Installation et configuration du serveur Vscan

ONTAP 9

NetApp
April 24, 2024

Sommaire

Installation et configuration du serveur Vscan

Installation et configuration du serveur Vscan

Configurez un ou plusieurs serveurs Vscan pour vous assurer que les fichiers de votre système sont analysés pour détecter d'éventuels virus. Suivez les instructions fournies par votre fournisseur pour installer et configurer le logiciel antivirus sur le serveur.

Suivez les instructions du fichier README fourni par NetApp pour installer et configurer ONTAP antivirus Connector. Vous pouvez également suivre les instructions du "Installez la page ONTAP antivirus Connector".

> Pour les configurations de reprise après incident et MetroCluster, vous devez installer et configurer des serveurs Vscan distincts pour les clusters ONTAP principal/local et secondaire/partenaire.

Configuration logicielle requise pour l'antivirus

- Pour plus d'informations sur la configuration requise pour le logiciel antivirus, reportez-vous à la documentation du fournisseur.
- Pour plus d'informations sur les fournisseurs, les logiciels et les versions pris en charge par Vscan, voir le "Solutions partenaires Vscan" page.

Conditions requises pour ONTAP antivirus Connector

- Vous pouvez télécharger ONTAP antivirus Connector à partir de la page **Téléchargement de logiciels** du site de support NetApp. "Téléchargements NetApp : logiciels"
- Pour plus d'informations sur les versions de Windows prises en charge par le connecteur antivirus ONTAP et les conditions d'interopérabilité, voir "Solutions partenaires Vscan".

> Vous pouvez installer différentes versions de serveurs Windows pour différents serveurs Vscan dans un cluster.

- .NET 3.0 ou version ultérieure doit être installé sur le serveur Windows.
- SMB 2.0 doit être activé sur le serveur Windows.

Installez ONTAP antivirus Connector

Installer le ONTAP antivirus Connector sur le serveur Vscan pour permettre la communication entre le système exécutant ONTAP et le serveur Vscan. Une fois ONTAP antivirus Connector installé, le logiciel antivirus peut communiquer avec un ou plusieurs SVM.

Description de la tâche

- Voir la "Solutions partenaires Vscan" Page pour plus d'informations sur les protocoles pris en charge, les versions de logiciels des fournisseurs antivirus, les versions de ONTAP, les conditions d'interopérabilité et les serveurs Windows.
- .NET 4.5.1 ou version ultérieure doit être installé.

- ONTAP antivirus Connector peut s'exécuter sur une machine virtuelle. Toutefois, pour de meilleures performances, NetApp recommande l'utilisation d'une machine virtuelle dédiée à l'analyse antivirus.
- SMB 2.0 doit être activé sur le serveur Windows sur lequel vous installez et exécutez ONTAP antivirus Connector.

Avant de commencer

- Téléchargez le fichier d'installation de ONTAP antivirus Connector à partir du site de support et enregistrez-le dans un répertoire de votre disque dur.
- Vérifiez que vous répondez aux exigences requises pour installer ONTAP antivirus Connector.
- Vérifiez que vous disposez des privilèges d'administrateur pour installer l'antivirus Connector.

