Planification

ONTAP 9

NetApp
February 04, 2026

Sommaire

Planification

Préparez-vous à utiliser ONTAP AutoSupport

Vous pouvez configurer un cluster ONTAP pour qu'il puisse transmettre des messages AutoSupport à NetApp. Dans ce cadre, vous pouvez également envoyer une copie des messages aux adresses e-mail locales, généralement au sein de votre entreprise. Vous devez préparer la configuration de AutoSupport en consultant les options disponibles.

Transmettre les messages AutoSupport à NetApp

Les messages AutoSupport peuvent être transmis à NetApp à l'aide des protocoles HTTPS ou SMTP. À partir de ONTAP 9.15.1, vous pouvez également utiliser TLS avec SMTP.

Utilisez HTTPS autant que possible pour communiquer avec AutoSupport OnDemand et pour télécharger des fichiers volumineux.

Notez également ce qui suit :

- Un seul canal de distribution vers NetApp peut être configuré pour les messages AutoSupport. Vous ne pouvez pas utiliser deux protocoles pour transmettre des messages AutoSupport à NetApp.
- AutoSupport limite la taille maximale de fichier pour chaque protocole. Si la taille d'un message AutoSupport dépasse la limite configurée, AutoSupport transmet autant de messages que possible, mais une troncature se produit.
- Vous pouvez modifier la taille maximale du fichier si nécessaire. Pour en savoir plus, `system node autosupport modify` consultez le "Référence de commande ONTAP".
- Les deux protocoles peuvent être transportés sur IPv4 ou IPv6 en fonction de la famille d'adresses à laquelle le nom résout.
- La connexion TCP établie par ONTAP pour envoyer des messages AutoSupport est temporaire et de courte durée.

HTTPS

Cela fournit les fonctionnalités les plus robustes. Notez ce qui suit :

- AutoSupport OnDemand et le transfert de fichiers volumineux sont pris en charge.
- Une requête HTTPS PUT est tentée en premier. Si la demande échoue pendant la transmission, la demande redémarre à l'endroit où elle s'est arrêtée.
- Si le serveur ne prend pas en charge PUT, la méthode HTTPS POST est utilisée à la place.
- La limite par défaut pour les transferts HTTPS est de 50 Mo.
- Le protocole HTTPS utilise le port 443.

SMTP

En règle générale, vous ne devez utiliser SMTP que si HTTPS n'est pas autorisé ou n'est pas pris en charge. Notez ce qui suit :

- AutoSupport OnDemand et les transferts de fichiers volumineux ne sont pas pris en charge.
- Si les informations d'identification de connexion SMTP sont configurées, elles sont envoyées sans cryptage et en clair.
- La limite par défaut pour les transferts est de 5 Mo.
- Le protocole SMTP non sécurisé utilise le port 25.

Améliorer la sécurité SMTP avec TLS

Lors de l'utilisation de SMTP, tout le trafic est non chiffré et peut être facilement intercepté et lu. À partir de ONTAP 9.15.1, vous pouvez également utiliser TLS avec SMTP (SMTPS). Dans ce cas, *Explicit TLS* est utilisé pour activer le canal sécurisé une fois la connexion TCP établie.

Le port suivant est généralement utilisé pour SMTPS : port 587

Autres considérations relatives à la configuration

D'autres considérations sont à prendre en compte lors de la configuration de AutoSupport.

Pour plus d'informations sur les commandes pertinentes à ces considérations, reportez-vous "Configurer AutoSupport"à la section .

Envoyez une copie locale par e-mail

Quel que soit le protocole utilisé pour transmettre des messages AutoSupport à NetApp, vous pouvez également envoyer une copie de chaque message à une ou plusieurs adresses e-mail locales. Par exemple, vous pouvez envoyer des messages à votre service de support interne ou à une entreprise partenaire.

> Si vous transmettez des messages à NetApp à l'aide de SMTP (ou SMTPS) et que vous envoyez également des copies locales de ces messages, la même configuration de serveur de messagerie est utilisée.

Proxy HTTP

Selon la configuration de votre réseau, le protocole HTTPS peut nécessiter une configuration supplémentaire d'une URL proxy. Si HTTPS est utilisé pour envoyer des messages AutoSupport au support technique et que vous disposez d'un proxy, vous devez identifier l'URL du proxy. Si le proxy utilise un port autre que le port par défaut (port 3128), vous pouvez spécifier le port de ce proxy. Vous pouvez également spécifier un nom d'utilisateur et un mot de passe pour l'authentification proxy.

