ISE en twee manieren om vertrouwen te stellen in AD configuratie

Inhoud

Inleiding

Dit document beschrijft de definitie van ‘tweerichtingsvertrouwen' op ISE, en een eenvoudig configuratievoorbeeld: hoe een gebruiker die niet aanwezig is in de AD, maar aanwezig is in een andere AD, te authentiseren.

Voorwaarden

Vereisten

Cisco beveelt aan dat u basiskennis hebt van:

- ISE 2.x en Active Directory-integratie .
- Externe identiteitscontrole op ISE.

Gebruikte componenten

- ISE 2.x.
- twee actieve directoraten.

Configureren

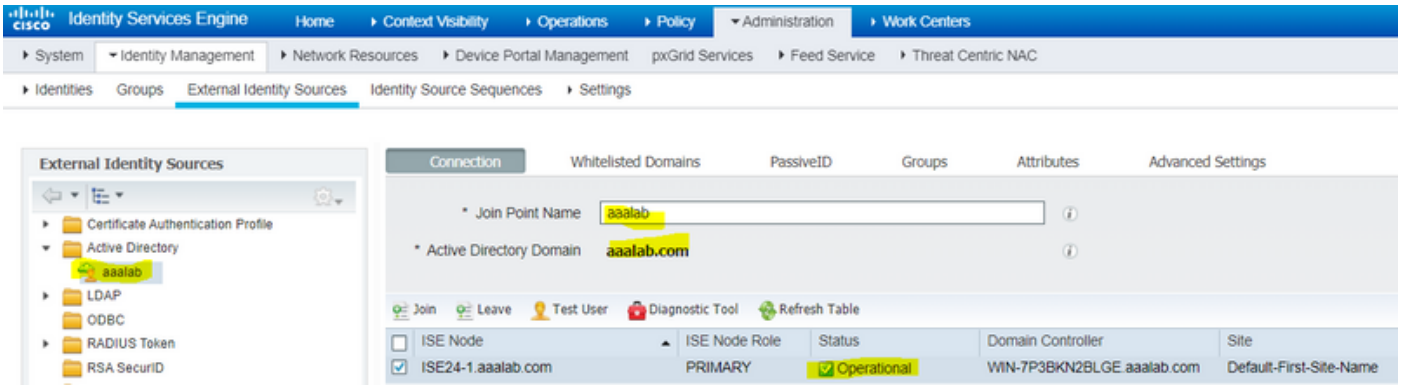
Om uw domein uit te breiden, en andere gebruikers in een ander domein op te nemen dan het gebied dat reeds aan ISE is aangesloten, hebt u twee manieren om dit te bereiken:

1. U kunt het domein handmatig en afzonderlijk op ISE toevoegen. Hierdoor hebt u twee afzonderlijke actieve directoraten.
2. Doe mee aan één AD met ISE en stel **wederzijdse vertrouwen** in tussen deze AD en de tweede AD zonder deze toe te voegen aan ISE. Dit is voornamelijk een tweerichtingsconfiguratie, het is een optie die tussen twee of meer actieve directoraten is

ingesteld. ISE zal deze vertrouwde domeinen automatisch detecteren via de AD-connector en ze toevoegen aan de 'gefloten domeinen' en ze behandelen als afzonderlijke AD's die zijn aangesloten bij ISE. Zo kan je een gebruiker authenticeren in de AD "zatar.jo", die geen lid is van ISE.

In de volgende stappen wordt de configuratieprocedure voor zowel ISE als AD beschreven:

stap 1. zorg ervoor dat ISE wordt aangesloten bij AD, in dit voorbeeld hebt u het domein alab:

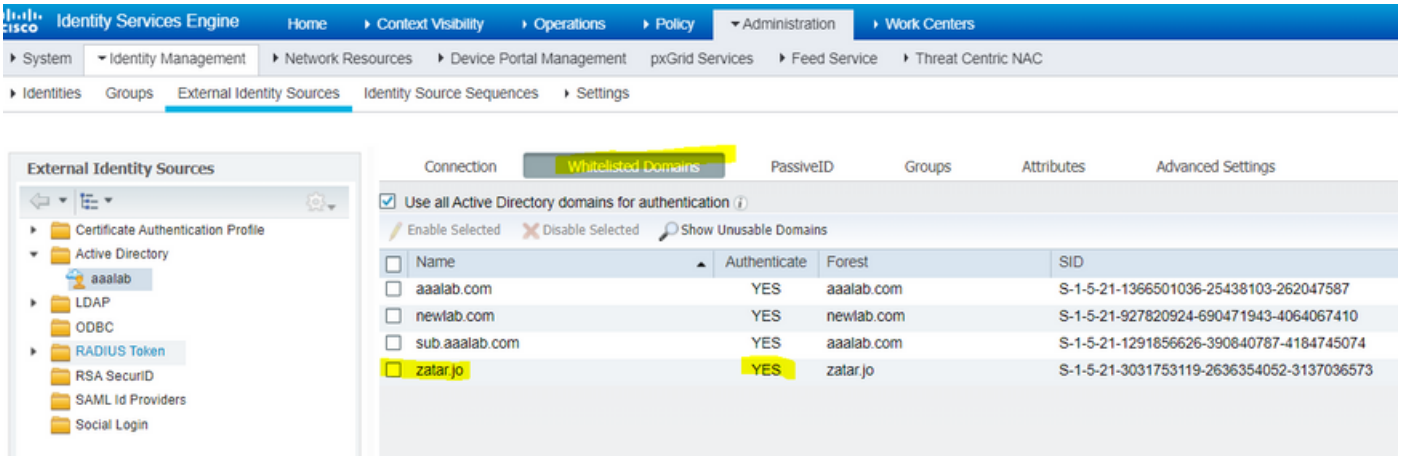


stap 2. zorg ervoor dat het wederzijdse vertrouwen tussen beide actieve directoraten is ingeschakeld, zoals hieronder:

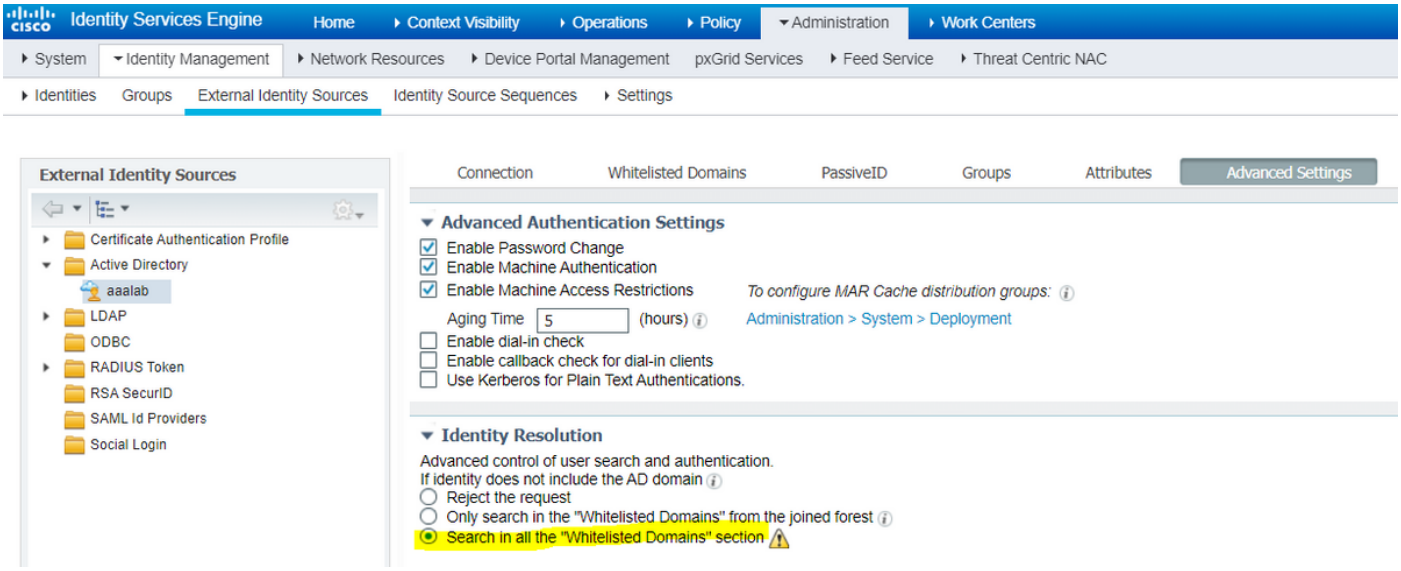
1. Open de magneetknop van de actieve adresgebieden en Trusts.
2. Klik in het linker deelvenster met de rechtermuisknop op het domein dat u wilt toevoegen aan een trust en selecteer Eigenschappen.
3. Klik op het tabblad Trusts.
4. Klik op de knop Nieuw vertrouwen.
5. Klik op Volgende nadat de wizard Nieuw vertrouwen wordt geopend.
6. Typ de DNS-naam van het AD-domein en klik op Volgende.
7. Aangenomen dat het AD-domein via DNS kan worden opgelost, zal het volgende scherm om de richting van het vertrouwen vragen. Selecteer tweevoudige en klik op Volgende.
8. Selecteer alle bronnen die voor authenticatie moeten worden geauthentiseerd in het geval van de vertrekkende trusteigenschappen en klik op Volgende.
9. Typ het wachtwoord voor het vertrouwen en klik op Volgende.
10. Klik twee keer op Volgende.

Opmerking: De AD-configuratie is niet binnen het bereik van Cisco. Microsoft-ondersteuning kan bij problemen worden gebruikt.

Als dit eenmaal is geconfigureerd kan het voorbeeld AD (aaalab) communiceren met het nieuwe AD (zatar.jo) en verschijnt het op het tabblad "witbare domeinen", zoals hieronder. Als deze niet wordt weergegeven, is de configuratie van het twee-wegtrust onjuist:



