ISE 및 양방향 신뢰 AD 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[구성](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[다음을 확인합니다.](#)

소개

이 문서에서는 ISE에서 "양방향 신뢰"의 정의 및 간단한 컨피그레이션 예를 설명합니다.ISE에 가입되어 있지 않지만 다른 AD에 있는 사용자를 인증하는 방법

사전 요구 사항

요구 사항

Cisco는 다음과 같은 기본적인 지식을 보유하고 있음을 권장합니다.

- ISE 2.x 및 Active Directory 통합.
- ISE의 외부 ID 인증.

사용되는 구성 요소

- ISE 2.x .
- 두 개의 활성 디렉토리

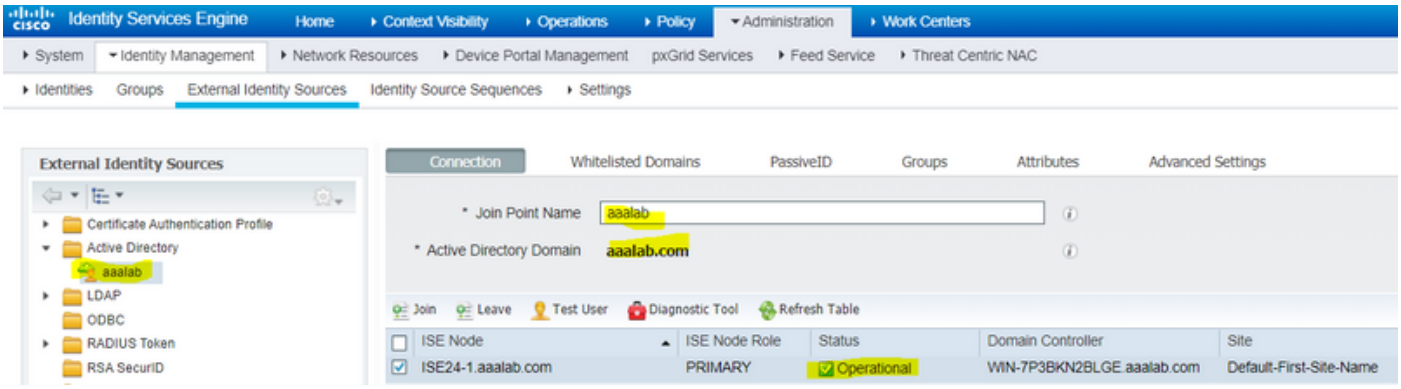
구성

도메인을 확장하고 이미 ISE에 가입된 사용자 이외의 다른 도메인에 다른 사용자를 포함하려면 두 가지 방법으로 이 작업을 수행할 수 있습니다.

1. ISE에서 도메인을 수동으로 그리고 별도로 추가할 수 있습니다. 이렇게 하면 두 개의 개별 Active Directory가 있습니다.
2. 하나의 AD를 ISE에 연결한 다음 ISE에 추가하지 않고 이 AD와 두 번째 AD 간에 **양방향 신뢰**를 구성합니다.이는 주로 두 가지 방식의 신뢰 구성이며 둘 이상의 활성 디렉토리 간에 구성된 옵션입니다.ISE는 AD 커넥터를 사용하여 이러한 트러스트된 도메인을 자동으로 탐지하고 "화이트리스트에 있는 도메인"에 추가하고 이들을 ISE에 조인된 별도의 AD로 처리합니다.이것은 ISE에 가입되지 않은 AD "zatar.jo"에서 사용자를 인증할 수 있는 방법입니다.

다음 단계에서는 ISE와 AD의 구성 절차를 설명합니다.

1단계. ISE가 AD에 조인되었는지 확인합니다. 이 예에서는 도메인 aaaalab가 있습니다.

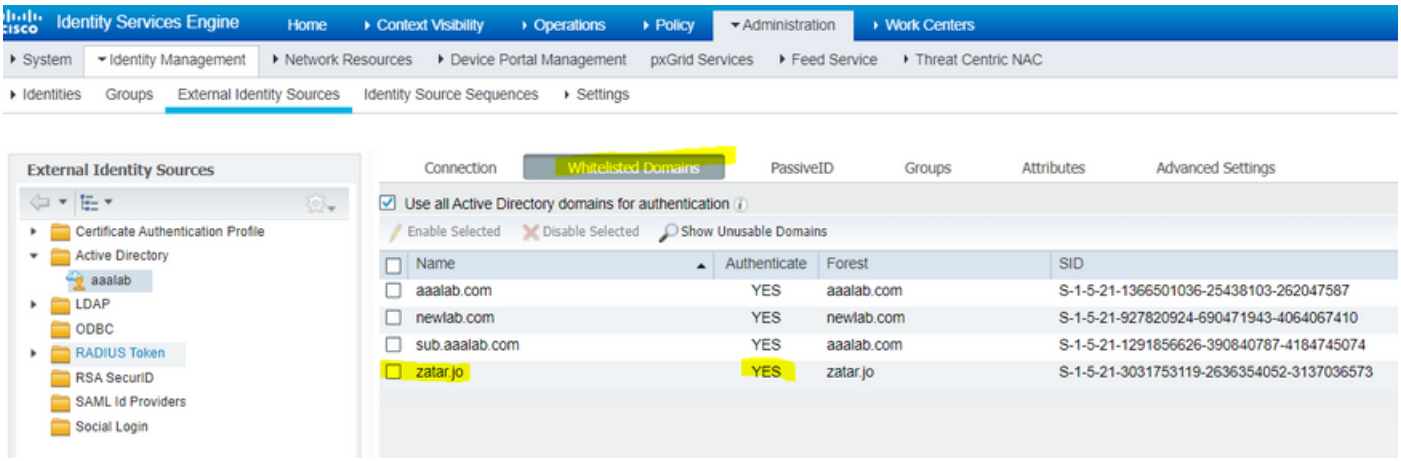


2단계. 아래와 같이 두 Active Directory 간에 양방향 트러스트가 활성화되었는지 확인합니다.

