ONTAP Mediator für MetroCluster und SnapMirror Active Sync

ONTAP 9

NetApp
February 12, 2026

Inhalt

ONTAP Mediator für MetroCluster und SnapMirror Active Sync . . . 1
Erfahren Sie mehr über ONTAP Mediator . . . 1
Für den Systemadministrator bereitgestellte Tools . . . 1
Besondere Hinweise . . . 2
Neue Funktionen in ONTAP Mediator . . . 2
Vorgestellt Werden . . . 2
OS Support-Matrix . . . 4
SCST Support-Matrix . . . 7
Installation oder Upgrade . . . 8
Zusammenfassung des Installationsablaufs von ONTAP Mediator . . . 8
Installieren oder aktualisieren Sie ONTAP Mediator . . . 9
Aktualisieren Sie das Host-Betriebssystem und den ONTAP Mediator . . . 15
Bereitstellung von Repository-Zugriff für die Installation von ONTAP Mediator . . . 20
Laden Sie das Installationspaket für ONTAP Mediator herunter . . . 27
Überprüfen Sie die ONTAP Mediator-Code-Signatur . . . 28
Installieren Sie das Installationspaket für den ONTAP Mediator . . . 30
Überprüfen Sie den Installationsstatus des ONTAP Mediators . . . 46
Konfiguration des ONTAP Mediators nach der Installation . . . 47
ONTAP Mediator verwalten . . . 52
Ändern Sie den Benutzernamen . . . 52
Ändern Sie das Passwort . . . 53
Stoppen Sie ONTAP Mediator . . . 54
ONTAP Mediator erneut aktivieren . . . 54
Überprüfen Sie, ob ONTAP Mediator fehlerfrei ist . . . 55
Deinstallieren Sie ONTAP Mediator . . . 56
Erstellen Sie ein temporäres selbstsigniertes Zertifikat neu . . . 57
Ersetzen Sie selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern . . . 58
Fehlerbehebung bei zertifikatbezogenen Problemen . . . 76
Warten Sie das Host-Betriebssystem für ONTAP Mediator . . . 83
Starten Sie den Host neu . . . 83
Updates des Host-Pakets . . . 83
Aktualisieren Sie den Kernel des Host-Betriebssystems. . . . 83
Durchführen von Host-Wartungsarbeiten . . . 83
Host ändert sich zum Hostnamen oder IP . . . 86

ONTAP Mediator für MetroCluster und SnapMirror Active Sync

Erfahren Sie mehr über ONTAP Mediator

Diese Dokumentation bezieht sich auf die On-Premise-Version von ONTAP Mediator. Informationen zum ONTAP Cloud Mediator, verfügbar ab ONTAP 9.17.1, finden Sie im "SnapMirror Active Sync-Dokumentation" .

ONTAP Mediator bietet mehrere Funktionen für ONTAP-Features:

- Persistenter Speicher mit Fencing für HA-Metadaten
- Dient als Ping-Proxy für Controller-Lebendigkeit.
- Bietet synchrone Funktionen für die Integritätsabfrage von Nodes zur Unterstützung der Quorumbestimmung.

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 Passwort angegeben werden.

- **`/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`**

  Generiert eine lokale tgz-Datei mit allen nützlichen Support-Informationen, die für die Kommunikation mit dem NetApp Kunden-Support benötigt werden. Dazu gehören Anwendungskonfiguration, Protokolle und einige Systeminformationen. Die Bundles werden auf der lokalen Festplatte generiert und können bei Bedarf manuell übertragen werden. Speicherort: /Opt/netapp/Data/Support_Bundles/

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

  Entfernt das Paket ONTAP Mediator und das SCST-Kernelmodul. Dies schließt sämtliche Konfigurations-,

Protokoll- und Mailbox-Daten ein.

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

  Gibt eine Sperre für das API-Benutzerkonto frei, wenn das Limit für Authentifizierungsversuche erreicht wurde. Diese Funktion wird verwendet, um die Herleitung von Brute Force-Passwörtern zu verhindern. Der Benutzer wird aufgefordert, den richtigen Benutzernamen und das richtige Passwort einzugeben.

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

  (Nur Support) wird verwendet, um den API-Benutzer bei der Installation hinzuzufügen.

Besondere Hinweise

ONTAP Mediator setzt bei der iSCSI-Bereitstellung auf SCST (siehe http://scst.sourceforge.net/index.html). Dieses Paket ist ein Kernelmodul, das während der Installation speziell für den Kernel kompiliert wird. Für Aktualisierungen des Kernels muss SCST möglicherweise neu installiert werden. Alternativ können Sie ONTAP Mediator deinstallieren und anschließend erneut installieren und anschließend die ONTAP-Beziehung neu konfigurieren.

> Alle Aktualisierungen des Server-OS-Kernels sollten mit einem Wartungsfenster in ONTAP koordiniert werden.

Neue Funktionen in ONTAP Mediator

Mit jeder Version werden neue Verbesserungen für ONTAP Mediator bereitgestellt. Was ist neu?

Vorgestellt Werden

Informationen zur SCST-Version finden Sie im SCST Support-Matrix.

Version des ONTAP Mediators	Vorgestellt Werden
1,11	• Unterstützung für RHEL: ◦ Kompatibel: 9.5. ◦ Empfohlen: 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. • Fügt Unterstützung für IPv6 für MetroCluster IP-Konfigurationen hinzu. • Fügt Unterstützung für fapolicyd hinzu.

1,10	• Unterstützung für RHEL: ◦ Kompatibel: 9.5. ◦ Empfohlen: 10.0, 9.6, 9.4 und 8.10. • Unterstützung für Rocky Linux 10.0, 9.6 und 8.10. • Aktualisiert die Basis-Python-Version von Python 3.9 auf Python 3.12.
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 Code-Signaturprüfungen mithilfe der `-skip-code-signature-check` Flagge. • 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. • Performance-Verbesserungen für mehr Skalierbarkeit. • Verbesserte Dateinamen, um die Einrichtung von PKI-signierten Zertifikaten zu vereinfachen.
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 von SAN-Daten (Subject Alternative Name) 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. • Nicht mehr unterstützte RHEL 7.x/CentOS-Versionen.
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 Abschreibungswarnungen 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. • Zusätzliche Unterstützung für Secure Boot (SB) der UFEI-basierten Firmware.
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. • Eliminiert Perl-Abhängigkeiten.
1,0	• Unterstützung von iSCSI-Mailboxen. • Zur Verwendung mit ONTAP 9.7+ MCC-IP AUSO. • Unterstützung für RHEL/CentOS 7.6.

OS Support-Matrix

Betriebssystem für ONTAP Mediator	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 10,1	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 10.0	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,7	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9.6	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,5	Kompatibel	Kompatibel	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,4	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,3	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,2	Nein	Nein	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,1	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,0	Nein	Nein	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8.10	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8,9	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8,8	Nein	Nein	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein

RHEL 8,7	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8,6	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8,5	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein
RHEL 8,4	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein
RHEL 8,3	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Nein	Nein	Nein
RHEL 8,2	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Nein	Nein	Nein
RHEL 8,1	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Nein	Nein
RHEL 8,0	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Ja.	Nein
RHEL und CentOS 7.9	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Kompatibel	Nein	Nein
RHEL und CentOS 7.8	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	Ja.	Ja.	Ja.	Ja.	Nein	Nein
RHEL und CentOS 7.6	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	1. A.	1. A.	1. A.
Rocky Linux 10,0	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Rocky Linux 9	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	1. A.	1. A.	1. A.	1. A.	1. A.	1. A.
Rocky Linux 8	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	1. A.	1. A.	1. A.	1. A.	1. A.	1. A.
Oracle Linux 10,0	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Oracle Linux 9	Ja.	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 und unterstützt ist.
- „Nein“ bedeutet, dass Betriebssystem und ONTAP Mediator nicht kompatibel sind.
- „Kompatibel“ bedeutet, dass Red Hat diese RHEL-Versionen nicht mehr unterstützt, ONTAP Mediator jedoch weiterhin darauf installiert werden kann.
- ONTAP Mediator 1.6 fügt Unterstützung für Rocky Linux 9 und 8 hinzu.
- ONTAP Mediator 1.5 war die letzte unterstützte Version für RHEL 7.x-Filialbetriebssysteme.
- CentOS 8 wurde für alle Versionen entfernt, da es erneut verzweigt wurde. CentOS Stream wurde als nicht geeignetes Produktionsziel-OS angesehen. Es ist keine Unterstützung geplant.

SCST Support-Matrix

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

Version des ONTAP Mediators	Unterstützte SCST Version
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

Version des ONTAP Mediators	Unterstützte SCST Version
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

Installation oder Upgrade

Zusammenfassung des Installationsablaufs von ONTAP Mediator

Die Installation von ONTAP Mediator umfasst die Vorbereitung der Installation, die Bereitstellung des Zugriffs auf Repositorys, das Herunterladen des Installationspakets, die Überprüfung der Codesignatur, die Installation des ONTAP Mediator-Pakets und die Durchführung von Konfigurationsaufgaben nach der Installation.

"Vorbereiten der Installation oder Aktualisierung von ONTAP Mediator"

Um ONTAP Mediator zu installieren oder zu aktualisieren, müssen Sie sicherstellen, dass alle Voraussetzungen erfüllt sind.

"Upgrade von Host-Betriebssystem und Mediator"

Wenn Sie eine vorhandene Version von ONTAP Mediator aktualisieren, müssen Sie zuerst die vorherige Version deinstallieren und dann die neue Version installieren. Wenn Sie ONTAP Mediator zum ersten Mal installieren, können Sie diesen Schritt überspringen.

"Gewähren von Repository-Zugriff"

Sie sollten den Zugriff auf Repositorys aktivieren, damit ONTAP Mediator während des Installationsvorgangs auf die erforderlichen Pakete zugreifen kann.

"Laden Sie das Installationspaket für ONTAP Mediator herunter"

Laden Sie das ONTAP Mediator-Installationspaket von der ONTAP Mediator-Downloadseite herunter.

5 **"Überprüfen Sie die Codesignatur des ONTAP Mediator-Installationspakets"**

NetApp empfiehlt, die Codesignatur des ONTAP Mediators zu überprüfen, bevor Sie das ONTAP Mediator-Installationspaket installieren.

6 **"Installieren Sie ONTAP Mediator"**

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

7 **"Überprüfen Sie die ONTAP Mediator-Installation"**

Überprüfen Sie nach der Installation von ONTAP Mediator, ob es erfolgreich ausgeführt wird.

8 **"Durchführen von Konfigurationsaufgaben nach der Installation"**

Nachdem ONTAP Mediator installiert und ausgeführt wird, müssen zusätzliche Konfigurationsaufgaben ausgeführt werden, um die Funktionen von ONTAP Mediator zu verwenden.

Installieren oder aktualisieren Sie ONTAP Mediator

Um ONTAP Mediator zu installieren oder zu aktualisieren, müssen Sie alle Voraussetzungen erfüllen, das Installationspaket herunterladen und das Installationsprogramm auf dem Host ausführen.

- Ab ONTAP 9.8 können Sie jede Version von ONTAP Mediator verwenden, um eine aktive SnapMirror Sync Beziehung zu überwachen.
- Sie können jede Version von ONTAP Mediator verwenden, um eine MetroCluster -IP-Konfiguration zu überwachen.

