt werden. Weitere Informationen unter ["ONTAP Mediator und Cluster für SnapMirror active sync konfigurieren"](#).

c. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:

- Linux Gruppeninhaber: `netapp:netapp`
- Linux-Berechtigungen: `600`

2. ONTAP Mediator wird neu gestartet, wenn die Zertifikate in der Konfigurationsdatei aktualisiert werden:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 und früher

Sie können Zertifikate von Drittanbietern mit einem anderen Namen als `ca.*` verwenden oder die Zertifikate von Drittanbietern an einem anderen Ort speichern.

Schritte

1. Die

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`-Datei wird so konfiguriert, dass die Standardwerte der Variablen in der `ontap_mediator.config.yaml`-Datei überschrieben werden.

Wenn Sie `ca.crt` von einer PKI-Zertifizierungsstelle erhalten haben und dessen privaten Schlüssel `ca.key` am Speicherort

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` ablegen, sollte die `ontap_mediator.user_config.yaml` Datei wie im folgenden Beispiel aussehen:



Wenn `ca.crt` zum Signieren des `ontap_mediator_server.crt` Zertifikats verwendet wurde, wird die `ca.srl` Datei generiert. Weitere Informationen finden Sie in [Schritt 2: Ein Serverzertifikat wird durch Signierung mit einer Drittanbieter-CA-Zertifizierung generiert](#).

```
[root@mediator_host server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- a. Wenn eine Zertifikatsstruktur verwendet wird, bei der das `root_ca.crt` Zertifikat ein `ca.crt` Zertifikat bereitstellt, das das `ontap_mediator_server.crt` Zertifikat signiert, wird eine Zertifikatskette aus den `ca.crt` und `ontap_mediator_server.crt` Zertifikaten erstellt:



Sie sollten die `ca.crt` und `ontap_mediator_server.crt` Zertifikate von einer PKI-Behörde bereits früher im Verfahren erhalten haben.

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

- b. Die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei wird aktualisiert.

Aktualisieren Sie die Werte von `mediator_cert`, `mediator_key` und `ca_certificate`:

```
set-placeholder = mediator_cert =
```

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt
```

```
set-placeholder = mediator_key =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
```

```
set-placeholder = ca_certificate =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der `mediator\_cert`Wert ist der Pfad der `ontap\_mediator\_server\_chain.crt`Datei.
- Der `mediator\_key`Wert ist der Schlüsselpfad in der `ontap\_mediator\_server.crt`Datei, was `ontap\_mediator\_server.key`ist.
- Der `ca\_certificate`Wert ist der Pfad der `root\_ca.crt`Datei.



Für SnapMirror Business Continuity (SM-BC) Cluster müssen die `ca.crt` und `root_ca.crt` Zertifikate zu einem ONTAP Cluster hinzugefügt werden. Weitere Informationen unter ["ONTAP Mediator und Cluster für SnapMirror active sync konfigurieren"](#).

c. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:

- Linux Gruppeninhaber: `netapp:netapp`
- Linux-Berechtigungen: `600`

2. ONTAP Mediator wird neu gestartet, wenn die Zertifikate in der Konfigurationsdatei aktualisiert werden:

```
systemctl restart ontap_mediator
```

Fehlerbehebung bei ONTAP Mediator Problemen im Zusammenhang mit Zertifikaten

Mit diesen Prüfungen lassen sich die Zertifikatseigenschaften bei der Fehlerbehebung von Zertifikatsproblemen überprüfen.

Zertifikatsablauf überprüfen

Mit dem folgenden Befehl lässt sich der Gültigkeitszeitraum des Zertifikats ermitteln.

ONTAP Mediator 1.9 und höher

```
[root@mediator_host server_config]# openssl x509 -in intermediate.crt  
-text -noout  
Certificate:  
    Data:  
    ...  
    Validity
```

```
Not Before: Feb 22 19:57:25 2024 GMT
```

```
Not After : Feb 15 19:57:25 2029 GMT
```

ONTAP Mediator 1.8 und früher

```
[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
    ...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

X509v3-Erweiterungen in der CA-Zertifizierung überprüfen

Mit dem folgenden Befehl lassen sich die X509v3-Erweiterungen in der CA-Zertifizierung überprüfen.