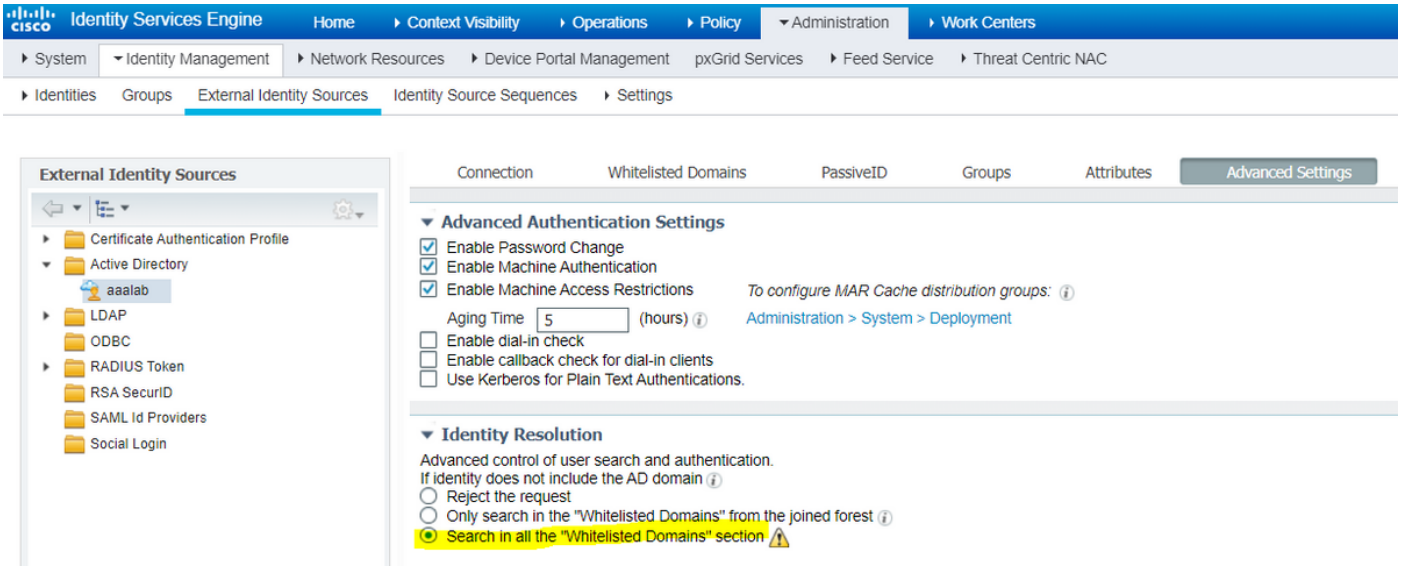
1. Active Directory 도메인 및 트러스트 스냅인을 엽니다.
2. 왼쪽 창에서 트러스트를 추가할 도메인을 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
3. Trust 탭을 클릭합니다.
4. New Trust(새 신뢰) 버튼을 클릭합니다.
5. 새 트러스트 마법사가 열리면 다음을 클릭합니다.
6. AD 도메인의 DNS 이름을 입력하고 Next(다음)를 클릭합니다.
7. AD 도메인을 DNS를 통해 확인할 수 있다고 가정하면 다음 화면에서 Direction of Trust를 요청합니다.양방향 을 선택하고 다음을 클릭합니다.
8. Outgoing Trust Properties(발신 신뢰 속성)에서 인증할 모든 리소스를 선택하고 Next(다음)를 클릭합니다.
9. 트러스트 암호를 입력하고 다시 입력하고 Next(다음)를 클릭합니다.
10. 다음을 두 번 클릭합니다.

참고:AD 컨피그레이션은 Cisco 지원 범위를 벗어납니다. 문제가 발생할 경우 Microsoft 지원이 참여할 수 있습니다.

이를 구성하면 예제 AD(aaalab)가 새 AD(zatar.jo)와 통신할 수 있으며 아래 "화이트리스트된 도메인" 탭에 팝업되어야 합니다.표시되지 않으면 다음과 같은 양방향 트러스트 구성이 올바르지 않습니다.