Installez le certificat du serveur

Avec TLS (HTTPS ou SMTPS), le certificat téléchargé à partir du serveur est validé par ONTAP sur la base du certificat de l'autorité de certification racine. Avant d'utiliser HTTPS ou SMTPS, vous devez vous assurer que le certificat racine est installé dans ONTAP et que ONTAP peut valider le certificat du serveur. Cette validation est effectuée sur la base de l'autorité de certification qui a signé le certificat du serveur.

ONTAP inclut un grand nombre de certificats d'autorité de certification racine pré-installés. Dans de nombreux cas, le certificat de votre serveur sera immédiatement reconnu par ONTAP sans configuration supplémentaire. Selon la façon dont le certificat de serveur a été signé, vous devrez peut-être installer un certificat d'autorité de certification racine et tous les certificats intermédiaires.

Procédez comme suit pour installer le certificat, si nécessaire. Vous devez installer tous les certificats requis au niveau du cluster.

Exemple 1. Étapes

System Manager

1. Dans System Manager, sélectionnez **Cluster** > **Paramètres**.
2. Faites défiler jusqu'à la section **sécurité**.
3. Sélectionnez → en regard de **certificats**.
4. Sous l'onglet **autorités de certification approuvées**, cliquez sur **Ajouter**.
5. Cliquez sur **Importer** et sélectionnez le fichier de certificat.
6. Renseignez les paramètres de configuration de votre environnement.
7. Cliquez sur **Ajouter**.

CLI

1. Commencez l'installation :

   ```
   security certificate install -type server-ca
   ```

   Pour en savoir plus, `security certificate install` consultez le "Référence de commande ONTAP".

2. Recherchez le message de console suivant :

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Ouvrez le fichier de certificat à l'aide d'un éditeur de texte.
4. Copiez l'intégralité du certificat, y compris les lignes suivantes :

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. Collez le certificat dans le terminal après l'invite de commande.
6. Appuyez sur **entrée** pour terminer l'installation.
7. Vérifiez que le certificat est installé en exécutant l'une des commandes suivantes :

   ```
   security certificate show-user-installed
   ```

   ```
   security certificate show
   ```

   Pour en savoir plus, `security certificate show` consultez le "Référence de commande ONTAP".

Informations associées

- "Configurer AutoSupport"
- "Référence de commande ONTAP"

Configuration de ONTAP AutoSupport

Vous pouvez configurer un cluster ONTAP pour qu'il envoie des messages AutoSupport au support technique NetApp et en envoie des copies à votre service de support interne. Dans ce cadre, vous pouvez également tester la configuration avant de l'utiliser dans un environnement de production.

Description de la tâche

Depuis ONTAP 9.5, vous activez et configurez AutoSupport pour tous les nœuds d'un cluster simultanément. Lorsqu'un nouveau nœud rejoint le cluster, il hérite automatiquement de la même configuration AutoSupport. Pour cela, le périmètre de la commande CLI `system node autosupport modify` est au niveau du cluster. Le `-node` l'option de commande est conservée pour la compatibilité descendante, mais elle est ignorée.

> Dans ONTAP 9.4 et versions antérieures, la commande `system node autosupport modify` est spécifique à chaque nœud. Si votre cluster exécute ONTAP 9.4 ou une version antérieure, vous devez activer et configurer AutoSupport sur chaque nœud du cluster.

Avant de commencer

La configuration de transport recommandée pour la transmission des messages AutoSupport à NetApp est HTTPS (HTTP avec TLS). Cette option offre les fonctionnalités les plus robustes et la meilleure sécurité.

Révision "Préparez-vous à utiliser AutoSupport" Pour plus d'informations avant de configurer votre cluster ONTAP.

Étapes

1. Assurez-vous que AutoSupport est activé :

   ```
   system node autosupport modify -state enable
   ```

2. Si vous souhaitez que le support technique NetApp reçoive des messages AutoSupport, utilisez la commande suivante :

   ```
   system node autosupport modify -support enable
   ```

   Vous devez activer cette option si vous souhaitez permettre à AutoSupport de travailler avec AutoSupport OnDemand ou si vous souhaitez télécharger des fichiers volumineux, tels que les fichiers core dump et d'archivage des performances, vers le support technique ou une URL spécifiée.

   > AutoSupport OnDemand est activé par défaut et fonctionnel lorsqu'il est configuré pour envoyer des messages au support technique à l'aide du protocole de transport HTTPS.

3. Si vous avez activé le support technique NetApp pour recevoir des messages AutoSupport, spécifiez le protocole de transport à utiliser pour ces messages.