Überlegungen zur Installation und zum Upgrade

Bitte beachten Sie diese Punkte, bevor Sie ONTAP Mediator aktualisieren oder installieren.

> ONTAP Mediator 1.8 und ältere Versionen sind nicht mit dem FIPS-Modus von Red Hat Enterprise Linux (RHEL) kompatibel und verhindern daher eine erfolgreiche Installation. Sie können mit folgendem Befehl überprüfen, ob der FIPS-Modus aktiviert ist: `fips-mode-setup --check` Befehl. Sie können den FIPS-Modus deaktivieren, indem Sie `fips-modesetup --disable` Befehl. Führen Sie nach dem Deaktivieren des FIPS-Modus einen Neustart durch, um ONTAP Mediator 1.8 oder früher erfolgreich zu installieren.

- Sie sollten ONTAP Mediator auf die neueste Version aktualisieren. Ältere Versionen funktionieren weiterhin mit allen ONTAP Releases, neuere Versionen enthalten jedoch Sicherheitspatches für Drittanbieterkomponenten.
- Wenn Sie ein Upgrade auf eine neue ONTAP Mediator-Version durchführen, wird das Installationsprogramm automatisch auf die empfohlene SCST-Version aktualisiert, sofern keine höhere Version verfügbar ist. Anweisungen zur manuellen Installation einer höheren SCST-Version finden Sie unter "ONTAP Mediator verwalten". Informationen zu unterstützten Versionen finden Sie im "SCST

Support-Matrix".

- Falls die Installation fehlschlägt, müssen Sie möglicherweise auf eine neuere Version von ONTAP Mediator aktualisieren.
- Ab dem 15. Juni 2025 können Sie ONTAP Mediator 1.9 und 1.8 nicht mehr installieren oder aktualisieren, da deren Code Signing-Zertifikate abgelaufen sind. Wenn die Installation oder das Upgrade fehlschlägt, verwenden Sie stattdessen die Patch-Version von ONTAP Mediator 1.9.1.

- 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.

Host-Anforderungen erfüllt

Befolgen Sie diese Anforderungen, wenn Sie RHEL oder Rocky Linux installieren und die zugehörigen Repositories konfigurieren.

Wenn Sie den Installations- oder Konfigurationsprozess ändern, müssen Sie möglicherweise weitere Schritte ausführen.

Anforderungen für die Linux-Distribution

- Installieren Sie RHEL oder Rocky Linux gemäß den Best Practices von Red Hat. Da CentOS 8.x das Ende seines Lebenszyklus erreicht hat, werden kompatible Versionen von CentOS 8.x nicht empfohlen.
- Stellen Sie bei der Installation von ONTAP Mediator sicher, dass das System Zugriff auf das erforderliche Repository hat, damit das Installationsprogramm alle erforderlichen Softwareabhängigkeiten abrufen und installieren kann.
- Um dem yum-Installer zu ermöglichen, abhängige Software in den RHEL-Repositorys zu finden, registrieren Sie das System während der Installation oder danach mit einer gültigen Red hat Subskription.

Weitere Informationen finden Sie in der Dokumentation zu Red hat Subscription Manager.

Netzwerkanforderungen

Stellen Sie sicher, dass die folgenden Ports für ONTAP Mediator verfügbar und nicht verwendet werden:

Port/Services	Quelle	Richtung	Ziel	Zweck
22/tcp	Management-Host	Eingehend	ONTAP Mediator	(Optional) SSH / ONTAP Mediatormanagement
31784/tcp	Cluster-Management-LIFs	Eingehend	Web-Server ONTAP Mediator	(ERFORDERLICH) REST-API (HTTPS)

3260/tcp [1]	Node-Daten-LIFs oder Node-Management-LIFs	Bidirektional	ONTAP Mediator iSCSI-Ziele	(Erforderlich für MetroCluster IP-Konfigurationen) iSCSI-Datenverbindung für Mailboxen

Für SMBC-Kunden muss für ONTAP Port 3260 nicht aktiviert oder verbunden sein.

- Wenn Sie eine Firewall eines Drittanbieters verwenden, siehe"Firewall-Anforderungen für ONTAP Mediator" Die
- Stellen Sie bei Linux-Hosts ohne Internetzugang sicher, dass die erforderlichen Pakete in einem lokalen Repository verfügbar sind.

  Wenn Sie Link Aggregation Control Protocol (LACP) in einer Linux-Umgebung verwenden, konfigurieren Sie den Kernel und setzen Sie den `sysctl net.ipv4.conf.all.arp_ignore` auf `2`.

Anforderungen an das Betriebssystem

Ihr Betriebssystem muss die folgenden Anforderungen erfüllen:

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

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

Version des ONTAP Mediators	Unterstützte Linux-Versionen
1,11	• Red Hat Enterprise Linux ◦ Kompatibel: 9.5 [1] ◦ Empfohlen: 10.1, 10.0, 9.7, 9.6, 9.4 und 8.10 • Rocky Linux 10,1, 9.7 und 8.10 • Oracle Linux 10.0 und 9.6
1,10	• Red Hat Enterprise Linux ◦ Kompatibel: 9.5 [1] ◦ Empfohlen: 10,0, 9,6, 9,4 und 8,10 • Rocky Linux 10,0, 9.6 und 8.10

1.9.1	• Red Hat Enterprise Linux ◦ Kompatibel: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.5, 9.4, 9.2, 9.0, 8.10 und 8.8 • Rocky Linux 9.5 und 8.10
1,9	• Red Hat Enterprise Linux ◦ Kompatibel: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.5, 9.4, 9.2, 9.0, 8.10 und 8.8 • Rocky Linux 9.5 und 8.10
1,8	• Red Hat Enterprise Linux: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 und 8.8 • Rocky Linux 9.4 und 8.10
1,7	• Red Hat Enterprise Linux: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.3, 9.2, 9.1, 9.0, 8.9 und 8.8 • Rocky Linux 9.3 und 8.9
1,6	• Red Hat Enterprise Linux: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.2, 9.1, 9.0 und 8.8 • Rocky Linux 9.2 und 8.8
1,5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6
1,4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6
1,3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6
1,2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6

1. Kompatibel bedeutet, dass Red Hat diese RHEL-Versionen nicht mehr unterstützt, ONTAP Mediator jedoch weiterhin darauf installiert werden kann.

BS-erforderliche Pakete

Die folgenden Pakete werden von ONTAP Mediator benötigt:

Die Pakete werden entweder vorinstalliert oder automatisch vom ONTAP Mediator Installer 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 • Make • Libselinux-utils • Patch • bzip2 • perl-Data-Dumper • perl-ExtUtils-MakeuMaker • Efibootmgr • Mokutil	• python3.12 • python3.12-devel	• Elfutils-libelf-devel • Politicoreutils-Python-utils • python3 • python3-devel	• Elfutils-libelf-devel • Politicoreutils-Python-utils • Redhat-lsb-Core • Python39 • Python39-devel

Das Mediator-Installationspaket ist eine selbst extrahierende komprimierte tar-Datei, die Folgendes enthält:

- Eine RPM-Datei, die alle Abhängigkeiten enthält, die nicht aus dem Repository des unterstützten Release abgerufen werden können.
- Ein Installationsskript.

Ein gültiges SSL-Zertifikat wird empfohlen.

Überlegungen zum Betriebssystem-Upgrade und zur Kernel-Kompatibilität

- Sie können alle Bibliothekspakete außer dem Kernel aktualisieren, aber möglicherweise müssen Sie das System neu starten, um die Änderungen im ONTAP Mediator anzuwenden. Planen Sie Ausfallzeiten ein, falls ein Neustart erforderlich ist.
- Sie sollten den Betriebssystemkernel auf dem neuesten Stand halten. Aktualisieren Sie den Kernel auf eine unterstützte Version, die in der Liste aufgeführt ist."ONTAP Mediator-Versionsmatrix" Die Das System muss neu gestartet werden, planen Sie daher ein Wartungsfenster für den Ausfall ein.
  - Deinstallieren Sie das SCST-Kernelmodul vor dem Neustart und installieren Sie es anschließend wieder.
  - Halten Sie eine unterstützte Version von SCST bereit, die Sie vor dem Kernel-OS-Upgrade neu installieren können.

- 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 wahrscheinlich nicht funktionieren wird.

Installieren Sie ONTAP Mediator, 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 den UEFI-sicheren Start vor der Installation von ONTAP Mediator deaktivieren, wenn dieser nicht benötigt wird oder wenn Sie Probleme bei der Installation von ONTAP Mediator beheben. Deaktivieren Sie die UEFI Secure Boot-Option in den Computereinstellungen.

Detaillierte Anweisungen zum Deaktivieren des UEFI Secure Boot finden Sie in der Dokumentation zu Ihrem Host-Betriebssystem.

Um ONTAP Mediator mit aktiviertem UEFI Secure Boot zu installieren, müssen Sie einen Sicherheitsschlüssel registrieren, bevor der Dienst gestartet werden kann. Der Schlüssel wird während des Kompilierungsschritts der SCST-Installation generiert und als privates öffentliches Schlüsselpaar auf Ihrer Maschine gespeichert. Verwenden Sie das `mokutil` Dienstprogramm, um den öffentlichen Schlüssel als Machine Owner Key (MOK) zu Ihrer UEFI-Firmware hinzuzufügen, sodass das System dem signierten Modul vertrauen und laden kann. Speichern Sie die `mokutil` Passphrase an einem sicheren Ort, da dies erforderlich ist, wenn Sie Ihr System neu starten, um das MOK zu aktivieren.

Schritte

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

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

   Die Ergebnisse zeigen an, ob UEFI Secure Boot auf diesem System aktiviert ist.

Wenn…	Gehe zu…
UEFI Secure Boot ist aktiviert	
UEFI Secure Boot ist deaktiviert	"Aktualisieren Sie das Host-Betriebssystem und dann ONTAP Mediator"

   - Sie werden aufgefordert, eine Passphrase zu erstellen, die Sie an einem sicheren Ort speichern 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. Wenn das `mokutil` Dienstprogramm nicht installiert ist, führen Sie den folgenden Befehl aus:

   ```
   yum install mokutil
   ```

Aktualisieren Sie das Host-Betriebssystem und den ONTAP Mediator

Um das Host-Betriebssystem für ONTAP Mediator auf eine neuere Version zu aktualisieren, müssen Sie ONTAP Mediator zuerst deinstallieren.

Über diese Aufgabe

Vor dem Upgrade des Host-Betriebssystems für ONTAP Mediator mit dem leapp-upgrade-Tool muss ONTAP Mediator deinstalliert werden. Das Tool prüft, ob in 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 das Installationsprogramm die Datei entpackt, anstatt sie aus einem registrierten Repository herunterzuladen, kann das Tool kein Upgrade finden. Sie müssen das Tool leapp-upgrade verwenden, um das Paket zu deinstallieren.

Schritte

1. Sichern Sie die Protokolldateien:

```
[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. Führen Sie das Upgrade mit dem leapp-upgrade-Tool durch:

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<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:

Führen Sie die restlichen Schritte unmittelbar nach der Neuinstallation von ONTAP Mediator aus, um einen Verlust von Protokolldateien zu verhindern.