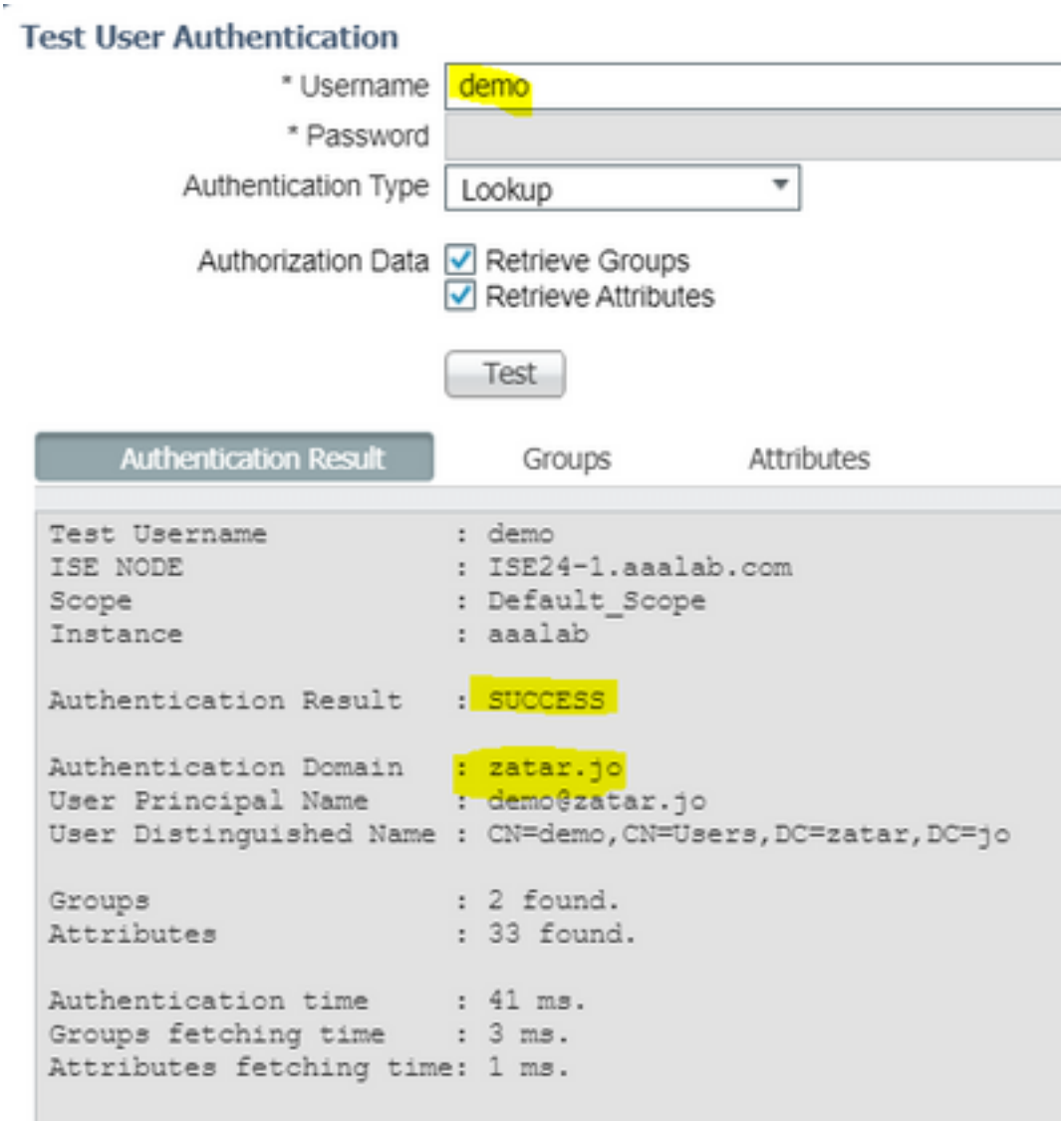
3단계. 아래와 같이 **"화이트리스트 도메인" 섹션**의 **모든** 옵션 **검색**이 활성화되었는지 확인합니다.양방향 트러스트된 도메인을 포함한 모든 화이트리스트 도메인에서 검색을 허용합니다.결합된 **포리스트의 "허용 목록에 있는 도메인"에서만 검색** 옵션이 활성화된 경우 기본 도메인의 "하위" 도메인에서만 검색됩니다.{ 하위 도메인 예:} 위의 스크린샷에서 sub.aalab.com을 참조하십시오.



