Configurez un serveur SMB dans un domaine Active Directory

ONTAP 9

NetApp
March 24, 2023

Table des matières

Configurez un serveur SMB dans un domaine Active Directory

Configurer les services de temps

Avant de créer un serveur SMB dans un contrôleur Active Domain, vous devez vous assurer que l'heure du cluster et l'heure sur les contrôleurs de domaine du domaine auquel le serveur SMB appartient correspondent dans les cinq minutes.

Description de la tâche

Vous devez configurer les services NTP du cluster de manière à utiliser les mêmes serveurs NTP pour la synchronisation horaire que le domaine Active Directory.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

Étapes

1. Configurer les services de temps à l'aide du `cluster time-service ntp server create` commande.
   - Pour configurer des services de temps sans authentification symétrique, entrez la commande suivante : `cluster time-service ntp server create -server server_ip_address`
   - Pour configurer des services de temps avec une authentification symétrique, entrez la commande suivante : `cluster time-service ntp server create -server server_ip_address -key-id key_id` `cluster time-service ntp server create -server 10.10.10.1` `cluster time-service ntp server create -server 10.10.10.2`
2. Vérifiez que les services de temps sont correctement configurés à l'aide du `cluster time-service ntp server show` commande.

   `cluster time-service ntp server show`

```
Server                         Version
------------------------------ -------
10.10.10.1                     auto
10.10.10.2                     auto
```

Commandes de gestion de l'authentification symétrique sur les serveurs NTP

Depuis ONTAP 9.5, le protocole NTP (Network Time Protocol) version 3 est pris en charge. NTPv3 inclut une authentification symétrique à l'aide de clés SHA-1 qui augmente la sécurité du réseau.

Pour cela…	Utilisez cette commande…
Configurer un serveur NTP sans authentification symétrique	`cluster time-service ntp server create -server server_name`
Configurez un serveur NTP avec une authentification symétrique	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Activer l'authentification symétrique pour un serveur NTP existant le serveur NTP existant peut être modifié pour activer l'authentification en ajoutant l'ID de clé requis	`cluster time-service ntp server modify -server server_name -key-id key_id`
Configurez une clé NTP partagée	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Les clés partagées sont désignées par un ID. L'ID, son type et la valeur doivent être identiques sur le nœud et le serveur NTP
Configurez un serveur NTP avec un ID de clé inconnu	`cluster time-service ntp server create -server server_name -key-id key_id`
Configurez un serveur dont l'ID de clé n'est pas configuré sur le serveur NTP.	`cluster time-service ntp server create -server server_name -key-id key_id` L'ID, le type et la valeur de clé doivent être identiques à l'ID, au type et à la valeur de clé configurés sur le serveur NTP.
Désactiver l'authentification symétrique	`cluster time-service ntp server modify -server server_name -authentication disabled`

Créez un serveur SMB dans un domaine Active Directory

Vous pouvez utiliser le `vserver cifs create` Commande pour créer un serveur SMB sur le SVM et spécifier le domaine Active Directory (AD) auquel il appartient.

Avant de commencer

Le SVM et les LIF que vous utilisez pour transmettre des données doivent avoir été configurés pour permettre le protocole SMB. Les LIFs doivent pouvoir se connecter aux serveurs DNS configurés sur le SVM et à un contrôleur de domaine AD du domaine auquel vous souhaitez rejoindre le serveur SMB.

Tout utilisateur autorisé à créer des comptes machine dans le domaine AD auquel vous rejoignez le serveur SMB peut créer le serveur SMB sur la SVM. Cela peut inclure des utilisateurs d'autres domaines.

À partir de ONTAP 9.7, votre administrateur AD peut vous fournir un URI vers un fichier keytab comme alternative à vous fournir un nom et un mot de passe à un compte Windows privilégié. Lorsque vous recevez l'URI, l'inclure dans le `-keytab-uri` paramètre avec le `vserver cifs` commandes.

Description de la tâche

Lors de la création d'un serveur SMB dans un domaine d'annuaire d'activités :

- Vous devez utiliser le nom de domaine complet (FQDN) lors de la spécification du domaine.
- Le paramètre par défaut consiste à ajouter le compte de machine du serveur SMB à l'objet CN=Computer Active Directory.
- Vous pouvez choisir d'ajouter le serveur SMB à une autre unité organisationnelle (ou) en utilisant le `-ou` option.
- Vous pouvez choisir d'ajouter une liste délimitée par des virgules d'un ou de plusieurs alias NetBIOS (jusqu'à 200) pour le serveur SMB.

  La configuration des alias NetBIOS d'un serveur SMB peut être utile lorsque vous regroupez des données provenant d'autres serveurs de fichiers vers le serveur SMB et que vous souhaitez que le serveur SMB réponde aux noms des serveurs d'origine.

Le `vserver cifs` les pages man contiennent des paramètres facultatifs supplémentaires et des exigences de dénomination.

