ISE 1.3 AD-Authentifizierungen fehlschlagen mit dem Fehler "Ungenügende Berechtigung zum Abrufen von Token-Gruppen"

Inhalt

Einführung

Dieses Dokument beschreibt die Lösung für ISE-Authentifizierungsfehler (Identity Services Engine) gegenüber Active Directory (AD) aufgrund des Fehlercodes "24371", der durch unzureichende ISE-Maschinenkontoberechtigungen verursacht wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- Konfiguration und Fehlerbehebung für die ISE
- Microsoft AD

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ISE Version 1.3.0.876
- Microsoft AD Version 2008 R2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

AD-Authentifizierungen sind aufgrund des Fehlers "24371" fehlgeschlagen

In ISE 1.3 und höher können Authentifizierungen mit dem AD-Fehler "24371" fehlschlagen. Der detaillierte Authentifizierungsbericht für den Fehler umfasst ähnliche Schritte wie die hier gezeigten:

```
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
```

Der AD-Status zeigt die Verbindung und Verbindung an, und die erforderlichen AD-Gruppen wurden der ISE-Konfiguration korrekt hinzugefügt.

Lösung

Ändern Sie die Berechtigungen für das ISE-Maschinenkonto auf AD

Der Fehler im detaillierten Authentifizierungsbericht impliziert, dass das Computerkonto der ISE im aktiven Verzeichnis nicht über ausreichende Berechtigungen zum Abrufen von Tokengruppen verfügt.

> **Hinweis**: Das Problem wird auf der AD-Seite behoben, da es nicht in der Lage ist, dem ISE-Computerkonto die richtigen Berechtigungen zuzuweisen. Danach müssen Sie möglicherweise die ISE mit AD trennen/erneut verbinden.

Die aktuellen Berechtigungen des Computerkontos können mit dem Befehl **dsacls** überprüft werden, wie in diesem Beispiel gezeigt:

```
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
```

Die Ausgabe ist lang und wird daher in eine Textdatei **dsacl_output.txt** umgeleitet, die dann in einem Texteditor wie z.B. Notepad geöffnet und angezeigt werden kann.

Wenn das Konto über die Berechtigung zum Lesen von Tokengruppen verfügt, enthält es diese Einträge in der Datei **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
```

Wenn die Berechtigungen nicht vorhanden sind, können Sie sie mit dem folgenden Befehl hinzufügen:

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

Wenn der FQDN oder die genaue Gruppe nicht bekannt ist, kann dieser Befehl gemäß den folgenden Befehlen schnell für die Domäne oder Organisationseinheit (OU) ausgeführt werden:

```
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
```

Die Befehle suchen in der gesamten Domäne nach dem Host-Lab-ise1 bzw. nach der Einheit.

Denken Sie daran, die Angaben zu Gruppe und Hostname in den Befehlen durch die entsprechende Gruppe und den ISE-Namen aus Ihrer Bereitstellung zu ersetzen. Dieser Befehl gewährt dem ISE-Computerkonto die Berechtigung, die Tokengruppen zu lesen. Er muss nur auf einem Domänencontroller ausgeführt werden und muss automatisch auf andere Controller repliziert werden.

Das Problem kann sofort behoben werden. Führen Sie den Befehl auf dem Domänen-Controller aus, der derzeit mit der ISE verbunden ist.

Um den aktuellen Domänen-Controller anzuzeigen, navigieren Sie zu **Administration > Identity Management > External Identity Sources > Active Directory > Select AD join point**.

Zugehörige Informationen

- Informationen zu anderen Kontoberechtigungen finden Sie in Active Directory Integration in Cisco ISE 1.3.
- Microsoft TechNet-Link
- **Technischer Support und Dokumentation - Cisco Systems**