Utilisation de Kerberos avec NFS pour une sécurité renforcée

ONTAP 9

NetApp
September 12, 2024

Sommaire

Utilisation de Kerberos avec NFS pour une sécurité renforcée

Prise en charge de ONTAP pour Kerberos

Kerberos fournit une authentification sécurisée renforcée pour les applications client/Server. L'authentification permet de vérifier les identités des utilisateurs et des processus à un serveur. Dans l'environnement ONTAP, Kerberos assure une authentification entre les SVM (Storage Virtual machine) et les clients NFS.

Dans ONTAP 9, les fonctionnalités Kerberos suivantes sont prises en charge :

- Authentification Kerberos 5 avec contrôle d'intégrité (krb5i)

  Krb5i utilise des checksums pour vérifier l'intégrité de chaque message NFS transféré entre le client et le serveur. Cette fonction est utile pour des raisons de sécurité (par exemple pour s'assurer que les données n'ont pas été falsifiées) et pour des raisons d'intégrité des données (par exemple, pour empêcher la corruption des données lors de l'utilisation de NFS sur des réseaux non fiables).

- Authentification Kerberos 5 avec vérification de la confidentialité (krb5p)

  Krb5p utilise des checksums pour chiffrer l'ensemble du trafic entre le client et le serveur. Ceci est plus sûr et entraîne également plus de charge.

- Chiffrement AES 128 bits et 256 bits

  Advanced Encryption Standard (AES) est un algorithme de cryptage permettant de sécuriser les données électroniques. ONTAP prend en charge AES avec des clés 128 bits (AES-128) et AES avec des clés 256 bits (AES-256) pour Kerberos pour une sécurité renforcée.

- Les configurations de Royaume Kerberos au niveau du SVM

  Les administrateurs des SVM peuvent désormais créer des configurations de domaine Kerberos au niveau du SVM. Les administrateurs des SVM n'ont plus besoin de se reposer sur l'administrateur du cluster pour la configuration des royaumes Kerberos. Ils peuvent donc créer des configurations de Royaume Kerberos individuelles dans un environnement mutualisé.

Conditions requises pour la configuration de Kerberos avec NFS

Avant de configurer Kerberos avec NFS sur votre système, vous devez vérifier que certains éléments de votre réseau et de votre environnement de stockage sont correctement configurés.

> Les étapes de configuration de votre environnement dépendent de la version et du type du système d'exploitation client, du contrôleur de domaine, de Kerberos, DNS, etc. Que vous utilisez. La documentation de toutes ces variables dépasse le cadre de ce document. Pour plus d'informations, reportez-vous à la documentation correspondante pour chaque composant.
>
> Pour obtenir un exemple détaillé de la configuration de ONTAP et de Kerberos 5 avec NFSv3 et NFSv4 dans un environnement utilisant des hôtes Windows Server 2008 R2 Active Directory et Linux, consultez le rapport technique 4073.

Les éléments suivants doivent d'abord être configurés :

Conditions requises pour l'environnement réseau

- Kerberos

  Vous devez avoir une configuration Kerberos fonctionnant avec un centre de distribution de clés (KDC), tel que Windows Active Directory Based Kerberos ou MIT Kerberos.

  Les serveurs NFS doivent utiliser `nfs` en tant que composant principal de leur machine principale.

- Service d'annuaire

  Vous devez utiliser un service d'annuaire sécurisé dans votre environnement, tel qu'Active Directory ou OpenLDAP, configuré pour utiliser LDAP sur SSL/TLS.

- NTP

  Vous devez disposer d'un serveur de temps de travail exécutant NTP. Cette opération est nécessaire pour éviter l'échec de l'authentification Kerberos en raison de l'inclinaison du temps.

- Résolution des noms de domaine (DNS)

  Chaque client UNIX et chaque LIF de SVM doivent avoir un enregistrement de service (SRV) correct enregistré auprès du KDC dans des zones de recherche avant et arrière. Tous les participants doivent être résolus correctement via DNS.

- Comptes d'utilisateur

  Chaque client doit disposer d'un compte utilisateur dans le domaine Kerberos. Les serveurs NFS doivent utiliser « nfs » comme composant principal de leur machine principale.

Exigences du client NFS

- NFS

  Chaque client doit être correctement configuré pour communiquer sur le réseau en utilisant NFSv3 ou NFSv4.

  Les clients doivent prendre en charge les RFC1964 et RFC2203.

- Kerberos

  Chaque client doit être correctement configuré pour utiliser l'authentification Kerberos, avec les informations suivantes :

    - Le chiffrement pour les communications TGS est activé.

      AES-256 pour une sécurité optimale.

    - Le type de cryptage le plus sécurisé pour les communications TGT est activé.
    - Le domaine et le domaine Kerberos sont configurés correctement.
    - GSS est activé.