```
[rootmediator-host ~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. Stoppen Sie ontap_mediator:

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

5. Ersetzen Sie die Protokolldateien:

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

6. Start ontap_mediator:

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

7. Verbinden Sie alle ONTAP Cluster wieder mit dem aktualisierten ONTAP Mediator:

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
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
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 keine Neuinstallation der außerhalb von /opt/netapp gespeicherten TLS-Zertifikate erforderlich. Sichern und stellen Sie die in /opt/netapp gespeicherten Zertifikate wieder her.

```
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
                            Owning
Job ID Name                 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
  ..<snip ONTAP Mediator CA public key>..

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
..<snip ONTAP Mediator CA public key>..


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
                            Owning
Job ID Name                 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 hinzufügen"
- "SnapMirror Mediator entfernen"
- "Speicher-ISCSI-Initiator anzeigen"

Bereitstellung von Repository-Zugriff für die Installation von ONTAP Mediator

Sie sollten den Zugriff auf Repositorys aktivieren, damit ONTAP Mediator während des Installationsvorgangs auf die erforderlichen Pakete zugreifen kann.

Schritte

1. Legen Sie fest, auf welche Repositorys zugegriffen werden muss, wie in der folgenden Tabelle dargestellt:

Wenn Ihr Betriebssystem…	Zugriff auf diese Repositorys ist erforderlich…
RHEL 10.x	• rhel-10-für-x86_64-baseos-rpms • rhel-10-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-für-x86_64-baseos-eff • rhel-9-für-x86_64-appstream-Effektivwert
RHEL 8.x	• rhel-8-für-x86_64-baseos-eff • rhel-8-für-x86_64-appstream-Effektivwert
RHEL 7.x	• rhel-7-Server-fakultative-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 Installationsvorgangs auf die erforderlichen Pakete zugreifen kann.

Wenn ONTAP Mediator Abhängigkeiten von Python-Modulen in den Repositories "Extras" und "Optional" hat, muss er möglicherweise auf die `rhel-X-for-x86_64-extras-rpms` Und `rhel-X-for-x86_64-optional-rpms` Dateien.

Vorgehensweise für das Betriebssystem RHEL 10.x

Verwenden Sie dieses Verfahren, wenn Ihr Betriebssystem **RHEL 10.x** ist, um den Zugriff auf Repositorys zu ermöglichen:

Schritte

1. Abonnieren Sie das erforderliche Repository:

```
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.
```

2. Führen Sie den `yum repolist` Befehl aus.

Die neu abonnierten Repositories sollten in der Liste angezeigt werden.

Verfahren für das RHEL 9.x-Betriebssystem

Gehen Sie folgendermaßen vor, wenn Ihr Betriebssystem **RHEL 9.x** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

1. Abonnieren Sie das erforderliche Repository:

```
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.
```

2. Führen Sie den `yum repolist` Befehl aus.

Die neu abonnierten Repositories sollten in der Liste angezeigt werden.

Verfahren für das RHEL 8.x-Betriebssystem

Gehen Sie folgendermaßen vor, wenn Ihr Betriebssystem **RHEL 8.x** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

1. Abonnieren Sie das erforderliche Repository:

```
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.
```

2. Führen Sie den `yum repolist` Befehl aus.

Die neu abonnierten Repositories sollten in der Liste angezeigt werden.

Verfahren für das RHEL 7.x-Betriebssystem

Gehen Sie folgendermaßen vor, wenn Ihr Betriebssystem **RHEL 7.x** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

1. Abonnieren Sie das erforderliche Repository:

```
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.
```

2. Führen Sie den `yum repolist` Befehl aus.

Das folgende Beispiel zeigt die Ausführung dieses Befehls. In der Liste sollte das Repository „RHEL-7-Server-fakultative-rpms“ 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 ~]#
```

Verfahren für das Betriebssystem CentOS 7.x

Gehen Sie folgendermaßen vor, 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 für andere CentOS-Versionen. Verwenden Sie das Basis-Repository für Ihre Version von CentOS.

Schritte

1. Fügen Sie das C7.6.1810 - Basis-Repository hinzu. Das C7.6.1810 - Base Vault Repository enthält das für ONTAP Mediator erforderliche "Kernel-devel" Paket.
2. 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
```

3. Führen Sie den `yum repolist` Befehl aus.

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

```
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 die Betriebssysteme Rocky Linux 10, 9 oder 8

Verwenden Sie dieses Verfahren, wenn Ihr Betriebssystem **Rocky Linux 10**, **Rocky Linux 9** oder **Rocky Linux 8** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

1. Abonnieren Sie die erforderlichen Repositorys:

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

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

2. Führen Sie einen `clean` Vorgang durch:

```
dnf clean all
```

3. Überprüfen Sie die Liste der Repositorys:

```
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 ~]#
```

Laden Sie das Installationspaket für ONTAP Mediator herunter

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

Schritte

1. Laden Sie das ONTAP Mediator-Installationspaket von der ONTAP Mediator-Downloadseite herunter.

   "Download-Seite für ONTAP Mediator"

2. Stellen Sie sicher, dass Sie das Mediator-Installationspaket im aktuellen Arbeitsverzeichnis abgelegt haben:

   ```
   [root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.11.0.tgz
   ```

   ```
   ontap-mediator-1.11.0.tgz
   ```

   Für ONTAP Mediator Versionen 1.4 und früher wird der Installer benannt `ontap-mediator`.

   Falls Ihr System keinen Internetzugang hat, stellen Sie sicher, dass das Installationsprogramm auf die erforderlichen Pakete zugreifen kann.

3. Verschieben Sie das Mediator-Installationspaket gegebenenfalls in das Installationsverzeichnis.
4. Entpacken Sie das Installationspaket:

   ```
   tar xvfz ontap-mediator-1.11.0.tgz
   ```

```
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
```

Überprüfen Sie die ONTAP Mediator-Code-Signatur

NetApp empfiehlt, die Codesignatur des ONTAP Mediators vor der Installation zu überprüfen. Dieser Schritt ist optional.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihr System diese Anforderungen erfüllt, bevor Sie die Codesignatur des ONTAP Mediators überprüfen.

- Ab dem 15. Juni 2025 ist eine Installation oder ein Upgrade auf ONTAP Mediator 1.9 und 1.8 nicht mehr möglich, da die Zertifikate zur Codesignatur-Verifizierung abgelaufen sind. Installieren oder aktualisieren Sie stattdessen ONTAP Mediator 1.11 oder 1.10.
- Wenn das System die folgenden Anforderungen nicht erfüllt, ist der Überprüfungsprozess nicht erforderlich und Sie können direkt zu gehen"Installieren Sie das Installationspaket für den ONTAP Mediator".

- openssl-Versionen 1.0.2 bis 3.0 für grundlegende Überprüfung
- openssl Version 1.1.0 oder höher für den Betrieb der TSA (Time Stamping Authority)
- Öffentlicher Internetzugang zur OCSP-Verifizierung

Das Downloadpaket enthält folgende Dateien:

Datei	Beschreibung
`ONTAP-Mediator-production.pub`	Der öffentliche Schlüssel, der zur Überprüfung der Signatur verwendet wird
`csc-prod-chain-ONTAP-Mediator.pem`	Die öffentliche Zertifizierung CA-Kette des Vertrauens
`csc-prod-ONTAP-Mediator.pem`	Das Zertifikat, mit dem der Schlüssel generiert wird
`ontap-mediator-1.11.0`	Die Installationsdatei für Version 1.11

`ontap-mediator-1.11.0.sig`	Der SHA-256 wurde gehasht, dann RSA-signiert mit dem csc-prod-Schlüssel, Signatur für das Installationsprogramm
`ontap-mediator-1.11.0.sig.tsr`	Die Annullierungsanfrage für die Verwendung durch OCSCP für die Unterschrift des Installers
`ontap-mediator-1.11.0.tsr`	Die Anforderungsdatei für die Zeitstempelsignierung
`tsa-prod-ONTAP-Mediator.pem`	Das öffentliche Zertifikat für den TSR
`tsa-prod-chain-ONTAP-Mediator.pem`	Das öffentliche Zertifikat CA-Kette für den TSR

Schritte

1. Führen Sie die Sperrprüfung `csc-prod-ONTAP-Mediator.pem` mit dem Online Certificate Status Protocol (OCSP) durch.
   a. Ermitteln Sie die OCSP-URL für das Zertifikat. Entwicklerzertifikate liefern möglicherweise keine URI:

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

   b. Erstellen Sie eine OCSP-Anfrage für das Zertifikat.

   ```
   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. Verbinden Sie sich mit dem OCSP-Manager, 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. Überprüfung der Vertrauenskette des Kundensupportzentrums und der Ablaufdaten am lokalen Host:

   `openssl verify`

   Die `openssl` Version vom PFAD muss eine gültige `cert.pem` (nicht selbstsignierte) Version haben.

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
Signature-Check certificate has expired or is invalid. Download a newer
version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
Stamp certificate has expired or is invalid. Download a newer version of
the ONTAP Mediator.
```

3. Überprüfen Sie die `ontap-mediator-1.11.0.sig.tsr` Und `ontap-mediator-1.11.0.tsr` Dateien, die die zugehörigen Zertifikate verwenden:

OpenSSL 3.x

```
openssl ts -verify -data ontap-mediator-1.11.0.sig -in ontap-mediator-
1.11.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
```

OpenSSL 1.x

```
openssl ts -verify -data ontap-mediator-1.11.0 -in ontap-mediator-
1.11.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -partial_chain
```

`.tsr`Die Dateien enthalten den Zeitstempel der Antwort des Installationsprogramms und die Codesignatur. Die Verarbeitung bestätigt, dass der Zeitstempel eine gültige Signatur der TSA aufweist und dass Ihre Eingabedatei nicht verändert wurde. Die Überprüfung wird lokal von Ihrem Rechner durchgeführt. Sie müssen nicht auf die TSA-Server zugreifen.