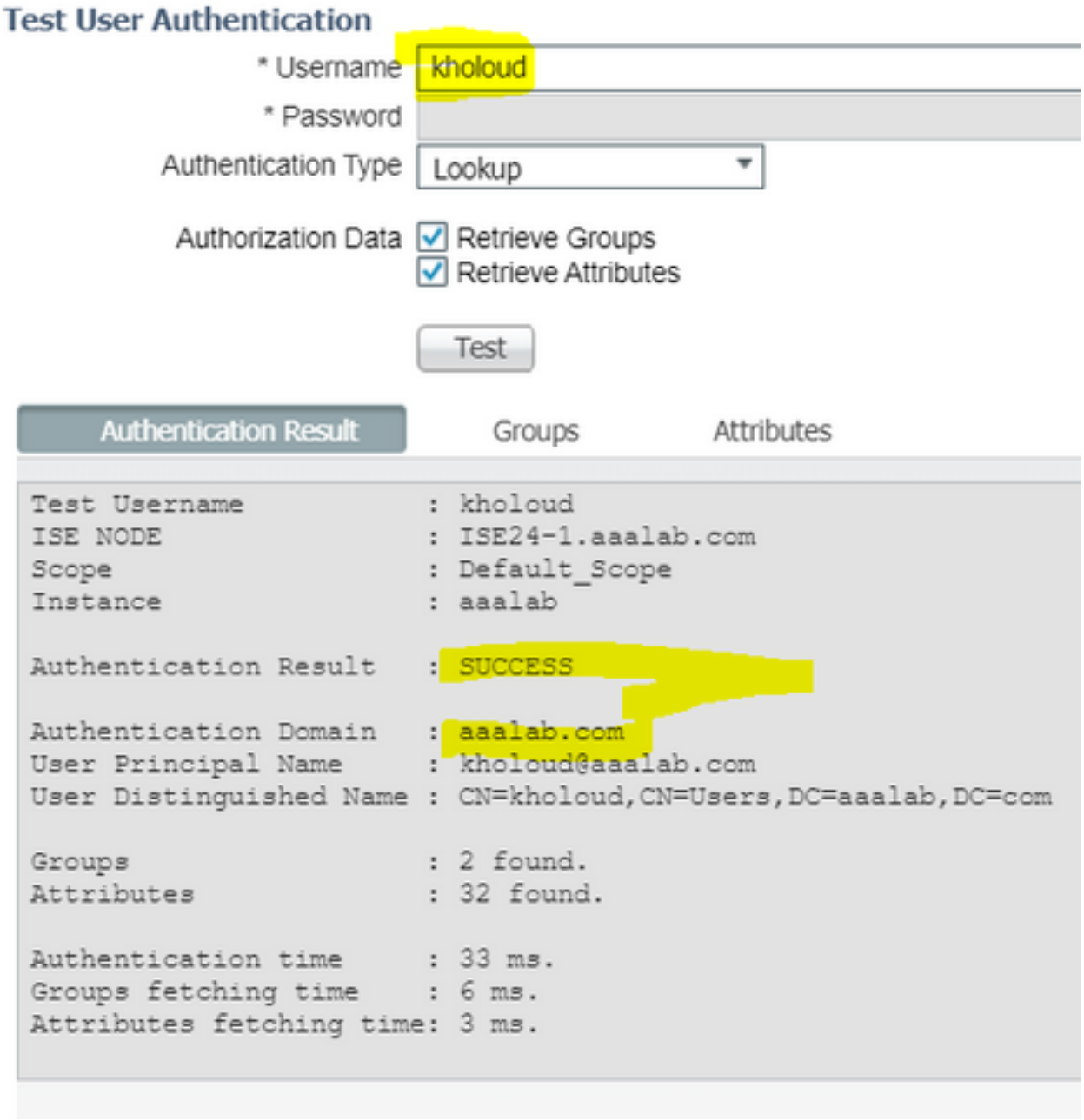
이제 ISE는 aaaalab.com 및 zatar.com에서 사용자를 검색할 수 있습니다.

다음을 확인합니다.

"test user" 옵션을 통해 작동하는지 확인하고 "zatar.jo" 도메인에 있는 사용자를 사용하십시오(이 예에서는 "demo" 사용자가 "zatar.jo" 도메인에만 있고 "aaalab.com"에 있지 않고 테스트 결과는 아래와 같습니다).



aaalab.com의 사용자도 작동하며, 사용자 khoud는 aaalab.com에 있습니다.



문제 해결

대부분의 AD/양방향 신뢰 문제를 트러블슈팅하는 두 가지 주요 절차, 심지어 대부분의 외부 ID 인증도 있습니다.

1.디버그가 활성화된 ISE 로그(지원 번들) 수집이 지원 번들의 특정 폴더에서 AD에서 인증 시도에 대한 모든 세부 정보를 찾을 수 있습니다.

2 .ISE와 AD 간에 패킷 캡처를 수집하는 중입니다.

1단계.ISE 로그 수집:

a.디버그를 활성화하고 다음 디버그를 "trace"로 설정합니다.

- Active Directory(ad_agent.log)
- identity-store-AD(ad_agent.log)
- runtime-aaa(prrt-server.log)

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

b.문제를 재현하고 문제가 있는 사용자와 연결합니다.

c. 지원 번들을 수집합니다.

작업 시나리오 "로그":

참고:인증 시도에 대한 세부 정보는 ad_agent.log 파일에서 확인할 수 있습니다.

ad_agent.log 파일에서:

zatar 양방향 트러스트 연결 확인:

```
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
```

주 도메인 aaalab에서 사용자 "demo"를 검색하는 중:

```
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
```

(데모 사용자는 zatar 도메인에 있지만 ise는 aaalab 도메인에서 먼저 확인한 다음 "화이트리스트" 도메인 탭(예: newlab.com)에서 다른 도메인을 확인합니다.주 도메인에서 체크하지 않고 zatar.jo를 직접 체크 인하려면 UPN 접미사를 사용하여 ISE에서 검색 위치를 파악해야 하므로 사용자는 다음 형식으로 로그인해야 합니다.demo.zatar.jo).

zatar.jo에서 "demo" 사용자 검색

```
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
```

zatar 도메인에 있는 사용자 "demo":

```
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"
```

2단계. 캡처 수집:

a.ISE와 AD/LDAP 간에 교환되는 패킷은 암호화되므로, 먼저 해독 없이 캡처를 수집하면 읽을 수 없습니다.

