ISE e configurazione AD con trust bidirezionale

Sommario

Introduzione

Questo documento descrive la definizione di "trust bidirezionale" su ISE e un semplice esempio di configurazione: come autenticare un utente non presente in Active Directory ma presente in un altro AD.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base di:

- Integrazione con ISE 2.x e Active Directory .
- Autenticazione di identità esterna su ISE.

Componenti usati

- ISE 2.x
- due Active Directory.

Configurazione

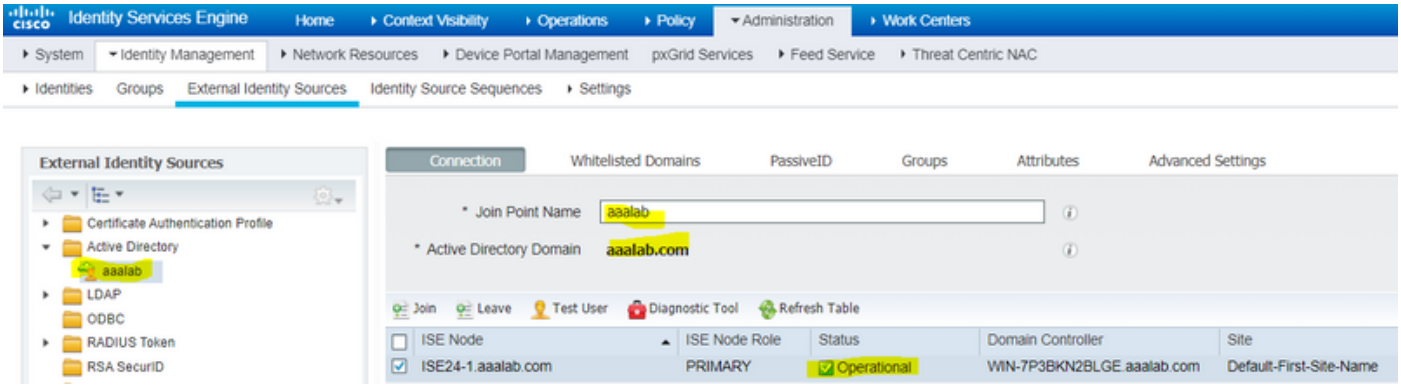
Per espandere il tuo dominio e includere altri utenti in un dominio diverso da quello che è già stato aggiunto ad ISE, devi procedere in due modi:

1. èpossibile aggiungere il dominio manualmente e separatamente in ISE. in questo modo, si disporrebbe di due Active Directory separate.
2. Unisci un AD ad ISE, quindi configura un trust **bidirezionale** tra questo AD e il secondo AD, senza aggiungerlo all'ISE. Si tratta principalmente di una configurazione di trust bidirezionale, è un'opzione configurata tra due o più Active Directory. ISE rileverà automaticamente questi domini trusted utilizzando il connettore AD e li aggiungerà ai "domini consentiti" e li tratterà come AD separati uniti ad ISE. Ecco come autenticare un utente

nell'AD "zatar.jo", che non è associato ad ISE.

La procedura di configurazione di ISE e AD è descritta nella procedura seguente:

passaggio 1. verificare che ISE sia stato aggiunto ad AD, nell'esempio riportato viene visualizzato il dominio aalab:

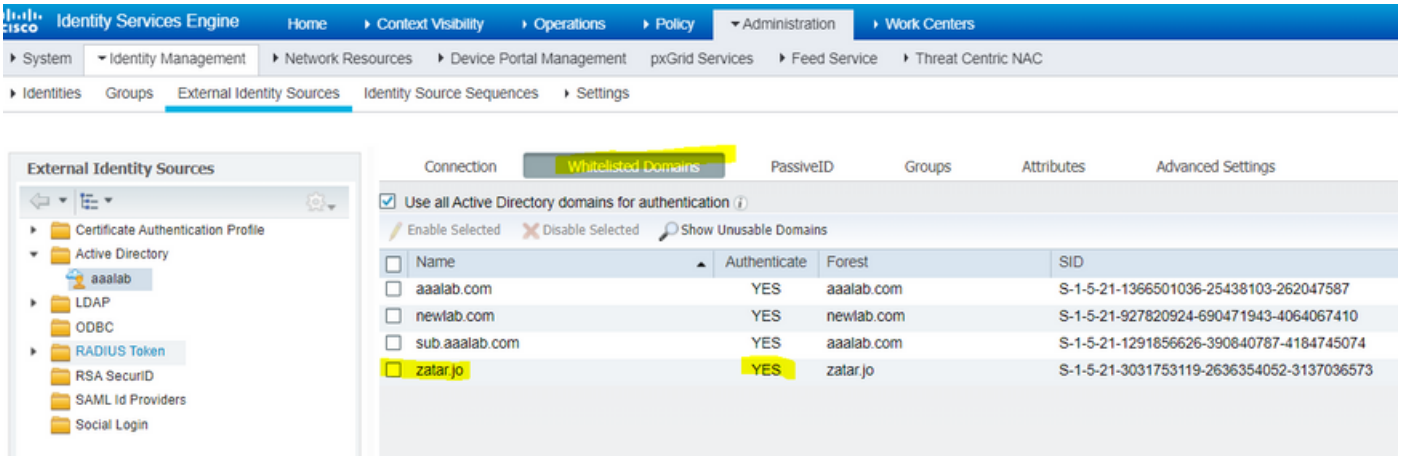


passaggio 2. verificare che il trust bidirezionale sia abilitato tra entrambe le directory, come indicato di seguito:

