



Documentation du médiateur ONTAP

ONTAP Mediator

NetApp
October 19, 2026

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

Sommaire

Documentation du médiateur ONTAP	1
Notes de version	2
Nouveautés d'ONTAP Mediator	2
Matrice de prise en charge d'ONTAP Mediator	4
Matrice de prise en charge des systèmes d'exploitation	4
Matrice de prise en charge SCST	7
Commencer	9
Découvrez ONTAP Mediator	9
Fonctionnement d'ONTAP Mediator	9
services ONTAP Mediator	9
Outils mis à la disposition de l'administrateur système	9
Mises à jour SCST et du noyau	10
Prise en charge de HTTPS et iSCSI	10
Démarrage rapide pour ONTAP Mediator	10
Et ensuite ?	11
Installation et configuration	12
Résumé du flux de travail d'installation d'ONTAP Mediator	12
Préparez-vous à installer ONTAP Mediator	12
exigences d'installation	13
Exigences de l'hôte	14
Exigences en matière de pare-feu et de réseau	14
exigences OS	15
Installez ONTAP Mediator lorsque le démarrage sécurisé UEFI est activé	16
Fournissez un accès au référentiel pour l'installation de ONTAP Mediator	17
Téléchargez le package d'installation d'ONTAP Mediator	25
Vérifiez la signature du code d'ONTAP Mediator	26
Installez le package d'installation de ONTAP Mediator	28
Enregistrez la clé de sécurité pour UEFI Secure Boot	46
Signer les modules du noyau SCST	47
Vérifiez l'état de l'installation d'ONTAP Mediator	48
Utiliser ONTAP Mediator	50
Utilisez ONTAP Mediator pour la synchronisation active de SnapMirror et MetroCluster IP	50
Surveiller les relations de synchronisation active de SnapMirror	50
Surveiller MetroCluster les configurations IP	50
Administrer ONTAP Mediator	52
Mettre à niveau ONTAP Mediator	52
Mettre à niveau ONTAP Mediator	52
Mettez à niveau le système d'exploitation hôte et réinstallez ou mettez à niveau ONTAP Mediator	60
Configurer les attributs de ONTAP Mediator	65
Paramètres configurables du médiateur ONTAP	65
Installer des certificats SSL tiers	66
Configurer la protection contre les attaques par mot de passe	68
Configurer les règles de complexité des mots de passe	69

Configurer le seuil d'espace libre	69
Configurer l'espace de journalisation réservé	69
Modifier le nom d'utilisateur et le mot de passe du médiateur ONTAP	70
Changer le nom d'utilisateur	70
Changer le mot de passe	71
Démarrer et arrêter ONTAP Mediator	72
Arrêtez ONTAP Mediator	72
Démarrer ONTAP Mediator	72
Vérifier l'état de santé de ONTAP Mediator	73
Vérifiez l'état du service	73
Vérifiez les ports d'écoute	74
Gérer les certificats	75
Régénérez un certificat temporaire auto-signé pour l'hôte ONTAP Mediator	75
Remplacez les certificats auto-signés d'ONTAP Mediator par des certificats tiers de confiance	76
Résoudre les problèmes liés aux certificats d'ONTAP Mediator	90
Maintenir le système d'exploitation hôte pour ONTAP Mediator	96
Redémarrez l'hôte	96
Mises à jour du package hôte	96
Mettre à niveau le noyau du système d'exploitation hôte	96
Effectuer la maintenance de l'hôte	97
Modifications du nom d'hôte ou de l'adresse IP de l'hôte	100
Désinstaller ONTAP Mediator	101
Mentions légales	102
Copyright	102
Marques déposées	102
Brevets	102
Politique de confidentialité	102
Open source	102
ONTAP Mediator pour MetroCluster IP et SnapMirror active sync	102

Documentation du médiateur ONTAP

Notes de version

Nouveautés d'ONTAP Mediator

Chaque nouvelle version d'ONTAP Mediator apporte de nouvelles améliorations.



Pour plus d'informations sur les versions du système d'exploitation et de SCST, consultez le ["Matrice de support"](#).

Version ONTAP Mediator	Améliorations
1.12.1	• Prise en charge de RHEL : ◦ Compatible : 10.1 et 9.7. ◦ Recommandé : 10.2, 10.0, 9.8, 9.6, 9.4 et 8.10. • Prise en charge de Rocky Linux 10.2, 9.8 et 8.10. • Prise en charge d'Oracle Linux 10.1 et 9.8 avec les noyaux rhck et uek. • À partir d'ONTAP Mediator 1.12.1 et ONTAP 9.19.1, une seule instance d'ONTAP Mediator configurée avec HTTPS peut surveiller simultanément les configurations suivantes : ◦ Un maximum de dix configurations IP MetroCluster à quatre nœuds ou cinq à huit nœuds si elles sont installées sur un hôte doté d'un processeur à 8 cœurs et d'au moins 16 Go de RAM. Voir "Utilisez ONTAP Mediator pour surveiller plusieurs configurations IP MetroCluster". ◦ Une configuration IP MetroCluster à quatre nœuds et une relation de synchronisation active entre pairs SnapMirror si elle est installée sur un hôte doté d'un processeur à 2 cœurs. Voir "Configurez ONTAP Mediator pour la synchronisation active SnapMirror". • Inclut un nouvel outil pour réparer une installation SCST défectueuse. Après l'installation d'ONTAP Mediator, vous pouvez trouver l'outil à <code>/usr/local/bin/mediator_repair_scst</code>. Vous pouvez utiliser l'outil après une mise à niveau du système d'exploitation, si le système d'exploitation mis à niveau requiert un correctif SCST qui n'est pas disponible dans le package SCST par défaut.
1,12	• Prise en charge de RHEL : ◦ Compatible : 10.1 et 9.7. ◦ Recommandé : 10.2, 10.0, 9.8, 9.6, 9.4 et 8.10. • Prise en charge de Rocky Linux 10.2, 9.8 et 8.10. • Prise en charge d'Oracle Linux 10.1 et 9.7 avec les noyaux rhck et uek. • À partir d'ONTAP 9.19.1 et ONTAP Mediator 1.12, vous pouvez configurer un ONTAP Mediator qui utilise HTTPS pour la communication dans les configurations IP MetroCluster. HTTPS offre une sécurité accrue en chiffrant l'intégralité des sessions à l'aide de SSL/TLS. Vous pouvez choisir d'installer ONTAP Mediator avec la prise en charge de HTTPS uniquement. Le package SCST n'est pas installé si cette méthode d'installation est utilisée. "En savoir plus sur les options d'installation HTTPS et iSCSI pour ONTAP Mediator".

1,11	• Prise en charge de RHEL 10.1, 10.0, 9.7, 9.6, 9.4 et 8.10. • Prise en charge de Rocky Linux 10.1, 9.7 et 8.10. • Prise en charge d'Oracle Linux 10.0 et 9.6 avec les noyaux rhck et uek. • Ajoute la prise en charge d'IPv6 pour les configurations IP MetroCluster. • Ajoute la prise en charge de fapolicyd.
1,10	• Prise en charge de RHEL 10.0, 9.6, 9.4 et 8.10. • Prise en charge de Rocky Linux 10.0, 9.6 et 8.10. • Met à jour la version Python de base de Python 3.9 à Python 3.12.
1.9.1	• Prise en charge de RHEL : ◦ Compatible : 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 et 8.4. ◦ Recommandé : 9.5, 9.4, 9.2, 9.0, 8.10 et 8.8. • Prise en charge de Rocky Linux 9.5 et 8.10. • Ajoute de nouveaux certificats pour la vérification de signature de code. • Ajout de la prise en charge du saut des vérifications de signature de code à l'aide de l'indicateur <code>-skip-code-signature-check</code>. • Le programme d'installation affiche des avertissements lorsqu'il détecte des certificats de signature de code expirés.
1,9	• Prise en charge de RHEL : ◦ Compatible : 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 et 8.4. ◦ Recommandé : 9.5, 9.4, 9.2, 9.0, 8.10 et 8.8. • Prise en charge de Rocky Linux 9.5 et 8.10. • Prise en charge FIPS pour RHEL et Rocky Linux. • Ajout d'améliorations des performances pour une plus grande évolutivité. • Amélioration des noms de fichiers afin de simplifier la configuration des certificats signés par une infrastructure à clés publiques (PKI).
1,8	• Prise en charge de RHEL : ◦ Compatible : 8.7, 8.6, 8.5 et 8.4. ◦ Recommandé: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 et 8.8. • Prise en charge de Rocky Linux 9.4 et 8.10.
1,7	• Prise en charge de RHEL : ◦ Compatible : 8.7, 8.6, 8.5 et 8.4. ◦ Recommandé : 9.3, 9.2, 9.1, 9.0, 8.9 et 8.8. • Prise en charge de Rocky Linux 9.3 et 8.9. • Prise en charge des données SAN (Subject Alternative Name) dans les certificats auto-signés et les certificats signés par un tiers.

1,6	• Mises à jour de Python 3.9. • Prise en charge de RHEL : ◦ Compatible : 8.7, 8.6, 8.5 et 8.4. ◦ Recommandé: 9.2, 9.1, 9.0 et 8.8. • Prise en charge de Rocky Linux 9.2 et 8.8. • Fin du support pour RHEL 7.x / CentOS toutes les versions.
1,5	• Prise en charge de RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 et 7.6. • Prise en charge de CentOS 7.9, 7.8, 7.7 et 7.6. • Inclut des avertissements de dépréciation pour RHEL 7.x / CentOS 7.x. • Optimise la vitesse pour les systèmes de synchronisation active SnapMirror à grande échelle. • Une signature de code cryptographique a été ajoutée au programme d'installation.
1,4	• Prise en charge de RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 et 7.6. • Prise en charge de CentOS 7.9, 7.8, 7.7 et 7.6. • Ajout de la prise en charge du démarrage sécurisé (SB) du firmware basé sur UEFI.
1,3	• Prise en charge de RHEL 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 et 7.6. • Prise en charge de CentOS 7.9, 7.8, 7.7 et 7.6.
1,2	• Prise en charge de RHEL 8.1, 8.0, 7.9, 7.8, 7.7 et 7.6. • Prise en charge de CentOS 7.9, 7.8, 7.7 et 7.6. • Prise en charge des boîtes aux lettres HTTPs. • À utiliser avec ONTAP 9.8+ MCC-IP AUSO et la synchronisation active SnapMirror ZRTO.
1,1	• Prise en charge de RHEL 8.0 et 7.6. • Prise en charge de CentOS 7.6. • Élimine les dépendances à Perl.
1,0	• Prise en charge des boîtes aux lettres iSCSI. • À utiliser avec ONTAP 9.7+ MCC-IP AUSO. • Prise en charge de RHEL/CentOS 7.6.

Matrice de prise en charge d'ONTAP Mediator

La matrice de compatibilité d'ONTAP Mediator inclut des informations sur la prise en charge des systèmes d'exploitation et des versions de SCST.

Matrice de prise en charge des systèmes d'exploitation

Le tableau suivant répertorie les systèmes d'exploitation pris en charge pour chaque version d'ONTAP Mediator.

Système d'exploitation pour ONT AP Mediator	1.12.1	1,12	1,11	1,10	1.9.1	1,9	1,8	1,7	1,6	1,5	1,4	1,3	1,2	1,1	1,0
RHEL 10,2	Oui	Oui	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
RHEL 10,1	Compatible	Compatible	Oui	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
RHEL 10,0	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
RHEL 9,8	Oui	Oui	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
RHEL 9,7	Compatible	Compatible	Oui	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
RHEL 9,6	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
RHEL 9,5	Non	Non	Non	Non	Oui	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
RHEL 9,4	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non	Non	Non
RHEL 9,3	Non	Non	Non	Non	Non	Non	Oui	Oui	Non	Non	Non	Non	Non	Non	Non
RHEL 9,2	Non	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non
RHEL 9,1	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non
RHEL 9,0	Non	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non
RHEL 8,10	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non	Non	Non
RHEL 8,9	Non	Non	Non	Non	Compatible	Compatible	Oui	Oui	Non	Non	Non	Non	Non	Non	Non
RHEL 8,8	Non	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non

RHEL 8,7	Non	Non	Non	Non	Compatible	Compatible	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non
RHEL 8,6	Non	Non	Non	Non	Compatible	Compatible	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non
RHEL 8,5	Non	Non	Non	Non	Compatible	Compatible	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non
RHEL 8,4	Non	Non	Non	Non	Compatible	Compatible	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non
RHEL 8,3	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Oui	Oui	Oui	Non	Non	Non
RHEL 8,2	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Oui	Oui	Oui	Non	Non	Non
RHEL 8,1	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Oui	Oui	Oui	Oui	Non	Non
RHEL 8,0	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Oui	Oui	Oui	Oui	Oui	Non
RHEL et CentOS 7.9	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Oui	Oui	Oui	Compatible	Non	Non
RHEL et CentOS 7.8	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Oui	Oui	Oui	Oui	Non	Non
RHEL et CentOS 7.7	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Oui	Oui	Oui	Oui	Non	Non
RHEL et CentOS 7.6	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Obsolète	Oui	Oui	Oui	Oui	Oui	Oui (RHEL uniquement)
CentOS 8 et stream	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	S/O	S/O	S/O

Rocky Linux 10	Oui (10.2)	Oui (10.2)	Oui (10.0 et 10.1)	Oui	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
Rocky Linux 9	Oui (9.8)	Oui (9.8)	Oui (9.7)	Oui (9.6 et 9.4)	Oui (9.5)	Oui (9.5)	Oui (9.4)	Oui (9.3)	Oui (9.2)	S/O	S/O	S/O	S/O	S/O	S/O
Rocky Linux 8	Oui (8.10)	Oui (8.10)	Oui (8.10)	Oui (8.10)	Oui (8.10)	Oui (8.10)	Oui (8.10)	Oui (8.9)	Oui (8.8)	S/O	S/O	S/O	S/O	S/O	S/O
Oracle Linux 10	Oui (10.1)	Oui (10.1)	Oui (10.0)	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
Oracle Linux 9	Oui (9.8)	Oui (9.7)	Oui (9.6)	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non

- « Oui » signifie que le système d'exploitation est recommandé pour l'installation d'ONTAP Mediator et qu'il est entièrement compatible et pris en charge.
- « Non » signifie que le système d'exploitation et ONTAP Mediator ne sont pas compatibles.
- « Compatible » signifie que Red Hat ne prend plus en charge ces versions de RHEL, mais ONTAP Mediator peut toujours y être installé.
- ONTAP Mediator 1.6 ajoute la prise en charge de Rocky Linux 9 et 8.
- ONTAP Mediator 1.5 était la dernière version prise en charge pour les systèmes d'exploitation de la branche RHEL 7.x.
- Centos 8 a été retiré de toutes les versions en raison de sa réorganisation des branches. Centos Stream a été jugé inadapté à une utilisation en production. Aucun support n'est prévu.

Matrice de prise en charge SCST

Le tableau suivant présente la version SCST prise en charge pour chaque version d'ONTAP Mediator.

Version ONTAP Mediator	Version SCST prise en charge
ONTAP Mediator 1.12.1	scst-3.10.tar.gz
ONTAP Mediator 1.12	scst-3.10.tar.gz
ONTAP Mediator 1.11	scst-3.9.tar.gz
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAP Mediator 1.9.1	scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	scst-3.8.0.tar.bz2

Version ONTAP Mediator	Version SCST prise en charge
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

Commencer

Découvrez ONTAP Mediator

ONTAP Mediator prend en charge les fonctionnalités ONTAP en fournissant un stockage persistant et isolé pour les métadonnées de haute disponibilité (HA), une fonctionnalité de requête synchrone de l'état des nœuds pour faciliter la détermination du quorum, et en servant de proxy ping pour la disponibilité du contrôleur.



Cette documentation concerne la version sur site de ONTAP Mediator. Pour plus d'informations sur ONTAP Cloud Mediator, disponible à partir de ONTAP 9.17.1, veuillez consulter la ["Documentation de SnapMirror active sync"](#).