Depuis ONTAP 9.1, vous pouvez activer SMB version 2.0 pour vous connecter à un contrôleur de domaine (DC). Cela est nécessaire si vous avez désactivé SMB 1.0 sur les contrôleurs de domaine. Depuis ONTAP 9.2, SMB 2.0 est activé par défaut.

Depuis ONTAP 9.8, vous pouvez spécifier le cryptage des connexions aux contrôleurs de domaine. ONTAP nécessite un cryptage pour les communications du contrôleur de domaine lorsque `-encryption-required -for-dc-connection` l'option est définie sur `true`; la valeur par défaut est `false`. Lorsque l'option est définie, seul le protocole SMB3 est utilisé pour les connexions ONTAP-DC, car le chiffrement n'est pris en charge que par SMB3. .

"Gestion SMB" Contient plus d'informations sur les options de configuration du serveur SMB.

Étapes

1. Vérifiez que SMB est sous licence sur le cluster : `system license show -package cifs`

   Si ce n'est pas le cas, contactez votre représentant commercial.

   Une licence CIFS n'est pas requise si le serveur SMB sera utilisé uniquement pour l'authentification.

2. Créez le serveur SMB dans un domaine AD : `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Lorsque vous entrez dans un domaine, cette commande peut prendre plusieurs minutes.

   La commande suivante crée le serveur SMB "`mb_server01"' dans le domaine ""example.com":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
smb_server01 -domain example.com
```

La commande suivante crée le serveur SMB “smb_server02” dans le domaine "m`ydomain.com`" et authentifie l’administrateur ONTAP avec un fichier keytab:

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. Vérifiez la configuration du serveur SMB à l’aide du `vserver cifs show` commande.

   Dans cet exemple, le résultat de la commande montre qu’un serveur SMB nommé « `SMB_SERVER01' » a été créé sur la SVM vs1.example.com et a été rejoint au domaine « example.com`" domain.

```
cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
```

4. Si vous le souhaitez, activez la communication chiffrée avec le contrôleur de domaine (ONTAP 9.8 et versions ultérieures) : `vserver cifs security modify -vserver svm_name -encryption -required-for-dc-connection true`

Exemples

La commande suivante crée un serveur SMB nommé « `smb_server02' » sur le SVM vs2.example.com dans le domaine « example.com`" domain. Le compte machine est créé dans le conteneur « ou=eng,ou=corp,DC=exemple,DC=com ». Un alias NetBIOS est attribué au serveur SMB.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                          Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

La commande suivante permet à un utilisateur d'un domaine différent, dans ce cas un administrateur d'un domaine de confiance, de créer un serveur SMB nommé « `MB_server03' » sur le SVM vs3.example.com. Le `-domain` Option spécifie le nom du domaine de départ (spécifié dans la configuration DNS) dans lequel vous souhaitez créer le serveur SMB. Le `username` spécifie l'administrateur du domaine de confiance.

- Home domain : example.com
- Domaine de confiance : trust.lab.com
- Nom d'utilisateur du domaine de confiance : Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Créez des fichiers keytab pour l'authentification SMB

Depuis ONTAP 9.7, ONTAP prend en charge l'authentification des SVM avec des serveurs Active Directory (AD) utilisant des fichiers keytab. Les administrateurs AD génèrent un fichier keytab et le rendent disponible aux administrateurs ONTAP sous la forme d'un URI (Uniform Resource identifier), qui est fourni lorsque `vserver cifs` Les commandes exigent une authentification Kerberos avec le domaine AD.

Les administrateurs D'AD peuvent créer les fichiers keytab à l'aide du serveur Windows standard `ktpass` commande. La commande doit être exécutée sur le domaine principal où une authentification est requise. Le `ktpass` la commande peut être utilisée pour générer des fichiers keytab uniquement pour les utilisateurs du domaine principal ; les clés générées à l'aide d'utilisateurs du domaine approuvé ne sont pas prises en charge.

Les fichiers keytab sont générés pour des utilisateurs ONTAP admin spécifiques. Tant que le mot de passe de

l’utilisateur administrateur ne change pas, les clés générées pour le type de cryptage et le domaine spécifiques ne changent pas. Par conséquent, un nouveau fichier keytab est requis chaque fois que le mot de passe de l’utilisateur admin est modifié.

Les types de cryptage suivants sont pris en charge :

- AES256-SHA1
- DES-CBC-MD5

  ONTAP ne prend pas en charge le type de cryptage DES-CBC-CRC.

- RC4-HMAC

AES256 est le type de cryptage le plus élevé et doit être utilisé si activé sur le système ONTAP.

Les fichiers keytab peuvent être générés en spécifiant le mot de passe admin ou en utilisant un mot de passe généré de manière aléatoire. Toutefois, une seule option de mot de passe peut être utilisée à un moment donné, car une clé privée spécifique à l’utilisateur admin est nécessaire au serveur AD pour déchiffrer les clés à l’intérieur du fichier keytab. Toute modification de la clé privée d’un administrateur spécifique invalidera le fichier keytab.