ISE 1.3 AD-verificaties ontbreken met "Onvoldoende voorrecht om Token Group te selecteren"-fout

Inhoud

Inleiding

Dit document beschrijft de oplossing voor authenticaties van Identity Services Engine (ISE) aan de hand van een fout in Active Directory (AD) vanwege foutcode "24371" veroorzaakt door ontoereikende ISE-rekenrechten.

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- ISE configureren en oplossen van problemen
- Microsoft AD

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ISE versie 1.3.0.876
- Microsoft AD versie 2008 R2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

AD-verificaties mislukt als gevolg van fout "24371"

In ISE 1.3 en hoger kunnen authenticaties falen tegen de AD met fout "24371". Het gedetailleerde

verificatierapport voor de mislukking bevat stappen die vergelijkbaar zijn met die welke hier worden getoond:

```
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
```

De AD status toont aangesloten en aangesloten en de vereiste AD groepen zijn correct toegevoegd in de ISE configuratie.

Oplossing

Wachtwoord voor ISE-machineverslag op AD wijzigen

De fout in het gedetailleerde authenticatierapport impliceert dat de machine account van ISE in de actieve folder niet voldoende privileges heeft om pro memorie groepen te halen.

> Opmerking: Het probleem wordt opgelost aan de AD-zijde omdat het niet mogelijk is het juiste voorrecht te geven aan de ISE-machineaccount. Mogelijk moet u ISE na deze beëindiging weer verbinden met AD.

De huidige privileges van de machineaccount kunnen worden gecontroleerd met de **dsacls-**opdracht zoals in dit voorbeeld:

```
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
```

De uitvoer is lang en daarom wordt **dsacl_output.txt** opnieuw **gericht** in een tekstbestand dat dan goed kan worden geopend en bekeken in een teksteditor, zoals het notebookpad.

Als de account rechten heeft om symbolische groepen te lezen, dan heeft hij deze waarden in het **dsacl_output.txt** bestand:

```
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
```

Als de permissies niet aanwezig zijn, dan kan deze met deze opdracht worden toegevoegd:

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

Als de FQDN of de exacte groep niet bekend is, kan deze opdracht snel voor het domein of de Organisatorische Eenheid (OU) worden uitgevoerd zoals in deze opdrachten:

```
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
```

De opdrachten zoeken naar het lab-ise1 van de host in het gehele domein of in OU respectievelijk.

Vergeet niet de groep- en hostnaamdetails in de opdrachten te vervangen door de corresponderende groep en ISE-naam in uw installatie. Deze opdracht verleent de ISE machine account het voorrecht om de symbolische groepen te lezen. Het moet alleen op één domeincontroller worden uitgevoerd en automatisch op andere controllers worden herhaald.

De kwestie kan onmiddellijk worden opgelost. Start de opdracht op de domeincontroller die momenteel op ISE is aangesloten.

Om het huidige domein controller te bekijken, navigeer dan naar **Beheer > Identity Management > Externe identiteitsbronnen > Active Directory > Select en Joden Point**.

Gerelateerde informatie

- Informatie over andere accountrechten kan in Active Directory Integration met Cisco ISE 1.3 worden gevonden
- Microsoft technische link
- **Technische ondersteuning en documentatie – Cisco Systems**