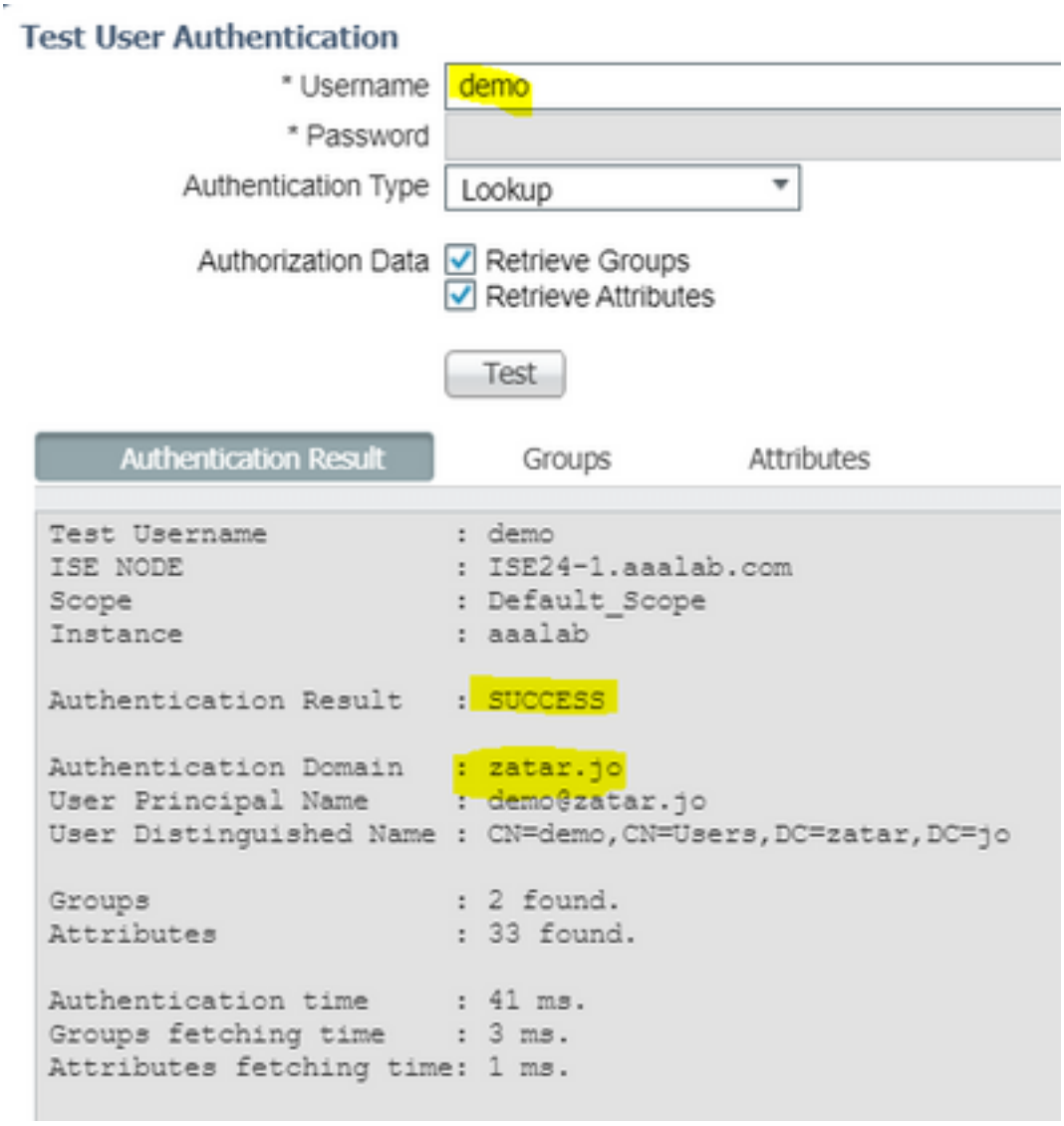
stap 3. Controleer of de optie-**zoekopdracht in het gedeelte "Grijswaarden"** is ingeschakeld, zoals hieronder wordt weergegeven. Het zal het zoeken in alle gefloten domeinen inclusief tweevoudige vertrouwde domeinen toestaan. als de optie **Alleen zoeken in de "Whitelisted Domain" van het aangesloten bos** is ingeschakeld, zal alleen zoeken in de "child" domeinen van het hoofddomein. { kinderdomeinvoorbeeld : sub.aaalab.com in het screenshot hierboven}.



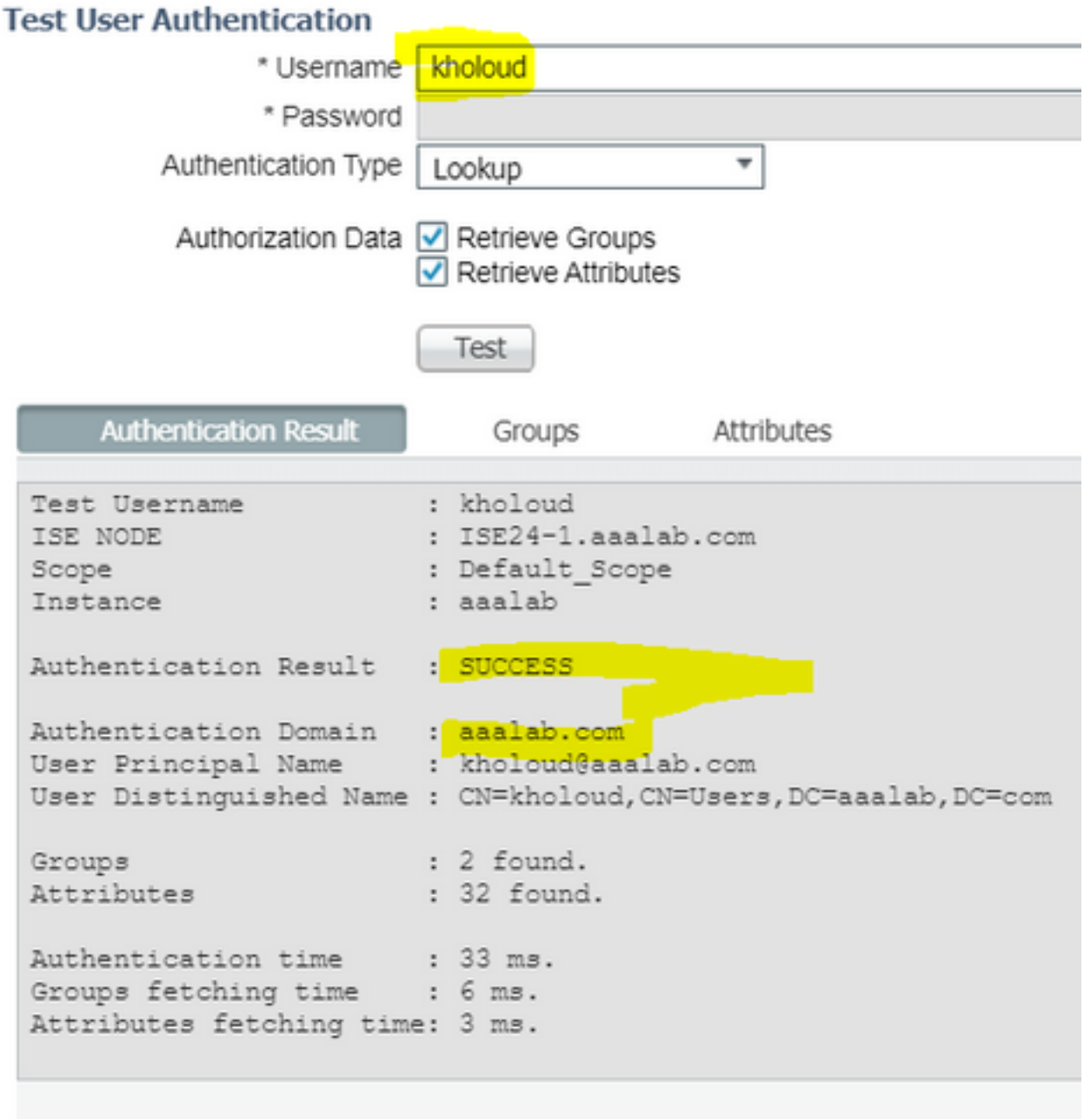
Nu kan ISE naar de gebruiker op Aalab.com en zatar.com zoeken.