ISE AD ( ):

1. ISE . ID -> Active Directory -> ->
2. ISE .
3. 'Name' .TROUBLESHOOTING.EncryptionOffPeriod.
4. 'Value' () .

< ()>

30 :

30

5. . .

6. ' ' .

7. 'Active Directory ' .

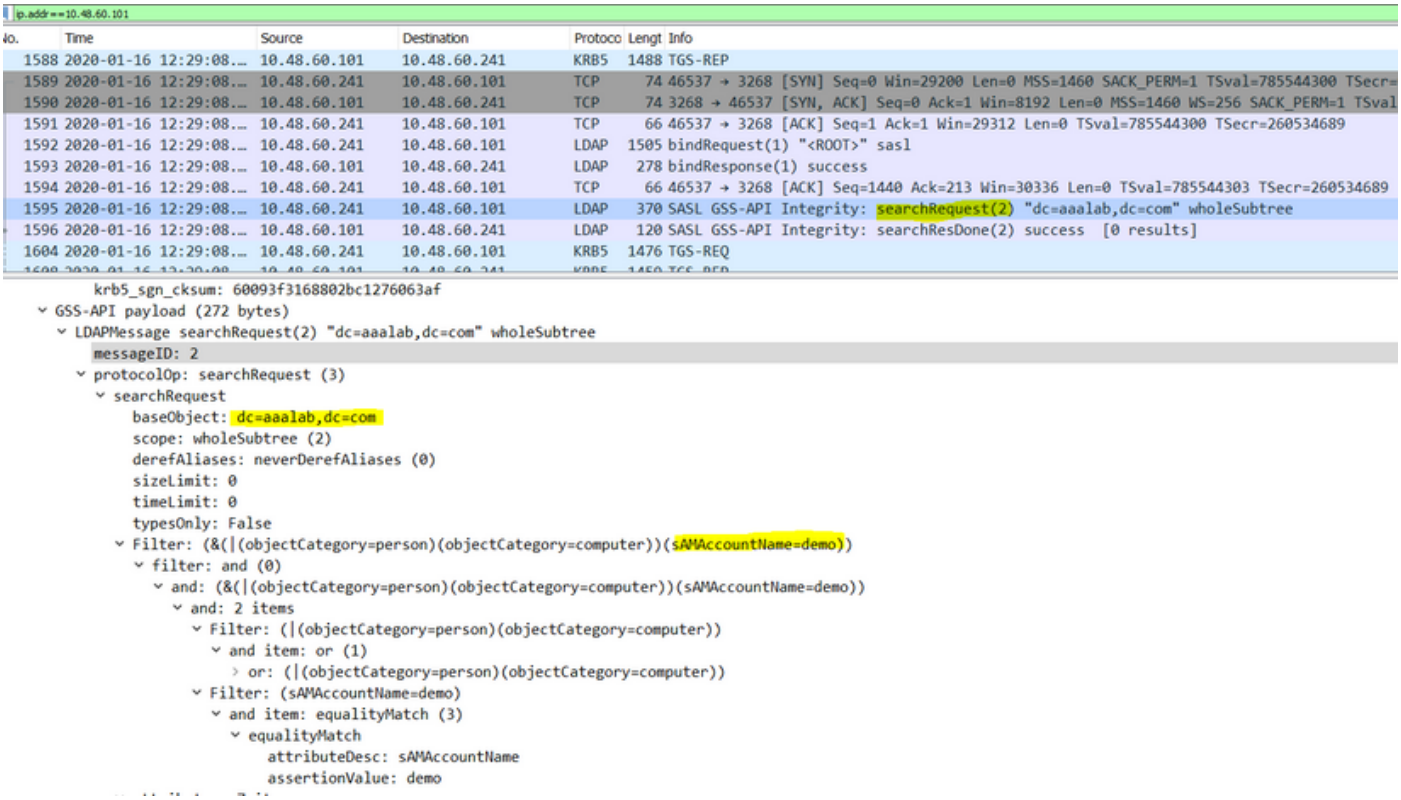
8. 10 .

b.ISE에서 캡처를 시작합니다.

c.문제를 재현합니다.

d.캡처를 중지하고 다운로드합니다.

작업 시나리오 "로그":



다음을 확인합니다.

다음은 발생할 수 있는 작업 및 비작업 상황과 이러한 상황이 생성하는 로그의 몇 가지 예입니다.

