Échouer d'authentifications d'AD ISE 1.3 avec « privilège insuffisant l'erreur de chercher groupes symboliques »

Contenu

Introduction

Ce document décrit la solution à la panne d'authentifications du Cisco Identity Services Engine (ISE) contre le Répertoire actif (AD) dû à code d'erreur "24371" provoqué par des privilèges insuffisants de compte d'ordinateur ISE.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configurez et dépannez ISE
- AD de Microsoft

Composants utilisés

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

- Version 1.3.0.876 ISE
- Version 2008 R2 d'AD de Microsoft

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Échouer d'authentifications d'AD dû à l'erreur "24371"

Dans ISE 1.3 et en haut, les authentifications peuvent échouer contre l'AD avec l'erreur "24371". L'état détaillé d'authentification pour la panne a des étapes semblables à ceux affichées 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 d'AD affiche que joint et connecté et les groupes priés d'AD ont été ajoutés correctement dans la configuration ISE.

Solution

Modifiez les autorisations pour le compte d'ordinateur ISE sur l'AD

L'erreur dans l'état détaillé d'authentification implique que le compte d'ordinateur d'ISE sur le répertoire actif, n'a pas des privilèges suffisants de chercher les groupes symboliques.

> **Note**: La difficulté est faite du côté d'AD car il ne peut pas donner le privilège correct au compte d'ordinateur ISE. Vous pourriez devoir déconnecter/rebranchez ISE à l'AD après ceci.

Les privilèges en cours du compte d'ordinateur peuvent être vérifiés avec les **dsacls** commandent suivant les indications de 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 réorientée dans un fichier texte **dsacl_output.txt** qui peut alors être ouvert et visualisé correctement dans un éditeur de texte, tel que le Notepad.

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


```
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
```

Si les autorisations ne sont pas présentes, alors il peut ajouter avec cette commande :

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

Si le FQDN ou le groupe précis n'est pas connu, cette commande peut être rapidement exécutée pour le domaine ou l'unité organisationnelle (OU) selon ces commandes :

```
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 au domaine ou à l'OU entier respectivement.

Souvenez-vous pour remplacer le groupe et les petits groupes de nom d'hôte dans les commandes par le groupe correspondant et le nom ISE de votre déploiement. Cette commande accorde au compte d'ordinateur ISE le privilège de lire les groupes symboliques. Il doit être exécuté sur un contrôleur de domaine seulement et doit répliquer vers d'autres contrôleurs automatiquement.

La question peut être résolue immédiatement. Exécutez la commande sur le contrôleur de domaine actuellement connecté sur ISE.

Afin de visualiser le contrôleur de domaine en cours, naviguez vers la **gestion > la Gestion de l'identité > les sources extérieures > le Répertoire actif d'identité > AD choisi joignent le point**.

Informations connexes

- Les informations concernant d'autres autorisations de compte peuvent être trouvées dans l'intégration de Répertoire actif avec Cisco ISE 1.3
- Lien de Microsoft Technet
- **Support et documentation techniques - Cisco Systems**