      Lors de l'utilisation des informations d'identification de la machine

    - Ne pas exécuter `gssd` avec le `-n` paramètre.
    - Ne pas exécuter `kinit` en tant qu'utilisateur root.
- Chaque client doit utiliser la version la plus récente et la plus récente du système d'exploitation.

  Cela offre la meilleure compatibilité et fiabilité pour le chiffrement AES avec Kerberos.

- DNS

  Chaque client doit être correctement configuré pour utiliser DNS pour la résolution correcte du nom.

- NTP

  Chaque client doit être en cours de synchronisation avec le serveur NTP.

- Informations sur l'hôte et le domaine

  Chaque client `/etc/hosts` et `/etc/resolv.conf` Les fichiers doivent contenir le nom d'hôte et les informations DNS correctes, respectivement.

- Fichiers keytab

  Chaque client doit avoir un fichier keytab du KDC. Le Royaume doit être en majuscules. Le type de chiffrement doit être AES-256 pour une sécurité optimale.

- Facultatif : pour des performances optimales, les clients bénéficient d'au moins deux interfaces réseau : l'une pour communiquer avec le réseau local et l'autre pour communiquer avec le réseau de stockage.

Configuration requise pour le système de stockage

- Licence NFS

  Une licence NFS valide doit être installée sur le système de stockage.

- Licence CIFS

  La licence CIFS est facultative. Il n'est nécessaire de vérifier les informations d'identification Windows que lors de l'utilisation du mappage de noms multiprotocole. Elle n'est pas requise dans un environnement UNIX strict.

- SVM

  Au moins un SVM doit être configuré sur le système.

- DNS sur le SVM

  On doit avoir configuré DNS sur chaque SVM.

- Serveur NFS

  Vous devez avoir configuré NFS sur le SVM.

- Cryptage AES

  Pour une sécurité optimale, vous devez configurer le serveur NFS de sorte qu'il n'autorise que le chiffrement AES-256 pour Kerberos.

- Serveur SMB

  Si vous exécutez un environnement multiprotocole, vous devez avoir configuré SMB sur le SVM. Le serveur SMB est requis pour le mappage de noms multiprotocole.

- Volumes

  On doit disposer d'un volume root et d'au moins un volume de données configuré pour une utilisation par la SVM.

- Volume racine

  Le volume root du SVM doit avoir la configuration suivante :

Nom	Réglage
Style de sécurité	UNIX
UID	Racine ou ID 0
GIDS	Racine ou ID 0
Autorisations UNIX	776

  Contrairement au volume racine, les volumes de données peuvent avoir n'importe quel style de sécurité.

- Groupes UNIX

  La SVM doit avoir les groupes UNIX suivants configurés :

Nom du groupe	ID de groupe
démon	1
racine	0
pcuser	65534 (créé automatiquement par ONTAP lors de la création du SVM)

- Utilisateurs UNIX

  Le SVM doit avoir les utilisateurs UNIX suivants configurés :

Nom d'utilisateur	ID d'utilisateur	ID de groupe principal	Commentaire
nfs	500	0	Requis pour la phase INITIALE GSS Le premier composant de l'utilisateur client NFS SPN est utilisé comme utilisateur.
pcuser	65534	65534	Obligatoire pour une utilisation multiprotocole NFS et CIFS Créé et ajouté au groupe pcuser automatiquement par ONTAP lors de la création de la SVM.
racine	0	0	Nécessaire pour le montage

  L'utilisateur nfs n'est pas requis si un mappage de nom Kerberos-UNIX existe pour le SPN de l'utilisateur client NFS.

- Export-policies et rules

  Vous devez avoir configuré des export policy avec les règles d'exportation nécessaires pour les volumes root et de données et les qtrees. Si tous les volumes du SVM sont accessibles via Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5` , `krb5i`, ou `krb5p`.

- Mapping de noms Kerberos-UNIX

  Si vous souhaitez que l'utilisateur identifié par l'utilisateur client NFS SPN dispose d'autorisations root, vous devez créer un mappage de nom à la racine.

Informations associées

"Rapport technique NetApp 4073 : authentification unifiée sécurisée"

"Matrice d'interopérabilité NetApp"

"Administration du système"

"Gestion du stockage logique"

Spécifiez le domaine ID utilisateur pour NFSv4

Pour spécifier le domaine d'ID utilisateur, vous pouvez définir le `-v4-id-domain` option.

Description de la tâche

Par défaut, ONTAP utilise le domaine NIS pour le mappage d'ID utilisateur NFSv4, si un est défini. Si aucun domaine NIS n'est défini, le domaine DNS est utilisé. Vous devrez peut-être définir le domaine d'ID utilisateur si, par exemple, vous disposez de plusieurs domaines d'ID utilisateur. Le nom de domaine doit correspondre à la configuration de domaine sur le contrôleur de domaine. Elle n'est pas requise pour NFSv3.

Étape

1. Saisissez la commande suivante :

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```