ONTAP Mediator 1.9 und höher

Die innerhalb von **v3_ca** in `openssl_ca.cnf` definierten Eigenschaften werden als X509v3 extensions in `intermediate.crt` angezeigt.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
    ...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:
```

```
keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
```

```
X509v3 Basic Constraints: critical
    CA:TRUE
X509v3 Key Usage: critical
    Digital Signature, Certificate Sign, CRL Sign
```

ONTAP Mediator 1.8 und früher

Die innerhalb von **v3_ca** in `openssl_ca.cnf` definierten Eigenschaften werden als X509v3 extensions in `ca.crt` angezeigt.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
    ...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

X509v3-Erweiterungen im Serverzertifikat und Subject Alt Names überprüfen

Die `v3_req` Eigenschaften, die in der `openssl_server.cnf` Konfigurationsdatei definiert sind, werden als X509v3 extensions im Zertifikat angezeigt.

Im folgenden Beispiel können die Variablen in den `alt_names` Abschnitten durch Ausführen der Befehle `hostname -A` und `hostname -I` auf der Linux-VM ermittelt werden, auf der ONTAP Mediator installiert ist.

Die korrekten Werte der Variablen sind beim Netzwerkadministrator zu erfragen.

ONTAP Mediator 1.9 und höher

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints          = CA:false
extendedKeyUsage          = serverAuth
keyUsage                  = keyEncipherment, dataEncipherment
subjectAltName            = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1  = 1.2.3.4
IP.2  = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
    ...

    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Extended Key Usage:
            TLS Web Server Authentication
        X509v3 Key Usage:
            Key Encipherment, Data Encipherment
        X509v3 Subject Alternative Name:
            DNS:abc.company.com, DNS:abc-v6.company.com, IP
            Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

ONTAP Mediator 1.8 und früher

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
```

```
[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints          = CA:false
extendedKeyUsage          = serverAuth
keyUsage                  = keyEncipherment, dataEncipherment
subjectAltName            = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
    ...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
                Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

Es wird überprüft, ob ein privater Schlüssel zu einem Zertifikat passt.

Es lässt sich überprüfen, ob ein bestimmter privater Schlüssel zu einem Zertifikat passt.

Die folgenden OpenSSL-Befehle werden jeweils auf den Schlüssel und das Zertifikat angewendet.

ONTAP Mediator 1.9 und höher

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
```

```
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAP Mediator 1.8 und früher

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in  
ca.key | openssl md5  
Enter pass phrase for ca.key:  
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc  
[root@mediator_host server_config]# openssl x509 -noout -modulus -in  
ca.crt | openssl md5  
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

Wenn das `-modulus`-Attribut bei beiden übereinstimmt, zeigt dies an, dass das private Schlüssel und Zertifikat Paar kompatibel ist und miteinander arbeiten kann.

Es sollte überprüft werden, ob ein Serverzertifikat von einem bestimmten CA-Zertifikat erstellt wurde.

Mit dem folgenden Befehl lässt sich überprüfen, ob das Serverzertifikat von einem bestimmten CA-Zertifikat erstellt wurde.

ONTAP Mediator 1.9 und höher

```
[root@mediator_host server_config]# openssl verify -CAfile root_ca.crt  
--untrusted intermediate.crt ontap_mediator_server.crt  
ontap_mediator_server.crt: OK  
[root@mediator_host server_config]#
```

ONTAP Mediator 1.8 und früher