Vous pouvez choisir parmi les options suivantes :

Les fonctions que vous recherchez…	Définissez ensuite les paramètres suivants du `system node autosupport modify` commande…
Utilisez le protocole HTTPS par défaut	a. Réglez `-transport` à `https`. b. Si vous utilisez un proxy, définissez `-proxy -url` À l'URL de votre proxy. Cette configuration prend en charge la communication avec AutoSupport OnDemand et les téléchargements de fichiers volumineux.
Utiliser SMTP	Réglez `-transport` à `smtp`. Cette configuration ne prend pas en charge AutoSupport OnDemand ni les téléchargements de fichiers volumineux.

4. Si vous souhaitez que votre service de support interne ou un partenaire de support reçoive les messages AutoSupport, effectuez les opérations suivantes :
   a. Identifiez les destinataires de votre organisation en définissant les paramètres suivants de l' `system node autosupport modify` commande :

Définir ce paramètre…	À ceci…
`-to`	Jusqu'à cinq adresses e-mail ou listes de distribution individuelles séparées par des virgules dans votre service de support interne qui recevront des messages AutoSupport clés
`-noteto`	Jusqu'à cinq adresses e-mail ou listes de distribution individuelles séparées par des virgules dans votre service d'assistance interne qui recevront une version abrégée des messages clés AutoSupport conçus pour les téléphones portables et autres appareils mobiles
`-partner-address`	Jusqu'à cinq adresses e-mail ou listes de distribution séparées par des virgules dans votre organisation partenaire de support qui recevront tous les messages AutoSupport

   b. Vérifiez que les adresses sont correctement configurées en répertoriant les destinations à l'aide de l' `system node autosupport destinations show` commande.
5. Si vous avez configuré les adresses des destinataires de votre organisation de support interne à l'étape précédente ou si vous avez choisi le transport SMTP pour les messages vers le support technique, configurez SMTP en définissant les paramètres suivants de la `system node autosupport modify` commande :

- Réglez `-mail-hosts` à un ou plusieurs hôtes de messagerie, séparés par des virgules.

  Vous pouvez définir un maximum de cinq.

  Vous pouvez configurer une valeur de port pour chaque hôte de messagerie en spécifiant un point-virgule et un numéro de port après le nom d'hôte de messagerie : par exemple, `mymailhost.example.com:5678`, où 5678 est le port de l'hôte de messagerie.

- Réglez `-from` À l'adresse e-mail qui envoie le message AutoSupport.

6. Configurez DNS.
7. Vous pouvez également ajouter des options de commande si vous souhaitez modifier des paramètres spécifiques :

Pour cela…	Définissez ensuite les paramètres suivants du `system node autosupport modify` commande…
Masquez des données privées en supprimant, masquant ou encodant des données sensibles dans les messages	Réglez `-remove-private-data` à `true`. Si vous changez de `false` à `true`, Tous les fichiers historiques AutoSupport et tous les fichiers associés sont supprimés.
Arrêt de l'envoi des données de performance dans des messages AutoSupport périodiques	Réglez `-perf` à `false`.

8. Si vous utilisez SMTP pour envoyer des messages AutoSupport à NetApp, vous pouvez éventuellement activer TLS pour améliorer la sécurité.
   a. Afficher les valeurs disponibles pour le nouveau paramètre :

   ```
   cluster1::> system node autosupport modify -smtp-encryption ?
   ```

   b. Activer TLS pour la livraison des messages SMTP :

   ```
   cluster1::> system node autosupport modify -smtp-encryption start_tls
   ```

   c. Afficher la configuration actuelle :

   ```
   cluster1::> system node autosupport show -fields smtp-encryption
   ```

9. Vérifiez la configuration globale à l'aide du `system node autosupport show` commande avec `-node` paramètre.
10. Vérifier le fonctionnement de AutoSupport à l'aide de l' `system node autosupport check show` commande.

    Si des problèmes sont signalés, utilisez le `system node autosupport check show-details` pour afficher plus d'informations.

11. Vérifiez que les messages AutoSupport sont en cours d'envoi et de réception :

    a. Utilisez le `system node autosupport invoke` commande avec `-type` paramètre défini sur `test`:

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. Vérifiez que NetApp reçoit vos messages AutoSupport :

    ```
    system node autosupport history show -node local
    ```

    Le statut du dernier message AutoSupport sortant doit finalement être défini sur `sent-successful` pour toutes les destinations de protocole appropriées.

    c. Vous pouvez également vérifier que les messages AutoSupport sont envoyés à votre service de support interne ou à votre partenaire de support en consultant l'e-mail de toute adresse configurée pour le `-to`, `-noteto`, ou `-partner-address` paramètres du `system node autosupport modify` commande.

Informations associées

- "Préparez-vous à utiliser AutoSupport"
- "Référence de commande ONTAP"

Informations sur le copyright

Informations sur les marques commerciales