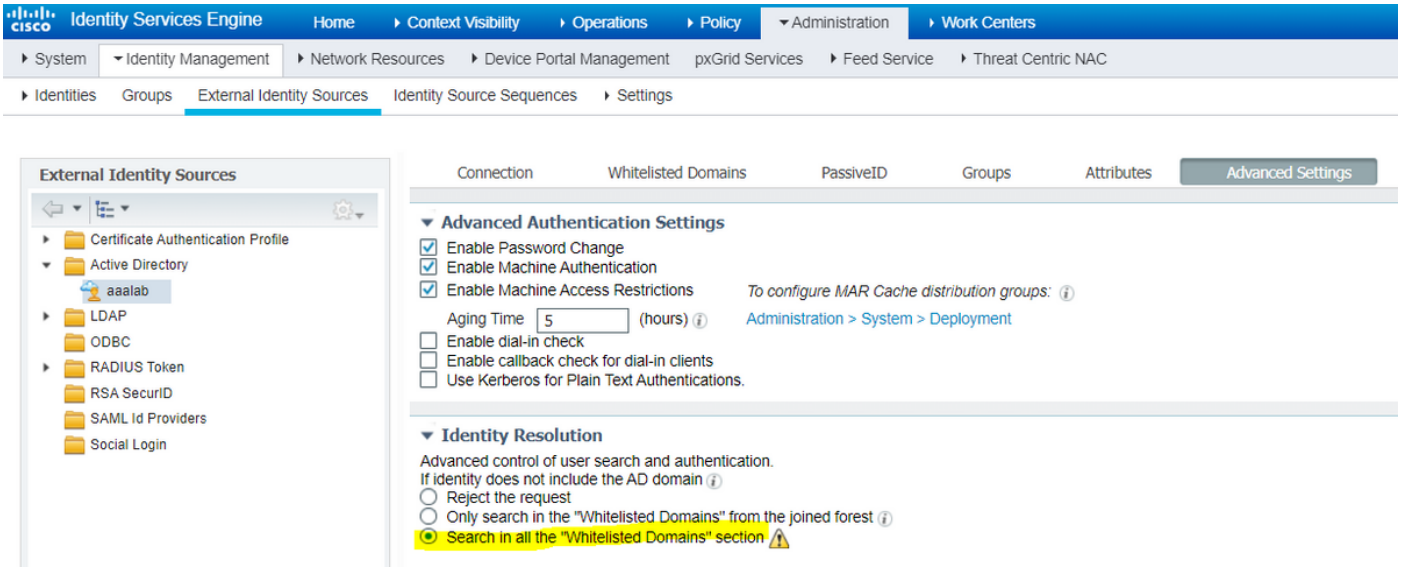
1. Aprire lo snap-in Domini e trust di Active Directory.
2. Nel riquadro sinistro fare clic con il pulsante destro del mouse sul dominio per cui si desidera aggiungere un trust e quindi scegliere Proprietà.
3. Fare clic sulla scheda Trust.
4. Fare clic sul pulsante Nuova relazione di trust.
5. Dopo aver aperto la Creazione guidata nuova relazione trust, fare clic su Avanti.
6. Digitare il nome DNS del dominio Active Directory e fare clic su Avanti.
7. Supponendo che il dominio Active Directory sia risolvibile tramite DNS, la schermata successiva richiederà la Direzione di attendibilità. Selezionare Bidirezionale e fare clic su Avanti.
8. Per Proprietà trust in uscita, selezionare tutte le risorse da autenticare e fare clic su Avanti.
9. Immettere e digitare nuovamente la password di trust e fare clic su Avanti.
10. Fare clic su Avanti due volte.

Nota: La configurazione di Active Directory non rientra nell'ambito del supporto Cisco. È possibile attivare il supporto Microsoft in caso di problemi.

Una volta configurata questa opzione, l'AD (aalab) di esempio può comunicare con il nuovo AD (zatar.jo) e dovrebbe essere visualizzato nella scheda "domini con elenchi bianchi", come indicato di seguito. se non viene visualizzata, la configurazione del trust bidirezionale non è corretta:



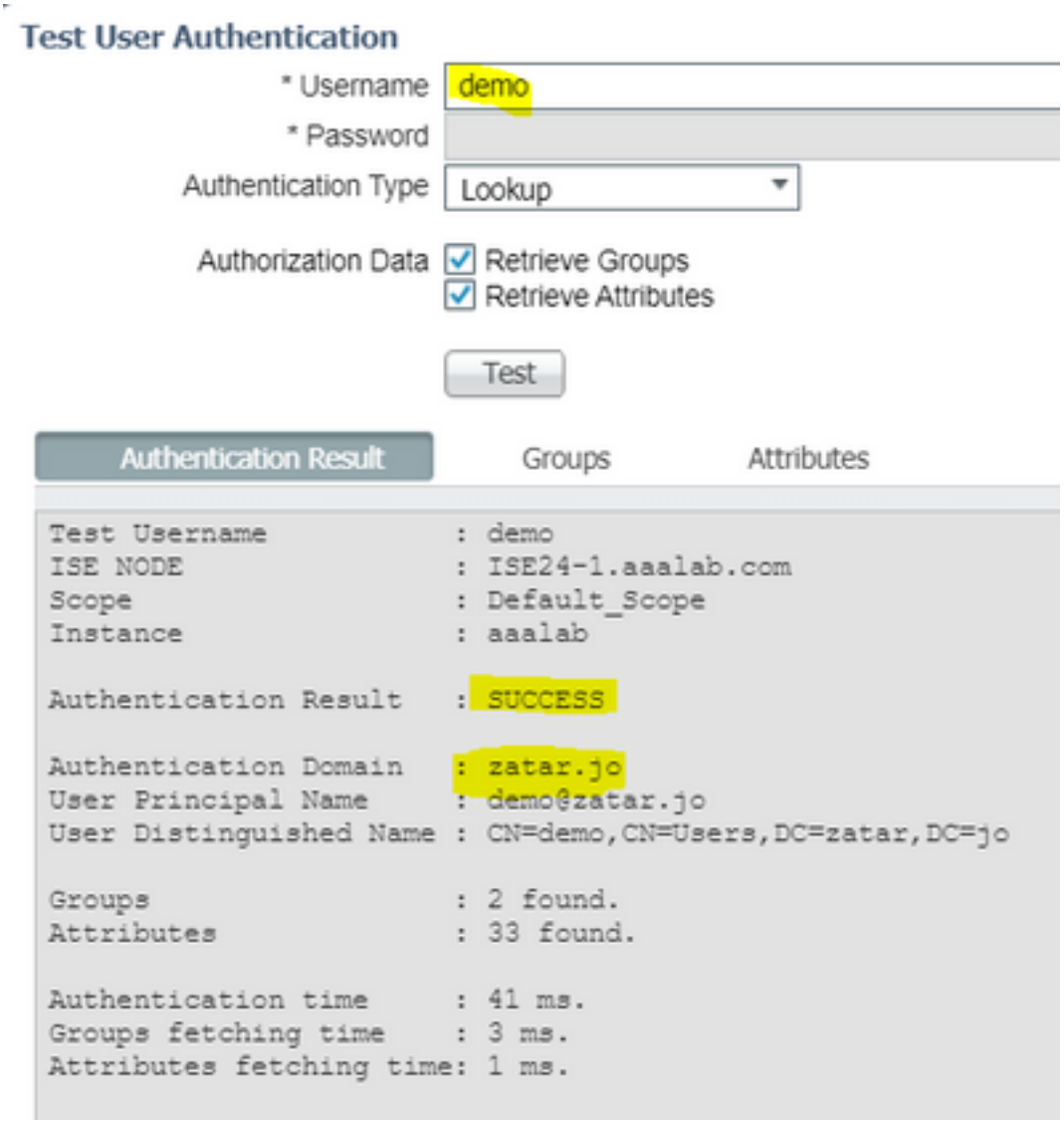
passaggio 3. Assicurarsi che l'opzione **search in all the "whitlested Domains" (Cerca in tutti i domini con whitlesting)** sia abilitata, come mostrato di seguito. Consentirà la ricerca in tutti i domini con elenco, inclusi i domini trusted bidirezionali. se l'opzione **Cerca solo nei "Domini inseriti nella lista bianca" della foresta aggiunta** è abilitata, la ricerca verrà eseguita solo nei domini "figlio" del dominio principale. { esempio di dominio figlio: sub.aaalab.com nello screenshot sopra }.