4. Überprüfen Sie die Signaturen gegen den Schlüssel:

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.11.0.sig ontap-mediator-1.11.0
```

Installieren Sie das Installationspaket für den ONTAP Mediator

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

Schritte

1. Führen Sie das Installationsprogramm aus, und reagieren Sie auf die Eingabeaufforderungen, falls erforderlich:

```
./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

```
[root@scs000099753 ~]# ./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

Um die Signaturprüfung während der Installation zu überspringen, verwenden Sie diesen Befehl: `./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y --skip-code -signature-check`

Das Installationsprogramm erstellt die erforderlichen Konten und installiert die benötigten Pakete. Falls der Mediator bereits installiert ist, werden Sie zum Upgrade aufgefordert.

Beispiel für die Installation des ONTAP Mediators (Konsolenausgang)

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.11.0.tgz
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
[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
Error querying OCSP responder
80BBA032607F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
data:crypto/http/http_client.c:549:
80BBA032607F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:901: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)? yes/no: yes
 SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ 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).
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
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.


Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use
"rhc" or "subscription-manager" to register.

Last metadata expiration check: 5 days, 14:34:13 ago on Thu 10 Jul 2025
01:28:32 AM EDT.
Package openssl-1:3.2.2-16.el10.x86_64 is already installed.
Package libselinux-utils-3.8-1.el10.x86_64 is already installed.
Package perl-Data-Dumper-2.189-512.el10.x86_64 is already installed.
Package bzip2-1.0.8-25.el10.x86_64 is already installed.
Package efibootmgr-18-8.el10.x86_64 is already installed.
Package mokutil-2:0.6.0-11.el10.x86_64 is already installed.
Package policycoreutils-python-utils-3.8-1.el10.noarch is already
installed.
Package python3-3.12.9-1.el10.x86_64 is already installed.
Dependencies resolved.
================================================================================
================================================================================
================================================================================
=========================
 Package
Architecture                                        Version
Repository                                              Size
================================================================================
================================================================================
================================================================================
=========================
Installing:
 elfutils-libelf-devel
x86_64                                              0.192-5.el10
```

```
AppStream                                              50 k
 gcc
x86_64                                            14.2.1-7.el10
AppStream                                              37 M
 kernel-devel
x86_64                                            6.12.0-55.9.1.el10_0
AppStream                                              22 M
 make
x86_64                                            1:4.4.1-9.el10
BaseOS                                                591 k
 openssl-devel
x86_64                                            1:3.2.2-16.el10
AppStream                                             3.9 M
 patch
x86_64                                            2.7.6-26.el10
AppStream                                             134 k
 perl-ExtUtils-MakeMaker
noarch                                            2:7.70-513.el10
AppStream                                              297 k
 python3-devel
x86_64                                            3.12.9-1.el10
AppStream
 334 k
 python3-pip
noarch                                            23.3.2-7.el10
AppStream                                             3.2 M
Installing dependencies:
 annobin-docs
noarch                                            12.92-1.el10
AppStream                                              94 k
 annobin-plugin-gcc
x86_64                                            12.92-1.el10
AppStream                                             985 k
 bison
x86_64                                            3.8.2-9.el10
AppStream                                             1.0 M
 cmake-filesystem
x86_64                                            3.30.5-2.el10
AppStream                                              29 k
 cpp
x86_64                                            14.2.1-7.el10
AppStream                                              12 M
 dwz
x86_64                                            0.15-7.el10
AppStream                                             139 k
 efi-srpm-macros
```

```
noarch                                          6-6.el10
AppStream                                           25 k
 flex
x86_64                                          2.6.4-19.el10
AppStream                                          303 k
 fonts-srpm-macros
noarch                                          1:2.0.5-18.el10
AppStream                                           29 k
 forge-srpm-macros
noarch                                          0.4.0-6.el10
AppStream                                           23 k
 gcc-plugin-annobin
x86_64                                          14.2.1-7.el10
AppStream                                           62 k
 glibc-devel
x86_64                                          2.39-37.el10
AppStream                                          641 k
 go-srpm-macros
noarch                                          3.6.0-4.el10
AppStream                                           29 k
 kernel-headers
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                          2.3 M
 kernel-srpm-macros
noarch                                          1.0-25.el10
AppStream                                           11 k
 libxcrypt-devel
x86_64                                          4.4.36-10.el10
AppStream                                           33 k
 libzstd-devel
x86_64                                          1.5.5-9.el10
AppStream
  53 k
 lua-srpm-macros
noarch                                          1-15.el10
AppStream                                           10 k
 m4
x86_64                                          1.4.19-11.el10
AppStream                                          309 k
 ocaml-srpm-macros
noarch                                          10-4.el10
AppStream                                           10 k
 openblas-srpm-macros
noarch                                          2-19.el10
AppStream                                          9.0 k
 package-notes-srpm-macros
```

```
noarch                                          0.5-13.el10
AppStream                                          11 k
 perl-AutoSplit
noarch                                          5.74-512.el10
AppStream                                          23 k
 perl-Benchmark
noarch                                          1.25-512.el10
AppStream                                          28 k
 perl-CPAN-Meta-Requirements
noarch                                          2.143-11.el10
AppStream                                          39 k
 perl-CPAN-Meta-YAML
noarch                                          0.018-512.el10
AppStream                                          29 k
 perl-Devel-PPPort
x86_64                                          3.72-512.el10
AppStream                                         223 k
 perl-ExtUtils-Command
noarch                                          2:7.70-513.el10
AppStream                                          16 k
 perl-ExtUtils-Constant
noarch                                          0.25-512.el10
AppStream                                          47 k
 perl-ExtUtils-Install
noarch                                          2.22-511.el10
AppStream                                          47 k
 perl-ExtUtils-Manifest
noarch                                          1:1.75-511.el10
AppStream                                          37 k
 perl-ExtUtils-ParseXS
noarch                                          1:3.51-512.el10
AppStream                                         190 k
 perl-File-Compare
noarch                                          1.100.800-512.el10
AppStream                                          15 k
 perl-File-Copy
noarch                                          2.41-512.el10
AppStream                                          22 k
 perl-I18N-Langinfo
x86_64                                          0.24-512.el10
AppStream                                          28 k
 perl-JSON-PP
noarch                                          1:4.16-512.el10
AppStream                                          69 k
 perl-Test-Harness
noarch                                          1:3.48-512.el10
```

```
AppStream                                          288 k
 perl-lib
x86_64                                          0.65-512.el10
AppStream                                           16 k
 perl-srpm-macros
noarch                                          1-57.el10
AppStream                                          9.7 k
 perl-version
x86_64                                          8:0.99.32-4.el10
AppStream                                           68 k
 pyproject-srpm-macros
noarch                                          1.16.2-1.el10
AppStream                                           16 k
 python-srpm-macros
noarch                                          3.12-9.1.el10
AppStream                                           26 k
 python3-pyparsing
noarch                                          3.1.1-7.el10
BaseOS                                             273 k
 qt6-srpm-macros
noarch                                          6.8.1-3.el10
AppStream
 11 k
 redhat-rpm-config
noarch                                          288-1.el10
AppStream                                           83 k
 rust-toolset-srpm-macros
noarch                                          1.84.1-1.el10
AppStream                                           13 k
 systemtap-sdt-devel
x86_64                                          5.2-2.el10
AppStream                                           78 k
 systemtap-sdt-dtrace
x86_64                                          5.2-2.el10
AppStream                                           72 k
 zlib-ng-compat-devel
x86_64                                          2.2.3-1.el10
AppStream                                           41 k
Installing weak dependencies:
 perl-CPAN-Meta
noarch                                          2.150010-511.el10
AppStream                                          202 k
 perl-Encode-Locale
noarch                                          1.05-31.el10
AppStream                                           21 k
 perl-Time-HiRes
```

```
x86_64                                                 4:1.9777-511.el10
AppStream                                                  62 k
 perl-devel
x86_64                                                 4:5.40.1-512.el10
AppStream                                                 772 k
 perl-doc
noarch                                                 5.40.1-512.el10
AppStream                                                 4.9 M

Transaction Summary
================================================================================
================================================================================
================================================================================
=========================
Install  63 Packages

Total size: 94 M
Installed size: 282 M
Downloading Packages:
BaseOS Packages Red Hat Enterprise Linux 10
439 kB/s | 3.7 kB     00:00
Importing GPG key 0xFD431D51:
 Userid     : "Red Hat, Inc. (release key 2) <security@redhat.com>"
 Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Importing GPG key 0x5A6340B3:
 Userid     : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"
  Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Installing       : perl-version-8:0.99.32-4.el10.x86_64
1/63
  Installing       : perl-File-Copy-2.41-512.el10.noarch
2/63
  Installing       : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
3/63
  Installing       : perl-Time-HiRes-4:1.9777-511.el10.x86_64
4/63
```

```
  Installing       : perl-JSON-PP-1:4.16-512.el10.noarch
5/63
  Installing       : perl-File-Compare-1.100.800-512.el10.noarch
6/63
  Installing       : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
7/63
  Installing       : m4-1.4.19-11.el10.x86_64
8/63
  Installing       : make-1:4.4.1-9.el10.x86_64
9/63
  Installing       : bison-3.8.2-9.el10.x86_64
10/63
  Installing       : flex-2.6.4-19.el10.x86_64
11/63
  Installing       : perl-ExtUtils-Command-2:7.70-513.el10.noarch
12/63
  Installing       : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
13/63
  Installing       : systemtap-sdt-devel-5.2-2.el10.x86_64
14/63
  Installing       : rust-toolset-srpm-macros-1.84.1-1.el10.noarch
15/63
  Installing       : qt6-srpm-macros-6.8.1-3.el10.noarch
16/63
  Installing       : python3-pip-23.3.2-7.el10.noarch
17/63
  Installing       : pyproject-srpm-macros-1.16.2-1.el10.noarch
18/63
  Installing       : perl-srpm-macros-1-57.el10.noarch
19/63
  Installing       : perl-lib-0.65-512.el10.x86_64
20/63
  Installing       : perl-doc-5.40.1-512.el10.noarch
21/63
  Installing       : perl-I18N-Langinfo-0.24-512.el10.x86_64
22/63
  Installing       : perl-Encode-Locale-1.05-31.el10.noarch
23/63
  Installing       : perl-ExtUtils-Constant-0.25-512.el10.noarch
24/63
  Installing       : perl-Devel-PPPort-3.72-512.el10.x86_64
25/63
  Installing       : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
26/63
  Installing       : perl-CPAN-Meta-2.150010-511.el10.noarch
27/63
```

```
  Installing       : perl-Benchmark-1.25-512.el10.noarch
28/63
  Installing       : perl-Test-Harness-1:3.48-512.el10.noarch
29/63
  Installing       : perl-AutoSplit-5.74-512.el10.noarch
30/63
  Installing       : package-notes-srpm-macros-0.5-13.el10.noarch
31/63
  Installing       : openssl-devel-1:3.2.2-16.el10.x86_64
32/63
  Installing       : openblas-srpm-macros-2-19.el10.noarch
33/63
  Installing       : ocaml-srpm-macros-10-4.el10.noarch
34/63
  Installing       : lua-srpm-macros-1-15.el10.noarch
35/63
  Installing       : libzstd-devel-1.5.5-9.el10.x86_64
36/63
  Installing       : kernel-srpm-macros-1.0-25.el10.noarch
37/63
  Installing       : kernel-headers-6.12.0-55.9.1.el10_0.x86_64
38/63
  Installing       : libxcrypt-devel-4.4.36-10.el10.x86_64
39/63
  Installing       : glibc-devel-2.39-37.el10.x86_64
40/63
  Installing       : efi-srpm-macros-6-6.el10.noarch
41/63
  Installing       : dwz-0.15-7.el10.x86_64
42/63
  Installing       : cpp-14.2.1-7.el10.x86_64
43/63
  Installing       : gcc-14.2.1-7.el10.x86_64
44/63
  Installing       : gcc-plugin-annobin-14.2.1-7.el10.x86_64
45/63
  Installing       : cmake-filesystem-3.30.5-2.el10.x86_64
46/63
  Installing       : zlib-ng-compat-devel-2.2.3-1.el10.x86_64
47/63
  Installing       : elfutils-libelf-devel-0.192-5.el10.x86_64
48/63
  Installing       : annobin-docs-12.92-1.el10.noarch
49/63
  Installing       : annobin-plugin-gcc-12.92-1.el10.x86_64
50/63
```

```
  Installing       : fonts-srpm-macros-1:2.0.5-18.el10.noarch
51/63
  Installing       : forge-srpm-macros-0.4.0-6.el10.noarch
52/63
  Installing       : go-srpm-macros-3.6.0-4.el10.noarch
53/63
  Installing       : python-srpm-macros-3.12-9.1.el10.noarch
54/63
  Installing       : redhat-rpm-config-288-1.el10.noarch
55/63
  Running scriptlet: redhat-rpm-config-288-1.el10.noarch
55/63
  Installing       : python3-pyparsing-3.1.1-7.el10.noarch
56/63
  Installing       : systemtap-sdt-dtrace-5.2-2.el10.x86_64
57/63
  Installing       : perl-devel-4:5.40.1-512.el10.x86_64
58/63
  Installing       : perl-ExtUtils-Install-2.22-511.el10.noarch
59/63
  Installing       : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
60/63
  Installing       : kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Running scriptlet: kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Installing       : python3-devel-3.12.9-1.el10.x86_64
62/63
  Installing       : patch-2.7.6-26.el10.x86_64
63/63
  Running scriptlet: patch-2.7.6-26.el10.x86_64
63/63
Installed products updated.

Installed:
  annobin-docs-12.92-1.el10.noarch              annobin-plugin-gcc-
12.92-1.el10.x86_64            bison-3.8.2-9.el10.x86_64
cmake-filesystem-3.30.5-2.el10.x86_64           cpp-14.2.1-
7.el10.x86_64
  dwz-0.15-7.el10.x86_64                        efi-srpm-macros-6-
6.el10.noarch                  elfutils-libelf-devel-0.192-
5.el10.x86_64   flex-2.6.4-19.el10.x86_64                       fonts-
srpm-macros-1:2.0.5-18.el10.noarch
  forge-srpm-macros-0.4.0-6.el10.noarch         gcc-14.2.1-
7.el10.x86_64                          gcc-plugin-annobin-14.2.1-
7.el10.x86_64     glibc-devel-2.39-37.el10.x86_64               go-
```

```
srpm-macros-3.6.0-4.el10.noarch
  kernel-devel-6.12.0-55.9.1.el10_0.x86_64      kernel-headers-6.12.0-
55.9.1.el10_0.x86_64        kernel-srpm-macros-1.0-25.el10.noarch
libxcrypt-devel-4.4.36-10.el10.x86_64           libzstd-devel-1.5.5-
9.el10.x86_64
  lua-srpm-macros-1-15.el10.noarch              m4-1.4.19-
11.el10.x86_64                          make-1:4.4.1-9.el10.x86_64
ocaml-srpm-macros-10-4.el10.noarch              openblas-srpm-macros-2-
19.el10.noarch
  openssl-devel-1:3.2.2-16.el10.x86_64          package-notes-srpm-
macros-0.5-13.el10.noarch      patch-2.7.6-26.el10.x86_64
perl-AutoSplit-5.74-512.el10.noarch             perl-Benchmark-1.25-
512.el10.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.el10.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.el10.noarch       perl-File-Copy-2.41-512.el10.noarch
perl-I18N-Langinfo-0.24-512.el10.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-4:5.40.1-512.el10.x86_64
perl-doc-5.40.1-512.el10.noarch                 perl-lib-0.65-
512.el10.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-3.12-9.1.el10.noarch         python3-devel-3.12.9-
1.el10.x86_64
  python3-pip-23.3.2-7.el10.noarch              python3-pyparsing-
3.1.1-7.el10.noarch             qt6-srpm-macros-6.8.1-3.el10.noarch
redhat-rpm-config-288-1.el10.noarch             rust-toolset-srpm-
macros-1.84.1-1.el10.noarch
  systemtap-sdt-devel-5.2-2.el10.x86_64         systemtap-sdt-dtrace-
5.2-2.el10.x86_64            zlib-ng-compat-devel-2.2.3-1.el10.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.vdizgQ/ontap-
mediator-1.11.0/ontap-mediator-1.11.0/install_20250715160240.log)
    This step takes several minutes. View progress in the log file.
    Sudoer config verified
```

```
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20250715160240.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.modu
le-signing
           to sign the SCST kernel module. Note that a reboot is
needed.
     SCST does 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:~# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
     Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
9s ago
 Invocation: 395e9479487e4e308be2ae030c800c7f
    Process: 28745
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
   Main PID: 28759 (python)
      Tasks: 1 (limit: 22990)
     Memory: 66.8M (peak: 68.8M)
        CPU: 2.865s
```

```
     CGroup: /system.slice/ontap_mediator.service
             └─28759 /opt/netapp/lib/ontap_mediator/pyenv/bin/python
/opt/netapp/lib/ontap_mediator/ontap_mediator/server

Jul 15 16:07:29 mediator_host systemd[1]: Starting
ontap_mediator.service - ONTAP Mediator...
Jul 15 16:07:29 mediator_host systemd[1]: Started
ontap_mediator.service - ONTAP Mediator.
root@mediator_host:~# systemctl status mediator-scst
● mediator-scst.service
     Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
15s ago
 Invocation: f1d3be6ca1f9492b943e61872676f384
    Process: 28653 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 28738 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 28696 (iscsi-scstd)
      Tasks: 1 (limit: 22990)
     Memory: 5.2M (peak: 35.2M)
        CPU: 547ms
     CGroup: /system.slice/mediator-scst.service
             └─28696 /usr/local/sbin/iscsi-scstd

Jul 15 16:07:28 mediator_host systemd[1]: Starting mediator-
scst.service...
Jul 15 16:07:29 mediator_host iscsi-scstd[28694]: max_data_seg_len
1048576, max_queued_cmds 2048
Jul 15 16:07:29 mediator_host scst[28653]: Loading and configuring SCST
Jul 15 16:07:29 mediator_host systemd[1]: Started mediator-
scst.service.
root@mediator_host:~#
```

