Autenticazioni ISE 1.3 AD non riuscite con errore "Privilegio insufficiente per recuperare i gruppi di token"

Sommario

Introduzione

In questo documento viene descritto il problema di autenticazione di Identity Services Engine (ISE) in Active Directory (AD) a causa del codice di errore "24371" causato da privilegi di account del computer ISE insufficienti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Configurazione e risoluzione dei problemi di ISE
- Microsoft AD

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ISE versione 1.3.0.876
- Microsoft AD versione 2008 R2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Autenticazioni AD non riuscite a causa dell'errore "24371"

Ad ISE 1.3 e versioni successive, le autenticazioni possono non essere eseguite sull'AD con l'errore "24371". Il report di autenticazione dettagliato per l'errore prevede procedure simili a quelle illustrate di seguito:

```
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
```

Lo stato di Active Directory indica che l'utente è connesso e connesso e i gruppi AD richiesti sono stati aggiunti correttamente nella configurazione ISE.

Soluzione

Modifica autorizzazioni per l'account computer ISE in AD

L'errore nel report di autenticazione dettagliato implica che l'account computer di ISE in Active Directory non dispone di privilegi sufficienti per recuperare i gruppi di token.

> **Nota:** La correzione viene eseguita sul lato AD perché non è in grado di assegnare il privilegio corretto all'account del computer ISE. In seguito potrebbe essere necessario disconnettere/riconnettere ISE ad AD.

I privilegi correnti dell'account computer possono essere controllati con il comando **dsacls**, come mostrato nell'esempio:

```
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
```

L'output è lungo e pertanto viene reindirizzato in un file di testo **dsacl_output.txt** che può essere aperto e visualizzato correttamente in un editor di testo, ad esempio il Blocco note.

Se l'account dispone delle autorizzazioni di lettura per i gruppi di token, avrà le seguenti voci nel file **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
```

Se le autorizzazioni non sono presenti, è possibile aggiungerle con questo comando:

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

Se il nome di dominio completo (FQDN) o il gruppo esatto non è noto, è possibile eseguire rapidamente questo comando per il dominio o l'unità organizzativa (OU), come indicato di seguito:

```
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
```

I comandi cercano l'host lab-ise1 rispettivamente nell'intero dominio o nell'intera unità organizzativa.

Ricordarsi di sostituire i dettagli dei nomi host e di gruppo nei comandi con il nome ISE e il gruppo corrispondente della distribuzione. Questo comando concede all'account ISE machine il privilegio di leggere i gruppi di token. Deve essere eseguito solo su un controller di dominio e deve essere replicato automaticamente su altri controller.

Il problema può essere risolto immediatamente. Eseguire il comando sul controller di dominio attualmente connesso ad ISE.

Per visualizzare il controller di dominio corrente, selezionare **Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory > Seleziona punto di join AD**.

Informazioni correlate

- Per informazioni sulle autorizzazioni di altri account, vedere Integrazione di Active Directory con Cisco ISE 1.3.
- Microsoft Technet Link
- Documentazione e supporto tecnico – Cisco Systems