Utilisez Kerberos avec NFS pour une sécurité renforcée

ONTAP 9

NetApp
April 24, 2024

Sommaire

Utilisez Kerberos avec NFS pour une sécurité renforcée

Présentation de l'utilisation de Kerberos avec NFS pour une sécurité renforcée

Si Kerberos est utilisé dans votre environnement pour une authentification renforcée, vous devez travailler avec votre administrateur Kerberos pour déterminer les exigences et les configurations de système de stockage appropriées, puis activer la SVM en tant que client Kerberos.

Votre environnement doit respecter les consignes suivantes :

- Votre déploiement de site doit respecter les bonnes pratiques en matière de configuration du serveur Kerberos et du client avant de configurer Kerberos pour ONTAP.
- Si possible, utilisez NFSv4 ou une version ultérieure si l'authentification Kerberos est requise.

  NFSv3 peut être utilisé avec Kerberos. Toutefois, les avantages de la sécurité totale de Kerberos ne sont réalisés que dans les déploiements ONTAP de NFSv4 ou versions ultérieures.

- Pour promouvoir un accès serveur redondant, Kerberos doit être activé sur plusieurs LIFs de données sur plusieurs nœuds du cluster à l'aide du même SPN.
- Lorsque Kerberos est activé sur le SVM, l'une des méthodes de sécurité suivantes doit être spécifiée dans des règles d'exportation pour les volumes ou les qtrees, en fonction de votre configuration client NFS.
  - `krb5` (Protocole Kerberos v5)
  - `krb5i` (Protocole Kerberos v5 avec contrôle d'intégrité à l'aide de checksums)
  - `krb5p` (Protocole Kerberos v5 avec service de confidentialité)

En plus du serveur Kerberos et des clients, les services externes suivants doivent être configurés pour ONTAP afin de prendre en charge Kerberos :

- 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. N'utilisez pas NIS, dont les demandes sont envoyées en clair et ne sont donc pas sécurisées.

- 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.

Vérifiez les autorisations pour la configuration Kerberos

Kerberos requiert que certaines autorisations UNIX soient définies pour le volume root du SVM et pour les utilisateurs et groupes locaux.

Étapes

1. Afficher les autorisations appropriées sur le volume root du SVM :

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

   Le volume root du SVM doit avoir la configuration suivante :

Nom…	Paramètre…
UID	Racine ou ID 0
GIDS	Racine ou ID 0
Autorisations UNIX	755

   Si ces valeurs ne sont pas affichées, utiliser le `volume modify` pour les mettre à jour.

2. Afficher les utilisateurs UNIX locaux :

   `vserver services name-service unix-user show -vserver` *`vserver_name`*

   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 INIT GSS. Le premier composant de l'utilisateur client NFS SPN est utilisé comme utilisateur. L'utilisateur nfs n'est pas requis si un mappage de nom Kerberos-UNIX existe pour le SPN de l'utilisateur client NFS.
racine	0	0	Nécessaire pour le montage.

   Si ces valeurs ne sont pas affichées, vous pouvez utiliser le `vserver services name-service unix-user modify` pour les mettre à jour.

3. Afficher les groupes UNIX locaux :

   `vserver services name-service unix-group show -vserver vserver _name`

   La SVM doit avoir les groupes UNIX suivants configurés :

Nom du groupe	ID de groupe
démon	1
racine	0

   Si ces valeurs ne sont pas affichées, vous pouvez utiliser le `vserver services name-service unix-group modify` pour les mettre à jour.

Créez une configuration de domaine NFS Kerberos

Si vous souhaitez que le ONTAP accède à des serveurs Kerberos externes dans votre environnement, vous devez d'abord configurer le SVM de manière à utiliser un Royaume Kerberos existant. Pour ce faire, vous devez rassembler les valeurs de configuration du serveur KDC Kerberos, puis utiliser l' `vserver nfs kerberos realm create` Commande pour créer la configuration du domaine Kerberos sur un SVM.

Ce dont vous avez besoin

L'administrateur du cluster doit avoir configuré le protocole NTP sur le système de stockage, le client et le serveur KDC afin d'éviter les problèmes d'authentification. Les différences de temps entre un client et un serveur (inclinaison de l'horloge) sont une cause courante d'échecs d'authentification.

Étapes

1. Consultez votre administrateur Kerberos pour déterminer les valeurs de configuration appropriées à fournir avec le `vserver nfs kerberos realm create` commande.
2. Créer une configuration de domaine Kerberos sur le SVM :

   `vserver nfs kerberos realm create -vserver vserver_name -realm realm_name {AD_KDC_server_values |AD_KDC_server_values} -comment "text"`

3. Vérifiez que la configuration du domaine Kerberos a bien été créée :

   `vserver nfs kerberos realm show`

Exemples

La commande suivante crée une configuration de domaine NFS Kerberos pour le SVM vs1 qui utilise un serveur Microsoft Active Directory comme serveur KDC. Le domaine Kerberos est AUTH.EXAMPLE.COM. Le serveur Active Directory est nommé ad-1 et son adresse IP est 10.10.8.14. L'inclinaison de l'horloge autorisée est de 300 secondes (par défaut). L'adresse IP du serveur KDC est 10.10.8.14 et son numéro de port est 88 (par défaut). « Microsoft Kerberos config » est le commentaire.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