Registrieren Sie den Sicherheitsschlüssel für UEFI Secure Boot

Ab ONTAP Mediator 1.4 ist der Secure-Boot-Mechanismus auf UEFI-Systemen aktiviert. Wenn Secure Boot aktiviert ist, müssen Sie nach der Installation zusätzliche Schritte unternehmen, um den Sicherheitsschlüssel zu registrieren.

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.module-
   signing
   ```

2. Suchen Sie die erforderlichen Schlüssel:

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

> Nach der Installation werden im System die README-Dateien und der Speicherort der Schlüssel angezeigt.

3. Öffentlichen Schlüssel zur MOK-Liste hinzufügen:

```
mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

> Sie können den privaten Schlüssel an seinem Standardspeicherort belassen oder ihn an einen sicheren Ort verschieben. Sie müssen den öffentlichen Schlüssel an seinem aktuellen Speicherort belassen, damit der Boot Manager ihn verwenden kann. Weitere Informationen finden Sie in der 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 das neue MOK zu genehmigen. Sie benötigen die mitgelieferte Passphrase für die `mokutil` Nutzen in"Installieren Sie ONTAP Mediator, wenn UEFI Secure Boot aktiviert ist" Die

Signieren von SCST-Kernelmodulen

Nach der Installation von ONTAP Mediator, wenn der systemctl-Status `mediator-scst` Wird als fehlgeschlagen (inaktiv) angezeigt, befolgen Sie diese Schritte, um das SCST-Kernelmodul zu signieren.

Schritte

1. Während des Build-Prozesses wird ein öffentliches/privates Schlüsselpaar generiert. `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/` Verzeichnis, indem Sie den folgenden Befehl verwenden:

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

2. Starten Sie den Vorgang des Importierens des öffentlichen Schlüssels in das UEFI-Schlüsselrepository, indem Sie die folgenden Befehle ausführen:

```
[root@mediator-host ~]# mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r input password: input password again:

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

3. Die Software mokutil verlangt während des Importvorgangs ein temporäres Passwort für diesen Schlüssel.
4. Überprüfen Sie, ob der Importvorgang mit dem `mokutil --list-new` und starten Sie das System anschließend neu. Der Bootloader startet den EFI MOK Manager.

5. Verwenden Sie die Menüs auf dem Bildschirm, um den SCST-Kernelmodulschlüssel zu aktivieren. Nach dem Booten ausführen `systemctl status mediator-scst` Die Sobald der Dienst startet, werden die SCST-Kernelmodule signiert.

Überprüfen Sie den Installationsstatus des ONTAP Mediators

Überprüfen Sie nach der Installation von ONTAP Mediator, ob es erfolgreich ausgeführt wird.

Schritte

1. Zeigen Sie den Status von ONTAP Mediator an:

   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# 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@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# 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@scspr1915530002 ~]#
```

2. Bestätigen Sie die von ONTAP Mediator verwendeten Ports:

   `netstat`

```
[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
```

Konfiguration des ONTAP Mediators nach der Installation

Nachdem ONTAP Mediator installiert und ausgeführt wird, müssen zusätzliche Konfigurationsaufgaben im ONTAP-Speichersystem ausgeführt werden, um die Funktionen von ONTAP Mediator nutzen zu können:

- Informationen zur Verwendung von ONTAP Mediator in einer MetroCluster-IP-Konfiguration finden Sie unter "Konfigurieren Sie ONTAP Mediator über eine MetroCluster-IP-Konfiguration" .
- Informationen zur Verwendung von SnapMirror Active Sync finden Sie unter "Installieren Sie ONTAP Mediator und bestätigen Sie die ONTAP-Clusterkonfiguration".

Konfigurieren Sie die Sicherheitsrichtlinien von ONTAP Mediator

ONTAP Mediator unterstützt mehrere konfigurierbare Sicherheitseinstellungen. Die Standardwerte für alle Einstellungen werden in einer schreibgeschützten Datei angegeben `low_space_threshold_mib: 10`:

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

Alle Werte, die in das gesetzt `ontap_mediator.user_config.yaml` werden, überschreiben die Standardwerte und werden bei allen ONTAP Mediator Upgrades beibehalten.

Nach der Änderung `ontap_mediator.user_config.yaml` , starten Sie ONTAP Mediator neu:

```
systemctl restart ontap_mediator
```

Attribute des ONTAP Mediators ändern

Die in diesem Abschnitt beschriebenen Attribute des ONTAP Mediators können bei Bedarf geändert werden.

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

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

Installieren Sie SSL-Zertifikate von Drittanbietern

Wenn Sie die selbstsignierten Standardzertifikate durch SSL-Zertifikate von Drittanbietern ersetzen müssen, ändern Sie bestimmte Attribute in den folgenden Dateien:

- `/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 werden verwendet, um die von ONTAP Mediator verwendeten Zertifikatsdateien zu steuern.

ONTAP Mediator 1.9 und höher

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

Variabel	Pfad
`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/intermediate.crt`
`ca_key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key`
`ca_serial_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl`
`cert_valid_days`	`1095`
`x509_passin_pwd`	`pass:ontap`

- `cert_valid_days` Dient zum Festlegen des Ablaufs von Clientzertifikaten. 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 Datei enthalten `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`.

Variabel	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/intermediate.crt`

ONTAP Mediator 1.8 und früher

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

Variabel	Pfad
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_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert_valid_days` Dient zum Festlegen des Ablaufs von Clientzertifikaten. 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 Datei enthalten `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`.

Variabel	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 Sie diese Attribute ändern, starten Sie ONTAP Mediator neu, um die Änderungen anzuwenden. Ausführliche Anweisungen zum Ersetzen von Standardzertifikaten durch Zertifikate von Drittanbietern finden Sie unter "Ersetzen Sie selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern".

Schutz vor Kennwortangriffen

Die folgenden Einstellungen bieten Schutz vor Brute-Force-Passwortraten.

Um die Funktion zu aktivieren, legen Sie einen Wert für die `window_seconds` und die `retry_limit`fest.

