Échec des authentifications AD ISE 1.3 avec l'erreur « Privilège insuffisant pour récupérer les groupes de jetons »

Contenu

Introduction

Ce document décrit la solution à l'échec d'authentification ISE (Identity Services Engine) contre Active Directory (AD) en raison du code d'erreur 24371 dû à des privilèges de compte d'ordinateur ISE insuffisants.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration et dépannage d'ISE
- Microsoft AD

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ISE version 1.3.0.876
- Microsoft AD version 2008 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Échec des authentifications AD en raison de l'erreur « 24371 »

Dans ISE 1.3 et versions ultérieures, les authentifications peuvent échouer par rapport à la

distance administrative avec l'erreur « 24371 ». Le rapport d'authentification détaillé pour la défaillance comporte des étapes similaires à celles indiquées ici :

```
15036     Evaluating Authorization Policy
24432     Looking up user in Active Directory - CISCO_LAB
24371     The ISE machine account does not have the required privileges to fetch groups. -
ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS
24371     The ISE machine account does not have the required privileges to fetch groups. -
CISCO_LAB 15048     Queried PIP - CISCO_LAB.ExternalGroups
```

L'état AD indique les groupes AD joints et connectés et les groupes AD requis ont été ajoutés correctement dans la configuration ISE.

Solution

Modifier les autorisations pour le compte d'ordinateur ISE sur AD

L'erreur dans le rapport d'authentification détaillé implique que le compte d'ordinateur d'ISE sur l'annuaire actif ne dispose pas des privilèges suffisants pour récupérer les groupes de jetons.

> **Note**: Le correctif est effectué côté AD car il n'est pas en mesure de donner le privilège correct au compte d'ordinateur ISE. Vous devrez peut-être déconnecter/reconnecter ISE à AD après cela.

Les privilèges actuels du compte d'ordinateur peuvent être vérifiés à l'aide de la commande **dsacls**, comme indiqué dans cet exemple :

```
Open a command prompt on your AD with administrator privilege.
The dsquery command can be used to find the Fully Qualified Domain Name (FQDN) of the ISE.
C:\Users\admin> dsquery computer -name lab-ise1  //here lab-ise1 is the hostname of the ISE
"CN=lab-ise1,CN=Computers,DC=ciscolab,DC=local"

The dsacls command can now be used to find the privileges assigned to the machine account
C:\Windows\system32> dsacls "CN=lab-ise1,CN=Computers,DC=ciscolab,DC=local" >>
C:\dsacl_output.txt
```

La sortie est longue et donc redirigée vers un fichier texte **dsacl_output.txt** qui peut ensuite être ouvert et affiché correctement dans un éditeur de texte, tel que le bloc-notes.

Si le compte a les autorisations pour lire des groupes de jetons, il aura ces entrées dans le fichier **dsacl_output.txt** :

```
Inherited to user
Allow NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
                                    SPECIAL ACCESS for tokenGroups   <Inherited from parent>
                                    READ PROPERTY Inherited to group
Allow NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
                                    SPECIAL ACCESS for tokenGroups   <Inherited from parent>
                                    READ PROPERTY
```

Si les autorisations ne sont pas présentes, vous pouvez les ajouter à l'aide de la commande suivante :

```
C:\Windows\system32>dsacls "CN=Computers,DC=ciscolab,DC=local" /I:T /G "lab-ise1$":rp;tokenGroups
```

Si le nom de domaine complet ou le groupe exact n'est pas connu, cette commande peut être exécutée rapidement pour le domaine ou l'unité d'organisation (OU) selon les commandes suivantes :

```
C:\Windows\system32>dsacls "DC=ciscolab,DC=local" /I:T /G "lab-ise1$":rp;tokenGroups
C:\Windows\system32>dsacls "OU=ExampleOU,DC=ciscolab,DC=local" /I:T /G "lab-ise1$":rp;tokenGroups
```

Les commandes recherchent l'hôte lab-ise1 dans l'ensemble du domaine ou de l'unité d'organisation respectivement.

N'oubliez pas de remplacer les détails du nom de groupe et d'hôte dans les commandes par le nom de groupe et ISE correspondants de votre déploiement. Cette commande accorde au compte d'ordinateur ISE le privilège de lire les groupes de jetons. Il doit être exécuté sur un seul contrôleur de domaine et doit être répliqué automatiquement vers d'autres contrôleurs.

Le problème peut être résolu immédiatement. Exécutez la commande sur le contrôleur de domaine actuellement connecté à ISE.

Afin d'afficher le contrôleur de domaine actuel, accédez à **Administration > Identity Management > External Identity Sources > Active Directory > Select AD join point**.

Informations connexes

- Des informations sur les autres autorisations de compte sont disponibles dans Active Directory Integration avec Cisco ISE 1.3
- Microsoft Technet Link
- **Support et documentation techniques - Cisco Systems**