La commande suivante crée une configuration de Royaume NFS Kerberos pour le SVM vs1 qui utilise un MIT KDC. Le domaine Kerberos est SECURITY.EXAMPLE.COM. L'inclinaison de l'horloge autorisée est de 300 secondes. L'adresse IP du serveur KDC est 10.10.9.1 et son numéro de port est 88. Le fournisseur de KDC est autre que d'indiquer un fournisseur UNIX. L'adresse IP du serveur d'administration est 10.10.9.1 et son numéro de port est 749 (par défaut). L'adresse IP du serveur de mots de passe est 10.10.9.1 et son numéro de port est 464 (par défaut). « UNIX Kerberos config » est le commentaire.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurez les types de chiffrement Kerberos NFS autorisés

Par défaut, ONTAP prend en charge les types de cryptage suivants pour Kerberos NFS : DES, 3DES, AES-128 et AES-256. Vous pouvez configurer les types de cryptage autorisés pour chaque SVM en fonction des exigences de sécurité de votre environnement en utilisant le `vserver nfs modify` commande avec `-permitted -enc-types` paramètre.

Description de la tâche

Pour une compatibilité client optimale, ONTAP prend en charge à la fois le chiffrement DES faible et le chiffrement AES fort par défaut. Cela signifie, par exemple, que si vous voulez augmenter la sécurité et que votre environnement le prend en charge, vous pouvez utiliser cette procédure pour désactiver DES et 3DES et demander aux clients d'utiliser uniquement le cryptage AES.

Vous devez utiliser le chiffrement le plus fort disponible. Pour ONTAP, c'est AES-256. Vous devez confirmer auprès de votre administrateur KDC que ce niveau de cryptage est pris en charge dans votre environnement.

- L'activation ou la désactivation totale d'AES (AES-128 et AES-256) sur les SVM provoque des perturbations, car elle détruit le fichier principal/keytab d'origine, ce qui requiert la désactivation de la configuration Kerberos sur toutes les LIFs du SVM.

  Avant d'effectuer ces modifications, vérifiez que les clients NFS ne reposent pas sur le chiffrement AES du SVM.

- L'activation ou la désactivation DES ou 3DES ne nécessite aucune modification de la configuration Kerberos sur les LIF.

Étape

1. Activez ou désactivez le type de cryptage autorisé que vous souhaitez :

Pour activer ou désactiver…	Suivez ces étapes…
DES ou 3DES	a. Configurer les types de cryptage NFS Kerberos autorisés du SVM : `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Séparez les différents types de cryptage par une virgule. b. Vérifiez que la modification a réussi : `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`
AES-128 ou AES-256	a. Identifier sur quel SVM et LIF Kerberos sont activés : `vserver nfs kerberos interface show` b. Désactiver Kerberos sur toutes les LIFs sur le SVM dont NFS Kerberos autorisé type de cryptage que vous souhaitez modifier : `vserver nfs kerberos interface disable -lif` *`lif_name`* c. Configurer les types de cryptage NFS Kerberos autorisés du SVM : `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Séparez les différents types de cryptage par une virgule. d. Vérifiez que la modification a réussi : `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types` e. Réactiver Kerberos sur toutes les LIFs sur le SVM : `vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`* f. Vérifier que Kerberos est activé sur toutes les LIFs : `vserver nfs kerberos interface show`

Activez Kerberos sur une LIF donnée

Vous pouvez utiliser le `vserver nfs kerberos interface enable` Commande pour activer Kerberos sur une LIF de données. Cela permet au SVM d'utiliser les services de sécurité Kerberos pour NFS.

Description de la tâche

Si vous utilisez un KDC Active Directory, les 15 premiers caractères de tous les noms de domaine utilisés doivent être uniques sur les SVM au sein d'un domaine ou d'un domaine.

Étapes

1. Créez la configuration NFS Kerberos :

   ```
   vserver nfs kerberos interface enable -vserver vserver_name -lif
   logical_interface -spn service_principal_name
   ```

   ONTAP nécessite la clé secrète pour le SPN à partir du KDC pour activer l'interface Kerberos.

   Pour les VDC Microsoft, le KDC est contacté et un nom d'utilisateur et un mot de passe sont émis sur l'CLI pour obtenir la clé secrète. Si vous devez créer le SPN dans une autre UO du domaine Kerberos, vous pouvez spécifier l'option `-ou` paramètre.

   Pour les KDC non Microsoft, la clé secrète peut être obtenue en utilisant l'une des deux méthodes suivantes :

Si…	Vous devez également inclure le paramètre suivant avec la commande…
Demandez à l'administrateur KDC de récupérer la clé directement à partir du KDC	`-admin-username` *kdc_admin_username*
Ne disposez pas des informations d'identification de l'administrateur KDC mais d'un fichier keytab du KDC contenant la clé	`-keytab-uri` {ftp

2. Vérifier que Kerberos a été activé sur la LIF :

   ```
   vserver nfs kerberos-config show
   ```

3. Répétez les étapes 1 et 2 pour activer Kerberos sur plusieurs LIFs.

Exemple

La commande suivante crée et vérifie une configuration Kerberos NFS pour le SVM nommé vs1 sur l'interface logique ves03-d1, avec le SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM dans l'UO lab2ou :

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- -------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```