Fonctionnement d'ONTAP Mediator

ONTAP Mediator s'exécute sur un hôte Linux dans un troisième domaine de défaillance, distinct de vos clusters ONTAP, où il fournit un stockage persistant et isolé pour les métadonnées HA. ONTAP utilise ce stockage, ainsi que les fonctions de requête d'état des nœuds et de proxy ping de Mediator, pour surveiller les relations de synchronisation active SnapMirror et les configurations IP MetroCluster.

- ONTAP Mediator utilise la LIF de gestion des nœuds et la LIF de gestion de cluster pour communiquer avec chaque cluster via plusieurs chemins redondants. Cela permet à ONTAP de distinguer une défaillance complète du site d'une défaillance unique de liaison InterSwitch (ISL).
- En mode de synchronisation active SnapMirror, si un cluster perd la connexion à la fois avec son homologue et avec ONTAP Mediator, ONTAP considère l'homologue comme inaccessible et peut basculer automatiquement vers la copie survivante.
- Dans les configurations IP MetroCluster, ONTAP Mediator facilite un basculement automatique non planifié assisté par médiateur (MAUSO) en stockant des informations d'état sur les nœuds MetroCluster et en aidant à déterminer la marche à suivre appropriée en cas de panne.

services ONTAP Mediator

ONTAP Mediator fournit deux services systemctl supplémentaires :

- **ontap_mediator.service**

Assure la maintenance du serveur d'API REST pour la gestion des relations ONTAP.

- **mediator-scst.service**

Contrôle le démarrage et l'arrêt du module iSCSI (SCST).

Outils mis à la disposition de l'administrateur système

Outils mis à la disposition de l'administrateur système :

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

Définit un nouveau mot de passe API lorsque le nom d'utilisateur API et le mot de passe actuels sont fournis.

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

Définit un nouveau nom d'utilisateur API lorsque le nom d'utilisateur et le mot de passe API actuels sont fournis.

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

Génère un fichier tgz local contenant toutes les informations de support utiles nécessaires pour communiquer avec le support client de NetApp. Cela inclut la configuration de l'application, les journaux et certaines informations système. Les bundles sont générés sur le disque local et peuvent être transférés manuellement, si nécessaire. Emplacement de stockage : `/opt/netapp/data/support_bundles/`

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

Supprime le package ONTAP Mediator et le module de noyau SCST. Cela inclut toute la configuration, les journaux et les données de boîte aux lettres.

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

Déverrouille le compte utilisateur de l'API si la limite de tentatives d'authentification a été atteinte. Cette fonctionnalité permet d'empêcher les attaques par force brute sur les mots de passe. Elle invite l'utilisateur à saisir le nom d'utilisateur et le mot de passe corrects.

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

(Support uniquement) Permet d'ajouter l'utilisateur de l'API lors de l'installation.

Mises à jour SCST et du noyau

ONTAP Mediator utilise SCST pour fournir iSCSI pour la communication dans les configurations IP MetroCluster. Le paquet SCST est un module noyau compilé lors de l'installation. Vous pourriez avoir besoin de réinstaller SCST après des mises à jour du noyau. Vous pouvez également désinstaller ONTAP Mediator, puis réinstaller et reconfigurer la relation ONTAP. Consultez ["SCST : un sous-système cible SCSI générique pour Linux"](#) pour en savoir plus sur SCST.



Vous devez coordonner toute mise à jour du noyau du système d'exploitation du serveur avec une fenêtre de maintenance dans ONTAP.

Prise en charge de HTTPS et iSCSI

À partir de ONTAP 9.19.1 et ONTAP Mediator 1.12, vous pouvez configurer un ONTAP Mediator qui utilise HTTPS ou iSCSI pour surveiller une configuration IP MetroCluster. Vous pouvez choisir d'installer ONTAP Mediator avec la prise en charge à la fois d'iSCSI et de HTTPS, ou uniquement de HTTPS. Si ONTAP Mediator est installé avec la prise en charge de HTTPS uniquement, le package SCST n'est pas installé. Consultez ["Options d'installation HTTPS et iSCSI pour ONTAP Mediator"](#) pour plus d'informations.

Démarrage rapide pour ONTAP Mediator

Pour commencer à utiliser ONTAP Mediator, vous installez le logiciel et le configurez pour qu'il fonctionne avec votre environnement ONTAP.

1**Installer ONTAP Mediator**

["Installer ONTAP Mediator"](#) sur votre système et assurez-vous que toutes les dépendances requises sont satisfaites.

2**Vérifiez l'installation d'ONTAP Mediator**

["Vérifiez que l'installation de ONTAP Mediator a réussi"](#) en vérifiant l'état du service et en consultant les journaux pour détecter toute erreur ou tout avertissement.

3**Configurez ONTAP Mediator pour votre environnement ONTAP**

Selon que vous souhaitez ["Utilisez ONTAP Mediator pour MetroCluster IP, SnapMirror active sync, ou les deux"](#), suivez les étapes de configuration appropriées pour vous assurer que tous les paramètres nécessaires sont correctement appliqués.

Et ensuite ?

Vous pouvez désormais utiliser ONTAP Mediator pour surveiller les configurations IP de MetroCluster, les configurations de synchronisation active de SnapMirror, ou les deux. Pour plus d'informations, consultez ["Documentation de SnapMirror active sync"](#) et ["Documentation MetroCluster"](#).

Installation et configuration

Résumé du flux de travail d'installation d'ONTAP Mediator

L'installation d'ONTAP Mediator comprend la préparation de l'installation, la fourniture de l'accès aux référentiels, le téléchargement du package d'installation, la vérification de la signature du code et l'installation du package ONTAP Mediator.

1

"Préparez-vous à installer ONTAP Mediator"

Pour installer ONTAP Mediator, vous devez vous assurer que toutes les conditions préalables sont remplies.

2

"Fournir l'accès au référentiel"

Vous devez autoriser l'accès aux référentiels afin qu'ONTAP Mediator puisse accéder aux packages requis pendant le processus d'installation.

3

"Téléchargez le package d'installation d'ONTAP Mediator"

Téléchargez le package d'installation d'ONTAP Mediator depuis la page de téléchargement d'ONTAP Mediator.

4

"Vérifiez la signature du code du package d'installation d'ONTAP Mediator"

NetApp recommande de vérifier la signature du code de ONTAP Mediator avant d'installer le package d'installation de ONTAP Mediator.

5

"Installez le package d'installation de ONTAP Mediator"

Téléchargez le package d'installation et exécutez le programme d'installation sur l'hôte.

6

"Vérifiez l'installation d'ONTAP Mediator"

Après avoir installé ONTAP Mediator, vérifiez qu'il fonctionne correctement.

Préparez-vous à installer ONTAP Mediator

Pour installer ONTAP Mediator, vous devez remplir toutes les conditions préalables, télécharger le package d'installation et exécuter le programme d'installation sur l'hôte.



- Pour mettre à niveau ONTAP Mediator vers une nouvelle version, consultez ["Mettre à niveau ONTAP Mediator"](#).
- Si vous devez mettre à niveau le système d'exploitation hôte et réinstaller ou mettre à niveau ONTAP Mediator dans le cadre de ce processus, consultez ["Mettez à niveau le système d'exploitation hôte et ONTAP Mediator"](#).

exigences d'installation

Veuillez prendre connaissance des exigences suivantes avant d'installer ONTAP Mediator.



- ONTAP Mediator 1.8 et les versions antérieures ne sont pas compatibles avec le mode FIPS de Red Hat Enterprise Linux (RHEL) et empêchent son installation correcte. Vous pouvez vérifier si le mode FIPS est activé à l'aide de la commande `fips-mode-setup --check`. Vous pouvez désactiver le mode FIPS à l'aide de la commande `fips-mode-setup --disable`. Redémarrez le système après avoir désactivé le mode FIPS pour installer correctement ONTAP Mediator 1.8 ou une version antérieure.
- Si l'installation échoue, vous devrez peut-être essayer une version plus récente d'ONTAP Mediator.
- À compter du 15 juin 2025, vous ne pouvez plus installer ni mettre à niveau ONTAP Mediator 1.9 et 1.8, car leurs certificats de signature de code ont expiré. Si l'installation échoue, utilisez plutôt la version de correctif ONTAP Mediator 1.9.1.

- Si vous installez le `yum-utils` paquet, vous pouvez utiliser la `needs-restarting` commande.
- À partir de ONTAP Mediator 1.11, IPv6 est pris en charge pour les configurations IP MetroCluster.

Options d'installation HTTPS et iSCSI pour ONTAP Mediator

Avant d'installer ONTAP Mediator, veuillez consulter les informations suivantes :

- Dans ONTAP Mediator, le package SCST est utilisé pour fournir iSCSI pour la communication dans les configurations IP MetroCluster. Le package SCST est un module du noyau compilé lors de l'installation. À partir de ONTAP 9.19.1 et Mediator 1.12, vous pouvez configurer un ONTAP Mediator qui utilise HTTPS au lieu d'iSCSI pour surveiller une configuration IP MetroCluster.
- À partir d'ONTAP 9.19.1 et ONTAP Mediator 1.12, vous avez la possibilité d'installer ONTAP Mediator avec la prise en charge d'iSCSI et d'HTTPS, ou uniquement avec la prise en charge d'HTTPS. Si vous choisissez d'installer ONTAP Mediator avec la prise en charge d'HTTPS uniquement, le package SCST n'est pas installé.
- Si vous effectuez une mise à niveau depuis ONTAP Mediator 1.11 ou une version antérieure avec SCST installé, et que vous choisissez l'option HTTPS uniquement lors de la mise à niveau, le package SCST est désinstallé et la nouvelle version d'ONTAP Mediator ne contient pas le package SCST.
- Si vous prévoyez d'utiliser ONTAP Mediator pour surveiller plusieurs configurations IP MetroCluster, la prise en charge dépend de votre type de Mediator, de la version d'ONTAP et du système d'exploitation. Consultez ["Utilisez ONTAP Mediator pour surveiller plusieurs configurations IP MetroCluster"](#) pour plus d'informations.
- L'installation ONTAP Mediator avec prise en charge du protocole HTTPS uniquement est prise en charge pour les cas d'utilisation suivants :
 - Vous prévoyez d'utiliser uniquement ONTAP Mediator pour surveiller vos clusters de synchronisation active SnapMirror.
 - Vous prévoyez de configurer ONTAP Mediator avec HTTPS pour surveiller une ou plusieurs configurations IP MetroCluster.
- ONTAP Mediator doit être installé avec la prise en charge d'iSCSI et de HTTPS dans le scénario suivant :
 - Vous prévoyez de configurer ONTAP Mediator avec iSCSI pour surveiller une ou plusieurs configurations IP MetroCluster.

Exigences de l'hôte

Respectez ces exigences lors de l'installation de RHEL ou Rocky Linux et de la configuration des dépôts associés.



Si vous modifiez le processus d'installation ou de configuration, vous devrez peut-être suivre des étapes supplémentaires.

Exigences relatives à la distribution Linux

- Installez RHEL ou Rocky Linux en suivant les meilleures pratiques de Red Hat. Comme CentOS 8.x a atteint sa fin de vie, les versions compatibles de CentOS 8.x ne sont pas recommandées.
- Lors de l'installation d'ONTAP Mediator, assurez-vous que le système a accès au référentiel requis afin que le programme d'installation puisse récupérer et installer toutes les dépendances logicielles requises.
- Pour permettre à l'installateur yum de trouver les logiciels dépendants dans les dépôts RHEL, enregistrez le système pendant l'installation ou ultérieurement à l'aide d'un abonnement Red Hat valide.



Consultez la documentation de Red Hat Subscription Manager pour plus d'informations.

Exigences en matière de pare-feu et de réseau

ONTAP Mediator utilise plusieurs ports pour communiquer avec des services spécifiques.

- Si vous utilisez un pare-feu tiers :
 - L'accès HTTPS doit être activé.
 - Il doit être configuré pour autoriser l'accès sur les ports 31784 et 3260.

Lors de l'utilisation du pare-feu par défaut de Red Hat ou CentOS, celui-ci est automatiquement configuré lors de l'installation de Mediator.

- Pour les hôtes Linux sans accès à Internet, assurez-vous que les paquets requis sont disponibles dans un dépôt local.

Si vous utilisez le protocole LACP (Link Aggregation Control Protocol) dans un environnement Linux, configurez le noyau et définissez le `sysctl net.ipv4.conf.all.arp_ignore` sur 2.

Le tableau suivant répertorie les ports que vous devez autoriser dans votre pare-feu :



- Le port iSCSI n'est requis que dans une configuration IP MetroCluster.
- Le port 22/tcp n'est pas nécessaire au fonctionnement normal, mais vous pouvez l'activer temporairement pour la maintenance et le désactiver une fois la session de maintenance terminée.

Ports/services	Source	Direction	Destination	But
22/tcp	Hôte de gestion	Entrant	ONTAP Mediator	(Facultatif) Gestion SSH / ONTAP Mediator
31784/tcp	LIF cluster-mgmt et node-mgmt	Entrant	Serveur web ONTAP Mediator	(Obligatoire) API REST (HTTPS)

3260/tcp	LIFs de gestion de nœud	Entrant	Cibles iSCSI du médiateur ONTAP	(Requis pour les configurations IP MetroCluster) connexion de données iSCSI pour les boîtes aux lettres
----------	-------------------------	---------	---------------------------------	---



Pour un SnapMirror active sync ou MetroCluster IP ONTAP Mediator qui utilise HTTPS pour la communication, ONTAP n'a pas besoin que le port 3260 soit activé ou connecté.

exigences OS

Votre système d'exploitation doit répondre aux exigences suivantes :

- installation physique 64 bits ou machine virtuelle
- 8 Go de RAM
- 1 Go d'espace disque (utilisé pour l'installation des applications, les journaux du serveur et la base de données)
- Utilisateur : accès root

Consultez "[Matrice de prise en charge des systèmes d'exploitation](#)" pour connaître les systèmes d'exploitation pris en charge pour chaque version d'ONTAP Mediator.

Paquets requis par le système d'exploitation

Les packages suivants sont requis par ONTAP Mediator:



Les packages sont soit préinstallés, soit installés automatiquement par le programme d'installation ONTAP Mediator.

Toutes les versions de RHEL/CentOS	Paquets supplémentaires pour RHEL 10.x / Rocky Linux 10	Paquets supplémentaires pour RHEL 9.x / Rocky Linux 9	Paquets supplémentaires pour RHEL 8.x / Rocky Linux 8
------------------------------------	---	---	---

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

Le paquet d'installation de Mediator est un fichier tar compressé auto-extractible qui comprend:

- Un fichier RPM contenant toutes les dépendances qui ne peuvent pas être obtenues à partir du dépôt de la version prise en charge.
- Un script d'installation.

Un certificat SSL valide est recommandé.



- La version du noyau doit correspondre à la version du système d'exploitation.
- Ne mettez pas à niveau le noyau au-delà de la version du système d'exploitation prise en charge pour votre version d'ONTAP Mediator, car le module SCST testé pourrait ne pas fonctionner.

Installez ONTAP Mediator lorsque le démarrage sécurisé UEFI est activé

ONTAP Mediator peut être installé sur un système avec ou sans démarrage sécurisé UEFI activé.

À propos de cette tâche

- Vous pouvez choisir de désactiver le démarrage sécurisé UEFI avant d'installer ONTAP Mediator si cela n'est pas nécessaire ou si vous résolvez des problèmes d'installation de ONTAP Mediator. Désactivez l'option de démarrage sécurisé UEFI dans les paramètres de votre ordinateur.
- Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure prenant uniquement en charge HTTPS, le package SCST n'est pas installé et vous pouvez ignorer cette tâche.



Pour obtenir des instructions détaillées sur la désactivation du démarrage sécurisé UEFI, reportez-vous à la documentation de votre système d'exploitation hôte.

Pour installer ONTAP Mediator avec le démarrage sécurisé UEFI activé, vous devez enregistrer une clé de sécurité avant que le service puisse démarrer. La clé est générée lors de l'étape de compilation de l'installation de SCST et enregistrée sous forme de paire de clés privée/publique sur votre machine. Utilisez l'`mokutil` utilitaire pour ajouter la clé publique en tant que Machine Owner Key (MOK) à votre micrologiciel

UEFI, afin de permettre au système de faire confiance au module signé et de le charger. Enregistrez la `mokutil` phrase secrète dans un emplacement sécurisé, car elle sera nécessaire lors du redémarrage de votre système pour activer la MOK.