```
[root@mediator_host server_config]# openssl verify -CAfile ca.crt  
ontap_mediator_server.crt  
ontap_mediator_server.crt: OK
```

Wenn die Online Certificate Status Protocol (OCSP)-Validierung verwendet wird, kann der Befehl `"openssl-verify"` genutzt werden.

Das Host-Betriebssystem für ONTAP Mediator warten

Das Host-Betriebssystem für ONTAP Mediator sollte regelmäßig gewartet werden, um eine optimale Leistung zu erzielen.

Den Host neu starten

Den Host nur neu starten, wenn die Cluster fehlerfrei sind. Cluster können auf Ausfälle nicht reagieren,

solange ONTAP Mediator offline ist. Vor dem Neustart einen Wartungszeitpunkt festlegen.

ONTAP Mediator wird während eines Neustarts automatisch wieder aufgenommen und tritt erneut in die zuvor konfigurierten Beziehungen mit ONTAP Clustern ein.

Host Paketaktualisierungen

Aktualisieren Sie jede Bibliothek oder jedes yum-Paket außer dem Kernel. Ein Neustart des Hosts ist erforderlich, damit die Änderungen wirksam werden. Vor dem Neustart des Hosts sollte ein Wartungsfenster eingeplant werden.

Wenn Sie das `yum-utils` Paket installieren, kann mit dem `needs-restarting` Befehl geprüft werden, ob Paketänderungen einen Neustart erfordern.

Nach der Aktualisierung der ONTAP Mediator Abhängigkeiten ist ein Neustart erforderlich, da die Änderungen nicht sofort wirksam werden.

Der Kernel des Host-Betriebssystems wird aktualisiert.

SCST muss für den verwendeten Kernel kompiliert werden. Für die Aktualisierung des Betriebssystems ist eine Wartungszeit einzuplanen.

Bevor Sie beginnen

Folgende Anforderungen gelten, wenn das SCST-Paket mit ONTAP Mediator installiert wird.

- Alle Bibliothekspakete außer dem Kernel können aktualisiert werden, jedoch ist möglicherweise ein Neustart erforderlich, um Änderungen im ONTAP Mediator anzuwenden. Bei einem erforderlichen Neustart sollte eine Ausfallzeit eingeplant werden.
- Der Betriebssystemkern sollte auf dem neuesten Stand gehalten werden. Der Kernel sollte auf eine unterstützte Version aktualisiert werden, die in der "[ONTAP Mediator Versionsmatrix](#)" aufgeführt ist. Da ein Neustart des Systems erforderlich ist, sollte ein Wartungsfenster für die Ausfallzeit eingeplant werden.
 - Das SCST-Kernelmodul sollte vor dem Neustart deinstalliert und danach wieder installiert werden.
 - Eine unterstützte Version von SCST sollte zur erneuten Installation bereitliegen, bevor das Kernel-OS-Upgrade begonnen wird.



Wenn Sie ONTAP Mediator 1.12 oder höher mit reiner HTTPS-Unterstützung installiert haben, wird das SCST-Paket nicht installiert und der Kernel des Host-Betriebssystems kann aktualisiert werden, ohne ONTAP Mediator zu beeinträchtigen. Weitere Informationen zur Aktualisierung finden Sie in der Dokumentation Ihres Host-Betriebssystems.

Schritte

Führen Sie diese Schritte aus, um den Kernel des Host-Betriebssystems zu aktualisieren.



Vor dem Upgrade des Kernels prüfen, ob das Betriebssystem und die ONTAP Mediator-Version kompatibel sind. Für unterstützte Versionen siehe die "[OS Support-Matrix](#)".

1. ONTAP Mediator wird gestoppt.
2. Das SCST-Paket deinstallieren, siehe [Hostwartung durchführen](#). (SCST bietet keinen Upgrade-Mechanismus.)
3. Das Betriebssystem wird aktualisiert und der Computer neu gestartet.

4. Das SCST Paket wird erneut installiert.
5. ONTAP Mediator erneut aktivieren.

Hostwartung durchführen

Ein Upgrade des VM-Kernels kann Kompatibilitätsprobleme mit SCST-Modulen verursachen. SCST manuell deinstallieren und erneut installieren.



Wenn Sie ONTAP Mediator 1.12 oder höher mit Unterstützung nur für HTTPS installiert haben, wird das SCST-Paket nicht installiert und Sie können diese Aufgabe überspringen.

Schritt 1: SCST deinstallieren

Zum Deinstallieren von SCST das Tar-Paket für Ihre ONTAP Mediator Version verwenden.

Schritte

1. Laden Sie das entsprechende SCST Paket (wie in der folgenden Tabelle dargestellt) herunter und extrahieren Sie es.

Für diese Version ...	Dieses Tar-Bundle kann verwendet werden...
ONTAP Mediator 1.12.1	scst-3.10.tar.gz
ONTAP Mediator 1.12	scst-3.10.tar.gz
ONTAP Mediator 1.11	scst-3.9.tar.gz
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAP Mediator 1.9.1	scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	scst-3.5.0.tar.bz2
ONTAP Mediator 1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	scst-3.3.0.tar.bz2

- a. Auf das Open-Source-Paket kann über die "[SCST SourceForge Downloads](#)" zugegriffen werden.
 - b. **Veröffentlichte Versionen herunterladen** auswählen.
 - c. Das Paket auf die VM extrahieren.
2. Die folgenden Deinstallationsbefehle sind im `scst` Verzeichnis auszuführen:
 - a. `systemctl stop mediator-scst`
 - b. `make scstadm_uninstall`
 - c. `make iscsi_uninstall`

- d. `make usr_uninstall`
- e. `make scst_uninstall`
- f. `depmod`

Schritt 2: Installation von SCST

Für die manuelle Installation von SCST benötigen Sie das SCST Tar-Bundle, das für die installierte Version von ONTAP Mediator verwendet wird (siehe die [SCST-Tabelle](#)).

Über diese Aufgabe

- Führen Sie diesen Schritt vor der Installation des ONTAP Mediator aus. Wenn die von Ihnen verwendete SCST-Version neuer ist als die im ONTAP Mediator Installer enthaltene Version, wird dieser Schritt vom Installer übersprungen.
- In einigen Szenarien kann die Standardinstallation von SCST auf dem aktualisierten Betriebssystem fehlschlagen, da das aktualisierte Betriebssystem einen Patch benötigt.

Ab ONTAP Mediator 1.12.1 kann bei einem Installationsfehler das SCST-Reparaturtool, das sich in `/usr/local/bin/mediator_repair_scst` befindet, zur Reparatur der Installation verwendet werden.

Falls das aktualisierte Betriebssystem einen Patch benötigt, enthält das Tool diesen für die im ONTAP Mediator Paket enthaltene SCST-Version. Das `mediator_repair_scst` Tool ist ein Standalone-Tool, das vom Hauptinstallationsprogramm getrennt ist und in der ONTAP Mediator `tgz` Datei enthalten ist. Die ONTAP Mediator Installation oder Upgrade-Pfade werden dadurch nicht beeinflusst.

Schritte

1. Führen Sie die folgenden Installationsbefehle im `scst` Verzeichnis aus:

- a. `make 2release`
- b. `make scst_install`
- c. `make usr_install`
- d. `make iscsi_install`
- e. `make scstadm_install`
- f. `depmod`



Wenn Sie eine Erstinstallation durchführen und ONTAP Mediator vorinstallieren möchten, führen Sie den folgenden Befehl aus, bevor Sie mit dem nächsten Schritt fortfahren:

```
mkdir -p  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

- g. `cp scst/src/certs/scst_module_key.der
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`
- h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`



Wenn Sie SCST vor ONTAP Mediator bei einer Erstinstallation vorinstallieren, kann dieser Schritt übersprungen werden. Das Installationsprogramm wendet die relevanten

2. Optional: Falls Secure Boot aktiviert ist, sind vor dem Neustart die folgenden Schritte auszuführen:

a. Bestimmen Sie die jeweiligen Dateinamen für die `scst_vdisk`, `scst` und `iscsi_scst` Module:

```
[root@localhost ~]# modinfo -n scst_vdisk
[root@localhost ~]# modinfo -n scst
[root@localhost ~]# modinfo -n iscsi_scst
```

b. Die Kernel-Version ermitteln:

```
[root@localhost ~]# uname -r
```

c. Jede Moduldatei mit dem Kernel signieren:

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
_module-filename_
```

d. Den UEFI-Schlüssel zusammen mit der Firmware installieren.

Die Anweisungen zur Installation des UEFI-Schlüssels befinden sich unter:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

Der generierte UEFI Schlüssel befindet sich unter:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

3. Das System neu starten:

```
reboot
```

Änderungen am Hostnamen oder an der IP

Über diese Aufgabe

- Diese Aufgabe ist auf dem Linux-Host auszuführen, auf dem ONTAP Mediator installiert wurde.
- Dies ist nur erforderlich, wenn die selbstsignierten Zertifikate nicht mehr gültig sind, weil sich der Hostname oder die IP-Adresse nach der Installation von ONTAP Mediator geändert hat.

- Nachdem das temporäre selbstsignierte Zertifikat durch ein vertrauenswürdiges Zertifikat eines Drittanbieters ersetzt wurde, wird diese Aufgabe *nicht* verwendet, um ein Zertifikat erneut zu generieren. Wenn kein selbstsigniertes Zertifikat vorhanden ist, kann dieses Verfahren nicht verwendet werden.

Schritt

Ein temporäres selbstsigniertes Zertifikat für den aktuellen Host erstellen:

1. ONTAP Mediator neu starten:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

ONTAP Mediator deinstallieren

Falls erforderlich, können Sie ONTAP Mediator deinstallieren, nachdem Sie die Verbindung zu ONTAP getrennt haben.

Bevor Sie beginnen

ONTAP Mediator muss von ONTAP getrennt werden, bevor er entfernt wird.

Über diese Aufgabe

Diese Aufgabe ist auf dem Linux-Host auszuführen, auf dem ONTAP Mediator installiert wurde.

Falls Sie diesen Befehl nicht erreichen können, ist es möglicherweise erforderlich, den Befehl mit dem vollständigen Pfad auszuführen, wie im folgenden Beispiel gezeigt:

```
/usr/local/bin/uninstall_ontap_mediator
```

Schritt

1. ONTAP Mediator deinstallieren:

```
uninstall_ontap_mediator
```

```
[root@mediator-host ~]# uninstall_ontap_mediator

ONTAP Mediator: Self Extracting Uninstaller

+ Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
+ Remove successful.
[root@mediator-host ~]#
```

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.

ONTAP Mediator für MetroCluster IP und SnapMirror active sync

- ["Hinweis für ONTAP Mediator 1.12.1"](#)
- ["Hinweis für ONTAP Mediator 1.11"](#)
- ["Hinweis für ONTAP Mediator 1.10"](#)
- ["Hinweis für ONTAP Mediator 1.9.1"](#)
- ["Hinweis für ONTAP Mediator 1.8"](#)
- ["Hinweis für ONTAP Mediator 1.7"](#)
- ["Hinweis für ONTAP Mediator 1.5"](#)

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.