Étapes

1. Démarrez l'assistant d'installation de l'antivirus Connector en exécutant le fichier d'installation approprié.
2. Sélectionnez *Suivant*. La boîte de dialogue dossier de destination s'ouvre.
3. Sélectionnez *Next* pour installer l'antivirus Connector dans le dossier qui est répertorié ou sélectionnez *change* pour l'installer dans un autre dossier.
4. La boîte de dialogue informations d'identification du service Windows du connecteur AV ONTAP s'ouvre.
5. Entrez vos informations d'identification de service Windows ou sélectionnez **Ajouter** pour sélectionner un utilisateur. Pour un système ONTAP, cet utilisateur doit être un utilisateur de domaine valide et doit exister dans la configuration scanner pool de la SVM.
6. Sélectionnez **Suivant**. La boîte de dialogue prêt à installer le programme s'ouvre.
7. Sélectionnez **installer** pour commencer l'installation ou sélectionnez **Précédent** si vous souhaitez modifier les paramètres. Une boîte de dialogue d'état s'ouvre et indique la progression de l'installation, suivie de la boîte de dialogue Assistant InstallShield terminé.
8. Cochez la case configurer les LIFs ONTAP si vous souhaitez poursuivre la configuration des LIFs de données ou de gestion ONTAP. Vous devez configurer au moins une LIF de données ou de gestion ONTAP avant d'utiliser ce serveur Vscan.
9. Cochez la case Afficher le journal **Windows installer** si vous souhaitez afficher les journaux d'installation.
10. Sélectionnez **Terminer** pour terminer l'installation et fermer l'assistant InstallShield. L'icône **Configure ONTAP LIFs** est enregistrée sur le bureau pour configurer les LIFs ONTAP.
11. Ajouter un SVM au antivirus Connector. Vous pouvez ajouter un SVM à l'antivirus Connector en ajoutant une LIF de gestion ONTAP, interrogée sur la liste des LIFs de données, ou en configurant directement la LIF de données. Si la LIF de gestion ONTAP est configurée, vous devez également fournir les informations d'interrogation et les informations d'identification du compte admin ONTAP.
    - Vérifier que la LIF de management ou l'adresse IP du SVM est Enabled for `management-https`. Cela n'est pas nécessaire lorsque vous configurez uniquement les LIFs de données.
    - Vérifiez que vous avez créé un compte d'utilisateur pour l'application HTTP et que vous avez attribué un rôle ayant (au moins en lecture seule) accès au système `/api/network/ip/interfaces` API REST. Pour plus d'informations sur la création d'un utilisateur, reportez-vous à la section "création d'un rôle de connexion de sécurité" et "création d'une connexion de sécurité" Pages de manuel ONTAP.

> Vous pouvez également utiliser l'utilisateur du domaine en tant que compte en ajoutant un SVM de tunnel d'authentification pour une SVM d'administration. Pour plus d'informations, reportez-vous à la section "connexion de sécurité domaine-tunnel créer" ONTAP ou utilisez `/api/security/acccounts` et `/api/security/roles` API REST pour configurer le compte et le rôle admin

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**.
2. Dans la boîte de dialogue Configure ONTAP LIFs, sélectionnez le type de configuration préféré, puis effectuez les actions suivantes :

Pour créer ce type de LIF…	Procédez comme suit…
LIF de données	a. Définissez « rôle » sur « données ». b. Définissez « protocole de données » sur « cifs ». c. Définissez la « politique de pare-feu » sur « données ». d. Définissez « stratégie de service » sur « fichiers-données-par-défaut ».
LIF de management	a. Définir « rôle* sur « données » b. Définissez « protocole de données » sur « aucun ». c. Définissez la « politique de pare-feu » sur « gestion ». d. Définissez « stratégie de service » sur « gestion par défaut ».

En savoir plus sur "Création d'une LIF".

Après avoir créé une LIF, entrer la LIF de données ou de gestion ou l'adresse IP du SVM que vous souhaitez ajouter. Vous pouvez également entrer dans la LIF de cluster management. Si vous spécifiez la LIF de cluster management, tous les SVM au sein de ce cluster qui servent SMB peuvent utiliser le serveur Vscan.

> Lorsque l'authentification Kerberos est requise pour les serveurs Vscan, chaque LIF de données du SVM doit avoir un nom DNS unique, et vous devez enregistrer ce nom en tant que nom principal du serveur (SPN) avec Windows Active Directory. Lorsqu'un nom DNS unique n'est pas disponible pour chaque LIF de données ou enregistré en tant que SPN, le serveur Vscan utilise le mécanisme NT LAN Manager pour l'authentification. Si vous ajoutez ou modifiez les noms DNS et les SPN après la connexion du serveur Vscan, vous devez redémarrer le service antivirus Connector sur le serveur Vscan pour appliquer les modifications.