Étapes

1. Vérifiez si le démarrage sécurisé UEFI est activé sur votre système :

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

Les résultats indiquent si le démarrage sécurisé UEFI est activé sur ce système.

Si...	Accédez à...
Le démarrage sécurisé UEFI est activé	
Le démarrage sécurisé UEFI est désactivé	"Fournissez un accès au référentiel pour l'installation de ONTAP Mediator"



- Vous êtes invité à créer une phrase de passe que vous devez conserver en lieu sûr. Vous aurez besoin de cette phrase de passe pour activer la clé dans le Gestionnaire de démarrage UEFI.
- ONTAP Mediator 1.2.0 et les versions antérieures ne prennent pas en charge ce mode.

2. Si l' `mokutil` utilitaire n'est pas installé, exécutez la commande suivante :

```
yum install mokutil
```

Quelle est la prochaine étape ?

["Fournissez un accès au référentiel pour l'installation de ONTAP Mediator"](#)

Fournissez un accès au référentiel pour l'installation de ONTAP Mediator

Vous devez autoriser l'accès aux référentiels afin qu'ONTAP Mediator puisse accéder aux packages requis pendant le processus d'installation.

Étapes

1. Déterminez les référentiels auxquels il faut accéder, comme indiqué dans le tableau suivant :

Si votre système d'exploitation est...	Vous devez autoriser l'accès à ces dépôts...
Oracle Linux 10.x	• ol-10-for-x86_64-baseos-rpms • ol-10-for-x86_64-appstream-rpms
Oracle Linux 9.x	• ol-9-for-x86_64-baseos-rpms • ol-9-for-x86_64-appstream-rpms

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

2. Utilisez l'une des procédures suivantes pour autoriser l'accès aux référentiels répertoriés ci-dessus afin qu'ONTAP Mediator puisse accéder aux paquets requis pendant le processus d'installation.



Si ONTAP Mediator dépend de modules Python présents dans les dépôts « extras » et « optional », il pourrait avoir besoin d'accéder aux `rhel-X-for-x86_64-extras-rpms` et `rhel-X-for-x86_64-optional-rpms` fichiers.

▼ Procédure pour le système d'exploitation Oracle Linux 10.x

Utilisez cette procédure si votre système d'exploitation est **Oracle Linux 10.x** pour activer l'accès aux référentiels :

Étapes

- a. Abonnez-vous au dépôt requis :

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

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

L'exemple suivant illustre l'exécution de cette commande :

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

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

- b. Exécutez la commande suivante pour répertorier les dépôts activés :

```
yum repolist
```

Les dépôts auxquels vous venez de vous abonner devraient apparaître dans la liste.

▼ Procédure pour le système d'exploitation Oracle Linux 9.x

Utilisez cette procédure si votre système d'exploitation est **Oracle Linux 9.x** pour activer l'accès aux référentiels :

Étapes

- a. Abonnez-vous au dépôt requis :

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

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

L'exemple suivant illustre l'exécution de cette commande :

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

- b. Exécutez la commande suivante pour répertorier les dépôts activés :

```
yum repolist
```

Les dépôts auxquels vous venez de vous abonner devraient apparaître dans la liste.

▼ Procédure pour le système d'exploitation RHEL 10.x

Utilisez cette procédure si votre système d'exploitation est **RHEL 10.x** pour activer l'accès aux dépôts :

Étapes

- a. Abonnez-vous au dépôt requis :

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

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

L'exemple suivant illustre l'exécution de cette commande :

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

b. Exécutez la commande suivante pour répertorier les dépôts activés :

```
yum repolist
```

Les dépôts auxquels vous venez de vous abonner devraient apparaître dans la liste.

▼ Procédure pour le système d'exploitation RHEL 9.x

Utilisez cette procédure si votre système d'exploitation est **RHEL 9.x** pour activer l'accès aux référentiels :

Étapes

a. Abonnez-vous au dépôt requis :

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

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

L'exemple suivant illustre l'exécution de cette commande :

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

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

b. Exécutez la commande suivante pour répertorier les dépôts activés :

```
yum repolist
```

Les dépôts auxquels vous venez de vous abonner devraient apparaître dans la liste.

▼ Procédure pour le système d'exploitation RHEL 8.x

Utilisez cette procédure si votre système d'exploitation est **RHEL 8.x** pour activer l'accès aux dépôts:

Étapes

a. Abonnez-vous au dépôt requis :

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

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

L'exemple suivant illustre l'exécution de cette commande :

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

b. Exécutez la commande suivante pour répertorier les dépôts activés :

```
yum repolist
```

Les dépôts auxquels vous venez de vous abonner devraient apparaître dans la liste.

▼ Procédure pour le système d'exploitation RHEL 7.x

Utilisez cette procédure si votre système d'exploitation est **RHEL 7.x** afin d'activer l'accès aux dépôts :

Étapes

- a. Abonnez-vous au dépôt requis :

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

L'exemple suivant illustre l'exécution de cette commande :

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

- b. Exécutez la commande suivante pour répertorier les dépôts activés :

```
yum repolist
```

L'exemple suivant illustre l'exécution de cette commande. Le dépôt « rhel-7-server-optional-rpms » devrait apparaître dans la liste.

```
[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 ~]#
```

▼ Procédure pour le système d'exploitation CentOS 7.x

Utilisez cette procédure si votre système d'exploitation est **CentOS 7.x** afin d'activer l'accès aux dépôts :



Les exemples suivants présentent un dépôt pour CentOS 7.6 et peuvent ne pas fonctionner avec d'autres versions de CentOS. Utilisez le dépôt de base correspondant à votre version de CentOS.

Étapes

- a. Ajoutez le dépôt C7.6.1810 - Base. Le dépôt vault C7.6.1810 - Base contient le paquet « kernel-devel » nécessaire à ONTAP Mediator.
- b. Ajoutez les lignes suivantes à /etc/yum.repos.d/CentOS-Vault.repo.

```
[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
```

- c. Exécutez la commande suivante pour répertorier les dépôts activés :

```
yum repolist
```

L'exemple suivant illustre l'exécution de cette commande. Le dépôt CentOS-7.6.1810 - Base devrait apparaître dans la liste.

```
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 ~]#
```

▼ Procédure pour les systèmes d'exploitation Rocky Linux 10, 9 ou 8

Utilisez cette procédure si votre système d'exploitation est **Rocky Linux 10**, **Rocky Linux 9** ou **Rocky Linux 8** pour activer l'accès aux dépôts:

Étapes

a. Abonnez-vous aux dépôts requis :

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

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

b. Effectuez une clean opération :

```
dnf clean all
```

c. Vérifiez la liste des dépôts :

```
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 ~]#
```

Quelle est la prochaine étape ?

"Téléchargez le package d'installation d'ONTAP Mediator"

Téléchargez le package d'installation d'ONTAP Mediator

Téléchargez le package d'installation de ONTAP Mediator et installez-le.

Étapes

1. Téléchargez le package d'installation d'ONTAP Mediator depuis la page de téléchargement d'ONTAP Mediator.

"Page de téléchargement d'ONTAP Mediator"

2. Placez le package d'installation de Mediator dans le répertoire de travail actuel :

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

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



Pour les versions 1.4 et antérieures d'ONTAP Mediator, le programme d'installation est nommé `ontap-mediator`.

Si votre système ne dispose pas d'accès à Internet, assurez-vous que le programme d'installation puisse accéder aux paquets requis.

3. Déplacez le package d'installation de Mediator vers le répertoire d'installation si nécessaire.
4. Décompressez le package d'installation :

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

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

Quelle est la prochaine étape ?

"Vérifiez la signature du code d'ONTAP Mediator"

Vérifiez la signature du code d'ONTAP Mediator

NetApp recommande de vérifier la signature du code de ONTAP Mediator avant l'installation. Cette étape est facultative.

Avant de commencer

Assurez-vous que votre système répond à ces exigences avant de vérifier la signature du code d'ONTAP Mediator.



- À compter du 15 juin 2025, vous ne pouvez pas installer ou mettre à niveau vers ONTAP Mediator 1.9 et 1.8, car les certificats de vérification de signature du code ont expiré. Installez ou mettez à niveau vers ONTAP Mediator 1.10 ou une version ultérieure.
- Si le système ne répond pas aux exigences ci-dessous, le processus de vérification n'est pas requis et vous pouvez passer directement à ["Installez le package d'installation de ONTAP Mediator"](#).

- versions d'openssl de 1.0.2 à 3.0 pour la vérification de base
- openssl version 1.1.0 ou ultérieure est requise pour les opérations de l'autorité d'horodatage (TSA)
- Accès à l'Internet public pour la vérification OCSP

Le package de téléchargement comprend les fichiers suivants :

Fichier	Description
ONTAP-Mediator-production.pub	La clé publique utilisée pour vérifier la signature
csc-prod-chain-ONTAP-Mediator.pem	La chaîne de confiance de l'autorité de certification publique
csc-prod-ONTAP-Mediator.pem	Le certificat utilisé pour générer la clé
ontap-mediator-1.12.1	Le fichier exécutable d'installation du produit pour la version 1.12
ontap-mediator-1.12.1.sig	La signature du programme d'installation, hachée en SHA-256 puis signée RSA à l'aide de la clé csc-prod
ontap-mediator-1.12.1.sig.tsr	La demande de révocation à utiliser par OCSP pour la signature de l'installateur
ontap-mediator-1.12.1.tsr	Le fichier de demande de signature horodatée
tsa-prod-ONTAP-Mediator.pem	Le certificat public pour le TSR
tsa-prod-chain-ONTAP-Mediator.pem	La chaîne de certificats publics CA pour le TSR

Étapes

1. Effectuez le contrôle de révocation sur `csc-prod-ONTAP-Mediator.pem` en utilisant le protocole OCSP (Online Certificate Status Protocol).
 - a. Trouvez l'URL OCSP du certificat. Les certificats de développeur peuvent ne pas fournir d'URI :

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

- b. Générez une requête OCSP pour le certificat.

```
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. Connectez-vous à OCSP Manager pour envoyer la requête OCSP :

```
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. Vérifiez la chaîne de confiance du CSC et les dates d'expiration par rapport à l'hôte local :

```
openssl verify
```



La openssl version provenant du PATH doit avoir un certificat valide cert.pem (non auto-signé).

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

La commande échoue si le certificat de vérification de signature du code ou le certificat d'horodatage est expiré ou invalide. Téléchargez une version plus récente d'ONTAP Mediator.

3. Vérifiez les `ontap-mediator-1.12.1.sig.tsr` et `ontap-mediator-1.12.1.tsr` fichiers à l'aide des certificats associés :

OpenSSL 3.x

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

OpenSSL 1.x

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



.tsr Les fichiers contiennent la réponse d'horodatage associée au programme d'installation et la signature du code. Le traitement confirme que l'horodatage possède une signature valide de la TSA et que votre fichier d'entrée n'a pas changé. Votre machine effectue la vérification localement. Vous n'avez pas besoin d'accéder aux serveurs de la TSA.

4. Vérifiez les signatures par rapport à la clé:

```
openssl -dgst -verify
```

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

Quelle est la prochaine étape ?

["Installez le package d'installation de ONTAP Mediator"](#)

Installez le package d'installation de ONTAP Mediator

Pour installer ONTAP Mediator, vous devez obtenir le package d'installation et exécuter le programme d'installation sur l'hôte.



Pour mettre à niveau une installation ONTAP Mediator existante, consultez plutôt ["Mettre à niveau ONTAP Mediator"](#).

À propos de cette tâche

- À partir d'ONTAP 9.19.1 et ONTAP Mediator 1.12, vous avez la possibilité d'installer ONTAP Mediator avec la prise en charge d'iSCSI et d'HTTPS, ou uniquement avec la prise en charge d'HTTPS. Si vous choisissez d'installer ONTAP Mediator avec la prise en charge d'HTTPS uniquement, le package SCST n'est pas installé.
- Si vous effectuez une mise à niveau depuis ONTAP Mediator 1.11 ou une version antérieure avec SCST installé, et que vous choisissez l'option HTTPS uniquement lors de la mise à niveau, le package SCST est désinstallé et la nouvelle version d'ONTAP Mediator ne contient pas le package SCST.
- Si vous prévoyez d'utiliser ONTAP Mediator pour surveiller plusieurs configurations IP MetroCluster, la prise en charge dépend de votre type de Mediator, de la version d'ONTAP et du système d'exploitation. Consultez ["Utilisez ONTAP Mediator pour surveiller plusieurs configurations IP MetroCluster"](#) pour plus d'informations.
- L'installation ONTAP Mediator avec prise en charge du protocole HTTPS uniquement est prise en charge pour les cas d'utilisation suivants :
 - Vous prévoyez d'utiliser uniquement ONTAP Mediator pour surveiller vos clusters de synchronisation

active SnapMirror.

- Vous prévoyez de configurer ONTAP Mediator avec HTTPS pour surveiller une ou plusieurs configurations IP MetroCluster.
- ONTAP Mediator doit être installé avec la prise en charge d'iSCSI et de HTTPS dans le scénario suivant :
 - Vous prévoyez de configurer ONTAP Mediator avec iSCSI pour surveiller une ou plusieurs configurations IP MetroCluster.
- Lors de l'installation ou de la mise à niveau vers ONTAP Mediator 1.12 ou une version ultérieure, le programme d'installation vous invite à répondre aux éléments suivants :

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

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

Y(es)/n(o) :

- Répondez **Yes** si vous prévoyez d'utiliser ONTAP Mediator configuré avec iSCSI pour surveiller une ou plusieurs configurations IP MetroCluster.
- Répondez **No** si vous prévoyez d'utiliser ONTAP Mediator uniquement pour la synchronisation active SnapMirror, ou si vous prévoyez de configurer ONTAP Mediator avec HTTPS pour surveiller une ou plusieurs configurations IP MetroCluster.

Vous pouvez également utiliser l'option `--https-only` dans la commande `./ontap-mediator-1.12.1/ontap-mediator-1.12.1` pour spécifier uniquement HTTPS.

- Pour les cas d'utilisation d'automatisation, vous pouvez utiliser la commande `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 -y` pour ignorer les invites de l'installateur.

Étapes

1. Exécutez le programme d'installation et répondez aux invites comme demandé :

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

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



Pour ignorer la vérification de signature lors de l'installation, utilisez la

`./ontap-mediator-1.12.1/ontap-mediator-1.12.1 --skip-code-signature -check` commande

Le programme d'installation crée les comptes requis et installe les packages nécessaires. Si ONTAP Mediator est déjà installé, le programme d'installation vous invite plutôt à le mettre à niveau ; pour les étapes et exemples spécifiques à la mise à niveau, consultez ["Mettre à niveau ONTAP Mediator"](#).