Beispiele:

- Geben Sie ein 5-Minuten-Fenster für Vermutungen ein, und setzen Sie dann die Anzahl auf Null-Fehler zurück:

  ```
  authentication_lock_window_seconds: 300
  ```

- Sperren Sie das Konto, wenn innerhalb des Zeitrahmens fünf Fehler auftreten:

  ```
  authentication_retry_limit: 5
  ```

- Verringern Sie die Auswirkungen von Brute-Force-Passwortraten, indem Sie eine Verzögerung festlegen, die vor der Ablehnung jedes Versuchs auftritt, 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
  ```

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)
```

Kontrolle des freien Speicherplatzes

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

Wenn der Platz unter dem festgelegten Schwellenwert liegt, gibt der Dienst ein Warnungsereignis aus.

```
low_space_threshold_mib: 10
```

Kontrolle des reservierten Protokollspeichers

Die RESERVE_LOG_SPACE wird durch bestimmte 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 explizit für die ONTAP Mediator-Protokollierung verwendet wird.

So deaktivieren Sie diese Funktion und verwenden den Standardspeicherplatz:

1. Ändern Sie den Wert von RESERVE_LOG_SPACE in der folgenden Datei von 1 auf 0:

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

2. Mediator neu starten:

   a. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

      ```
      RESERVE_LOG_SPACE=0
      ```

   b. `systemctl restart ontap_mediator`

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

> Durch Umschalten zwischen Festplattenspeicherplätzen werden vorhandene Protokolle nicht gelöscht. Alle vorherigen Protokolle werden gesichert und anschließend auf den aktuellen Speicherplatz verschoben, nachdem Mediator gewechselt und neu gestartet wurde.

ONTAP Mediator verwalten

Verwalten Sie ONTAP Mediator, einschließlich der Änderung der Benutzeranmeldeinformationen, des Stoppens und erneuten Aktivierens des Dienstes, der Überprüfung seines Zustands und der Installation oder Deinstallation von SCST zur Hostwartung. Sie können auch Zertifikate verwalten, z. B. selbstsignierte Zertifikate neu generieren, diese durch vertrauenswürdige Zertifikate von Drittanbietern ersetzen und Probleme mit Zertifikaten beheben.

Ändern Sie den Benutzernamen

Sie können den Benutzernamen wie folgt ändern.

Über diese Aufgabe

Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.

Wenn Sie diesen Befehl nicht erreichen können, müssen Sie möglicherweise den Befehl mit dem vollständigen Pfad ausführen, wie im folgenden Beispiel dargestellt:

`/usr/local/bin/mediator_username`

Schritte

Ändern Sie den Benutzernamen durch Auswahl einer der folgenden Optionen:

- **Option (a)**: Führen Sie den Befehl aus `mediator_change_user` und antworten Sie auf 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)**: Führen Sie den folgenden Befehl aus:

```
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 ~]#
```

Ändern Sie das Passwort

Sie können das Passwort wie folgt ändern.

Über diese Aufgabe

Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.

Wenn Sie diesen Befehl nicht erreichen können, müssen Sie möglicherweise den Befehl mit dem vollständigen Pfad ausführen, wie im folgenden Beispiel dargestellt:

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

Schritte

Ändern Sie das Passwort, indem Sie eine der folgenden Optionen auswählen:

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

```
[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)**: Führen Sie den folgenden Befehl aus:

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

Das Beispiel zeigt, dass das Passwort von „mediator1“ in „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 ~]#
```

Stoppen Sie ONTAP Mediator

Um ONTAP Mediator zu stoppen, führen Sie die folgenden Schritte aus:

Schritte

1. Stoppen Sie ONTAP Mediator:

```
systemctl stop ontap_mediator
```

2. SCST stoppen:

```
systemctl stop mediator-scst
```

3. Deaktivieren Sie ONTAP Mediator und SCST:

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

ONTAP Mediator erneut aktivieren

Um ONTAP Mediator wieder zu aktivieren, führen Sie die folgenden Schritte aus:

Schritte

1. Aktivieren Sie ONTAP Mediator und SCST:

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

2. SCST starten:

```
systemctl start mediator-scst
```

3. ONTAP Mediator starten:

```
systemctl start ontap_mediator
```

Überprüfen Sie, ob ONTAP Mediator fehlerfrei ist

Überprüfen Sie nach der Installation von ONTAP Mediator, ob es erfolgreich ausgeführt wird.

Schritte

1. Zeigen Sie den Status von ONTAP Mediator an:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# 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@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# 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@scspr1915530002 ~]#
```

2. Bestätigen Sie die von ONTAP Mediator verwendeten Ports:

   `netstat`

```
[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
```

Deinstallieren Sie ONTAP Mediator

Bei Bedarf können Sie ONTAP Mediator entfernen.

Bevor Sie beginnen

Sie müssen ONTAP Mediator von ONTAP trennen, bevor Sie es entfernen.

Über diese Aufgabe

Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.

Wenn Sie diesen Befehl nicht erreichen können, müssen Sie möglicherweise den Befehl mit dem vollständigen Pfad ausführen, wie im folgenden Beispiel dargestellt:

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

Schritt

1. Deinstallieren Sie ONTAP Mediator:

   `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 ~]#
```

Erstellen Sie ein temporäres selbstsigniertes Zertifikat neu

Ab ONTAP Mediator 1.7 können Sie ein temporäres selbstsigniertes Zertifikat mithilfe des folgenden Verfahrens neu erstellen.

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

Über diese Aufgabe

- Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.
- Sie können diese Aufgabe nur ausführen, wenn die generierten selbstsignierten Zertifikate aufgrund von Änderungen am Hostnamen 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, führen Sie *Not* mit dieser Aufgabe aus, um ein Zertifikat zu regenerieren. Wenn kein selbstsigniertes Zertifikat vorhanden ist, schlägt dieses Verfahren fehl.

Schritt

Führen Sie den folgenden Schritt durch, um ein neues temporäres selbstsigniertes Zertifikat für den aktuellen Host zu erstellen:

1. Starten Sie ONTAP Mediator neu:

   ```
   ./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
```

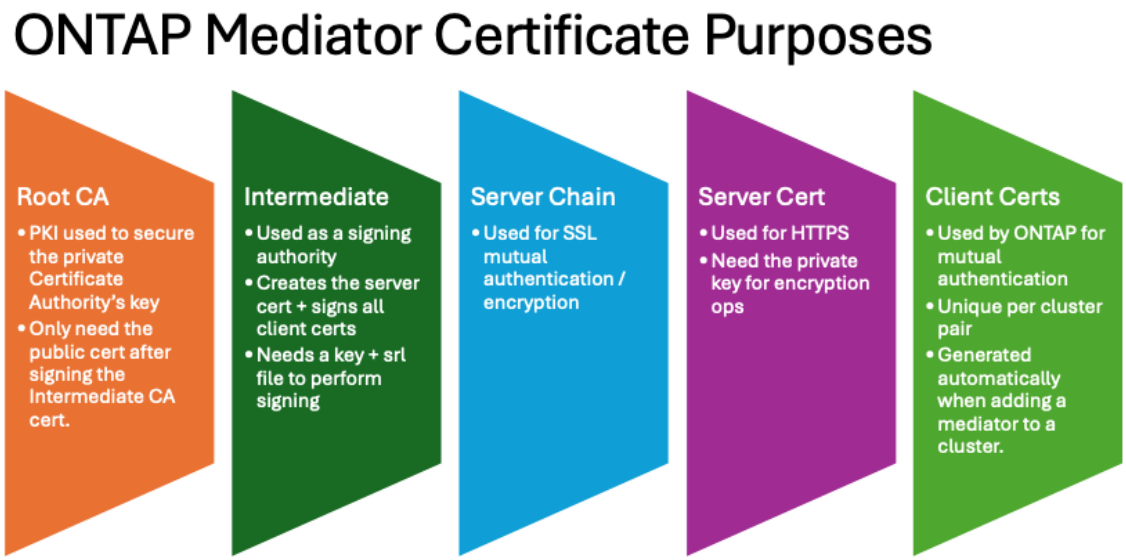
Ersetzen Sie selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern

Wenn unterstützt, können Sie selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern ersetzen.

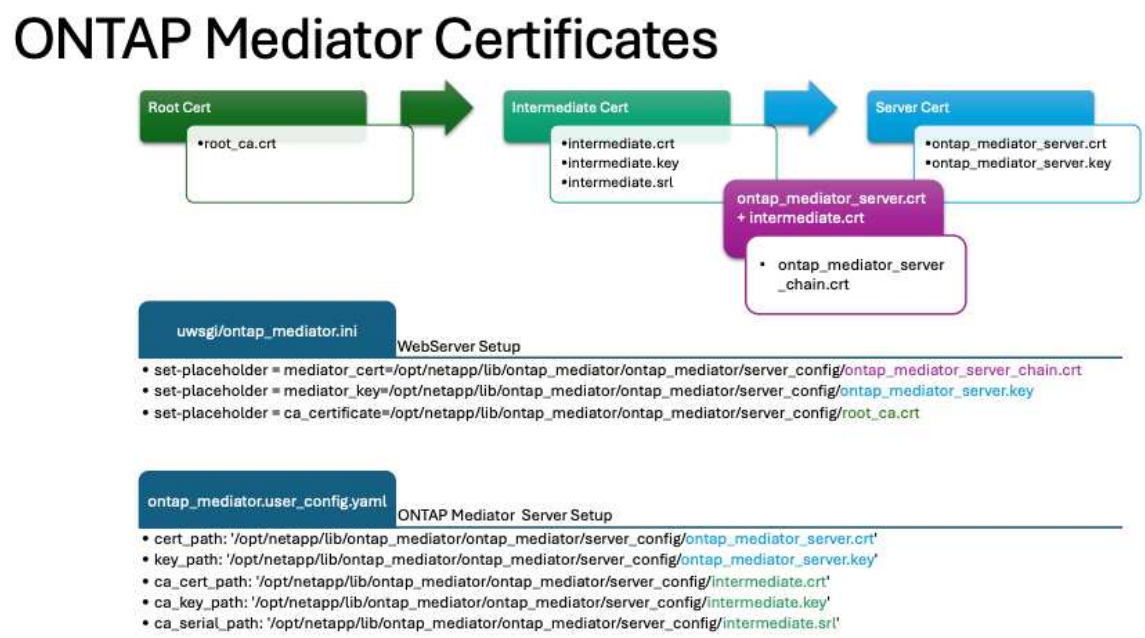
- Zertifikate von Drittanbietern werden erst ab ONTAP 9.16.1 und einigen früheren ONTAP Patch-Versionen unterstützt. Siehe "NetApp Bugs Online Fehler-ID CONTAP-243278".
- Zertifikate von Drittanbietern werden nur auf Systemen unterstützt, auf denen ONTAP Mediator 1.7 oder höher ausgeführt wird.

Über diese Aufgabe

- Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.
- Sie können diese Aufgabe ausführen, wenn die generierten selbstsignierten Zertifikate durch Zertifikate ersetzt werden müssen, die von einer vertrauenswürdigen untergeordneten Zertifizierungsstelle (CA) erhalten wurden. Um dies zu erreichen, sollten Sie Zugriff auf eine vertrauenswürdige Public-Key-Infrastruktur (PKI) haben.
- Die folgende Abbildung zeigt die Zwecke jedes ONTAP Mediatorzertifikats.