Verifiëren

Controleer dat deze functie werkt via de optie "testgebruiker" en gebruik de gebruiker die zich in het domein "zatar.jo" bevindt (in dit voorbeeld bestaat de gebruiker "demo" alleen in het domein "zatar.jo" en het resultaat staat niet in "aaalab.com").



gebruiker kholoud is in aaalab.com en heeft ook een baan :



Problemen oplossen

Er zijn twee belangrijke procedures om problemen op te lossen bij de meeste AD/two-way-trust kwesties, zelfs de meeste Externe Identiteiten:

1. het verzamelen van ISE-loggen (steunbundel) met behulp van debugs. in specifieke mappen in deze steunbundel kunnen we alle details vinden van elke authenticatie poging op AD.

2. pakketvastlegging tussen ISE en AD verzamelen.

stap 1. ISE-logbestanden verzamelen:

a. Schakel de uitwerpselen in en stel de volgende uitwerpselen in op "overtrekken":

- Active Directory (ad_agent.log)
- Identity-store-AD (ad_agent.log)
- run-AAA (prt-server.log)

- nsf (ise-psc.log)
- nsf-sessie (ise-psc.log)

b. Reproduceert het probleem en sluit het aan bij een problematische gebruiker.

c. Verzamel een ondersteuningsbundel.

Werkscenario "loggen":

> Opmerking: Details van de authenticatiepogingen worden gevonden in het bestand ad_agent.log

uit het bestand ad_agent.log :

zatar , op twee manieren , verificatie van vertrouwensrelaties :

```
2020-01-16 12:26:21,210 VERBOSE,140568698918656,LsaDmEnginepDiscoverTrustsForDomain: Adding
trust info zatar.jo (Other Forest, Two way) in forest
zatar.jo,LsaDmEnginepDiscoverTrustsForDomain(),lsass/server/auth-providers/ad-open-
provider/lsadmengine.c:472
2020-01-16 12:26:21,210 DEBUG ,140568698918656,New domain zatar.jo will be added to the trusted
domain list.,LsaDmAddTrustedDomain(),lsass/server/auth-providers/ad-open-provider/lsadm.c:1997
```

op zoek naar de gebruiker " demo " in het hoofddomein ab :

```
2020-01-16 12:29:08,579 DEBUG ,140568690480896,AdIdentityResolver::search: do
(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=demo)) search in forest
aaalab.com,searchIdentity(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:738
```

(Merk op dat demo gebruiker zich in zatar domein bevindt, maar ise zal het eerst in alab domein controleren en dan andere domeinen in het tabblad 'witlested' domeinen zoals newlab.com. Om te voorkomen dat u op het hoofddomein knippert en om direct op zatar.jo te controleren, moet u het UPN-achtervoegsel gebruiken zodat ISE weet waar u een zoekopdracht kunt uitvoeren. De gebruiker dient dus in deze bestandsindeling in te loggen: demo.zatar.jo).

op zoek naar de gebruiker " demo " in zatar.jo .

```
2020-01-16 12:29:08,604 DEBUG ,140568690480896,AdIdentityResolver::search: do
(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=demo)) search in forest
zatar.jo,searchIdentity(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:738
2020-01-16 12:29:08,604 DEBUG ,140568690480896,LsaDmpLdapOpen: gc=1,
domain=zatar.jo,LsaDmpLdapOpen(),lsass/server/auth-providers/ad-open-provider/lsadm.c:4102
2020-01-16 12:29:08,604 DEBUG ,140568690480896,LsaDmpIsDomainOffline: checking status of domain
zatar.jo,LsaDmpIsDomainOffline(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3158
```

gebruiker " demo " , gevonden in zatar domein :

```
18037: pszResolvedIdentity = "demo@zatar.jo"
Line 18039: pszResolvedDN = "CN=demo,CN=Users,DC=zatar,DC=jo"
Line 18044: pszResolvedSAM = "demo"
Line 18045: pszResolvedExplicitUPN = "demo@zatar.jo"
```

```
Line 18056: "1579177748579 24325 "demo" AD-Log-Id=1579177581/40,
Line 18095: pszBase = "CN=demo,CN=Users,DC=zatar,DC=jo"
```

stap2. Verzamel de volgende opnamen:

a. De pakketten die tussen ISE en AD/LDAP worden uitgewisseld, worden versleuteld zodat ze niet leesbaar zouden zijn als we de beelden zouden verzamelen zonder ze eerst te decrypteren.