▼ Exemple d'installation d'ONTAP Mediator avec prise en charge HTTPS et iSCSI (sortie console)

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

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

ONTAP Mediator: Self Extracting Installer

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

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

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

Y(es)/n(o): yes

ONTAP Mediator will be installed with mode: ISCSI_HTTPS

+ Selected install package mode: ISCSI_HTTPS

+ Checking that required ports 3260 and 31784 are free

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

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

Enter ONTAP Mediator user account (mediatoradmin) password:

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

+ Checking if SELinux is in enforcing mode

SELinux is set to Enforcing. ONTAP Mediator server requires modifying

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

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

```
+ Installing required packages.
```

```
Last metadata expiration check: 2:16:00 ago on Tue 24 Mar 2026
12:58:28 PM EDT.
```

```
Package openssl-1:3.5.1-7.0.1.el9_7.x86_64 is already installed.
```

```
Package openssl-devel-1:3.5.1-7.0.1.el9_7.x86_64 is already installed.
```

```
Package kernel-uek-devel-6.12.0-109.67.6.el9uek.x86_64 is already
installed.
```

```
Package gcc-11.5.0-11.0.2.el9.x86_64 is already installed.
```

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

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

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

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

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

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

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

```
Package efibootmgr-16-12.0.1.el9.x86_64 is already installed.
```

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

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

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

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

```
Package python3.12-3.12.12-4.0.1.el9_7.1.x86_64 is already installed.
```

```
Package python3.12-devel-3.12.12-4.0.1.el9_7.1.x86_64 is already
installed.
```

```
Package gcc-toolset-14-14.0-2.el9.x86_64 is already installed.
```

```
Dependencies resolved.
```

```
=====
=====
Package                                Architecture      Version
```

Repository	Size
=====	
Installing:	
efibootmgr	x86_64 18-
8.el10	baseos 47 k
mokutil	x86_64
2:0.7.2-1.el10	baseos 48 k
patch	x86_64 2.7.6-
26.el10	appstream 131 k
perl-ExtUtils-MakeMaker	noarch 2:7.70-
513.el10	appstream 295 k
python3-devel	x86_64
3.12.12-4.el10_1	appstream 329 k
python3-pip	noarch 23.3.2-
7.el10	appstream 3.2 M
Upgrading:	
libselinux	x86_64 3.9-
1.el10	baseos 97 k
libselinux-utils	x86_64 3.9-
1.el10	baseos 122 k
libsemanage	x86_64 3.9-
1.el10	baseos 122 k
libsepol	x86_64 3.9-
1.el10	baseos 348 k
policycoreutils	x86_64 3.9-
1.el10	baseos 224 k
policycoreutils-python-utils	noarch 3.9-
1.el10	appstream 51 k
python-unversioned-command	noarch
3.12.12-4.el10_1	appstream 11 k
python3	x86_64
3.12.12-4.el10_1	baseos 28 k
python3-libs	x86_64
3.12.12-4.el10_1	baseos 9.4 M
python3-libselinux	x86_64 3.9-
1.el10	appstream 200 k
python3-libsemanage	x86_64 3.9-
1.el10	appstream 81 k
python3-policycoreutils	noarch 3.9-
1.el10	appstream 2.2 M
Installing dependencies:	
annobin-docs	noarch 12.99-
1.el10	appstream 88 k
annobin-plugin-gcc	x86_64 12.99-
1.el10	appstream 998 k

dwz	x86_64	0.16-
1.el10	appstream	139 k
efi-filesystem	noarch	6-
7.el10.rocky.0.1	baseos	7.8 k
efi-srpm-macros	noarch	6-
7.el10.rocky.0.1	appstream	22 k
efivar-libs	x86_64	39-
3.el10	baseos	127 k
fonts-srpm-macros	noarch	
1:2.0.5-18.el10	appstream	26 k
forge-srpm-macros	noarch	0.4.0-
6.el10	appstream	20 k
gcc-plugin-annobin	x86_64	14.3.1-
2.1.el10	appstream	67 k
go-srpm-macros	noarch	3.6.0-
7.el10_1	appstream	27 k
kernel-srpm-macros	noarch	1.0-
26.el10	appstream	9.4 k
lua-srpm-macros	noarch	1-
15.el10	appstream	8.8 k
ocaml-srpm-macros	noarch	10-
4.el10	appstream	9.2 k
openblas-srpm-macros	noarch	2-
19.el10	appstream	7.7 k
package-notes-srpm-macros	noarch	0.5-
13.el10	appstream	9.2 k
perl-AutoSplit	noarch	5.74-
512.2.el10_0	appstream	21 k
perl-Benchmark	noarch	1.25-
512.2.el10_0	appstream	27 k
perl-CPAN-Meta-Requirements	noarch	2.143-
11.el10	appstream	35 k
perl-CPAN-Meta-YAML	noarch	0.018-
512.el10	appstream	26 k
perl-Devel-PPPort	x86_64	3.72-
512.el10	appstream	219 k
perl-ExtUtils-Command	noarch	2:7.70-
513.el10	appstream	14 k
perl-ExtUtils-Constant	noarch	0.25-
512.2.el10_0	appstream	43 k
perl-ExtUtils-Install	noarch	2.22-
511.el10	appstream	43 k
perl-ExtUtils-Manifest	noarch	1:1.75-
511.el10	appstream	34 k
perl-ExtUtils-ParseXS	noarch	1:3.51-
512.el10	appstream	189 k

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

Transaction Summary

=====

```

=====
Install  52 Packages
Upgrade  12 Packages

Total download size: 26 M
Is this ok [y/N]: y
Downloading Packages:
(1/64): efi-filesystem-6-7.el10.rocky.0.1.noarch.rpm
206 kB/s | 7.8 kB      00:00
(2/64): efibootmgr-18-8.el10.x86_64.rpm
1.2 MB/s | 47 kB      00:00
(3/64): efivar-libs-39-3.el10.x86_64.rpm
2.8 MB/s | 127 kB     00:00
(4/64): mokutil-0.7.2-1.el10.x86_64.rpm
6.4 MB/s | 48 kB      00:00
(5/64): annobin-docs-12.99-1.el10.noarch.rpm
11 MB/s | 88 kB       00:00
(6/64): python3-pyparsing-3.1.1-7.el10.noarch.rpm
13 MB/s | 271 kB      00:00
(7/64): dwz-0.16-1.el10.x86_64.rpm
12 MB/s | 139 kB      00:00
(8/64): efi-srpm-macros-6-7.el10.rocky.0.1.noarch.rpm
2.7 MB/s | 22 kB      00:00
(9/64): fonts-srpm-macros-2.0.5-18.el10.noarch.rpm
5.1 MB/s | 26 kB      00:00
(10/64): forge-srpm-macros-0.4.0-6.el10.noarch.rpm
4.3 MB/s | 20 kB      00:00
(11/64): gcc-plugin-annobin-14.3.1-2.1.el10.x86_64.rpm
10 MB/s | 67 kB       00:00
(12/64): go-srpm-macros-3.6.0-7.el10_1.noarch.rpm
4.7 MB/s | 27 kB      00:00
(13/64): kernel-srpm-macros-1.0-26.el10.noarch.rpm
2.0 MB/s | 9.4 kB     00:00
(14/64): lua-srpm-macros-1-15.el10.noarch.rpm
2.0 MB/s | 8.8 kB     00:00
(15/64): ocaml-srpm-macros-10-4.el10.noarch.rpm
2.0 MB/s | 9.2 kB     00:00
(16/64): annobin-plugin-gcc-12.99-1.el10.x86_64.rpm
16 MB/s | 998 kB      00:00
(17/64): openblas-srpm-macros-2-19.el10.noarch.rpm
432 kB/s | 7.7 kB     00:00
(18/64): package-notes-srpm-macros-0.5-13.el10.noarch.rpm
519 kB/s | 9.2 kB     00:00
(19/64): perl-AutoSplit-5.74-512.2.el10_0.noarch.rpm
4.5 MB/s | 21 kB      00:00
(20/64): patch-2.7.6-26.el10.x86_64.rpm

```

```

14 MB/s | 131 kB      00:00
(21/64): perl-Benchmark-1.25-512.2.el10_0.noarch.rpm
3.5 MB/s | 27 kB      00:00
(22/64): perl-CPAN-Meta-Requirements-2.143-11.el10.noarch.rpm
10 MB/s | 35 kB      00:00
(23/64): perl-CPAN-Meta-YAML-0.018-512.el10.noarch.rpm
5.3 MB/s | 26 kB      00:00
(24/64): perl-CPAN-Meta-2.150010-511.el10.noarch.rpm
12 MB/s | 197 kB     00:00
(25/64): perl-Encode-Locale-1.05-31.el10.noarch.rpm
2.6 MB/s | 18 kB      00:00
(26/64): perl-ExtUtils-Command-7.70-513.el10.noarch.rpm
3.0 MB/s | 14 kB      00:00
(27/64): perl-Devel-PPPort-3.72-512.el10.x86_64.rpm
13 MB/s | 219 kB     00:00
(28/64): perl-ExtUtils-Constant-0.25-512.2.el10_0.noarch.rpm
4.9 MB/s | 43 kB      00:00
(29/64): perl-ExtUtils-Install-2.22-511.el10.noarch.rpm
4.7 MB/s | 43 kB      00:00
(30/64): perl-ExtUtils-Manifest-1.75-511.el10.noarch.rpm
6.2 MB/s | 34 kB      00:00
(31/64): perl-File-Compare-1.100.800-512.2.el10_0.noarch.rpm
4.2 MB/s | 13 kB      00:00
(32/64): perl-ExtUtils-MakeMaker-7.70-513.el10.noarch.rpm
17 MB/s | 295 kB     00:00
(33/64): perl-ExtUtils-ParseXS-3.51-512.el10.noarch.rpm
11 MB/s | 189 kB     00:00
(34/64): perl-File-Copy-2.41-512.2.el10_0.noarch.rpm
1.7 MB/s | 20 kB      00:00
(35/64): perl-Il8N-Langinfo-0.24-512.2.el10_0.x86_64.rpm
5.0 MB/s | 25 kB      00:00
(36/64): perl-JSON-PP-4.16-512.el10.noarch.rpm
9.3 MB/s | 66 kB      00:00
(37/64): perl-Time-HiRes-1.9777-511.el10.x86_64.rpm
11 MB/s | 58 kB      00:00
(38/64): perl-Test-Harness-3.48-512.el10.noarch.rpm
13 MB/s | 282 kB     00:00
(39/64): perl-lib-0.65-512.2.el10_0.x86_64.rpm
4.4 MB/s | 15 kB      00:00
(40/64): perl-srpm-macros-1-57.el10.noarch.rpm
2.7 MB/s | 8.5 kB     00:00
(41/64): perl-devel-5.40.2-512.2.el10_0.x86_64.rpm
19 MB/s | 770 kB     00:00
(42/64): perl-version-0.99.32-4.el10.x86_64.rpm
4.3 MB/s | 63 kB      00:00
(43/64): pyproject-srpm-macros-1.16.2-1.el10.noarch.rpm

```

```

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

```

Total

```

19 MB/s | 26 MB      00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing          :
1/1
  Upgrading           : python3-libs-3.12.12-4.el10_1.x86_64
1/76
  Upgrading           : python-unversioned-command-3.12.12-
4.el10_1.noarch
2/76
  Upgrading           : python3-3.12.12-4.el10_1.x86_64
3/76
  Upgrading           : libsepol-3.9-1.el10.x86_64
4/76
  Upgrading           : libselinux-3.9-1.el10.x86_64
5/76
  Running scriptlet: libselinux-3.9-1.el10.x86_64
5/76
  Installing          : perl-version-8:0.99.32-4.el10.x86_64
6/76
  Installing          : perl-File-Copy-2.41-512.2.el10_0.noarch
7/76
  Installing          : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
8/76
  Upgrading           : libsemanage-3.9-1.el10.x86_64
9/76
  Upgrading           : python3-libselinux-3.9-1.el10.x86_64
10/76
  Installing          : perl-Time-HiRes-4:1.9777-511.el10.x86_64
11/76
  Installing          : perl-JSON-PP-1:4.16-512.el10.noarch
12/76
  Installing          : perl-File-Compare-1.100.800-512.2.el10_0.noarch
13/76
  Installing          : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
14/76
  Installing          : efivar-libs-39-3.el10.x86_64
15/76
  Upgrading           : python3-libsemanage-3.9-1.el10.x86_64
16/76
  Installing          : perl-ExtUtils-Command-2:7.70-513.el10.noarch
17/76
  Installing          : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch

```

```

18/76
  Upgrading      : libselinux-utils-3.9-1.el10.x86_64
19/76
  Upgrading      : polycoreutils-3.9-1.el10.x86_64
20/76
  Running scriptlet: polycoreutils-3.9-1.el10.x86_64
20/76
  Upgrading      : python3-polycoreutils-3.9-1.el10.noarch
21/76
  Installing     : python3-pyparsing-3.1.1-7.el10.noarch
22/76
  Installing     : systemtap-sdt-dtrace-5.3-3b.el10.x86_64
23/76
  Installing     : systemtap-sdt-devel-5.3-3b.el10.x86_64
24/76
  Installing     : python3-pip-23.3.2-7.el10.noarch
25/76
  Installing     : rust-toolset-srpm-macros-1.88.0-1.el10.noarch
26/76
  Installing     : qt6-srpm-macros-6.9.1-1.el10.noarch
27/76
  Installing     : pyproject-srpm-macros-1.16.2-1.el10.noarch
28/76
  Installing     : perl-srpm-macros-1-57.el10.noarch
29/76
  Installing     : perl-lib-0.65-512.2.el10_0.x86_64
30/76
  Installing     : perl-doc-5.40.2-512.2.el10_0.noarch
31/76
  Installing     : perl-I18N-Langinfo-0.24-512.2.el10_0.x86_64
32/76
  Installing     : perl-Encode-Locale-1.05-31.el10.noarch
33/76
  Installing     : perl-ExtUtils-Constant-0.25-512.2.el10_0.noarch
34/76
  Installing     : perl-Devel-PPPort-3.72-512.el10.x86_64
35/76
  Installing     : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
36/76
  Installing     : perl-CPAN-Meta-2.150010-511.el10.noarch
37/76
  Installing     : perl-Benchmark-1.25-512.2.el10_0.noarch
38/76
  Installing     : perl-Test-Harness-1:3.48-512.el10.noarch
39/76
  Installing     : perl-AutoSplit-5.74-512.2.el10_0.noarch

```

```

40/76      Installing      : package-notes-srpm-macros-0.5-13.el10.noarch
41/76      Installing      : openblas-srpm-macros-2-19.el10.noarch
42/76      Installing      : ocaml-srpm-macros-10-4.el10.noarch
43/76      Installing      : lua-srpm-macros-1-15.el10.noarch
44/76      Installing      : kernel-srpm-macros-1.0-26.el10.noarch
45/76      Installing      : gcc-plugin-annobin-14.3.1-2.1.el10.x86_64
46/76      Installing      : efi-srpm-macros-6-7.el10.rocky.0.1.noarch
47/76      Installing      : dwz-0.16-1.el10.x86_64
48/76      Installing      : annobin-docs-12.99-1.el10.noarch
49/76      Installing      : annobin-plugin-gcc-12.99-1.el10.x86_64
50/76      Installing      : fonts-srpm-macros-1:2.0.5-18.el10.noarch
51/76      Installing      : forge-srpm-macros-0.4.0-6.el10.noarch
52/76      Installing      : go-srpm-macros-3.6.0-7.el10_1.noarch
53/76      Installing      : python-srpm-macros-3.12-10.el10.noarch
54/76      Installing      : redhat-rpm-config-293-1.el10.rocky.0.2.noarch
55/76      Running scriptlet: redhat-rpm-config-293-1.el10.rocky.0.2.noarch
55/76      Installing      : perl-ExtUtils-Install-2.22-511.el10.noarch
56/76      Installing      : perl-devel-4:5.40.2-512.2.el10_0.x86_64
57/76      Installing      : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
58/76      Installing      : efi-filesystem-6-7.el10.rocky.0.1.noarch
59/76      Installing      : efibootmgr-18-8.el10.x86_64
60/76      Installing      : python3-devel-3.12.12-4.el10_1.x86_64
61/76      Upgrading       : policycoreutils-python-utils-3.9-1.el10.noarch

```

```

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

Upgraded:
    libselinux-3.9-1.el10.x86_64
    libselinux-utils-3.9-1.el10.x86_64
    libsemanage-3.9-1.el10.x86_64
    libsepol-3.9-1.el10.x86_64
    policycoreutils-3.9-1.el10.x86_64
    policycoreutils-python-utils-3.9-1.el10.noarch
    python-unversioned-command-3.12.12-4.el10_1.noarch
    python3-3.12.12-4.el10_1.x86_64
    python3-libs-3.12.12-4.el10_1.x86_64
    python3-libselinux-3.9-1.el10.x86_64

```

```

python3-libsemanage-3.9-1.el10.x86_64
python3-policycoreutils-3.9-1.el10.noarch
Installed:
  annobin-docs-12.99-1.el10.noarch
annobin-plugin-gcc-12.99-1.el10.x86_64
  dwz-0.16-1.el10.x86_64                                efi-
filesystem-6-7.el10.rocky.0.1.noarch
  efi-srpm-macros-6-7.el10.rocky.0.1.noarch
efibootmgr-18-8.el10.x86_64
  efivar-libs-39-3.el10.x86_64
fonts-srpm-macros-1:2.0.5-18.el10.noarch
  forge-srpm-macros-0.4.0-6.el10.noarch                  gcc-
plugin-annobin-14.3.1-2.1.el10.x86_64
  go-srpm-macros-3.6.0-7.el10_1.noarch
kernel-srpm-macros-1.0-26.el10.noarch
  lua-srpm-macros-1-15.el10.noarch
mokutil-2:0.7.2-1.el10.x86_64
  ocaml-srpm-macros-10-4.el10.noarch
openblas-srpm-macros-2-19.el10.noarch
  package-notes-srpm-macros-0.5-13.el10.noarch
patch-2.7.6-26.el10.x86_64
  perl-AutoSplit-5.74-512.2.el10_0.noarch
perl-Benchmark-1.25-512.2.el10_0.noarch
  perl-CPAN-Meta-2.150010-511.el10.noarch
perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
  perl-CPAN-Meta-YAML-0.018-512.el10.noarch
perl-Devel-PPPort-3.72-512.el10.x86_64
  perl-Encode-Locale-1.05-31.el10.noarch
perl-ExtUtils-Command-2:7.70-513.el10.noarch
  perl-ExtUtils-Constant-0.25-512.2.el10_0.noarch
perl-ExtUtils-Install-2.22-511.el10.noarch
  perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
  perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
perl-File-Compare-1.100.800-512.2.el10_0.noarch
  perl-File-Copy-2.41-512.2.el10_0.noarch
perl-I18N-Langinfo-0.24-512.2.el10_0.x86_64
  perl-JSON-PP-1:4.16-512.el10.noarch
perl-Test-Harness-1:3.48-512.el10.noarch
  perl-Time-HiRes-4:1.9777-511.el10.x86_64
perl-devel-4:5.40.2-512.2.el10_0.x86_64
  perl-doc-5.40.2-512.2.el10_0.noarch
perl-lib-0.65-512.2.el10_0.x86_64
  perl-srpm-macros-1-57.el10.noarch
perl-version-8:0.99.32-4.el10.x86_64
  pyproject-srpm-macros-1.16.2-1.el10.noarch

```

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

Complete!