3. Pour configurer une LIF de gestion, entrez la durée d'interrogation en secondes. La durée de l'interrogation est la fréquence à laquelle l'antivirus Connector recherche des modifications des SVM ou de la configuration LIF du cluster. L'intervalle d'interrogation par défaut est de 60 secondes.
4. Entrez le nom et le mot de passe du compte admin ONTAP pour configurer une LIF de gestion.
5. Cliquez sur **Test** pour vérifier la connectivité et l'authentification. L'authentification est uniquement vérifiée pour une configuration LIF de management.
6. Cliquez sur **mettre à jour** pour ajouter la LIF à la liste des LIFs à interroger ou à se connecter.
7. Cliquez sur **Enregistrer** pour enregistrer la connexion au registre.
8. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers un fichier d'importation de registre ou d'exportation de registre. Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Voir la "Configurez la page ONTAP antivirus Connector" pour les options de configuration.

Configurer ONTAP antivirus Connector

Configurer ONTAP antivirus Connector pour spécifier un ou plusieurs SVM (Storage Virtual machines) auxquels vous souhaitez vous connecter en entrant dans la LIF de gestion ONTAP, en interrotant qu'information et les informations d'identification du compte d'administrateur ONTAP, ou simplement dans la LIF de données. Vous pouvez également modifier les détails d'une connexion SVM ou supprimer une connexion SVM. Par défaut, ONTAP antivirus Connector utilise les API REST pour récupérer la liste des LIFs de données si le LIF de management ONTAP est configuré.

Modifier le détail d'une connexion SVM

Vous pouvez mettre à jour les détails d'une connexion SVM (Storage Virtual machine), qui a été ajoutée à l'antivirus Connector, en modifiant la LIF de gestion ONTAP et les informations d'interrogation. Une fois ajoutées, les LIF de données ne peuvent pas être mises à jour. Pour mettre à jour les LIF de données, vous devez d'abord les supprimer, puis les ajouter de nouveau avec la nouvelle LIF ou adresse IP.

Avant de commencer

Vérifiez que vous avez créé un compte d'utilisateur pour l'application HTTP et que vous avez attribué un rôle ayant (au moins en lecture seule) accès au système `/api/network/ip/interfaces` API REST. Pour plus d'informations sur la création d'un utilisateur, reportez-vous à la section "création d'un rôle de connexion de sécurité" et le "création d'une connexion de sécurité" commandes. Vous pouvez également utiliser l'utilisateur du domaine en tant que compte en ajoutant un SVM de tunnel d'authentification pour une SVM d'administration. Pour plus d'informations, reportez-vous à la section "connexion de sécurité domaine-tunnel créer" Page de manuel ONTAP.

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**. La boîte de dialogue Configure ONTAP LIFs s'ouvre.
2. Sélectionner l'adresse IP du SVM, puis cliquer sur **Update**.
3. Mettez à jour les informations, si nécessaire.
4. Cliquez sur **Enregistrer** pour mettre à jour les détails de la connexion dans le registre.
5. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers une importation de registre ou un fichier d'exportation de registre. Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Retirer une connexion SVM du connecteur antivirus

Si vous n'avez plus besoin d'une connexion SVM, vous pouvez la supprimer.

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**. La boîte de dialogue Configure ONTAP LIFs s'ouvre.
2. Sélectionner une ou plusieurs adresses IP de SVM, puis cliquer sur **Supprimer**.

3. Cliquez sur **Enregistrer** pour mettre à jour les détails de la connexion dans le registre.
4. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers un fichier d'importation de registre ou d'exportation de registre. Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Résoudre les problèmes

Avant de commencer

Lorsque vous créez des valeurs de registre dans cette procédure, utilisez le volet droit.