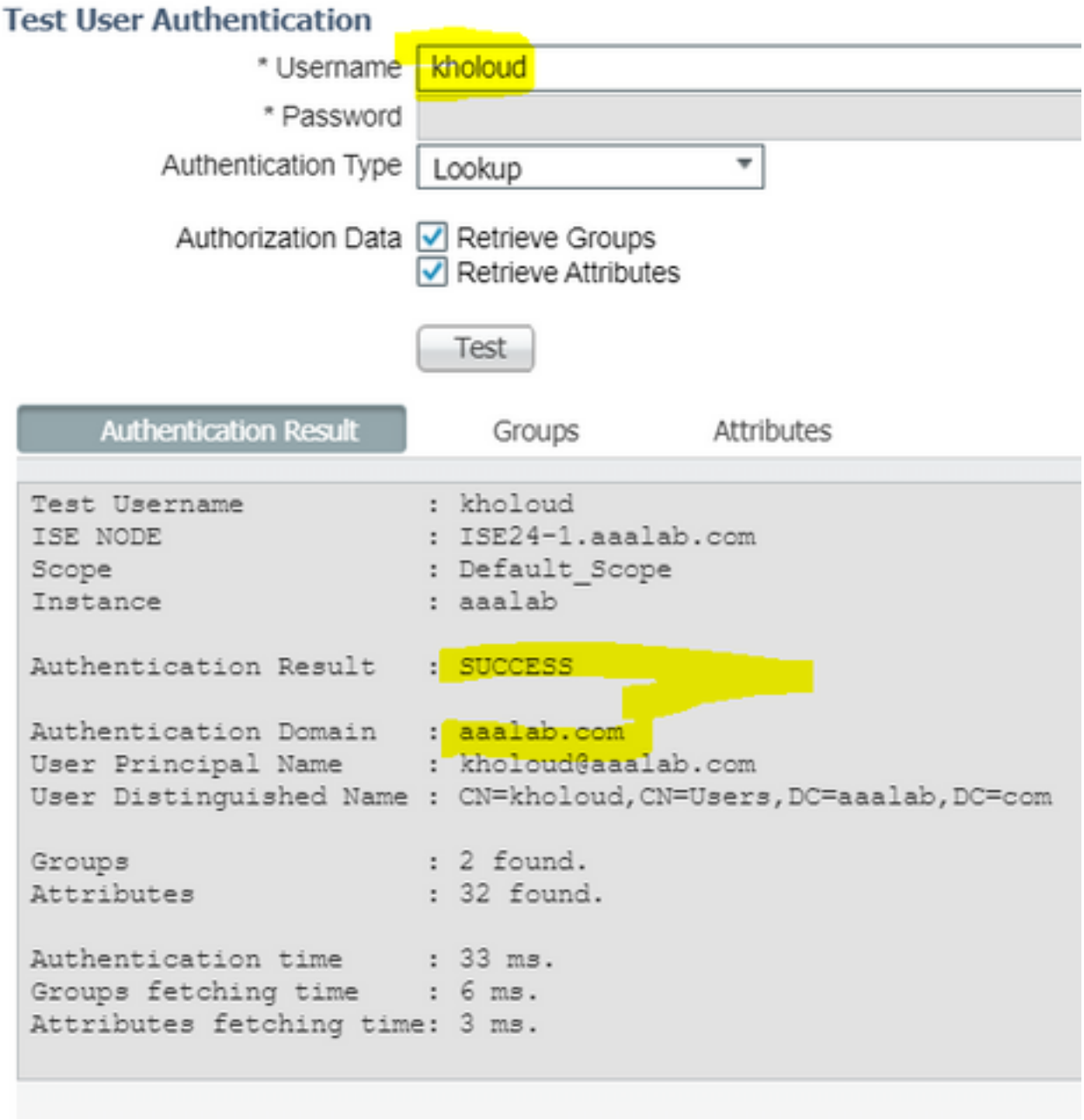
Ora ISE può cercare l'utente nei siti aaalab.com e zatar.com.

Verifica

Verificare che funzioni tramite l'opzione "test user", utilizzare l'utente che si trova nel dominio "zatar.jo" (in questo esempio, l'utente "demo" esiste solo nel dominio "zatar.jo", e non è in "aalab.com", i risultati del test sono riportati di seguito):



gli utenti di aaalab.com, stanno lavorando, l'utente kholoud si trova su aaalab.com :



Risoluzione dei problemi

Esistono due procedure principali per risolvere la maggior parte dei problemi di trust bidirezionale/AD, anche la maggior parte delle autenticazioni di identità esterne:

1. raccolta dei log ISE (bundle di supporto) con i debug abilitati. in cartelle specifiche di questo pacchetto di supporto, sono disponibili tutti i dettagli di qualsiasi tentativo di autenticazione in AD.

2. raccogliere le acquisizioni di pacchetti tra ISE e AD.

passaggio 1. raccogliere i log ISE:

r. Abilitare i debug e impostare i seguenti debug su "trace":

- Active Directory (ad_agent.log)
- identity-store-AD (ad_agent.log)
- runtime-AAA (prt-server.log)

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

b. Riprodurre il problema, connettersi con un utente con problemi.

c. Raccogliere un pacchetto di supporto.

"Log" dello scenario di lavoro:

Nota: I dettagli dei tentativi di autenticazione sono disponibili nel file ad_agent.log

dal file ad_agent.log:

verifica connessione trust bidirezionale zatar:

```
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
```

ricerca dell'utente "demo" nella scheda del dominio principale:

```
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
```

(notare che l'utente demo si trova nel dominio zatar, tuttavia ise lo controllerà prima nel dominio aalab, poi altri domini nella scheda "whitlested" domini come newlab.com. per evitare il check-in nel dominio principale e per il check-in diretto di zatar.jo, è necessario usare il suffisso UPN in modo che ISE sappia dove cercare, quindi l'utente dovrebbe effettuare il login in questo formato: demo.zatar.jo).

ricerca dell'utente "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
```

utente "demo" trovato nel dominio zatar:

```
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"
```

passaggio 2. Raccogli clip:

r. I pacchetti scambiati tra ISE e AD/LDAP sono crittografati, quindi non sarebbero leggibili se le clip venissero raccolte senza essere prima decriptate.

Per decrittografare i pacchetti tra ISE e AD (questo passaggio deve essere applicato prima di raccogliere le clip e applicare il tentativo):

1. Ad ISE passare alla scheda : Archivi di ID esterni -> Active Directory -> Strumenti avanzati -> Ottimizzazione avanzata
2. Scegli il tuo nodo ISE.
3. Il campo 'Nome' ottiene una stringa di RISOLUZIONE DEI PROBLEMI specifica: Risoluzione dei problemi.EncryptionOffPeriod.
4. Nel campo 'Valore' viene visualizzato il numero di minuti per cui si desidera eseguire la risoluzione dei problemi

<Intero positivo in minuti>

Esempio per mezz'ora:

30

5. Digitare una descrizione. Obbligatorio prima del passaggio successivo.

6. Fare clic sul pulsante 'Aggiorna valore'

7. Fare clic su 'Riavvia Active Directory Connector.

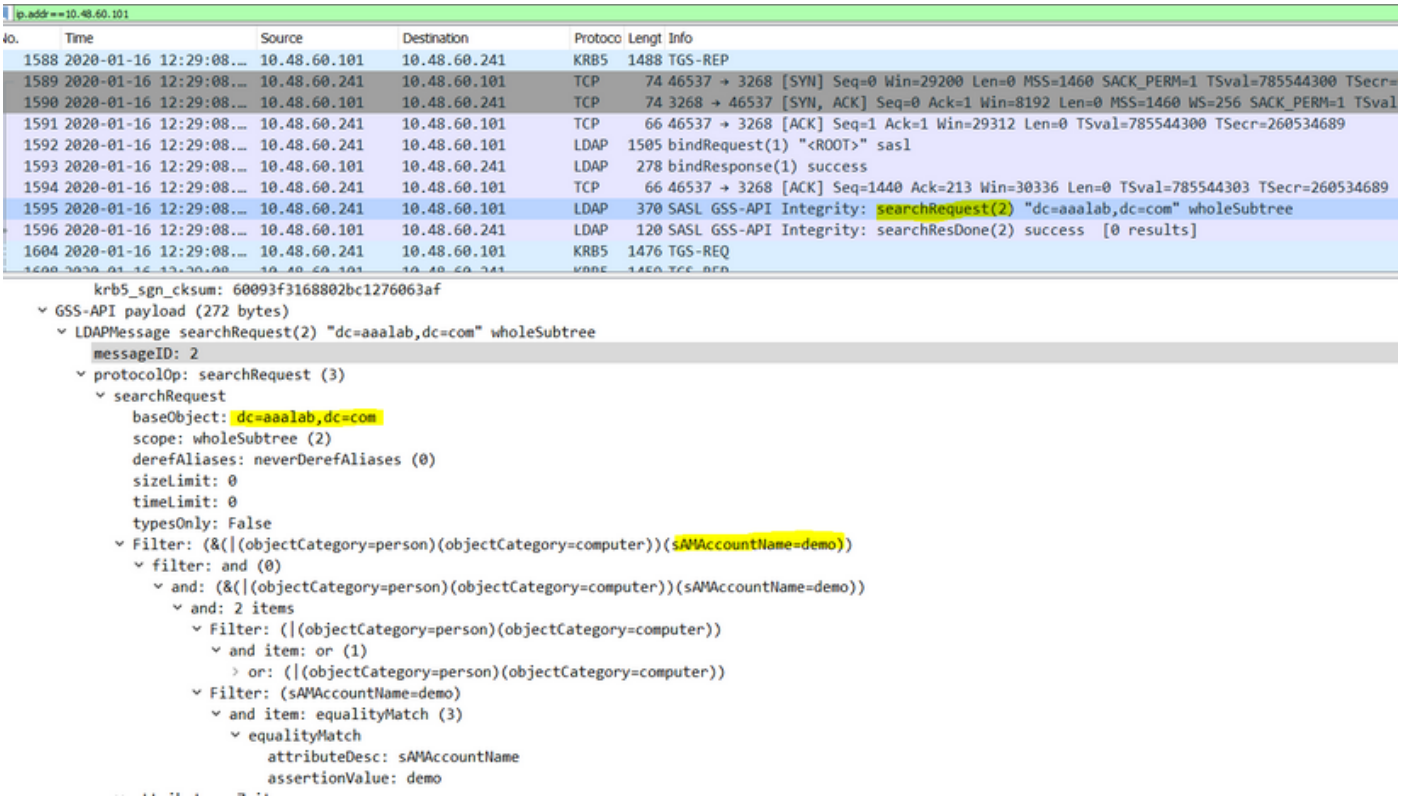
8. attendere 10 minuti prima che la decrittografia diventi effettiva.

b. inizia le clip da ISE.

c. riprodurre il problema.

d. quindi interrompi e scarica la clip

"Log" dello scenario di lavoro:



Verifica

Di seguito sono riportati un paio di esempi di situazioni lavorative e non lavorative che possono verificarsi e i registri che vengono prodotti.

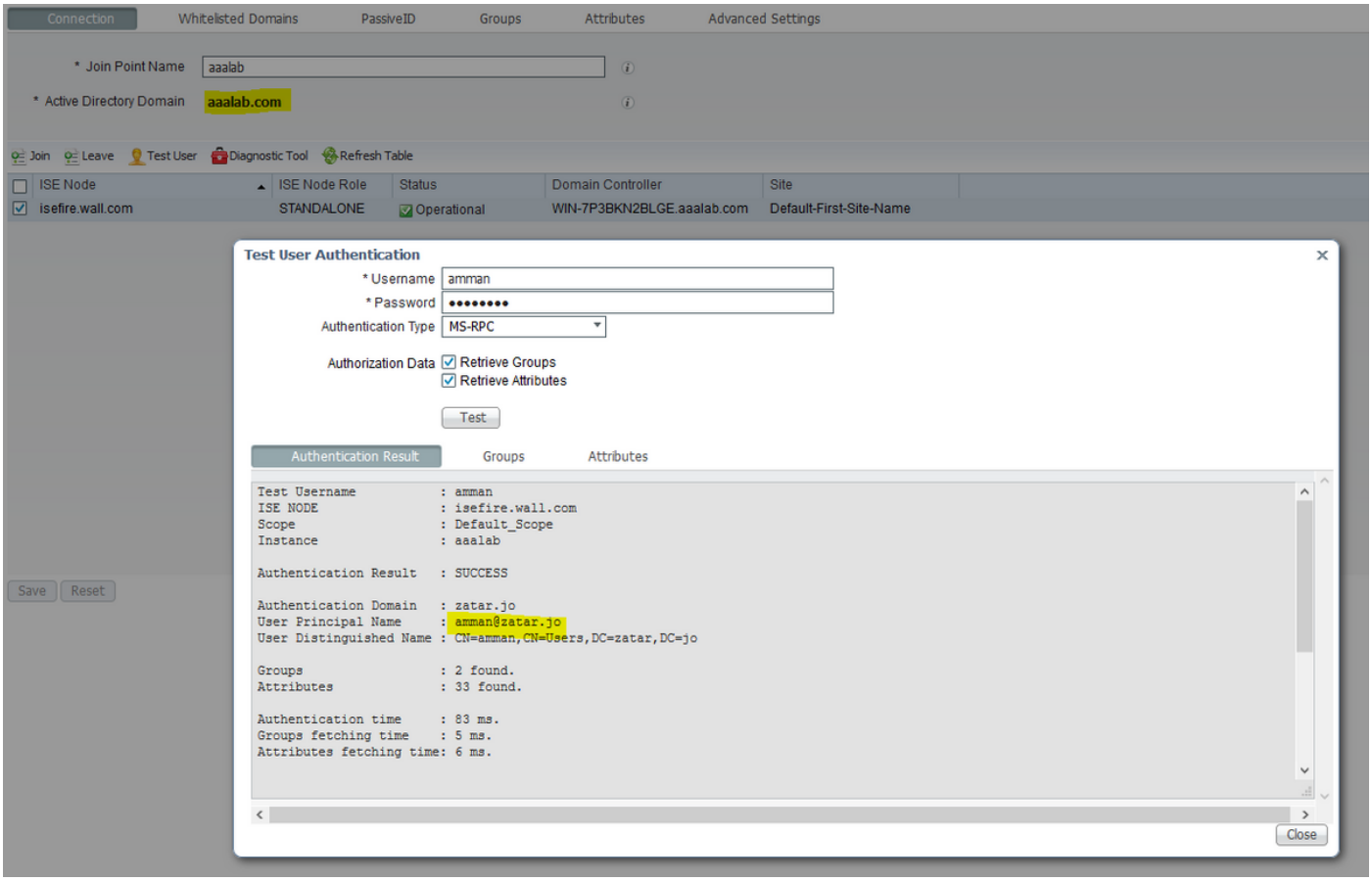
1. Autenticazione basata sui gruppi AD "zatar.jo":

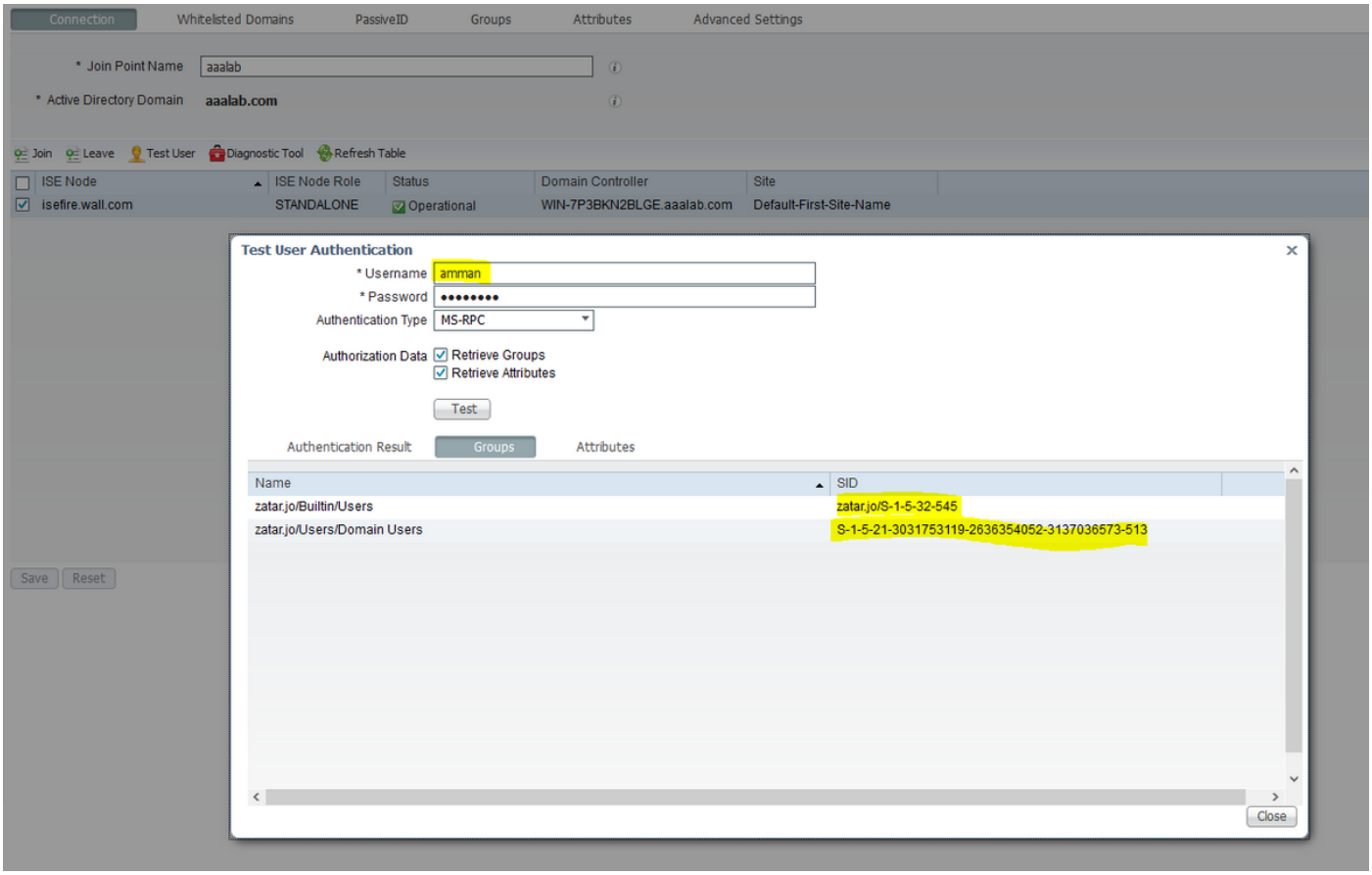
Se il gruppo non è stato recuperato dalla scheda gruppo, verrà visualizzato questo messaggio di registro:

```
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
```

Ènecessario recuperare i gruppi in zatar.jo dalla scheda Gruppi.

Verifica dei recuperi del gruppo AD dalla scheda AD:





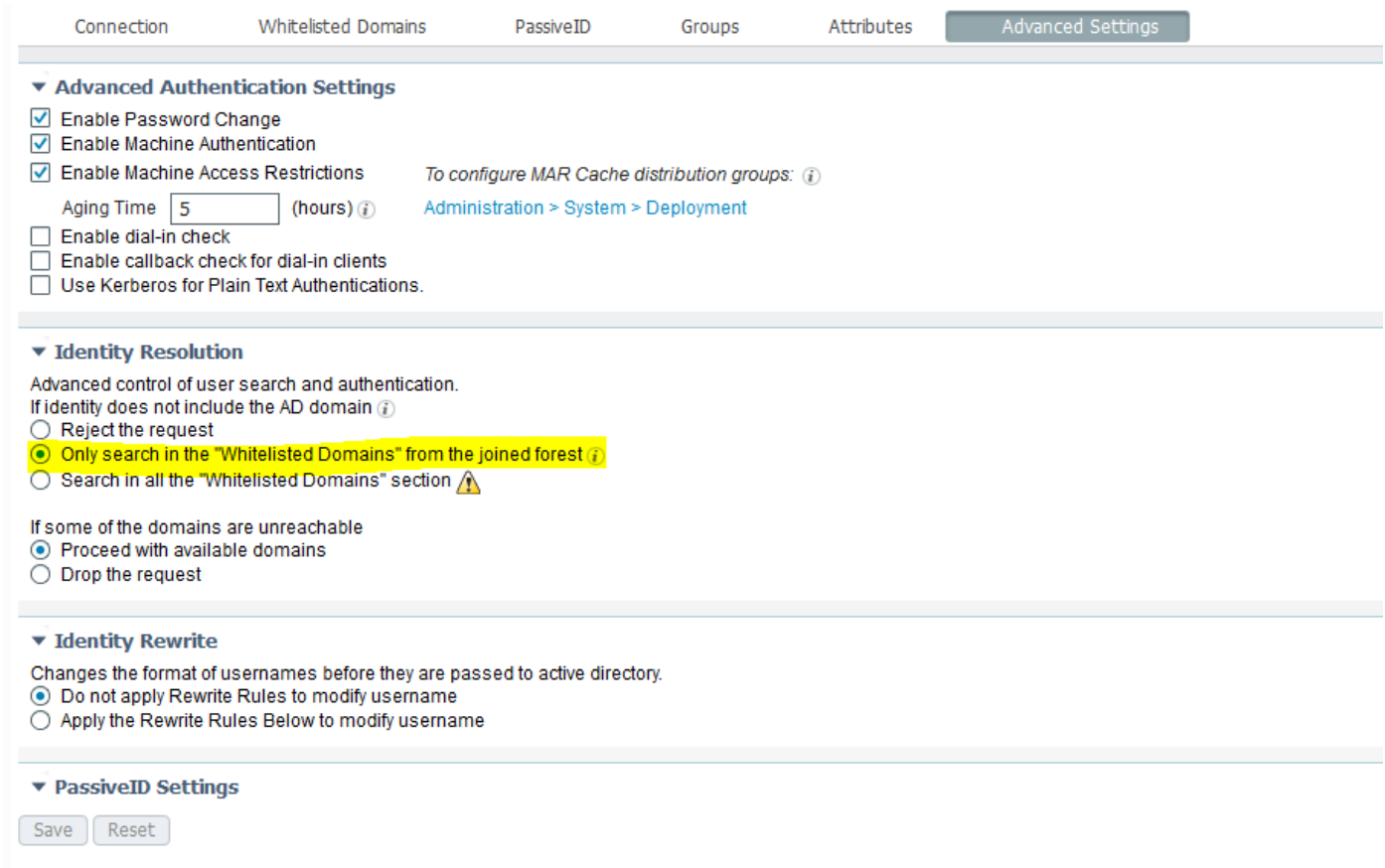
scenario di lavoro Dai log AD_agent.log:

```
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"
}
}
```

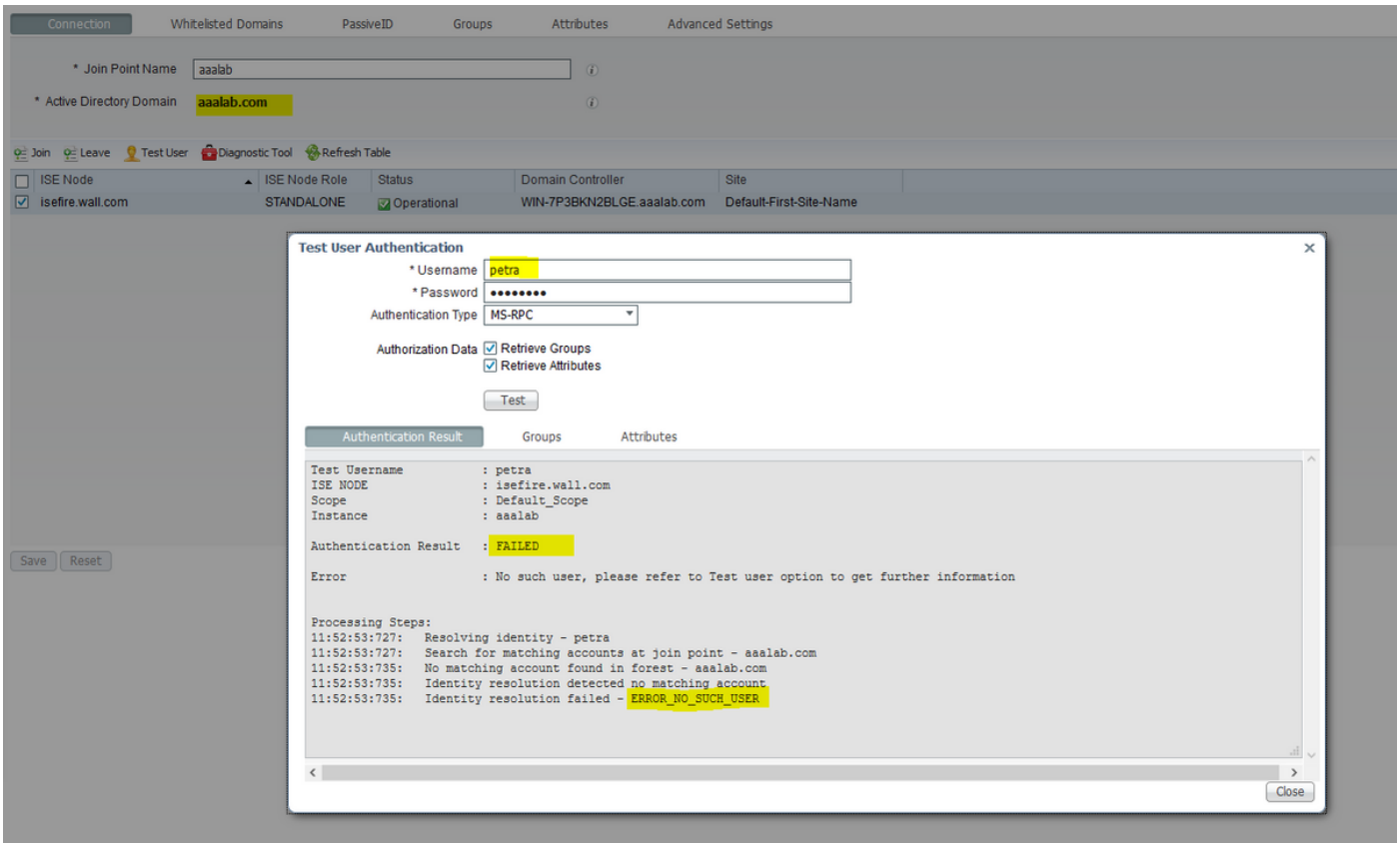
2. Se è selezionata l'opzione di ricerca avanzata "Cerca solo nei "Domini inseriti nella lista bianca" dalla foresta aggiunta:



Quando si sceglie l'opzione "Cerca solo nei "Domini inseriti nella lista bianca" dalla foresta aggiunta", ISE li ha contrassegnati 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
```

L'utente "petra" si trova in zatar.jo e non riuscirà nell'autenticazione, come si vede nello screenshot seguente:



Nei registri:

ISE non è riuscita a raggiungere altri domini, a causa dell'opzione avanzata "Cerca solo nei "Domini whitelist" dalla foresta aggiunta":

```
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
```