OS package installations finished

OS package installations finished

+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.pJBcIv/ontap-mediator-1.12.1/ontap-mediator-1.12.1/install_20260324151410.log)

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

Sudoer config verified

ONTAP Mediator rsyslog and logging rotation enabled

+ Install successful. (Moving log to /opt/netapp/lib/ontap_mediator/log/install_20260324151410.log)

+ WARNING: This system supports UEFI

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

If SB is enabled in the future, SCST will not work unless the following action is taken:

Using the keys in /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow instructions in /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing

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

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

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

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

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

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

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

[root@mediator_host ~]#

▼ Exemple d'installation d'ONTAP Mediator avec prise en charge de HTTPS uniquement (sortie console)

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

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive

+ Performing the ONTAP Mediator run-time code signature check

Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls

Error querying OCSP responder

40E72F35407F0000:error:1E800080:HTTP

routines:OSSL_HTTP_REQ_CTX_nbio:failed reading

data:crypto/http/http_client.c:596:

40E72F35407F0000:error:1E800067:HTTP

routines:OSSL_HTTP_REQ_CTX_exchange:error

receiving:crypto/http/http_client.c:1045:server=http://ocsp.entrust.net:80

WARNING: The OCSP check failed while attempting to test the Code-Signature-Check certificate

Continue without code signature checking (only recommended if integrity has been established manually)? y(es)/N(o): yes

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

+ Unpacking the ONTAP Mediator installer

```
+ ONTAP_MEDIATOR_INSTALL_HTTPS_ONLY is set to '1', args are: ''
+ Starting ONTAP Mediator install/update process: previous
installation_mode is ''
+ Selected install package mode: HTTPS_ONLY
```

```
+ Checking that required port 31784 is free
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API
(mediatoradmin).
Would you like to use the default account names: netapp +
mediatoradmin? (Y(es)/n(o)): yes
```

Enter ONTAP Mediator user account (mediatoradmin) password:

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

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

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

```
+ Installing required packages.
```

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

Package openssl-1:3.5.1-7.el9_7.x86_64 is already installed.
Package openssl-devel-1:3.5.1-7.el9_7.x86_64 is already installed.
Package gcc-11.5.0-11.el9.x86_64 is already installed.
Package make-1:4.3-8.el9.x86_64 is already installed.
Package which-2.21-30.el9_6.x86_64 is already installed.
Package libselinux-utils-3.6-3.el9.x86_64 is already installed.
Package patch-2.7.6-16.el9.x86_64 is already installed.
Package perl-Data-Dumper-2.174-462.el9.x86_64 is already installed.
Package perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch is already
installed.
Package bzip2-1.0.8-10.el9_5.x86_64 is already installed.
Package efibootmgr-16-12.el9.x86_64 is already installed.
Package mokutil-2:0.7.2-1.el9.x86_64 is already installed.
Package python3-pip-21.3.1-1.el9.noarch is already installed.

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

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

Enregistrez la clé de sécurité pour UEFI Secure Boot

À partir de ONTAP Mediator 1.4, le mécanisme de démarrage sécurisé est activé sur les systèmes UEFI. Lorsque le démarrage sécurisé est activé, vous devez prendre des mesures supplémentaires pour enregistrer la clé de sécurité après l'installation.



Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure prenant uniquement en charge HTTPS, le package SCST n'est pas installé et vous pouvez ignorer cette tâche.

Étapes

1. Suivez les instructions du fichier README pour signer le module du noyau SCST :

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modul
e-signing
```

2. Localisez les clés requises :

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



Après l'installation, la sortie système affiche les fichiers README et l'emplacement de la clé.

3. Ajoutez la clé publique à la liste MOK:

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



Vous pouvez laisser la clé privée à son emplacement par défaut ou la déplacer vers un emplacement sécurisé. Vous devez conserver la clé publique à son emplacement actuel afin que le Boot Manager puisse l'utiliser. Pour plus d'informations, consultez le fichier 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. Redémarrez l'hôte et utilisez le gestionnaire de démarrage UEFI de votre appareil pour approuver la nouvelle clé MOK. Vous aurez besoin de la phrase secrète fournie pour l'`mokutil` utilitaire dans ["Installez ONTAP Mediator lorsque le démarrage sécurisé UEFI est activé"](#).

Signer les modules du noyau SCST

Une fois ONTAP Mediator installé, si `systemctl status mediator-scst` affiche `failed (inactive)`, suivez ces étapes pour signer le module de noyau SCST.



Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure prenant uniquement en charge HTTPS, le package SCST n'est pas installé et vous pouvez ignorer cette tâche.

Étapes

1. Lors du processus de compilation, une paire de clés publique/privée est générée dans le `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/` répertoire. Exécutez la commande suivante pour afficher les clés générées :

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

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

2. Démarrez le processus d'importation de la clé publique dans le référentiel de clés UEFI en exécutant la commande suivante :

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

L'`mokutil`utilitaire vous invite à saisir un mot de passe à deux reprises.

3. Le logiciel mokutil demande un mot de passe temporaire pour cette clé lors du processus d'importation.
4. Vérifiez si le processus d'importation a démarré à l'aide de la commande suivante, puis redémarrez le système. Le chargeur de démarrage lance le gestionnaire EFI MOK.

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

5. Utilisez les menus à l'écran pour activer la clé du module noyau SCST. Après le démarrage, exécutez la commande suivante. Une fois le service lancé, les modules noyau SCST sont signés.

```
systemctl status mediator-scst
```

Quelle est la prochaine étape ?

["Vérifiez l'état de l'installation d'ONTAP Mediator"](#)

Vérifiez l'état de l'installation d'ONTAP Mediator

Après avoir installé ONTAP Mediator, vérifiez qu'il fonctionne correctement.

Étapes

1. Consultez l'état d'ONTAP Mediator :

```
systemctl status ontap_mediator
```

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

```

/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

```

2. Consultez l'état de SCST :

```
systemctl status mediator-scst
```



Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure prenant uniquement en charge HTTPS, le package SCST n'est pas installé et vous pouvez ignorer cette étape.

```

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

```

3. Veuillez confirmer les ports utilisés par ONTAP Mediator :

```
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

```

Et ensuite ?

Une fois ONTAP Mediator installé et vérifié, vous pouvez procéder aux tâches de configuration post-installation suivantes :

- ["Utilisez ONTAP Mediator pour la synchronisation active de SnapMirror et MetroCluster IP"](#)
- ["Configurer les attributs de ONTAP Mediator"](#) (Facultatif)

Utiliser ONTAP Mediator

Utilisez ONTAP Mediator pour la synchronisation active de SnapMirror et MetroCluster IP

ONTAP Mediator s'exécute sur un hôte Linux dans un troisième domaine de défaillance, distinct de vos clusters ONTAP, où il fournit un stockage persistant et isolé pour les métadonnées de haute disponibilité (HA). ONTAP utilise ce stockage, ainsi que les fonctions de requête d'état des nœuds et de proxy de ping de Mediator, pour surveiller les relations de synchronisation active SnapMirror et les configurations IP MetroCluster.



Cette documentation concerne la version sur site d'ONTAP Mediator. Pour plus d'informations sur ONTAP Cloud Mediator, disponible à partir d'ONTAP 9.17.1, consultez ["Documentation de SnapMirror active sync"](#).

Surveiller les relations de synchronisation active de SnapMirror

SnapMirror active sync utilise ONTAP Mediator comme témoin passif pour les copies principale et miroir dans un groupe de cohérence. En cas de partitionnement du réseau ou si une copie devient indisponible, SnapMirror active sync interroge ONTAP Mediator pour déterminer quelle copie continue de traiter les E/S et interrompt les E/S sur l'autre copie.

À partir d'ONTAP 9.8, vous pouvez utiliser n'importe quelle version d'ONTAP Mediator pour surveiller une relation de synchronisation active SnapMirror.



Pour connaître les limites du nombre de paires de clusters SnapMirror active sync qu'une seule instance ONTAP Mediator peut surveiller, voir ["Limites d'objets pour la synchronisation active ONTAP SnapMirror"](#).

["Configurez ONTAP Mediator pour la synchronisation active SnapMirror"](#)

Surveiller MetroCluster les configurations IP

Dans une configuration IP MetroCluster, ONTAP Mediator stocke des informations d'état sur les nœuds MetroCluster dans des LUN de boîte aux lettres et aide les nœuds à effectuer un basculement automatique non planifié assisté par Mediator (MAUSO) en cas de catastrophe ou dans des scénarios de panne spécifiques.

À partir de ONTAP 9.19.1 et de ONTAP Mediator 1.12, vous pouvez configurer un ONTAP Mediator qui utilise HTTPS pour la communication afin de surveiller votre configuration IP MetroCluster. Lorsque vous configurez ONTAP Mediator avec le protocole iSCSI, vous pouvez utiliser n'importe quelle version de ONTAP Mediator pour surveiller une configuration IP MetroCluster.



Pour connaître les limites du nombre de configurations IP MetroCluster qu'une seule instance ONTAP Mediator peut surveiller, consultez ["Utilisez ONTAP Mediator pour surveiller plusieurs configurations IP MetroCluster"](#)

["Configurer ONTAP Mediator pour une configuration MetroCluster IP"](#)

Informations connexes

- "Architecture de synchronisation active ONTAP SnapMirror"
- "Découvrez la prise en charge par ONTAP Mediator du basculement automatique non planifié dans une configuration IP MetroCluster"

Administrer ONTAP Mediator

Mettre à niveau ONTAP Mediator

Mettre à niveau ONTAP Mediator

Pour mettre à niveau ONTAP Mediator vers une version plus récente sans mettre à niveau le système d'exploitation hôte, téléchargez le package d'installation de la nouvelle version et exécutez le programme d'installation sur l'hôte sur lequel ONTAP Mediator est déjà installé.



Si vous devez mettre à niveau le système d'exploitation hôte vers une nouvelle version et réinstaller ou mettre à niveau ONTAP Mediator dans le cadre de ce processus, consultez plutôt ["Mettez à niveau le système d'exploitation hôte et ONTAP Mediator"](#).

Avant de commencer

- Vérifiez que votre hôte répond aux prérequis décrits dans ["Préparez-vous à installer ONTAP Mediator"](#), y compris les exigences relatives à l'hôte, au pare-feu et au système d'exploitation.
- Téléchargez le package d'installation de la nouvelle version. Consultez ["Téléchargez le package d'installation d'ONTAP Mediator"](#).
- NetApp recommande de vérifier la signature du code du nouveau package d'installation. Voir ["Vérifiez la signature du code du package d'installation d'ONTAP Mediator"](#).

À propos de cette tâche

Veuillez consulter les informations suivantes avant de mettre à niveau ONTAP Mediator.

- Vous devez mettre à niveau ONTAP Mediator vers la dernière version. Les versions antérieures restent compatibles avec toutes les versions d'ONTAP, mais les versions plus récentes intègrent des correctifs de sécurité pour les composants tiers.
- Lors de la mise à niveau vers une nouvelle version d'ONTAP Mediator incluant le package SCST, le programme d'installation effectue automatiquement la mise à niveau vers la version SCST recommandée, sauf si une version supérieure est disponible. Pour obtenir des instructions sur l'installation manuelle d'une version SCST supérieure, consultez ["Maintenir le système d'exploitation hôte pour ONTAP Mediator"](#). Pour les versions prises en charge, consultez le ["Matrice de prise en charge SCST"](#).



- Si la mise à niveau échoue, vous devrez peut-être essayer une version plus récente d'ONTAP Mediator.
- À compter du 15 juin 2025, vous ne pourrez plus installer ni mettre à niveau ONTAP Mediator 1.9 et 1.8, car leurs certificats de signature de code ont expiré. Si la mise à niveau échoue, utilisez plutôt la version de correctif ONTAP Mediator 1.9.1.
- À partir d'ONTAP 9.19.1 et ONTAP Mediator 1.12, vous avez la possibilité d'installer ONTAP Mediator avec la prise en charge d'iSCSI et d'HTTPS, ou uniquement avec la prise en charge d'HTTPS. Si vous choisissez d'installer ONTAP Mediator avec la prise en charge d'HTTPS uniquement, le package SCST n'est pas installé.
- Si vous effectuez une mise à niveau depuis ONTAP Mediator 1.11 ou une version antérieure avec SCST installé, et que vous choisissez l'option HTTPS uniquement lors de la mise à niveau, le package SCST est désinstallé et la nouvelle version d'ONTAP Mediator ne contient pas le package SCST.

- Si vous prévoyez d'utiliser ONTAP Mediator pour surveiller plusieurs configurations IP MetroCluster, la prise en charge dépend de votre type de Mediator, de la version d'ONTAP et du système d'exploitation. Consultez "[Utilisez ONTAP Mediator pour surveiller plusieurs configurations IP MetroCluster](#)" pour plus d'informations.
- L'installation ONTAP Mediator avec prise en charge du protocole HTTPS uniquement est prise en charge pour les cas d'utilisation suivants :
 - Vous prévoyez d'utiliser uniquement ONTAP Mediator pour surveiller vos clusters de synchronisation active SnapMirror.
 - Vous prévoyez de configurer ONTAP Mediator avec HTTPS pour surveiller une ou plusieurs configurations IP MetroCluster.
- ONTAP Mediator doit être installé avec la prise en charge d'iSCSI et de HTTPS dans le scénario suivant :
 - Vous prévoyez de configurer ONTAP Mediator avec iSCSI pour surveiller une ou plusieurs configurations IP MetroCluster.
- Lorsque vous exécutez le programme d'installation sur une installation existante de ONTAP Mediator, il détecte la version actuelle et vous invite à confirmer la mise à niveau :

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

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

- Dans le cadre de la mise à niveau, le programme d'installation capture un ensemble de support de votre configuration antérieure à la mise à niveau et migre la base de données avant de mettre à niveau le logiciel ONTAP Mediator.
- Pour les cas d'utilisation d'automatisation, vous pouvez utiliser la commande `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 -y` pour ignorer les invites de l'installateur.

Étapes

1. Exécutez le programme d'installation de la nouvelle version et répondez aux invites comme demandé :

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



Pour ignorer la vérification de signature lors de la mise à niveau, utilisez la commande `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 --skip-code-signature -check`

Le programme d'installation détecte l'installation existante et vous invite à la mettre à niveau, puis installe les paquets requis et migre votre configuration.

▼ Exemple de mise à niveau d'ONTAP Mediator avec prise en charge HTTPS et iSCSI (sortie console)

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

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
```

Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls

+ Unpacking the ONTAP Mediator installer

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

Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

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

+ Checking if SELinux is in enforcing mode

+ Checking for default Linux firewall

+ Installing required packages.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```

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

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

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

ONTAP Mediator: Self Extracting Installer

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

```

```

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

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

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

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

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
    OS. Using 'yum update' to upgrade the kernel might cause
service interruption.

```

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

▼ **Exemple de mise à niveau d'ONTAP Mediator avec prise en charge de HTTPS uniquement (sortie console)**

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

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API
(mediatoradmin).
Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

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

+ Checking if SELinux is in enforcing mode

+ Checking for default Linux firewall

+ Installing required packages.

Last metadata expiration check: 0:33:41 ago on Tue 21 Apr 2026
10:48:35 AM EDT.
Package openssl-1:3.5.1-7.el9_7.x86_64 is already installed.
Package openssl-devel-1:3.5.1-7.el9_7.x86_64 is already installed.
Package kernel-devel-5.14.0-611.45.1.el9_7.x86_64 is already
installed.
Package kernel-modules-core-5.14.0-611.45.1.el9_7.x86_64 is already
installed.
Package gcc-11.5.0-11.el9.x86_64 is already installed.
```

```

Package make-1:4.3-8.el9.x86_64 is already installed.
Package which-2.21-30.el9_6.x86_64 is already installed.
Package libselinux-utils-3.6-3.el9.x86_64 is already installed.
Package patch-2.7.6-16.el9.x86_64 is already installed.
Package perl-Data-Dumper-2.174-462.el9.x86_64 is already installed.
Package perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch is already
installed.
Package bzip2-1.0.8-10.el9_5.x86_64 is already installed.
Package efibootmgr-16-12.el9.x86_64 is already installed.
Package mokutil-2:0.7.2-1.el9.x86_64 is already installed.
Package python3-pip-21.3.1-1.el9.noarch is already installed.
Package elfutils-libelf-devel-0.193-1.el9.x86_64 is already installed.
Package policycoreutils-python-utils-3.6-3.el9.noarch is already
installed.
Package python3.12-3.12.12-4.el9_7.2.x86_64 is already installed.
Package python3.12-devel-3.12.12-4.el9_7.2.x86_64 is already
installed.
Dependencies resolved.
Nothing to do.
Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.JclgnS/ontap-
mediator-1.11.0/ontap-mediator-1.11.0/install_20260421112205.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20260421112205.log)

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

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

```

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

ONTAP Mediator: Self Extracting Installer

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

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

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

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

```
Creating tar archive...
```

```
Support bundle has been generated at
```

```
/opt/netapp/data/support_bundles/scs001097036-1_1776785423_BASIC.tgz
```

```
Testing the DB can be upgraded
```

```
Cloning database...
```

```
Cloning successful.
```

```
Verifying database is up-to-date...
```

```
Database out-of-date.Migrations are necessary:
```

```
Current revision: 0d5dcf349b27, Head revision: 758e4873c40d
```

```
Performing database migrations against clone...
```

```

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

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

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

[root@mediator_host ~]#

```

Mettez à niveau le système d'exploitation hôte et réinstallez ou mettez à niveau ONTAP Mediator

Pour mettre à niveau le système d'exploitation hôte pour ONTAP Mediator avec SCST installé vers une version ultérieure, vous devez désinstaller ONTAP Mediator. Après la mise à niveau du système d'exploitation, vous pouvez réinstaller votre version actuelle de ONTAP Mediator ou effectuer une mise à niveau vers une version plus récente.

À propos de cette tâche

- Cette tâche s'applique aux versions d'ONTAP Mediator avec SCST installé. Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure avec prise en charge de HTTPS uniquement, le package SCST n'est pas installé et vous pouvez mettre à niveau le système d'exploitation hôte sans affecter ONTAP Mediator. Consultez la documentation du fournisseur du système d'exploitation hôte pour obtenir les instructions de mise à niveau.
- Si vous devez uniquement mettre à jour le noyau du système d'exploitation hôte vers une version prise en charge sans passer à une nouvelle version du système d'exploitation, consultez plutôt ["Maintenir le système d'exploitation hôte pour ONTAP Mediator"](#).

- Avant de mettre à niveau le système d'exploitation hôte d'ONTAP Mediator avec l'outil leapp-upgrade, "[désinstaller ONTAP Mediator](#)". L'outil vérifie la présence de nouvelles versions RPM dans les dépôts enregistrés.
- Le programme d'installation d'ONTAP Mediator installe un fichier .rpm, que l'outil leapp-upgrade inclut dans la recherche. Comme le programme d'installation décompresse le fichier au lieu de le télécharger depuis un dépôt enregistré, l'outil ne peut pas trouver de mise à niveau. Vous devez utiliser l'outil leapp-upgrade pour désinstaller le package.

Étapes

1. Sauvegardez les fichiers journaux :

```
[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. Effectuez la mise à niveau avec l'outil leapp-upgrade :

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

3. Réinstaller ONTAP Mediator:



Effectuez les étapes restantes immédiatement après la réinstallation de ONTAP Mediator afin d'éviter toute perte de fichiers journaux.

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

```
ONTAP Mediator: Self Extracting Installer
```

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

4. Arrêtez ontap_mediator:

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

5. Remplacez les fichiers journaux :

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

6. Démarrer ontap_mediator:

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

7. Reconnectez tous les clusters ONTAP à ONTAP Mediator mis à niveau :

MetroCluster sur IP

```
siteA::> metrocluster configuration-settings mediator show  
Mediator IP      Port    Node                               Configuration  
Connection  
  
-----  
-----  
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	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

Pour SnapMirror active sync, vous n'avez pas besoin de réinstaller les certificats TLS stockés en dehors de /opt/netapp. Sauvegardez et restaurez les certificats stockés dans /opt/netapp.

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

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

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

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

```
peer1::> job show -id 39
```

Job ID	Name	Owning 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
```

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

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

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

```
peer1::>
```

Informations connexes

- ["security certificate delete"](#)
- ["installation du certificat de sécurité"](#)
- ["security certificate show"](#)
- ["snapmirror mediator add"](#)
- ["snapmirror mediator remove"](#)
- ["storage iscsi-initiator show"](#)

Configurer les attributs de ONTAP Mediator

Vous pouvez configurer les attributs côté hôte de ONTAP Mediator, y compris les paramètres liés aux certificats et les remplacements de configuration.

Paramètres configurables du médiateur ONTAP

ONTAP Mediator prend en charge plusieurs paramètres configurables. Les valeurs par défaut de ces paramètres sont fournies dans un `low_space_threshold_mib`: 10 fichier en lecture seule. Le fichier se trouve à l'emplacement suivant :

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

Toutes les valeurs placées dans le `ontap_mediator.user_config.yaml` remplaceront les valeurs par défaut et seront conservées lors de toutes les mises à niveau d'ONTAP Mediator.

Après avoir modifié `ontap_mediator.user_config.yaml`, redémarrez ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Les attributs du médiateur ONTAP décrits dans cette section peuvent être modifiés si nécessaire.



Les autres valeurs par défaut dans le `ontap_mediator.config.yaml` ne doivent pas être modifiées, car les valeurs modifiées ne sont pas conservées lors des mises à niveau d'ONTAP Mediator.

Vous modifiez les attributs de ONTAP Mediator en copiant les variables requises dans le fichier `ontap_mediator.user_config.yaml` afin de remplacer les paramètres par défaut.

Installer des certificats SSL tiers

Vous pouvez remplacer les certificats auto-signés par défaut par des certificats SSL tiers en modifiant les fichiers de configuration de ONTAP Mediator.

Pour remplacer les certificats auto-signés par défaut par des certificats SSL tiers, vous devez modifier certains attributs dans les fichiers suivants :

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

Les variables contenues dans ces fichiers servent à contrôler les fichiers de certificats utilisés par ONTAP Mediator.

ONTAP Mediator 1.9 et versions ultérieures

Les variables par défaut répertoriées dans le tableau suivant sont incluses dans le `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` fichier.

Variable	Chemin
cert_path	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt</code>
key_path	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key</code>
ca_cert_path	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt</code>

Variable	Chemin
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 sert à définir la durée de validité des certificats clients. La valeur maximale est de trois ans (1095 jours).
- x509_passin_pwd est la phrase de passe du certificat client signé.

Les variables par défaut répertoriées dans le tableau suivant sont incluses dans le `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` fichier.

Variable	Chemin
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 et versions antérieures

Les variables par défaut répertoriées dans le tableau suivant sont incluses dans le `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` fichier.

Variable	Chemin
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

Variable	Chemin
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- cert_valid_days sert à définir la durée de validité des certificats clients. La valeur maximale est de trois ans (1095 jours).
- x509_passin_pwd est la phrase de passe du certificat client signé.

Les variables par défaut répertoriées dans le tableau suivant sont incluses dans le `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` fichier.

Variable	Chemin
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

Si vous modifiez ces attributs, redémarrez ONTAP Mediator pour appliquer les modifications. Pour obtenir des instructions détaillées sur la façon de remplacer les certificats par défaut par des certificats tiers, consultez ["Remplacez les certificats auto-signés par des certificats tiers de confiance"](#).

Configurer la protection contre les attaques par mot de passe

Les paramètres suivants offrent une protection contre les attaques par force brute visant à deviner les mots de passe.

Pour activer cette fonctionnalité, définissez une valeur pour `window_seconds` et `retry_limit`.

Exemples :

- Accordez une fenêtre de 5 minutes pour les tentatives, puis réinitialisez le compteur des échecs à zéro :

```
authentication_lock_window_seconds: 300
```

- Bloquez le compte si cinq échecs se produisent dans la période définie:

```
authentication_retry_limit: 5
```

- Réduisez l'impact des attaques de devinette de mots de passe par force brute en instaurant un délai avant le rejet de chaque tentative, ce qui ralentit les attaques.

```
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
```

Configurer les règles de complexité des mots de passe

Les champs suivants contrôlent les règles de complexité du mot de passe du compte utilisateur de l'API ONTAP Mediator.

```
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)
```

Configurez les paramètres d'espace disque et d'espace de journalisation pour ONTAP Mediator, y compris le seuil d'espace libre et l'espace de journalisation réservé.

Configurer le seuil d'espace libre

Il existe des paramètres permettant de contrôler l'espace libre requis sur le `/opt/netapp/lib/ontap_mediator` disque.

Si l'espace est inférieur au seuil défini, le service émet un événement d'avertissement.

```
low_space_threshold_mib: 10
```

Configurer l'espace de journalisation réservé

Cette `RESERVE_LOG_SPACE` fonctionnalité est contrôlée par des paramètres spécifiques. Par défaut, l'installation de ONTAP Mediator crée un espace disque distinct pour les journaux. Le programme d'installation crée un nouveau fichier de taille fixe avec un total de 700MB d'espace disque destiné explicitement à la journalisation de ONTAP Mediator.

Pour désactiver cette fonctionnalité et utiliser l'espace disque par défaut, procédez comme suit :

1. Modifiez la valeur de `RESERVE_LOG_SPACE` de 1 à 0 dans le fichier suivant :

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

a. Exécutez la commande suivante :

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

```
RESERVE_LOG_SPACE=0
```

b. Redémarrer ONTAP Mediator :

```
systemctl restart ontap_mediator
```

Pour réactiver la fonctionnalité, modifiez la valeur de 0 à 1 et redémarrez le Mediator.



Le passage d'un espace disque à un autre ne supprime pas les journaux existants. Tous les journaux précédents sont sauvegardés puis déplacés vers l'espace disque actuel après le basculement et le redémarrage du Mediator.

Modifier le nom d'utilisateur et le mot de passe du médiateur ONTAP

Modifiez le nom d'utilisateur ou le mot de passe de ONTAP Mediator depuis l'hôte Linux sur lequel ONTAP Mediator est installé.

Changer le nom d'utilisateur

Vous pouvez modifier le nom d'utilisateur en suivant la procédure suivante.

À propos de cette tâche

Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.

Si vous ne parvenez pas à exécuter cette commande, vous devrez peut-être l'exécuter en utilisant le chemin complet comme indiqué dans l'exemple suivant :

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

Étapes

Modifiez votre nom d'utilisateur en choisissant l'une des options suivantes :

- **Option (a) :** Exécutez la commande `mediator_change_user` et répondez aux invites comme indiqué dans l'exemple suivant :

```
[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):** Exécutez la commande suivante:

```
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 ~]#
```

Changer le mot de passe

Vous pouvez modifier le mot de passe en suivant la procédure ci-dessous.

À propos de cette tâche

Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.

Si vous ne parvenez pas à exécuter cette commande, vous devrez peut-être l'exécuter en utilisant le chemin complet comme indiqué dans l'exemple suivant :

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

Étapes

Modifiez le mot de passe en choisissant l'une des options suivantes :

- **Option (a):** Exécutez la `mediator_change_password` commande et répondez aux invites comme indiqué dans l'exemple suivant :

```
[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):** Exécutez la commande suivante:

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

L'exemple montre que le mot de passe est modifié de « mediator1 » à « mediator2 ».

```
[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 ~]#
```

Démarrer et arrêter ONTAP Mediator

Arrêtez ou redémarrez ONTAP Mediator et SCST lorsque vous devez effectuer la maintenance de l'hôte ou réactiver le service.

Arrêtez ONTAP Mediator

Pour arrêter ONTAP Mediator, procédez comme suit :

Étapes

1. Arrêter ONTAP Mediator:

```
systemctl stop ontap_mediator
```

2. Arrêter SCST:

```
systemctl stop mediator-scst
```

3. Désactiver ONTAP Mediator et SCST:

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

Démarrer ONTAP Mediator

Pour réactiver ONTAP Mediator, procédez comme suit :

Étapes

1. Activez ONTAP Mediator et SCST:

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

2. Démarrer SCST:

```
systemctl start mediator-scst
```

3. Démarrer ONTAP Mediator :

```
systemctl start ontap_mediator
```

Vérifier l'état de santé de ONTAP Mediator

Vérifiez qu'ONTAP Mediator fonctionne normalement.

Vérifiez l'état du service

Étapes

1. Consultez l'état d'ONTAP Mediator :

a. Exécutez la commande suivante :

```
systemctl status ontap_mediator
```

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

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

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

b. Consultez l'état du service SCST:



Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure prenant uniquement en charge HTTPS, le package SCST n'est pas installé et vous pouvez ignorer cette tâche.

```
systemctl status mediator-scst
```

+

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

[root@mediator_host ~]#
```

Vérifiez les ports d'écoute

1. Veuillez confirmer les ports utilisés par ONTAP Mediator :

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

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

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

Gérer les certificats

Régénérez un certificat temporaire auto-signé pour l'hôte ONTAP Mediator

Régénérer un certificat auto-signé temporaire pour l'hôte actuel lorsqu'un changement de nom de l'hôte ou d'adresse IP invalide le certificat existant.



Cette procédure n'est prise en charge que sur les systèmes exécutant ONTAP Mediator 1.7 ou une version ultérieure.

À propos de cette tâche

- Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.
- Vous pouvez effectuer cette tâche uniquement si les certificats auto-signés générés sont devenus obsolètes en raison de modifications apportées au nom de l'hôte ou à l'adresse IP de l'hôte après l'installation d'ONTAP Mediator.
- Une fois le certificat auto-signé temporaire remplacé par un certificat tiers de confiance, vous ne devez *pas* utiliser cette tâche pour régénérer un certificat. L'absence de certificat auto-signé entraînera l'échec de cette procédure.