Om pakketten tussen ISE en AD te decrypteren (deze stap moet worden toegepast vóór het verzamelen van de opnamen en het toepassen van de poging):

1. Klik op ISE aan het tabblad : Externe ID-winkels -> Actieve map -> Geavanceerde tools -> Geavanceerde tuning
2. Kies uw ISE-knooppunt.
3. Het veld 'Naam' krijgt een specifieke PROBLESHOOTING-string: PROBLEMEN OPLOSSEN.EncryptionOffPeriod.
4. Het veld 'Waarde' krijgt het aantal minuten dat u wilt oplossen

‹Positief geheel in minuten›

Voorbeeld over een half uur:

30

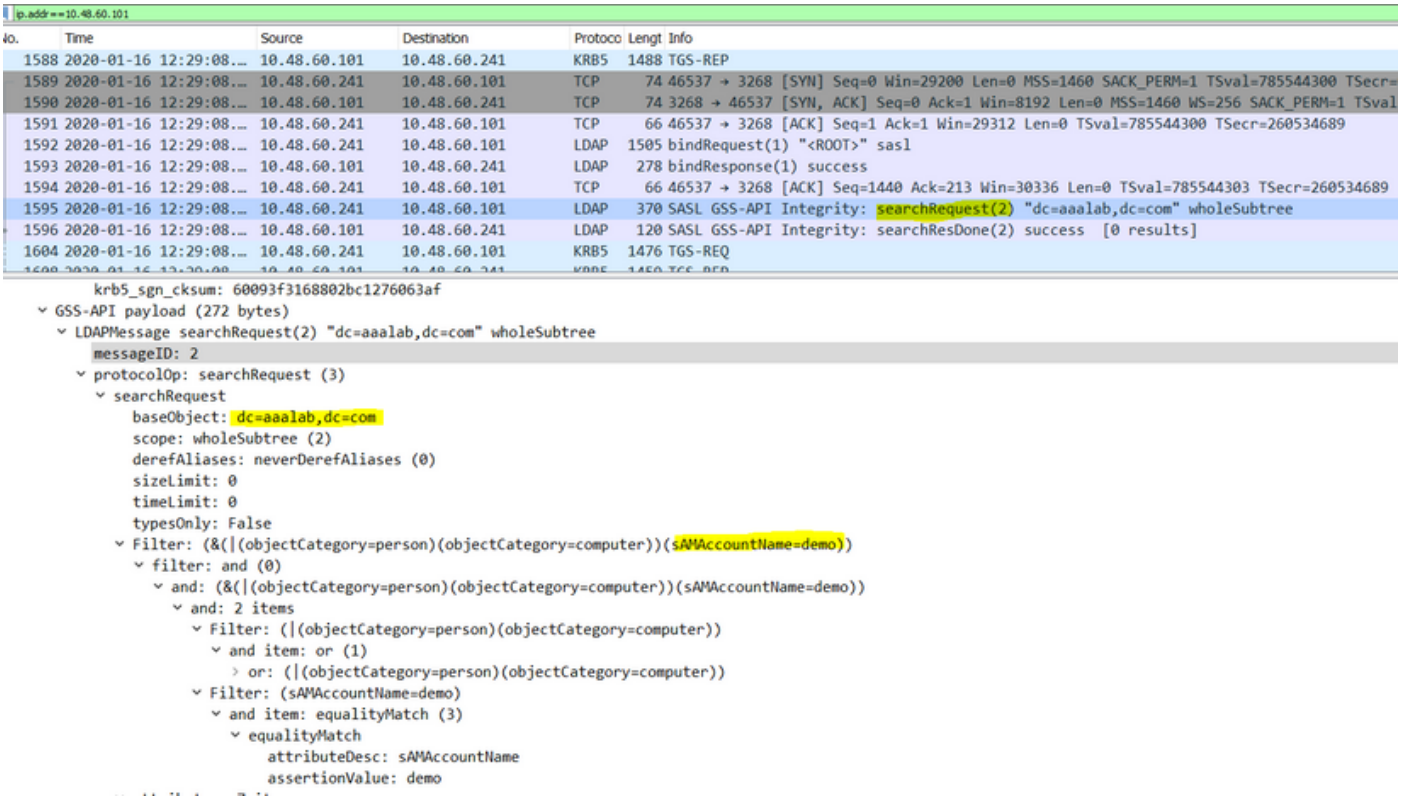
5. Typ een beschrijving. Vereist voor volgende stap.
6. Klik op de knop 'Waarde bijwerken'
7. Klik op 'Start Active Directory-connector'.
8. 10 minuten wachten tot de decrypt effect heeft .

b. start de opname op ISE.

c. reproduceren.

d. dan stoppen en downloaden

Werkscenario "loggen":



Verifiëren

Hier zijn een paar voorbeelden van al dan niet werkende situaties waar je mee te maken zou kunnen krijgen en de boeken die ze produceren.