- Das folgende Bild zeigt die Konfiguration für die Einrichtung des Webservers und des ONTAP Mediators.



Schritt 1: Erhalten Sie ein Zertifikat von einem Drittanbieter, der ein CA-Zertifikat ausstellt

Sie können ein Zertifikat von einer PKI-Autorität über das folgende Verfahren erhalten.

Das folgende Beispiel zeigt, wie die selbstsignierten Zertifikatakteure durch die Zertifikatakteure von Drittanbietern ersetzt werden, die sich unter befinden

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

Das Beispiel veranschaulicht die notwendigen Kriterien für die für ONTAP Mediator erforderlichen Zertifikate. Sie können die Zertifikate von einer PKI-Autorität auf eine andere Weise beziehen als bei diesem Verfahren. Passen Sie das Verfahren an Ihre Geschäftsanforderungen an.

ONTAP Mediator 1.9 und höher

1. Erstellen Sie einen privaten Schlüssel `intermediate.key` und eine Konfigurationsdatei `openssl_ca.cnf`, die von der PKI-Autorität zur Generierung eines Zertifikats verwendet wird.

   a. Generieren Sie den privaten Schlüssel `intermediate.key`:

      Beispiel

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

   a. Die Konfigurationsdatei `openssl_ca.cnf` (unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) definiert die Eigenschaften, über die das generierte Zertifikat verfügen muss.

2. Verwenden Sie den privaten Schlüssel und die Konfigurationsdatei, 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@scs000216655 server_config]# openssl req -key intermediate.key
   -new -config openssl_ca.cnf -out intermediate.csr
   Enter pass phrase for intermediate.key:
   [root@scs000216655 server_config]# cat intermediate.csr
   -----BEGIN CERTIFICATE REQUEST-----
   <certificate_value>
   -----END CERTIFICATE REQUEST-----
   ```

3. Senden Sie die Zertifikatsignierungsanforderung `intermediate.csr` an eine PKI-Autorität zur Signatur.

   Die PKI-Behörde prüft die Anfrage und unterzeichnet die `.csr` , Generieren des Zertifikats `intermediate.crt` . Darüber hinaus benötigen Sie die `root_ca.crt` Zertifikat, das die `intermediate.crt` Zertifikat der PKI-Behörde.

   Für SnapMirror Business Continuity (SM-BC)-Cluster müssen Sie die `intermediate.crt` Und `root_ca.crt` Zertifikate an einen ONTAP Cluster. Sehen"Konfigurieren Sie ONTAP Mediator und Cluster für SnapMirror Active Sync" .

ONTAP Mediator 1.8 und früher

1. Erstellen Sie einen privaten Schlüssel `ca.key` und eine Konfigurationsdatei `openssl_ca.cnf`, die von der PKI-Autorität zur Generierung eines Zertifikats verwendet wird.

   a. Generieren Sie den privaten Schlüssel `ca.key`:

      Beispiel

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

a. Die Konfigurationsdatei `openssl_ca.cnf` (unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) definiert die Eigenschaften, über die das generierte Zertifikat verfügen muss.

2. Verwenden Sie den privaten Schlüssel und die Konfigurationsdatei, 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@scs000216655 server_config]# openssl req -key ca.key -new
-config openssl_ca.cnf -out ca.csr
Enter pass phrase for ca.key:
[root@scs000216655 server_config]# cat ca.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. Senden Sie die Zertifikatsignierungsanforderung `ca.csr` an eine PKI-Autorität zur Signatur.

Die PKI-Autorität überprüft die Anforderung und signiert den `.csr`, das Zertifikat zu generieren `ca.crt`. Darüber hinaus müssen Sie das Zertifikat von der PKI-Behörde erhalten `root_ca.crt that signed the `ca.crt`.

Für SnapMirror-Cluster für Business Continuity (SM-BC) müssen Sie einem ONTAP-Cluster die Zertifikate und hinzufügen `ca.crt root_ca.crt` . Siehe "Konfigurieren Sie ONTAP Mediator und Cluster für SnapMirror Active Sync".

Schritt 2: Erstellen Sie ein Serverzertifikat, indem Sie mit einer Drittanbieter-CA-Zertifizierung signieren

ONTAP Mediator 1.9 und höher

Ein Server-Zertifikat muss durch den privaten Schlüssel `intermediate.key` und das Drittanbieter-Zertifikat signiert werden `intermediate.crt`. Darüber hinaus `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` enthält die Konfigurationsdatei bestimmte Attribute, die die Eigenschaften angeben, die für von OpenSSL ausgegebene Serverzertifikate erforderlich sind.

Die folgenden Befehle können ein Serverzertifikat generieren.

Schritte

1. Um eine Serverzertifikatsignierungsanforderung (CSR) zu generieren, führen Sie den folgenden Befehl aus dem Ordner aus `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`:

   ```
   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 der CSR zu generieren, führen Sie den folgenden Befehl aus dem `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` Ordner:

   > Diese Dateien wurden von einer PKI-Behörde abgerufen. Wenn Sie einen anderen Zertifikatnamen verwenden, ersetzen Sie `intermediate.crt` und `intermediate.key` durch die entsprechenden Dateinamen.

   ```
   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 Dateien zu generieren `intermediate.srl`.

ONTAP Mediator 1.8 und früher

Ein Server-Zertifikat muss durch den privaten Schlüssel `ca.key` und das Drittanbieter-Zertifikat signiert werden `ca.crt`. Darüber hinaus `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` enthält die Konfigurationsdatei bestimmte Attribute, die die Eigenschaften angeben, die für von OpenSSL ausgegebene Serverzertifikate erforderlich sind.

Die folgenden Befehle können ein Serverzertifikat generieren.

Schritte

1. Um eine Serverzertifikatsignierungsanforderung (CSR) zu generieren, führen Sie den folgenden Befehl aus dem Ordner aus `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`:

   ```
   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 der CSR zu generieren, führen Sie den folgenden Befehl aus dem

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` Ordner:

> Diese Dateien wurden von einer PKI-Behörde abgerufen. Wenn Sie einen anderen Zertifikatnamen verwenden, ersetzen Sie `ca.crt` und `ca.key` durch die entsprechenden Dateinamen.

```
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 Dateien zu generieren `ca.srl`.

Schritt 3: Ersetzen Sie neue Drittanbieter-CA-Zertifikat und Server-Zertifikat in ONTAP Mediator-Konfiguration

ONTAP Mediator 1.10 und höher

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei bereitgestellt, die sich unter befindet. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . 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/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` Und `key_path` sind Serverzertifikatvariablen.
- `ca_cert_path`, `ca_key_path` Und `ca_serial_path` sind CA-Zertifikatvariablen.

Schritte

1. Ersetzen Sie alle `intermediate.*` Dateien durch Zertifikate von Drittanbietern.
2. Erstellen Sie eine Zertifikatskette aus den `intermediate.crt` Zertifikaten und `ontap_mediator_server.crt` :

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

3. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` Datei.

   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, die ontap_mediator_server.key .
- Der ssl_certfile Wert ist der Pfad des ontap_mediator_server_chain.crt Datei.
- Der ssl_ca_certs Wert ist der Pfad des root_ca.crt Datei.

4. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:
   - Eigentümer Der Linux-Gruppe: netapp:netapp
   - Linux-Berechtigungen: 600
5. Starten Sie ONTAP Mediator neu:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 und 1.9

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei bereitgestellt, die sich unter befindet. /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml . 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/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- cert_path Und key_path sind Serverzertifikatvariablen.
- ca_cert_path, ca_key_path Und ca_serial_path sind CA-Zertifikatvariablen.

Schritte

1. Ersetzen Sie alle intermediate.* Dateien durch Zertifikate von Drittanbietern.
2. Erstellen Sie eine Zertifikatskette aus den intermediate.crt Zertifikaten und ontap_mediator_server.crt :

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

```
ontap_mediator_server_chain.crt
```

3. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei.

   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.
   - Das `mediator_key value` ist der Schlüsselpfad in der `ontap_mediator_server.crt` Datei, das heißt `ontap_mediator_server.key`.
   - Der `ca_certificate` Wert ist der Pfad der `root_ca.crt` Datei.

4. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:
   - Eigentümer Der Linux-Gruppe: `netapp:netapp`
   - Linux-Berechtigungen: `600`
5. Starten Sie ONTAP Mediator neu:

   ```
   systemctl restart ontap_mediator
   ```

ONTAP Mediator 1.8 und früher

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei bereitgestellt, die sich unter befindet. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . 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/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 Serverzertifikatvariablen.
- `ca_cert_path`, `ca_key_path` Und `ca_serial_path` sind CA-Zertifikatvariablen.

Schritte

1. Ersetzen Sie alle `ca.*` Dateien durch Zertifikate von Drittanbietern.
2. Erstellen Sie eine Zertifikatskette aus den `ca.crt` Zertifikaten und `ontap_mediator_server.crt` :

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

3. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei.

   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.
   - Das `mediator_key value` ist der Schlüsselpfad in der `ontap_mediator_server.crt` Datei, das heißt `ontap_mediator_server.key`.
   - Der `ca_certificate` Wert ist der Pfad der `root_ca.crt` Datei.
4. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:
   - Eigentümer Der Linux-Gruppe: `netapp:netapp`

- Linux-Berechtigungen: `600`

5. Starten Sie ONTAP Mediator neu:

```
systemctl restart ontap_mediator
```

Schritt 4: Verwenden Sie optional einen anderen Pfad oder Namen für Ihre Drittanbieter-Zertifikate

ONTAP Mediator 1.10 und höher

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

Schritte

1. Konfigurieren Sie die `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` Datei so, dass die standardmäßigen Variablenwerte in der Datei überschrieben `ontap_mediator.config.yaml` werden.

   Wenn Sie von einer PKI-Autorität erhalten `intermediate.crt` haben und den privaten Schlüssel am Speicherort speichern `intermediate.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, sollte die `ontap_mediator.user_config.yaml` Datei wie folgt aussehen:

   > Wenn Sie `intermediate.crt` das Zertifikat signiert `ontap_mediator_server.crt` haben, wird die `intermediate.srl` Datei generiert. Weitere Informationen finden Sie unter Schritt 2: Erstellen Sie ein Serverzertifikat, indem Sie mit einer Drittanbieter-CA-Zertifizierung signieren .

```
[root@scs000216655 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 Sie eine Zertifikatsstruktur verwenden, bei der die `root_ca.crt` Zertifikat bietet eine `intermediate.crt` Zertifikat, das die `ontap_mediator_server.crt` Zertifikat, erstellen Sie eine Zertifikatskette aus dem `intermediate.crt` Und `ontap_mediator_server.crt` Zertifikate:

> Sie sollten die Zertifikate und von einer PKI-Behörde erhalten haben, die Sie zuvor im Verfahren erhalten haben `intermediate.crt` `ontap_mediator_server.crt` .

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

b. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` Datei.

   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_mediat
   or_server.key

   ssl_certfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
   or_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, die `ontap_mediator_server.key` .
   - Der `ssl_certfile` Wert ist der Pfad des `ontap_mediator_server_chain.crt` Datei.
   - Der `ssl_ca_certs` Wert ist der Pfad des `root_ca.crt` Datei.