Étape

Pour régénérer un nouveau certificat temporaire auto-signé pour l'hôte actuel, procédez comme suit :

1. Redémarrer ONTAP Mediator :

```
./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
```

Remplacez les certificats auto-signés d'ONTAP Mediator par des certificats tiers de confiance

Si votre environnement le permet, remplacez les certificats auto-signés par des certificats de confiance émis par une autorité de certification.

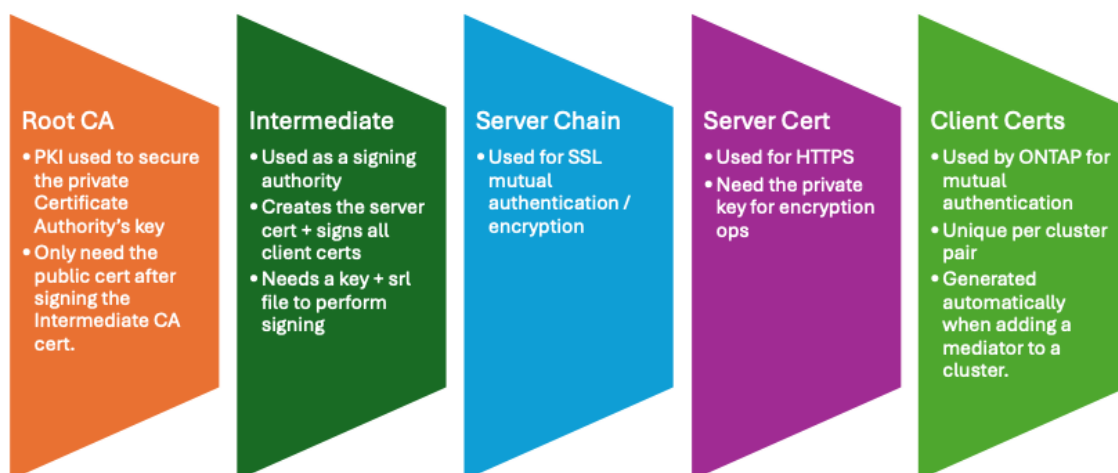


- Les certificats tiers ne sont pris en charge qu'à partir d'ONTAP 9.16.1 et dans certaines versions correctives antérieures d'ONTAP. Voir ["NetApp Identifiant du bogue Bugs Online CONTAP-243278"](#).
- Les certificats tiers ne sont pris en charge que sur les systèmes exécutant ONTAP Mediator 1.7 ou une version ultérieure.

À propos de cette tâche

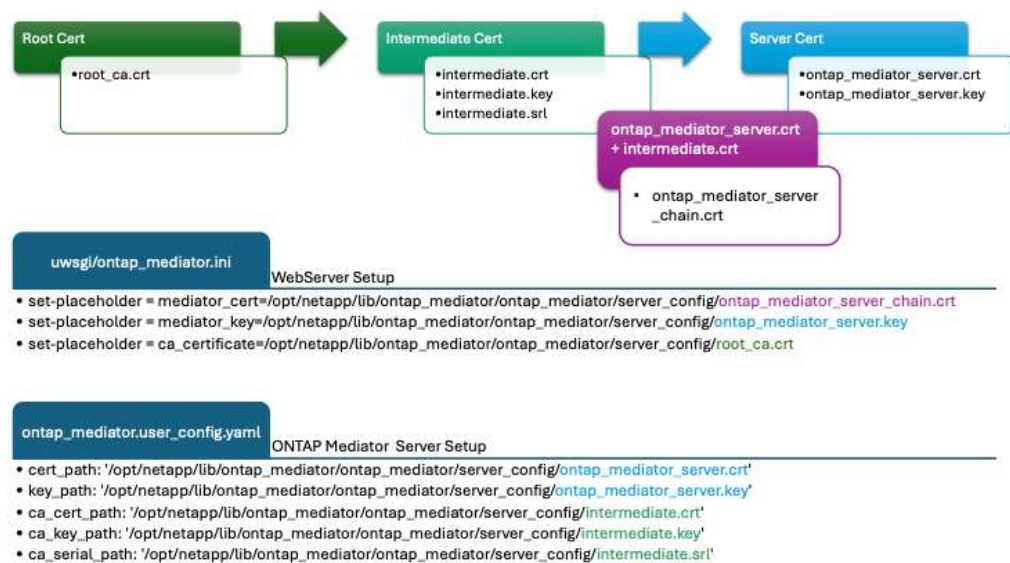
- Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.
- Vous pouvez effectuer cette opération si les certificats auto-signés générés doivent être remplacés par des certificats obtenus auprès d'une autorité de certification (CA) subordonnée de confiance. Pour ce faire, vous devez avoir accès à une autorité d'infrastructure à clés publiques (PKI) de confiance.
- L'image suivante illustre la finalité de chaque certificat ONTAP Mediator.

ONTAP Mediator Certificate Purposes



- L'image suivante illustre la configuration du serveur web et d'ONTAP Mediator.

ONTAP Mediator Certificates



Étape 1 : Obtenir un certificat auprès d'un organisme tiers délivrant un certificat d'autorité de certification

Vous pouvez obtenir un certificat auprès d'une autorité PKI en suivant la procédure ci-dessous.

L'exemple suivant illustre le remplacement des acteurs de certificats auto-signés par les acteurs de certificats tiers situés à `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`.



Cet exemple illustre les critères nécessaires pour les certificats requis pour ONTAP Mediator. Vous pouvez obtenir les certificats auprès d'une autorité PKI d'une manière qui peut différer de cette procédure. Adaptez la procédure en fonction de vos besoins métier.

ONTAP Mediator 1.9 et versions ultérieures

1. Créez une clé privée `intermediate.key` et un fichier de configuration `openssl_ca.cnf` que l'autorité PKI utilisera pour générer un certificat.

- a. Générer la clé privée `intermediate.key`:

Exemple

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

- b. Le fichier de configuration `openssl_ca.cnf` (situé à `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) définit les propriétés que le certificat généré doit avoir.

2. Utilisez la clé privée et le fichier de configuration pour créer une demande de signature de certificat `intermediate.csr`:

Exemple :

```
openssl req -key <private_key_name>.key -new -out
```

```
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

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

3. Envoyez la demande de signature de certificat `intermediate.csr` à une autorité PKI pour signature.

L'autorité PKI vérifie la requête et la signe `.csr`, générant ainsi le certificat `intermediate.crt`. De plus, vous devez obtenir auprès de l'autorité PKI le certificat `root_ca.crt` qui a signé le certificat `intermediate.crt`.



Pour les clusters SnapMirror active sync et les configurations IP MetroCluster utilisant ONTAP Mediator configuré avec HTTPS, vous devez ajouter les `intermediate.crt` et `root_ca.crt` certificats à un cluster ONTAP. Voir ["Configurez ONTAP Mediator et les clusters pour la synchronisation active SnapMirror"](#) et ["Configurez le médiateur ONTAP pour une configuration IP MetroCluster"](#).

ONTAP Mediator 1.8 et versions antérieures

1. Créez une clé privée `ca.key` et un fichier de configuration `openssl_ca.cnf` qui seront utilisés par l'autorité PKI pour générer un certificat.

- a. Générer la clé privée `ca.key` :

Exemple :

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

- b. Le fichier de configuration `openssl_ca.cnf` (situé à `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) définit les propriétés que le certificat généré doit avoir.

2. Utilisez la clé privée et le fichier de configuration pour créer une demande de signature de certificat `ca.csr`:

Exemple :

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

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

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

3. Envoyez la demande de signature de certificat `ca.csr` à une autorité PKI pour sa signature.

L'autorité PKI vérifie la requête et signe la `.csr`, générant le certificat `ca.crt`. De plus, vous devez obtenir auprès de l'autorité PKI le `root_ca.crt` certificat qui a signé le `ca.crt` certificat.



Pour les clusters de synchronisation active SnapMirror, vous devez ajouter les certificats `ca.crt` et `root_ca.crt` à un cluster ONTAP. Voir ["Configurez ONTAP Mediator et les clusters pour la synchronisation active SnapMirror"](#).

Étape 2 : Générez un certificat de serveur en le signant à l'aide d'une certification d'autorité de certification tierce

ONTAP Mediator 1.9 et versions ultérieures

Un certificat serveur doit être signé par la clé privée `intermediate.key` et le certificat tiers `intermediate.crt`. De plus, le fichier de configuration `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contient certains attributs qui spécifient les propriétés requises pour les certificats serveur émis par OpenSSL.

Les commandes suivantes permettent de générer un certificat serveur.

Étapes

1. Pour générer une demande de signature de certificat de serveur (CSR), exécutez la commande suivante depuis le `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` dossier :

```
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. Pour générer un certificat serveur à partir de la CSR, exécutez la commande suivante depuis le `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` dossier :



Ces fichiers proviennent d'une autorité de certification PKI. Si vous utilisez un autre nom de certificat, remplacez `intermediate.crt` et `intermediate.key` par les noms de fichiers correspondants.

```
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
```

◦ L'option `-CAcreateserial` permet de générer les `intermediate.srl` fichiers.

ONTAP Mediator 1.8 et versions antérieures

Un certificat serveur doit être signé par la clé privée `ca.key` et le certificat tiers `ca.crt`. De plus, le fichier de configuration

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf contient certains attributs qui spécifient les propriétés requises pour les certificats serveur émis par OpenSSL.

Les commandes suivantes permettent de générer un certificat serveur.

Étapes

1. Pour générer une demande de signature de certificat de serveur (CSR), exécutez la commande suivante depuis le /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config dossier :

```
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. Pour générer un certificat serveur à partir de la CSR, exécutez la commande suivante depuis le /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config dossier:



Ces fichiers ont été obtenus auprès d'une autorité PKI. Si vous utilisez un autre nom de certificat, remplacez `ca.crt` et `ca.key` par les noms de fichiers correspondants.

```
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
```

° L' `-CAcreateserial` option permet de générer les `ca.srl` fichiers.

Étape 3 : Remplacez le nouveau certificat d'autorité de certification tierce et le certificat du serveur dans la configuration de ONTAP Mediator.

ONTAP Mediator 1.10 et versions ultérieures

La configuration du certificat est fournie à ONTAP Mediator dans le fichier de configuration situé à /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml. Le fichier comprend les attributs suivants :

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

```
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` et `key_path` sont des variables de certificat serveur.
- `ca_cert_path`, `ca_key_path` et `ca_serial_path` sont des variables de certificat d'autorité de certification.

Étapes

1. Remplacez tous `intermediate.*` les fichiers par les certificats tiers.
2. Créez une chaîne de certificats à partir des certificats `intermediate.crt` et `ontap_mediator_server.crt`:

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

3. Mettez à jour le `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` fichier.

Mettez à jour les valeurs de `ssl_keyfile`, `ssl_certfile` et `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
```

- La `ssl_keyfile` valeur correspond au chemin d'accès à la clé dans le `ontap_mediator_server.crt` fichier, qui est `ontap_mediator_server.key`.
 - La `ssl_certfile` valeur correspond au chemin d'accès du `ontap_mediator_server_chain.crt` fichier.
 - La `ssl_ca_certs` valeur correspond au chemin d'accès du `root_ca.crt` fichier.
4. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :
 - Propriétaire du groupe Linux: `netapp:netapp`
 - Autorisations Linux: `600`
 5. Redémarrer ONTAP Mediator :

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 et 1.9

La configuration du certificat est fournie à ONTAP Mediator dans le fichier de configuration situé à `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. Le fichier comprend les attributs suivants :

```

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

```

- `cert_path` et `key_path` sont des variables de certificat serveur.
- `ca_cert_path`, `ca_key_path` et `ca_serial_path` sont des variables de certificat d'autorité de certification.

Étapes

1. Remplacez tous `intermediate.*` les fichiers par les certificats tiers.
2. Créez une chaîne de certificats à partir des certificats `intermediate.crt` et `ontap_mediator_server.crt`:

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

3. Mettez à jour le `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` fichier.

Mettez à jour les valeurs de `mediator_cert`, `mediator_key` et `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

```

- La `mediator_cert` valeur correspond au chemin d'accès du `ontap_mediator_server_chain.crt` fichier.
- Le `mediator_key` value est le chemin d'accès principal dans le fichier `ontap_mediator_server.crt`, qui est `ontap_mediator_server.key`.

- La `ca_certificate` valeur correspond au chemin d'accès du `root_ca.crt` fichier.

4. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :

- Propriétaire du groupe Linux: `netapp:netapp`
- Autorisations Linux: `600`

5. Redémarrer ONTAP Mediator :

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 et versions antérieures

La configuration du certificat est fournie à ONTAP Mediator dans le fichier de configuration situé à `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. Le fichier comprend les attributs suivants :

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

- `cert_path` et `key_path` sont des variables de certificat serveur.
- `ca_cert_path`, `ca_key_path` et `ca_serial_path` sont des variables de certificat d'autorité de certification.

Étapes

1. Remplacez tous `ca.*` les fichiers par les certificats tiers.
2. Créez une chaîne de certificats à partir des certificats `ca.crt` et `ontap_mediator_server.crt` :

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

3. Mettez à jour le `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` fichier.

Mettez à jour les valeurs de `mediator_cert`, `mediator_key` et `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.crt
```

```
server.key
```

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

- La mediator_cert valeur correspond au chemin d'accès du ontap_mediator_server_chain.crt fichier.
 - Le mediator_key value est le chemin d'accès principal dans le fichier ontap_mediator_server.crt, qui est ontap_mediator_server.key.
 - La ca_certificate valeur correspond au chemin d'accès du root_ca.crt fichier.
4. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :
- Propriétaire du groupe Linux: netapp:netapp
 - Autorisations Linux: 600
5. Redémarrer ONTAP Mediator :

```
systemctl restart ontap_mediator
```

Étape 4 : Vous pouvez, si vous le souhaitez, utiliser un chemin d'accès ou un nom différent pour vos certificats tiers

ONTAP Mediator 1.10 et versions ultérieures

Vous pouvez utiliser des certificats tiers avec un nom autre que intermediate.* ou stocker les certificats tiers dans un autre emplacement.

Étapes

1. Configurez le

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml fichier pour remplacer les valeurs par défaut des variables dans le ontap_mediator.config.yaml fichier.

Si vous avez obtenu intermediate.crt auprès d'une autorité PKI et que vous stockez sa clé privée intermediate.key à l'emplacement

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config, le fichier ontap_mediator.user_config.yaml devrait ressembler à l'exemple suivant :



Si vous avez utilisé intermediate.crt pour signer le `ontap\_mediator\_server.crt` certificat, le fichier `intermediate.srl` est généré. Consultez [Étape 2 : Générez un certificat de serveur en le signant à l'aide d'une certification d'autorité de certification tierce](#) pour plus d'informations.

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

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

```

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

```

- a. Si vous utilisez une structure de certificats où le `root_ca.crt` certificat fournit un `intermediate.crt` certificat qui signe le `ontap_mediator_server.crt` certificat, créez une chaîne de certificats à partir des `intermediate.crt` et `ontap_mediator_server.crt` certificats :



Vous auriez dû obtenir les `intermediate.crt` et `ontap_mediator_server.crt` certificats auprès d'une autorité PKI plus tôt dans la procédure.

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

- b. Mettez à jour le `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` fichier.

Mettez à jour les valeurs de `ssl_keyfile`, `ssl_certfile` et `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
```

- La `ssl_keyfile` valeur correspond au chemin d'accès à la clé dans le `ontap_mediator_server.crt` fichier, qui est `ontap_mediator_server.key`.
- La `ssl_certfile` valeur correspond au chemin d'accès du `ontap_mediator_server_chain.crt` fichier.
- La `ssl_ca_certs` valeur correspond au chemin d'accès du `root_ca.crt` fichier.



Pour les clusters SnapMirror active sync et les configurations IP MetroCluster utilisant ONTAP Mediator configuré avec HTTPS, vous devez ajouter les `intermediate.crt` et `root_ca.crt` certificats à un cluster ONTAP. Voir ["Configurez ONTAP Mediator et les clusters pour la synchronisation active SnapMirror"](#) et ["Configurez le médiateur ONTAP pour une configuration IP MetroCluster"](#).

c. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :

- Propriétaire du groupe Linux: `netapp:netapp`
- Autorisations Linux: `600`

2. Redémarrez ONTAP Mediator une fois les certificats mis à jour dans le fichier de configuration :

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 et 1.9

Vous pouvez utiliser des certificats tiers avec un nom autre que `intermediate.*` ou stocker les certificats tiers dans un autre emplacement.