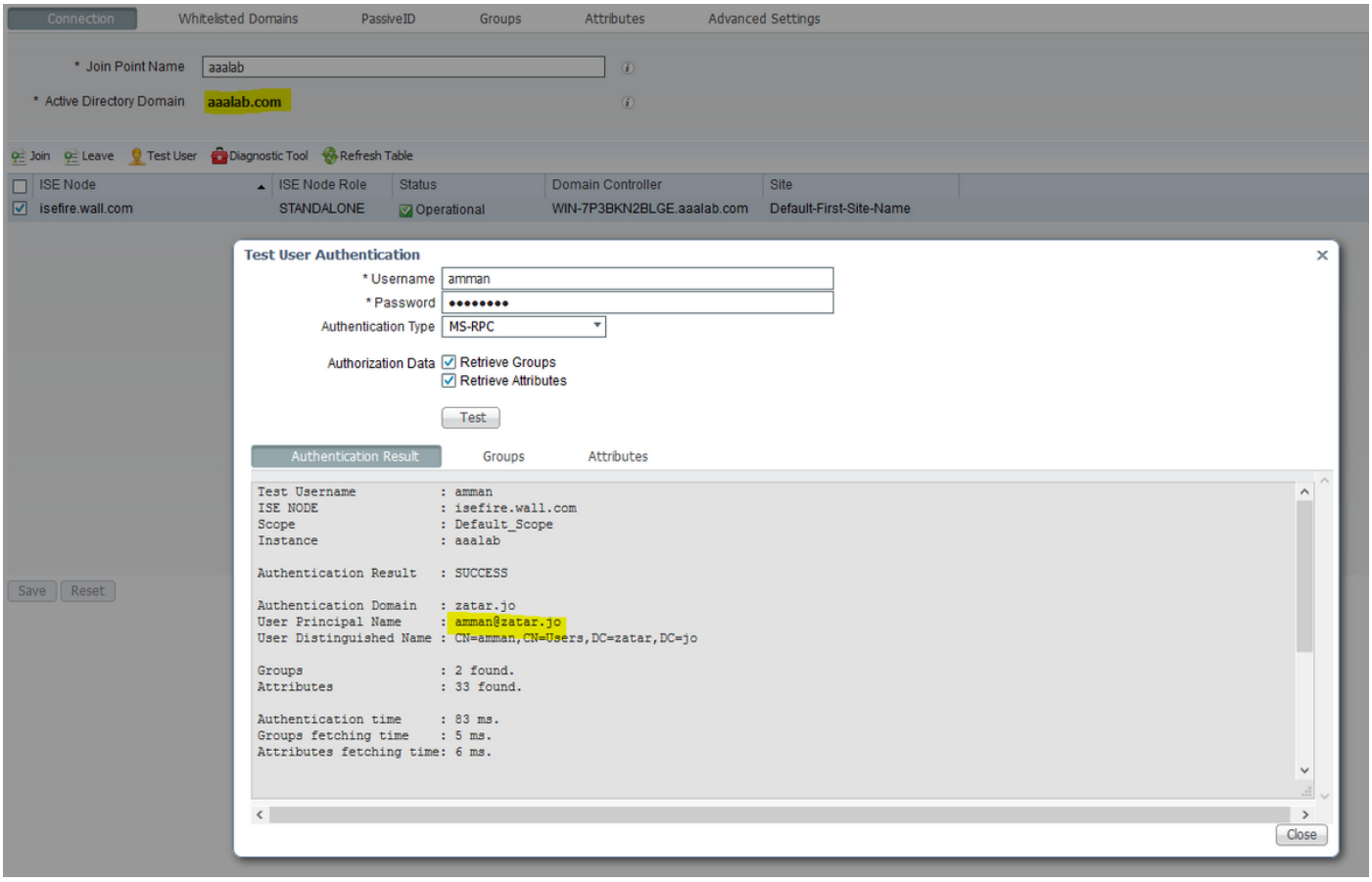
1. Verificatie op basis van AD "zatar.jo"-groepen:

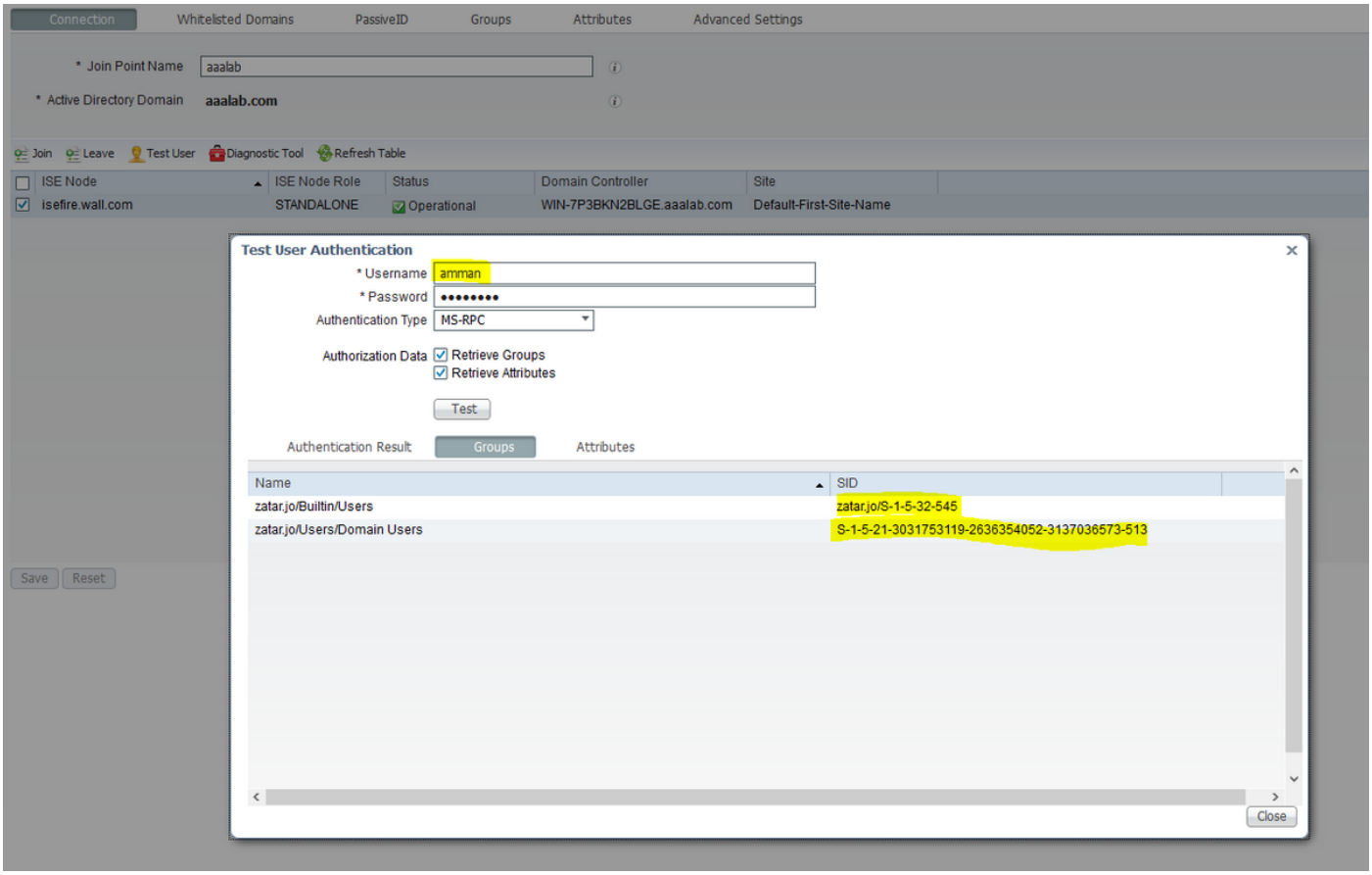
Als de groep niet uit het tabblad groep is teruggekeerd, krijgt u dit logbericht:

```
2020-01-22 10:41:01,526 DEBUG ,140390418061056,Do not know about domain for object SID 'S-1-5-21-3031753119-2636354052-3137036573-513',LsaDmpMustFindDomainByObjectSid(),lsass/server/auth-providers/ad-open-provider/lsadm.c:1574
```

We moeten de groepen in zatar.jo uit het tabblad Groepen halen.