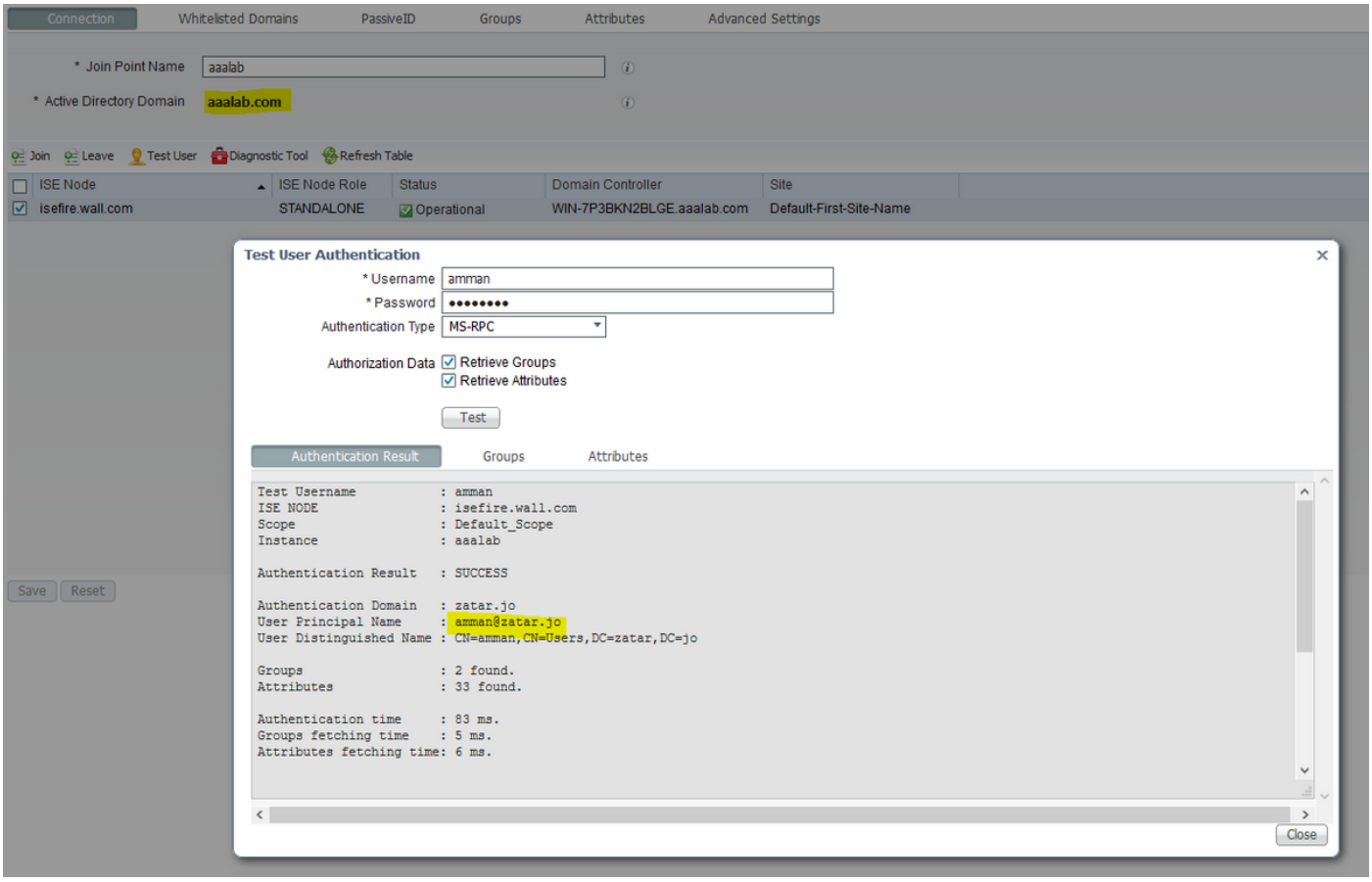
1. AD "zatar.jo" 그룹을 기반으로 한 인증

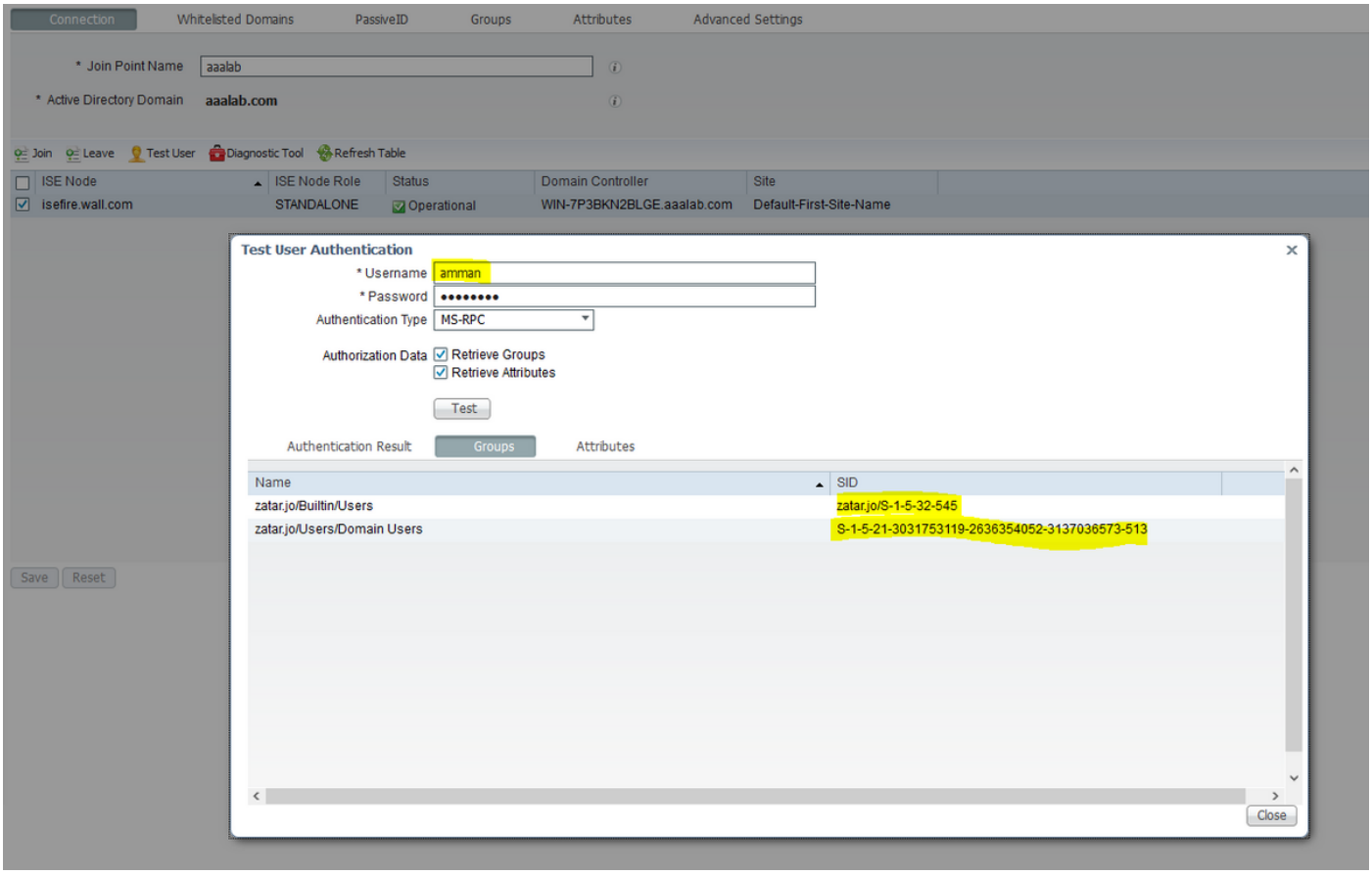
그룹이 그룹 탭에서 검색되지 않으면 다음 로그 메시지가 표시됩니다.

```
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
```