   > Für SnapMirror Business Continuity (SM-BC)-Cluster müssen Sie die `intermediate.crt` Und `root_ca.crt` Zertifikate an einen ONTAP Cluster. Sehen"Konfigurieren Sie ONTAP Mediator und Cluster für SnapMirror Active Sync" .

c. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:

   - Eigentümer Der Linux-Gruppe: `netapp:netapp`
   - Linux-Berechtigungen: `600`

2. Starten Sie ONTAP Mediator neu, wenn die Zertifikate in der Konfigurationsdatei aktualisiert wurden:

   ```
   systemctl restart ontap_mediator
   ```

ONTAP Mediator 1.9.1 und 1.9

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

Schritte

1. Konfigurieren Sie die `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` Datei so, dass die standardmäßigen Variablenwerte in der Datei überschrieben `ontap_mediator.config.yaml` werden.

   Wenn Sie von einer PKI-Autorität erhalten `intermediate.crt` haben und den privaten Schlüssel am Speicherort speichern `intermediate.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, sollte die `ontap_mediator.user_config.yaml` Datei wie folgt aussehen:

Wenn Sie `intermediate.crt` das Zertifikat signiert `ontap_mediator_server.crt` haben, wird die `intermediate.srl` Datei generiert. Weitere Informationen finden Sie unter Schritt 2: Erstellen Sie ein Serverzertifikat, indem Sie mit einer Drittanbieter-CA-Zertifizierung signieren .

```
[root@scs000216655 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 Sie eine Zertifikatsstruktur verwenden, bei der die `root_ca.crt` Zertifikat bietet eine `intermediate.crt` Zertifikat, das die `ontap_mediator_server.crt` Zertifikat, erstellen Sie eine Zertifikatskette aus dem `intermediate.crt` Und `ontap_mediator_server.crt` Zertifikate:

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

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

b. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei.

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_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_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 `ontap_mediator_server.key`.
- Der `ca_certificate` Wert ist der Pfad der `root_ca.crt` Datei.

Für SnapMirror Business Continuity (SM-BC)-Cluster müssen Sie die `intermediate.crt` Und `root_ca.crt` Zertifikate an einen ONTAP Cluster. Sehen"Konfigurieren Sie ONTAP Mediator und Cluster für SnapMirror Active Sync" .

c. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:

- Eigentümer Der Linux-Gruppe: `netapp:netapp`
- Linux-Berechtigungen: `600`

2. Starten Sie ONTAP Mediator neu, wenn die Zertifikate in der Konfigurationsdatei aktualisiert wurden:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 und früher

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

Schritte

1. Konfigurieren Sie die `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.`

`user_config.yaml` Datei so, dass die standardmäßigen Variablenwerte in der Datei überschrieben `ontap_mediator.config.yaml` werden.

Wenn Sie von einer PKI-Autorität erhalten `ca.crt` haben und den privaten Schlüssel am Speicherort speichern `ca.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, sollte die `ontap_mediator.user_config.yaml` Datei wie folgt aussehen:

> Wenn Sie `ca.crt` das Zertifikat signiert `ontap_mediator_server.crt` haben, wird die `ca.srl` Datei generiert. Weitere Informationen finden Sie unter Schritt 2: Erstellen Sie ein Serverzertifikat, indem Sie mit einer Drittanbieter-CA-Zertifizierung signieren .

```
[root@scs000216655 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 Sie eine Zertifikatstruktur verwenden, in der das `root_ca.crt` Zertifikat ein Zertifikat bereitstellt `ca.crt` , das das Zertifikat signiert `ontap_mediator_server.crt` , erstellen Sie eine Zertifikatskette aus den `ca.crt` Zertifikaten und `ontap_mediator_server.crt` :

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

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

b. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei.

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_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_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 `ontap_mediator_server.key`.
- Der `ca_certificate` Wert ist der Pfad der `root_ca.crt` Datei.

Für SnapMirror-Cluster für Business Continuity (SM-BC) müssen Sie einem ONTAP-Cluster die Zertifikate und hinzufügen `ca.crt` `root_ca.crt` . Siehe "Konfigurieren Sie ONTAP Mediator und Cluster für SnapMirror Active Sync".

c. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:

- Eigentümer Der Linux-Gruppe: `netapp:netapp`
- Linux-Berechtigungen: `600`

2. Starten Sie ONTAP Mediator neu, wenn die Zertifikate in der Konfigurationsdatei aktualisiert wurden:

```
systemctl restart ontap_mediator
```

Fehlerbehebung bei zertifikatbezogenen Problemen

Sie können bestimmte Eigenschaften der Zertifikate überprüfen.

Überprüfen Sie den Ablauf des Zertifikats

Verwenden Sie den folgenden Befehl, um den Gültigkeitsbereich des Zertifikats zu identifizieren.

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
```

Überprüfen Sie die X509v3-Erweiterungen in der CA-Zertifizierung

Verwenden Sie den folgenden Befehl, um die X509v3-Erweiterungen in der CA-Zertifizierung zu überprüfen.

ONTAP Mediator 1.9 und höher

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

```
[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 **v3_ca** in definierten Eigenschaften `openssl_ca.cnf` werden wie in angezeigt `X509v3 extensions` `ca.crt`.

```
[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
```

Überprüfen Sie X509v3-Erweiterungen in Serverzertifikaten und Subject Alt-Namen

Die `v3_req` in der `openssl_server.cnf` Konfigurationsdatei definierten Eigenschaften werden als `X509v3 extensions` im Zertifikat angezeigt.

Im folgenden Beispiel erhalten Sie die Variablen in der `alt_names` Abschnitte durch Ausführen der Befehle `hostname -A` Und `hostname -I` auf der Linux-VM, auf der ONTAP Mediator installiert ist.

Erkundigen Sie sich bei Ihrem Netzwerkadministrator nach den korrekten Werten der Variablen.

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
```

Vergewissern Sie sich, dass ein privater Schlüssel mit einem Zertifikat übereinstimmt

Sie können überprüfen, ob ein bestimmter privater Schlüssel mit einem Zertifikat übereinstimmt.

Verwenden Sie die folgenden OpenSSL-Befehle auf dem Schlüssel bzw. dem Zertifikat.

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 für beide übereinstimmen, zeigt es an, dass der private Schlüssel und das Zertifikatspaar kompatibel sind und miteinander arbeiten können.

Überprüfen Sie, ob ein Serverzertifikat aus einem bestimmten CA-Zertifikat erstellt wurde

Mit dem folgenden Befehl können Sie überprüfen, ob das Serverzertifikat aus einem bestimmten CA-Zertifikat erstellt wird.

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 OCSP-Validierung (Online Certificate Status Protocol) verwendet wird, verwenden Sie den Befehl "openssl-Verify".

Warten Sie das Host-Betriebssystem für ONTAP Mediator

Um eine optimale Leistung zu erzielen, stellen Sie sicher, dass das Host-Betriebssystem für ONTAP Mediator regelmäßig gewartet wird.

Starten Sie den Host neu

Starten Sie den Host nur neu, wenn die Cluster fehlerfrei sind. Cluster können nicht auf Fehler reagieren, während ONTAP Mediator offline ist. Legen Sie einen Zeitpunkt für die Wartung fest, bevor Sie das System neu starten.

ONTAP Mediator wird während eines Neustarts automatisch fortgesetzt und stellt zuvor konfigurierte Beziehungen mit ONTAP Clustern wieder her.

Updates des Host-Pakets

Aktualisieren Sie alle Bibliotheken oder Yum-Pakete außer dem Kernel. Starten Sie den Host bei Bedarf neu, damit die Änderungen wirksam werden. Planen Sie vor dem Neustart des Hosts ein Servicefenster ein.

Wenn Sie das `yum-utils` Paket installieren, verwenden Sie den `needs-restarting` Befehl, um zu erkennen, ob Paketänderungen einen Neustart erfordern.

Führen Sie nach der Aktualisierung der ONTAP Mediator-Abhängigkeiten einen Neustart durch, da die Änderungen nicht sofort wirksam werden.

Aktualisieren Sie den Kernel des Host-Betriebssystems.

SCST muss für den von Ihnen verwendeten Kernel kompiliert werden. Um das Betriebssystem zu aktualisieren, müssen Sie einen Wartungstermin einplanen.

Schritte

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

> ⓘ Überprüfen Sie vor dem Upgrade des Kernels, ob das Betriebssystem und die ONTAP Mediator-Version kompatibel sind. Informationen zu unterstützten Versionen finden Sie im"OS Support-Matrix" .

1. Stoppen Sie ONTAP Mediator.
2. Deinstallieren Sie das SCST-Paket, siheDurchführen von Host-Wartungsarbeiten . (SCST bietet keinen Upgrade-Mechanismus.)
3. Aktualisieren Sie das Betriebssystem, und starten Sie es neu.
4. Installieren Sie das SCST-Paket erneut.
5. Aktivieren Sie ONTAP Mediator erneut.

Durchführen von Host-Wartungsarbeiten

Das Upgrade des VM-Kernels kann Kompatibilitätsprobleme mit SCST-Modulen verursachen. Deinstallieren Sie SCST manuell und installieren Sie es erneut.

Schritt 1: Deinstallieren Sie SCST

Um SCST zu deinstallieren, verwenden Sie das Tar-Paket für Ihre ONTAP Mediator-Version.

Schritte

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

Für diese Version …	Verwenden Sie dieses tar-Bündel…
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. Greifen Sie auf das Open Source-Paket zu über"SCST Sourceforge-Downloads" .
   b. Wählen Sie **Freigegebene Versionen herunterladen**.
   c. Extrahieren Sie das Paket auf Ihre VM.

2. Führen Sie die folgenden Deinstallationsbefehle im `scst` Verzeichnis:
   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: SCST installieren

Um SCST manuell zu installieren, benötigen Sie das SCST-Tar-Bundle, das für die installierte Version von ONTAP Mediator verwendet wird (sieheSCST-Tabelle).

Führen Sie diesen Schritt aus, bevor Sie den ONTAP Mediator installieren. Wenn die von Ihnen verwendete SCST-Version neuer ist als die mit dem ONTAP Mediator-Installationsprogramm gebündelte Version, überspringt das Installationsprogramm diesen Schritt.

1. Führen Sie die folgenden Installationsbefehle im `scst` Verzeichnis:
   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 bei einer Erstinstallation vor ONTAP Mediator vorinstallieren, überspringen Sie diesen Schritt. Das Installationsprogramm wendet relevante SCST-Patches an.

2. Wenn Secure Boot aktiviert ist, führen Sie vor dem Neustart optional die folgenden Schritte aus:
   a. Bestimmen Sie jeden 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. Bestimmen Sie die Kernel-Version:

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

c. Signieren Sie jede Moduldatei mit dem Kernel:

```
[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. Installieren Sie den UEFI-Schlüssel mit der Firmware.

Anweisungen zur Installation des UEFI-Schlüssels finden Sie 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. Starten Sie das System neu:

```
reboot
```

Host ändert sich zum Hostnamen oder IP

Über diese Aufgabe

- Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.
- Führen Sie diese Schritte nur durch, 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 Drittanbieterzertifikat ersetzt wurde, verwenden Sie diese Aufgabe *nicht*, um ein Zertifikat neu zu generieren. Wenn Sie kein selbstsigniertes Zertifikat besitzen, können Sie dieses Verfahren nicht verwenden.

Schritt

Erstellen Sie ein temporäres selbstsigniertes Zertifikat für den aktuellen Host:

1. Starten Sie ONTAP Mediator neu:

```
./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
```