Verificatie van AD-groepsleden uit AD-tabblad:





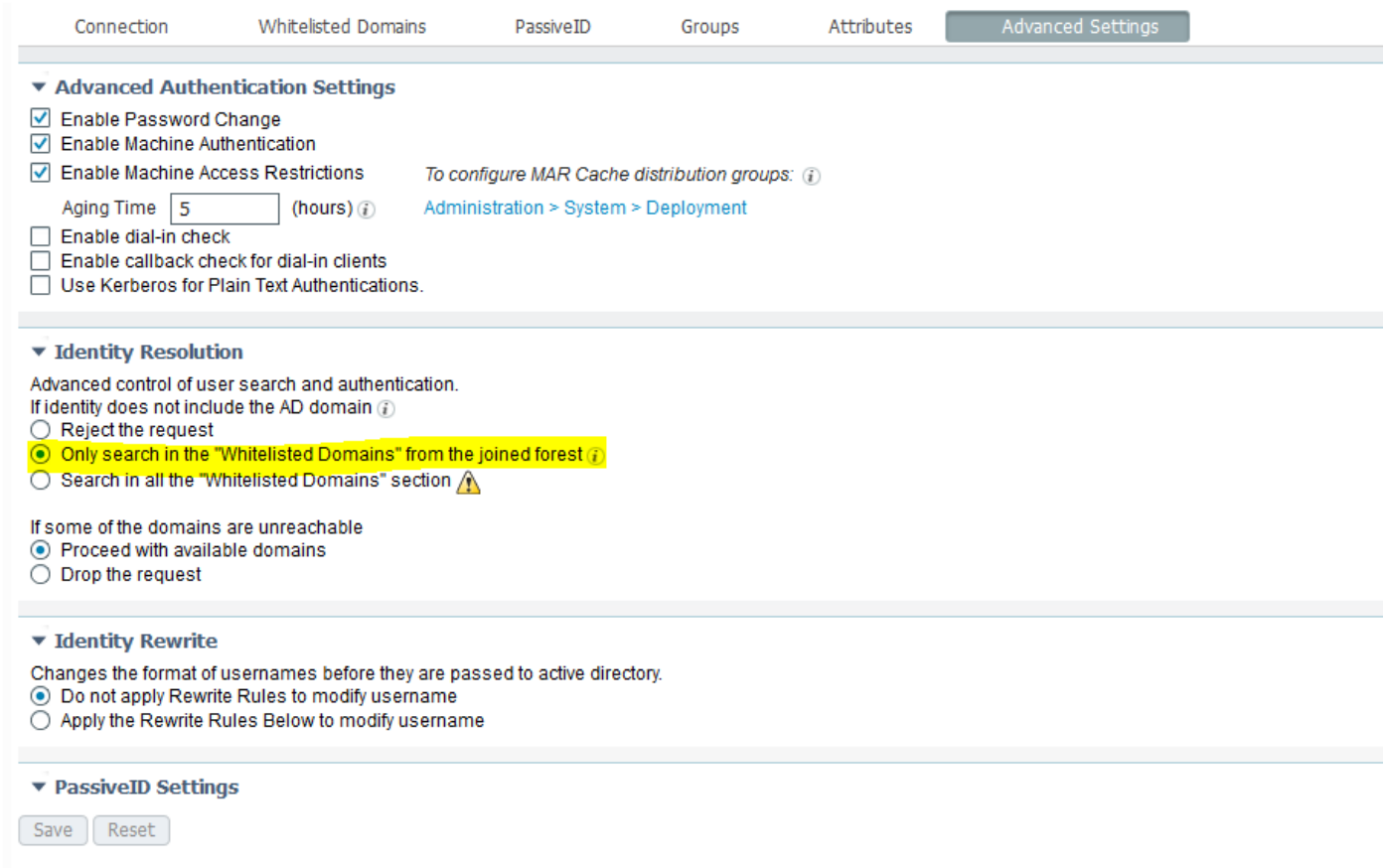
werkscenario Van de logs AD_agent.log:

```
2020-01-22 10:41:01,516 DEBUG ,140390418061056,AD_GetTokenGroups: SID selected: [zatar.jo/S-1-5-
32-545],AD_GetTokenGroups(),lsass/server/auth-providers/ad-open-provider/provider-main.c:9669
2020-01-22 10:41:01,516 DEBUG ,140390418061056,AD_GetTokenGroups: SID selected: [S-1-5-21-
```

```
3031753119-2636354052-3137036573-513],AD_GetTokenGroups(),lsass/server/auth-providers/ad-open-provider/provider-main.c:9669


pTokenGroupsList =
{
dwStringsCount = 2
ppszStrings =
{
"zatar.jo/S-1-5-32-545"
"S-1-5-21-3031753119-2636354052-3137036573-513"
}
}
```