Groups(그룹) 탭에서 zatar.jo에서 그룹을 검색해야 합니다.

AD 탭에서 AD 그룹 검색 확인:





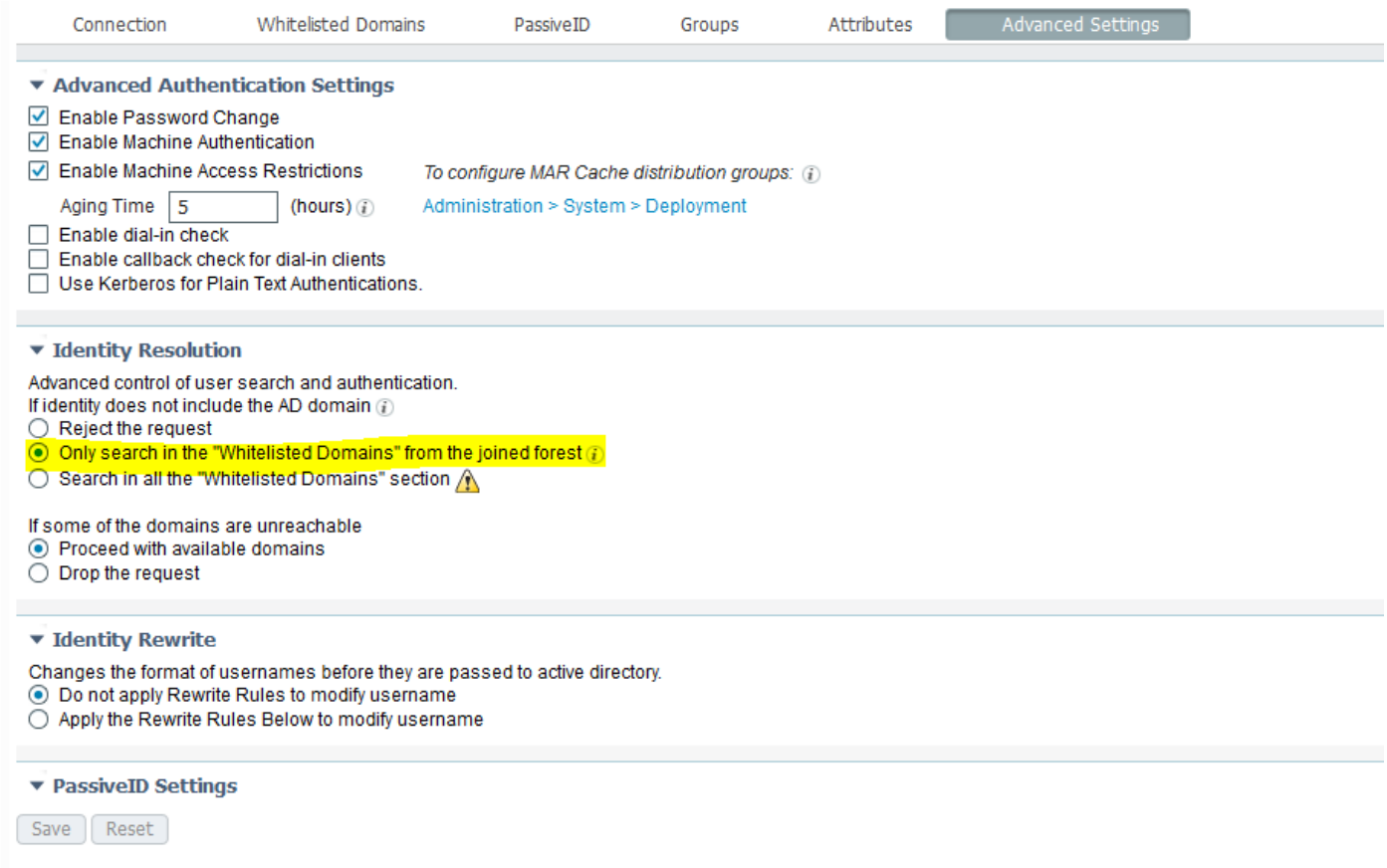
로그 AD_agent.log에서 작업 시나리오:

```
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"
}
}
```