Étapes

1. Configurez le

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

 fichier pour remplacer les valeurs par défaut des variables dans le `ontap_mediator.config.yaml` fichier.

Si vous avez obtenu `intermediate.crt` auprès d'une autorité PKI et que vous stockez sa clé privée `intermediate.key` à l'emplacement

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config,
```

 le fichier `ontap_mediator.user_config.yaml` devrait ressembler à l'exemple suivant :

Si vous avez utilisé `intermediate.crt` pour signer le `ontap_mediator_server.crt` certificat, le fichier `intermediate.srl` est généré. Consultez [Étape 2 : Générez un certificat de serveur en le signant à l'aide d'une certification d'autorité de certification tierce](#) pour

plus d'informations.

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

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

- a. Si vous utilisez une structure de certificats où le `root_ca.crt` certificat fournit un `intermediate.crt` certificat qui signe le `ontap_mediator_server.crt` certificat, créez une chaîne de certificats à partir des `intermediate.crt` et `ontap_mediator_server.crt` certificats :



Vous auriez dû obtenir les `intermediate.crt` et `ontap_mediator_server.crt` certificats auprès d'une autorité PKI plus tôt dans la procédure.

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

ontap_mediator_server_chain.crt

- b. Mettez à jour le /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini fichier.

Mettez à jour les valeurs de mediator_cert, mediator_key et 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
```

- La mediator_cert valeur correspond au chemin d'accès du ontap_mediator_server_chain.crt fichier.
- La mediator_key valeur correspond au chemin d'accès à la clé dans le ontap_mediator_server.crt fichier, qui est ontap_mediator_server.key.
- La ca_certificate valeur correspond au chemin d'accès du root_ca.crt fichier.



Pour les clusters de continuité d'activité SnapMirror Business Continuity (SM-BC), vous devez ajouter les certificats intermediate.crt et root_ca.crt à un cluster ONTAP. Voir ["Configurez ONTAP Mediator et les clusters pour la synchronisation active SnapMirror"](#).

- c. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :

- Propriétaire du groupe Linux: netapp:netapp
- Autorisations Linux: 600

2. Redémarrez ONTAP Mediator une fois les certificats mis à jour dans le fichier de configuration :

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 et versions antérieures

Vous pouvez utiliser des certificats tiers avec un nom autre que ca.* ou stocker les certificats tiers dans un emplacement différent.

Étapes

1. Configurez le

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml fichier pour remplacer les valeurs par défaut des variables dans le ontap_mediator.config.yaml fichier.

Si vous avez obtenu ca.crt auprès d'une autorité PKI et que vous stockez sa clé privée ca.key à l'emplacement /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config, le fichier ontap_mediator.user_config.yaml devrait ressembler à l'exemple suivant :



Si vous avez utilisé `ca.crt` pour signer le `ontap_mediator_server.crt` certificat, le `ca.srl` fichier est généré. Consultez [Étape 2 : Générez un certificat de serveur en le signant à l'aide d'une certification d'autorité de certification tierce](#) pour plus d'informations.

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

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

- a. Si vous utilisez une structure de certificats où le `root_ca.crt` certificat fournit un `ca.crt` certificat qui signe le `ontap_mediator_server.crt` certificat, créez une chaîne de certificats à partir du `ca.crt` et du `ontap_mediator_server.crt` certificat :



Vous auriez dû obtenir les `ca.crt` et `ontap_mediator_server.crt` certificats auprès d'une autorité PKI plus tôt dans la procédure.

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

b. Mettez à jour le `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` fichier.

Mettez à jour les valeurs de `mediator_cert`, `mediator_key` et `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
```

- La `mediator_cert` valeur correspond au chemin d'accès du `ontap_mediator_server_chain.crt` fichier.
- La `mediator_key` valeur correspond au chemin d'accès à la clé dans le `ontap_mediator_server.crt` fichier, qui est `ontap_mediator_server.key`.
- La `ca_certificate` valeur correspond au chemin d'accès du `root_ca.crt` fichier.



Pour les clusters SnapMirror Business Continuity (SM-BC), vous devez ajouter les `ca.crt` et `root_ca.crt` certificats à un cluster ONTAP. Voir "[Configurez ONTAP Mediator et les clusters pour la synchronisation active SnapMirror](#)".

c. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :

- Propriétaire du groupe Linux: `netapp:netapp`
- Autorisations Linux: `600`

2. Redémarrez ONTAP Mediator une fois les certificats mis à jour dans le fichier de configuration :

```
systemctl restart ontap_mediator
```

Résoudre les problèmes liés aux certificats d'ONTAP Mediator

Utilisez ces vérifications pour contrôler les propriétés du certificat lors du dépannage des problèmes de certificat.

Vérifier l'expiration du certificat

Utilisez la commande suivante pour identifier la plage de validité du certificat.

ONTAP Mediator 1.9 et versions ultérieures

```
[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 et versions antérieures

```
[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
```

Vérifier les extensions X509v3 dans le certificat de l'autorité de certification

Utilisez la commande suivante pour vérifier les extensions X509v3 dans le certificat de l'autorité de certification.

ONTAP Mediator 1.9 et versions ultérieures

Les propriétés définies dans **v3_ca** dans `openssl_ca.cnf` sont affichées comme X509v3 extensions dans `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 et versions antérieures

Les propriétés définies dans **v3_ca** dans `openssl_ca.cnf` sont affichées comme X509v3 extensions dans `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

```

Vérifiez les extensions X509v3 dans le certificat du serveur et les noms alternatifs du sujet

Les `v3_req` propriétés définies dans le `openssl_server.cnf` fichier de configuration sont affichées telles qu'elles figurent X509v3 extensions dans le certificat.

Dans l'exemple suivant, vous pouvez obtenir les variables dans les sections `alt_names` en exécutant les commandes `hostname -A` et `hostname -I` sur la machine virtuelle Linux sur laquelle ONTAP Mediator est installé.

Vérifiez auprès de votre administrateur réseau les valeurs correctes des variables.

ONTAP Mediator 1.9 et versions ultérieures

```
[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 et versions antérieures

```
[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
```

Vérifiez qu'une clé privée correspond à un certificat

Vous pouvez vérifier si une clé privée particulière correspond à un certificat.

Utilisez les commandes OpenSSL suivantes respectivement sur la clé et le certificat.

ONTAP Mediator 1.9 et versions ultérieures

```
[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 et versions antérieures

```
[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
```

Si l'attribut `-modulus` correspond pour les deux, cela indique que la paire clé privée-certificat est compatible et peut fonctionner ensemble.

Vérifiez qu'un certificat de serveur est créé à partir d'un certificat d'autorité de certification particulier

Vous pouvez utiliser la commande suivante pour vérifier que le certificat du serveur est créé à partir d'un certificat d'autorité de certification spécifique.

ONTAP Mediator 1.9 et versions ultérieures

```
[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 et versions antérieures

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

Si la validation du protocole OCSP (Online Certificate Status Protocol) est utilisée, utilisez la commande `"openssl-verify"`.

Maintenir le système d'exploitation hôte pour ONTAP Mediator

Assurez-vous que le système d'exploitation hôte de ONTAP Mediator bénéficie d'une maintenance régulière afin d'obtenir des performances optimales.

Redémarrez l'hôte

Redémarrez l'hôte uniquement lorsque les clusters sont opérationnels. Les clusters ne peuvent pas réagir aux pannes lorsque ONTAP Mediator est hors ligne. Planifiez une maintenance avant de redémarrer.

ONTAP Mediator reprend automatiquement son activité lors d'un redémarrage et rétablit les relations précédemment configurées avec les clusters ONTAP.

Mises à jour du package hôte

Mettez à jour toute bibliothèque ou tout paquet yum, à l'exception du noyau. Redémarrez l'hôte si nécessaire pour que les modifications prennent effet. Planifiez une fenêtre de maintenance avant de redémarrer l'hôte.

Si vous installez le `yum-utils` paquet, utilisez la `needs-restarting` commande pour détecter si des modifications apportées au paquet nécessitent un redémarrage.

Redémarrez après la mise à jour des dépendances d'ONTAP Mediator, car les modifications ne prennent pas effet immédiatement.

Mettre à niveau le noyau du système d'exploitation hôte

SCST doit être compilé pour le noyau que vous utilisez. Pour mettre à jour le système d'exploitation, vous devez planifier du temps pour la maintenance.

Avant de commencer

Les exigences suivantes s'appliquent lorsque le package SCST est installé avec ONTAP Mediator.

- Vous pouvez mettre à jour tous les paquets de bibliothèque, à l'exception du noyau, mais un redémarrage peut être nécessaire pour appliquer les modifications dans ONTAP Mediator. Prévoyez une interruption si vous devez redémarrer.
- Il est recommandé de maintenir le noyau du système d'exploitation à jour. Mettez à niveau le noyau vers une version prise en charge répertoriée dans "[Matrice des versions d'ONTAP Mediator](#)". Un redémarrage du système est nécessaire ; prévoyez donc une interruption de service pour la maintenance.
 - Désinstallez le module du noyau SCST avant de redémarrer, puis réinstallez-le après le redémarrage.
 - Préparez une version compatible de SCST à réinstaller avant de commencer la mise à niveau du noyau du système d'exploitation.



Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure prenant uniquement en charge HTTPS, le paquet SCST n'est pas installé et le noyau du système d'exploitation hôte peut être mis à niveau sans incidence sur ONTAP Mediator. Consultez la documentation de votre système d'exploitation hôte pour obtenir les instructions de mise à niveau.

Étapes

Suivez ces étapes pour mettre à niveau le noyau du système d'exploitation hôte.



Avant de mettre à niveau le noyau, vérifiez que le système d'exploitation et la version d'ONTAP Mediator sont compatibles. Pour connaître les versions prises en charge, consultez le "[Matrice de prise en charge des systèmes d'exploitation](#)".

1. Arrêtez ONTAP Mediator.
2. Désinstallez le package SCST, voir [Effectuer la maintenance de l'hôte](#). (SCST ne propose pas de mécanisme de mise à niveau.)
3. Mettez à jour le système d'exploitation, puis redémarrez.
4. Réinstallez le package SCST.
5. Réactivez ONTAP Mediator.

Effectuer la maintenance de l'hôte

La mise à jour du noyau de la machine virtuelle peut entraîner des problèmes de compatibilité avec les modules SCST. Désinstallez puis réinstallez SCST manuellement.



Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure prenant uniquement en charge HTTPS, le package SCST n'est pas installé et vous pouvez ignorer cette tâche.

Étape 1 : Désinstaller SCST

Pour désinstaller SCST, utilisez l'archive tar correspondant à votre version d'ONTAP Mediator.

Étapes

1. Téléchargez le paquet SCST approprié (comme indiqué dans le tableau suivant) et extrayez-le.

Pour cette version ...	Utilisez ce bundle tar...
ONTAP Mediator 1.12.1	scst-3.10.tar.gz
ONTAP Mediator 1.12	scst-3.10.tar.gz
ONTAP Mediator 1.11	scst-3.9.tar.gz
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAP Mediator 1.9.1	scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	scst-3.5.0.tar.bz2
ONTAP Mediator 1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	scst-3.3.0.tar.bz2

- a. Accédez au package open source depuis le "[Téléchargements SCST sur sourceforge](#)".

- b. Sélectionnez **Télécharger les versions publiées**.
 - c. Extrayez l'archive sur votre VM.
2. Exécutez les commandes de désinstallation suivantes dans le `scst` répertoire :
 - a. `systemctl stop mediator-scst`
 - b. `make scstadm_uninstall`
 - c. `make iscsi_uninstall`
 - d. `make usr_uninstall`
 - e. `make scst_uninstall`
 - f. `depmod`

Étape 2 : Installer SCST

Pour installer manuellement SCST, vous avez besoin du paquet tar SCST utilisé pour la version installée d'ONTAP Mediator (voir le [Table SCST](#)).

À propos de cette tâche

- Effectuez cette étape avant d'installer ONTAP Mediator. Si la version de SCST que vous utilisez est plus récente que la version fournie avec le programme d'installation de ONTAP Mediator, celui-ci ignore cette étape.
- Dans certains scénarios, l'installation par défaut de SCST sur le système d'exploitation mis à niveau peut échouer car le système d'exploitation mis à niveau nécessite un correctif.

À partir d'ONTAP Mediator 1.12.1, si l'installation échoue, vous pouvez utiliser l'outil de réparation SCST situé dans `/usr/local/bin/mediator_repair_scst` pour réparer l'installation.

Si le système d'exploitation mis à niveau nécessite un correctif, l'outil le contient pour la version de SCST fournie avec le package ONTAP Mediator. L'`mediator_repair_scst` outil est un outil autonome distinct du programme d'installation principal et est inclus dans le fichier ONTAP Mediator `.tgz`. Il n'affecte pas l'installation ni les chemins de mise à niveau d'ONTAP Mediator.

Étapes

1. Exécutez les commandes d'installation suivantes dans le `scst` répertoire:
 - a. `make 2release`
 - b. `make scst_install`
 - c. `make usr_install`
 - d. `make iscsi_install`
 - e. `make scstadm_install`
 - f. `depmod`



Si vous effectuez une première installation et souhaitez préinstaller ONTAP Mediator, exécutez la commande suivante avant de passer à l'étape suivante :

```
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`



Si vous préinstallez SCST avant ONTAP Mediator lors d'une première installation, ignorez cette étape. Le programme d'installation applique les correctifs SCST nécessaires.

2. Si vous le souhaitez, si le démarrage sécurisé est activé, avant de redémarrer, effectuez les étapes suivantes :

a. Déterminez le nom de chaque fichier pour les modules `scst_vdisk`, `scst` et `iscsi_scst` :

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

b. Déterminez la version du noyau :

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

c. Signez chaque fichier de module avec le noyau:

```
[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. Installez la clé UEFI avec le micrologiciel.

Les instructions pour installer la clé UEFI se trouvent à l'adresse suivante :

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

La clé UEFI générée se trouve à l'emplacement suivant :

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

3. Redémarrez le système :

Modifications du nom d'hôte ou de l'adresse IP de l'hôte

À propos de cette tâche

- Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.
- Ne faites cela que si les certificats auto-signés ne sont plus valides parce que le nom d'hôte ou l'adresse IP changent après l'installation de ONTAP Mediator.
- Une fois le certificat temporaire auto-signé remplacé par un certificat tiers de confiance, vous ne devez *pas* utiliser cette tâche pour régénérer un certificat. Si vous ne possédez pas de certificat auto-signé, vous ne pouvez pas utiliser cette procédure.

Étape

Créez un certificat auto-signé temporaire pour l'hôte actuel :

1. Redémarrer ONTAP Mediator :

```
./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
```

Désinstaller ONTAP Mediator

Si nécessaire, désinstallez ONTAP Mediator après l'avoir déconnecté d'ONTAP.

Avant de commencer

Vous devez déconnecter ONTAP Mediator d'ONTAP avant de le supprimer.

À propos de cette tâche

Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.

Si vous ne parvenez pas à exécuter cette commande, vous devrez peut-être l'exécuter en utilisant le chemin complet comme indiqué dans l'exemple suivant :

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

Étape

1. Désinstaller 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 ~]#
```

Mentions légales

Les mentions légales donnent accès aux déclarations de droits d’auteur, aux marques de commerce, aux brevets et plus encore.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marques déposées

NETAPP, le logo NETAPP et les marques figurant sur la page NetApp Trademarks sont des marques de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques de leurs propriétaires respectifs.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Brevets

Une liste actuelle des brevets détenus par NetApp peut être trouvée à :

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Politique de confidentialité

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Open source

Les fichiers de notification fournissent des informations sur les droits d’auteur et les licences de tiers utilisés dans les logiciels NetApp.

ONTAP Mediator pour MetroCluster IP et SnapMirror active sync

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

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.