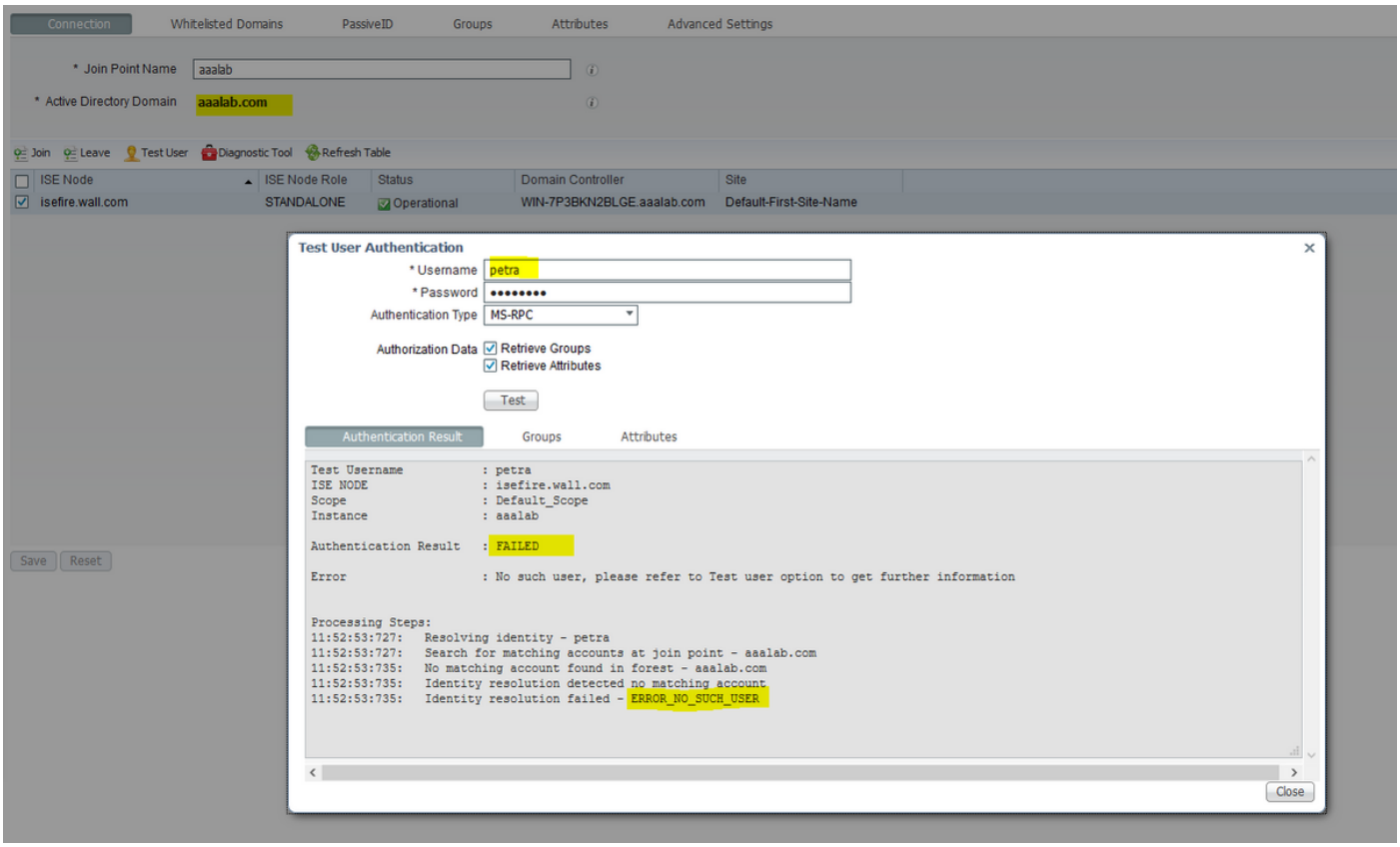
2. Indien de geavanceerde optie "Alleen zoeken in de "Whitelisted Domain" uit het aangehechte bos" is ingeschakeld:



Wanneer u de optie "Alleen zoeken in de "Witte Domeinen" uit het aangesloten bos" kiest, markeerde ISE ze offline:

```
2020-01-22 13:53:31,000 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: examine domain newlab.com,LsaDmpFilterOfflineCallback(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3423
2020-01-22 13:53:31,001 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: domain newlab.com is usable and is marked offline (DC or GC).,LsaDmpFilterOfflineCallback(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3498
2020-01-22 13:53:31,001 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: examine domain zatar.jo,LsaDmpFilterOfflineCallback(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3423
2020-01-22 13:53:31,001 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: domain zatar.jo is not marked offline (DC or GC).,LsaDmpFilterOfflineCallback(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3454
```

De gebruiker "petra" bevindt zich in zatar.jo en is niet geauthentiseerd, zoals hieronder wordt getoond:



In de stammen:

ISE kon andere domeinen niet bereiken, door geavanceerde optie "Alleen zoeken in de "Whitelisted Domain" uit het gezamenlijke bos":

```
2020-01-22 13:52:53,735 DEBUG ,140629511296768,AdIdentityResolver::search: already did
(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=petra)) search in forest
aaalab.com,searchIdentity(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:735
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AdIdentityResolver::examineDomains:
newlab.com,examineDomains(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:601
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AdIdentityResolver::examineDomains:
zatar.jo,examineDomains(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:601
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AdIdentityResolver::finalizeResult: result:
40008 (symbol: LW_ERROR_NO_SUCH_USER),finalizeResult(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:491
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AD_ResolveIdentity: identity=[petra], flags=0,
dwError=40008,AD_ResolveIdentity(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver.cpp:131
2020-01-22 13:52:53,735 VERBOSE,140629511296768,LsaSrvResolveIdentity: identity=[petra],
flags=0, dwError=40008,LsaSrvResolveIdentity(),lsass/server/api/api2.c:2877
2020-01-22 13:52:53,735 VERBOSE,140629511296768,Error code: 40008 (symbol:
LW_ERROR_NO_SUCH_USER),LsaSrvResolveIdentity(),lsass/server/api/api2.c:2890
2020-01-22 13:52:53,735 VERBOSE,140629511296768,LsaSrvResolveIdentity: identity=[petra],
flags=0, dwError=40008, resolved identity list returned =
NO,LsaSrvIpcResolveIdentity(),lsass/server/api/ipc_dispatch.c:2738
```