Vous pouvez activer ou désactiver les journaux antivirus Connector à des fins de diagnostic. Par défaut, ces journaux sont désactivés. Pour améliorer les performances, vous devez conserver les journaux du connecteur antivirus désactivés et les activer uniquement pour les événements critiques.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, localisez la sous-clé suivante pour ONTAP antivirus Connector : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Créez des valeurs de registre en fournissant le type, le nom et les valeurs indiqués dans le tableau suivant :

Type	Nom	Valeurs
Chaîne	Chemin de traçabilité	c:\avshim.log

   Cette valeur de registre peut être n'importe quel autre chemin valide.

4. Créez une autre valeur de registre en fournissant le type, le nom, les valeurs et les informations de journalisation indiquées dans le tableau suivant :

Type	Nom	Journalisation critique	Journalisation intermédiaire	Journalisation détaillée
DWORD	TRACELEVEL	1	2 ou 3	4

   Cela active les journaux antivirus Connector qui sont enregistrés à la valeur de chemin fournie dans TracePath à l'étape 3.

5. Désactivez les journaux du connecteur antivirus en supprimant les valeurs de registre que vous avez créées aux étapes 3 et 4.
6. Créez une autre valeur de registre de type "MULTI_SZ" avec le nom "LogRotation" (sans guillemets). Dans « LogRotation », Indiquez « logFileSize:1 » comme entrée pour la taille de rotation (où 1 représente 1 Mo) et dans la ligne suivante, indiquez « logFileCount:5 » comme entrée pour la limite de rotation (5 est la limite).

> Ces valeurs sont facultatives. Si elles ne sont pas fournies, les valeurs par défaut des fichiers 20 Mo et 10 sont utilisées respectivement pour la taille de rotation et la limite de rotation. Les valeurs entières fournies ne fournissent pas de valeurs décimales ou de fraction. Si vous indiquez des valeurs supérieures aux valeurs par défaut, les valeurs par défaut sont utilisées à la place.

7. Pour désactiver la rotation du journal configurée par l'utilisateur, supprimez les valeurs de registre que vous avez créées à l'étape 6.

Bannière personnalisable

Une bannière personnalisée vous permet de placer une déclaration juridiquement contraignante et une clause de non-responsabilité d'accès au système dans la fenêtre *Configure ONTAP LIF API*.

Étape

1. Modifiez la bannière par défaut en mettant à jour le contenu de l' `banner.txt` dans le répertoire d'installation, puis en enregistrant les modifications. Vous devez rouvrir la fenêtre configurer l'API LIF ONTAP pour voir les modifications reflétées dans la bannière.

Activer le mode Eo (Extended Ordinance)

Vous pouvez activer et désactiver le mode Extended Ordinance (EO) pour un fonctionnement sécurisé.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, localisez la sous-clé suivante pour ONTAP antivirus Connector : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Dans le volet de droite, créez une nouvelle valeur de registre de type "DWORD" avec le nom "EO_mode" (sans guillemets) et la valeur "1" (sans guillemets) pour activer le mode EO ou la valeur "0" (sans guillemets) pour désactiver le mode EO.

> Par défaut, si l' `EO_Mode` L'entrée de registre est absente, le mode EO est désactivé. Lorsque vous activez le mode EO, vous devez configurer à la fois le serveur syslog externe et l'authentification mutuelle des certificats.

Configurez le serveur syslog externe

Avant de commencer

Notez que lorsque vous créez des valeurs de registre dans cette procédure, utilisez le volet de droite.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, créez la sous-clé suivante pour ONTAP antivirus Connector pour la configuration syslog : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Créez une valeur de registre en fournissant le type, le nom et la valeur, comme indiqué dans le tableau

suivant :

Type	Nom	Valeur
DWORD	syslog_enabled	1 ou 0

Veuillez noter qu'une valeur « 1 » active le syslog et qu'une valeur « 0 » le désactive.

4. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Hôte_syslog

Indiquez l'adresse IP ou le nom de domaine de l'hôte syslog pour le champ valeur.

5. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Syslog_port

Indiquez le numéro de port sur lequel le serveur syslog s'exécute dans le champ valeur.

6. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Protocole_syslog

Saisissez le protocole utilisé sur le serveur syslog, soit « tcp », soit « udp », dans le champ valeur.

7. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom	JOURNAL_CRIT	LOG_NOTICE	INFO_JOURNAL	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom	Valeur
DWORD	syslog_tls	1 ou 0

Notez qu'une valeur « 1 » active syslog avec TLS (transport Layer Security) et une valeur « 0 » désactive syslog avec TLS.

Assurez-vous qu'un serveur syslog externe configuré fonctionne correctement

- Si la clé est absente ou a une valeur nulle :
  - Le protocole par défaut est « tcp ».
  - Le port par défaut est "514" pour "tcp/udp" et par défaut "6514" pour TLS.
  - Par défaut, le niveau syslog est 5 (LOG_NOTICE).
- Vous pouvez confirmer que syslog est activé en vérifiant que le système `syslog_enabled` la valeur est « 1 ». Lorsque le `syslog_enabled` La valeur est "1", vous devriez pouvoir vous connecter au serveur distant configuré, que le mode EO soit activé ou non.
- Si le mode EO est réglé sur « 1 » et que vous modifiez le `syslog_enabled` valeur comprise entre « 1 » et « 0 », ce qui suit s'applique :
  - Vous ne pouvez pas démarrer le service si syslog n'est pas activé en mode EO.
  - Si le système fonctionne dans un état stable, un avertissement s'affiche indiquant que syslog ne peut pas être désactivé en mode EO et que syslog est fermement défini sur « 1 », que vous pouvez voir dans le registre. Si cela se produit, vous devez d'abord désactiver le mode EO, puis désactiver syslog.
- Si le serveur syslog ne peut pas fonctionner correctement lorsque le mode EO et syslog sont activés, le service s'arrête. Ceci peut se produire pour l'une des raisons suivantes :
  - Un hôte syslog_non valide ou non configuré.
  - Un protocole non valide, hormis UDP ou TCP, est configuré.
  - Un numéro de port n'est pas valide.
- Dans le cas d'une configuration TCP ou TLS sur TCP, si le serveur n'écoute pas le port IP, la connexion échoue et le service s'arrête.

Configurer l'authentification de certificat mutuel X.509

L'authentification mutuelle basée sur certificat X.509 est possible pour la communication SSL (Secure Sockets Layer) entre l'antivirus Connector et ONTAP dans le chemin de gestion. Si le mode EO est activé et que le certificat n'est pas trouvé, le connecteur AV se termine. Effectuez la procédure suivante sur l'antivirus Connector :

Étapes

1. Le connecteur antivirus recherche le certificat client du connecteur antivirus et le certificat de l'autorité de certification du serveur NetApp dans le chemin d'accès au répertoire à partir duquel le connecteur antivirus exécute le répertoire d'installation. Copiez les certificats dans ce chemin de répertoire fixe.
2. Intégrez le certificat client et sa clé privée au format PKCS12 et nommez-le « AV_client.P12 ».
3. Assurez-vous que le certificat de l'autorité de certification (ainsi que toute autorité de signature intermédiaire jusqu'à l'autorité de certification racine) utilisé pour signer le certificat du serveur NetApp est au format PEM (Privacy Enhanced Mail) et nommé ONTAP_CA.pem. Placez-le dans le répertoire d'installation de l'antivirus Connector. Sur le système NetApp ONTAP, installez le certificat de l'autorité de certification (ainsi que toute autorité de signature intermédiaire jusqu'à l'autorité de certification racine) utilisé pour signer le certificat client pour le connecteur antivirus à « ONTAP » en tant que certificat de type « client-ca ».