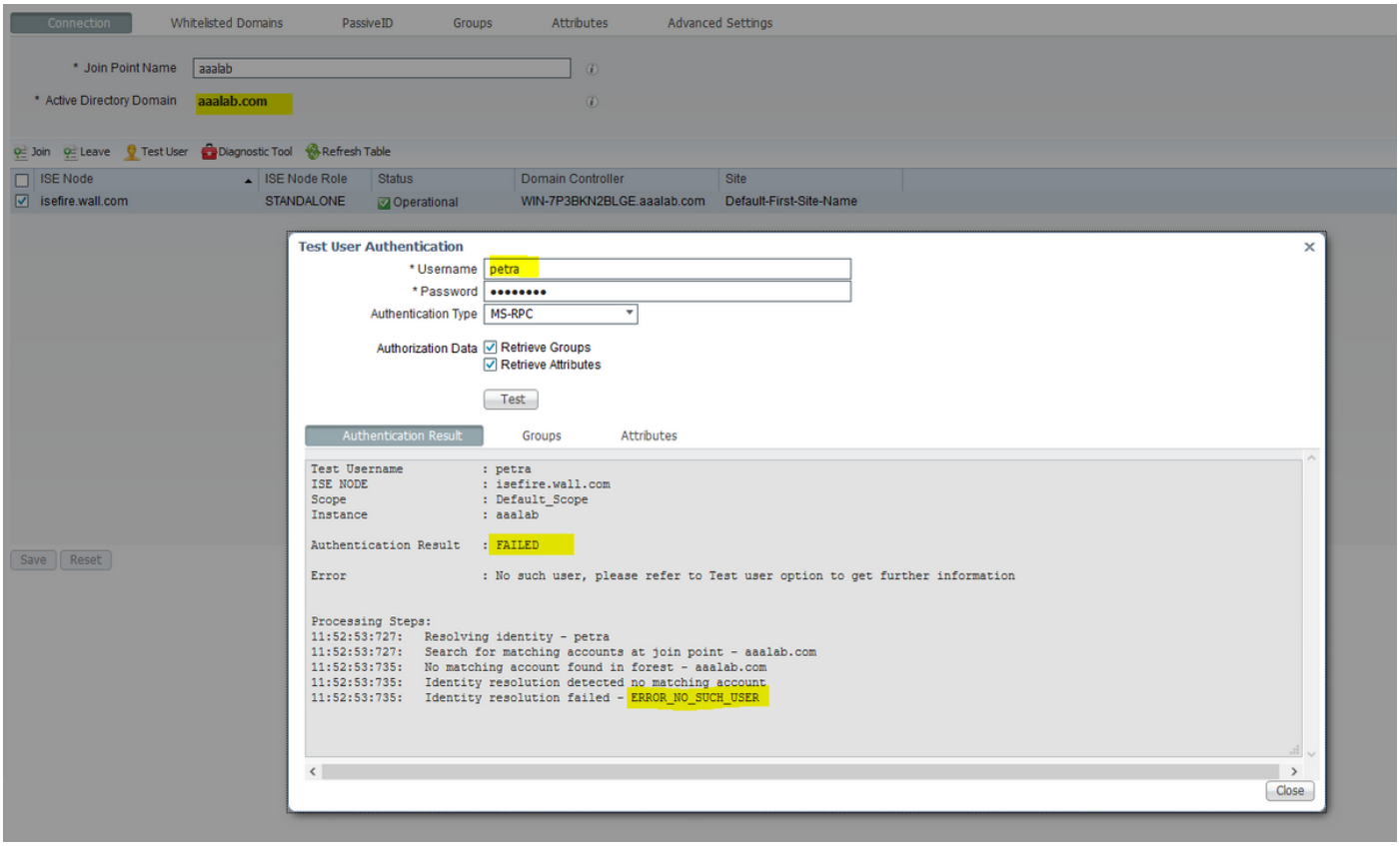
2. "조인된 포리스트에서 "허용 목록에 있는 도메인"에서만 검색"을 선택한 경우



"Only search in the "Whitelist Domains" from the joined forest(연결된 포리스트에서 "화이트리스트에 있는 도메인" 검색만)" 옵션을 선택하면 ISE는 이들을 오프라인으로 표시합니다.

```
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
```

"petra" 사용자는 zatar.jo에 있으며 아래 스크린샷과 같이 인증에 실패합니다.



로그에서:

고급 옵션 "Only search in the "Whitelist Domains" from the joined forest(연결된 포리스트에서 "화이트리스트에 있는 도메인"만 검색)" 때문에 ISE가 다른 도메인에 연결할 수 없습니다.

```
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
```