ISE und Zwei-Wege-Trust-AD-Konfiguration

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konfigurieren](#)
[Überprüfen](#)
[Fehlerbehebung](#)
[Überprüfen](#)

Einführung

In diesem Dokument wird die Definition von "Two-Way-Trust" für die ISE beschrieben, und es wird ein einfaches Konfigurationsbeispiel gezeigt: die Authentifizierung eines Benutzers, der nicht im AD vorhanden ist, der der ISE beigetreten ist, aber in einem anderen AD vorhanden ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, grundlegende Kenntnisse in folgenden Bereichen zu erwerben:

- ISE 2.x- und Active Directory-Integration
- Externe Identitätsauthentifizierung auf der ISE.

Verwendete Komponenten

- ISE 2.x
- zwei aktive Verzeichnisse.

Konfigurieren

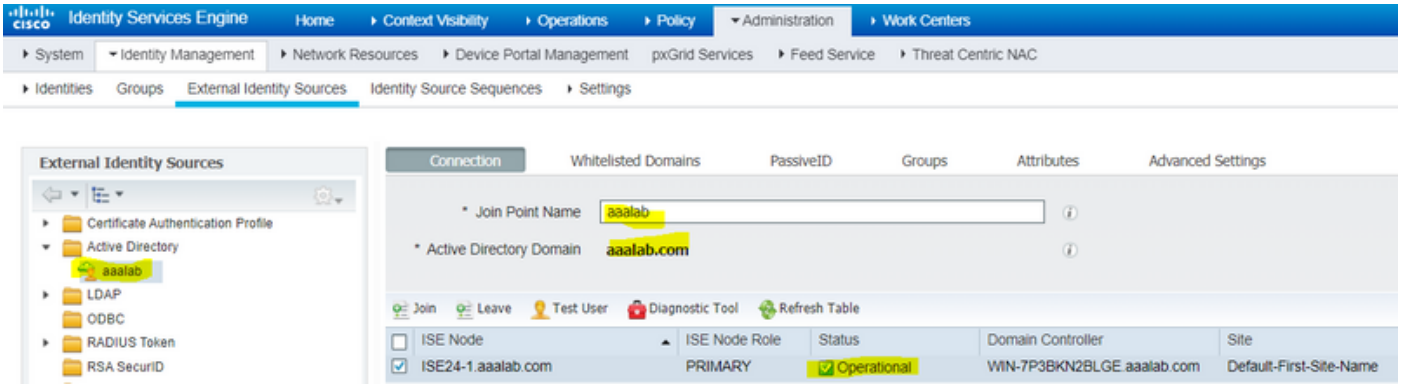
Um Ihre Domäne zu erweitern und andere Benutzer in eine andere Domäne als die Domäne einzubinden, die bereits der ISE beigetreten ist, haben Sie zwei Möglichkeiten:

1. können Sie die Domäne manuell und separat auf der ISE hinzufügen. Dadurch würden Sie zwei separate aktive Verzeichnisse haben.
2. Nehmen Sie an einer AD-zu-ISE teil, und konfigurieren Sie dann **Zwei-Wege-Vertrauenswürdigkeit** zwischen dieser AD und der zweiten AD, ohne sie der ISE hinzuzufügen. Dies ist in der Regel eine Zwei-Wege-Trust-Konfiguration. Sie ist eine Option, die zwischen zwei oder mehr aktiven Verzeichnissen konfiguriert wird. Die ISE erkennt diese vertrauenswürdigen Domänen automatisch mithilfe des AD-Connectors und fügt sie den

"Whitelisted Domains" hinzu und behandelt sie als separate ADs, die der ISE hinzugefügt werden. Auf diese Weise können Sie einen Benutzer im AD "zatar.jo" authentifizieren, das nicht zur ISE gehört.

Die folgenden Schritte beschreiben das Konfigurationsverfahren für ISE und AD:

Schritt 1. Stellen Sie sicher, dass die ISE AD zugeordnet ist. In diesem Beispiel haben Sie die Domäne aalab:

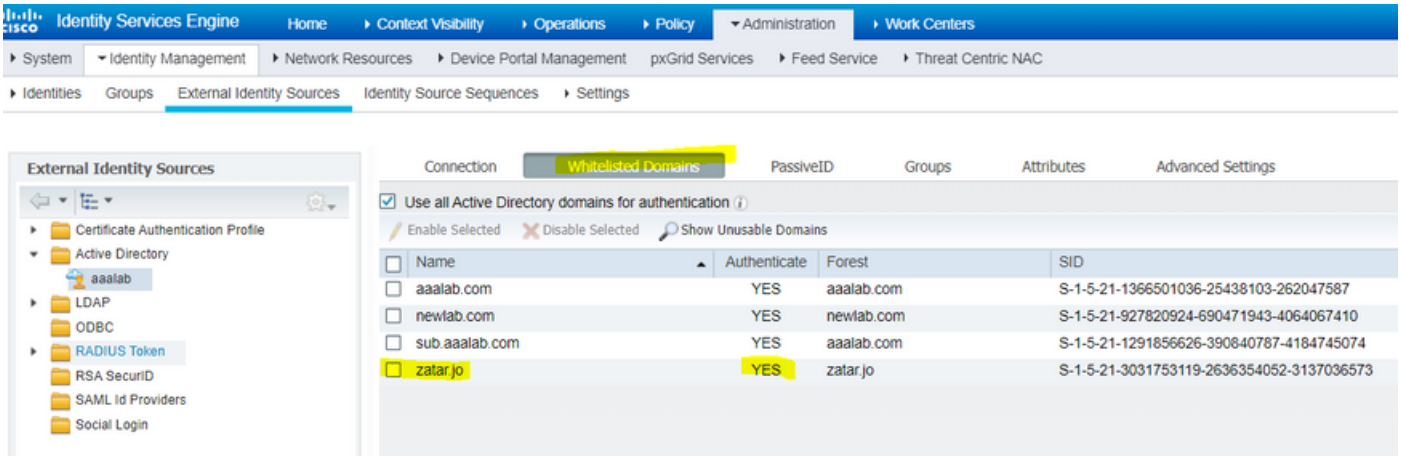


Schritt 2. Stellen Sie sicher, dass die Zwei-Wege-Vertrauenswürdigkeit zwischen beiden aktiven Verzeichnissen aktiviert ist (siehe unten):

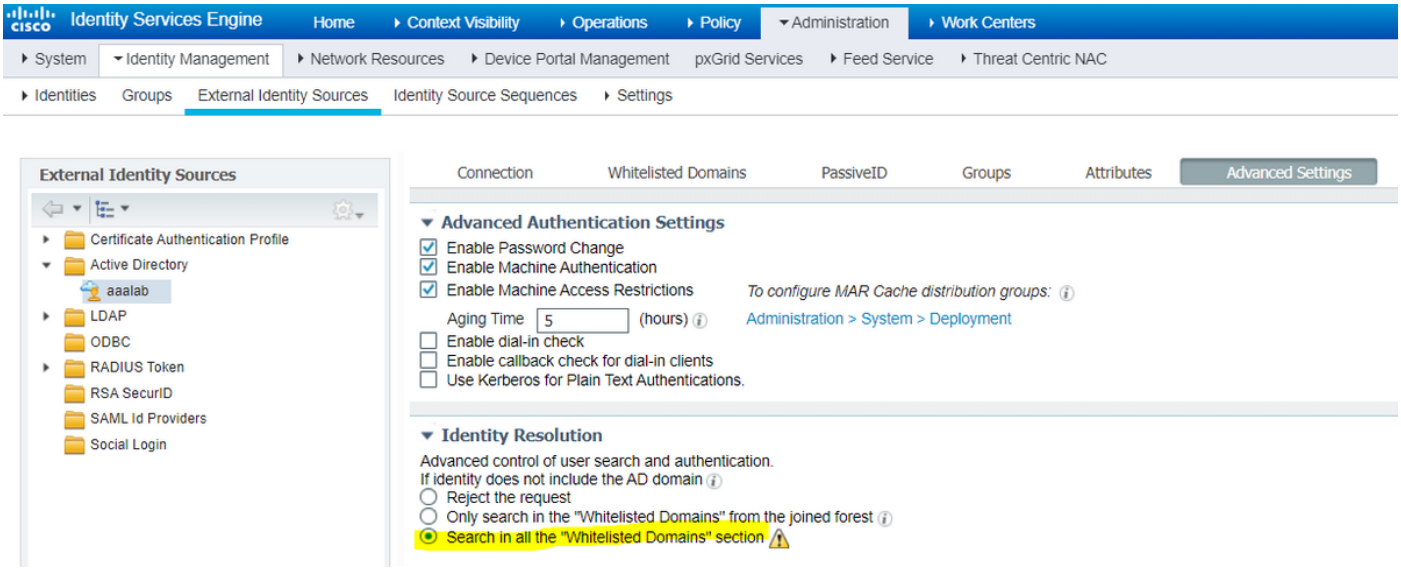
1. Öffnen Sie das Snap-In Active Directory-Domänen und Trusts.
2. Klicken Sie im linken Bereich mit der rechten Maustaste auf die Domäne, der Sie eine Vertrauenswürdigkeit hinzufügen möchten, und wählen Sie Eigenschaften aus.
3. Klicken Sie auf die Registerkarte Trusts.
4. Klicken Sie auf die Schaltfläche Neue Vertrauenswürdigkeit.
5. Wenn der Assistent für neue Vertrauenswürdigkeit geöffnet wurde, klicken Sie auf Weiter.
6. Geben Sie den DNS-Namen der AD-Domäne ein, und klicken Sie auf Weiter.
7. Wenn die AD-Domäne über DNS aufgelöst werden kann, wird im nächsten Bildschirm die Richtung der Vertrauenswürdigkeit gefragt. Wählen Sie Zwei-Wege aus, und klicken Sie auf Weiter.
8. Wählen Sie für die Eigenschaften der ausgehenden Vertrauenswürdigkeit alle zu authentifizierenden Ressourcen aus, und klicken Sie auf Weiter.
9. Geben Sie das Kennwort trust ein, und wiederholen Sie die Eingabe, und klicken Sie auf Weiter.
10. Klicken Sie zweimal auf Weiter.

Hinweis: Die AD-Konfiguration fällt nicht in den Support von Cisco, bei Problemen kann der Microsoft-Support aktiviert werden.

Sobald dies konfiguriert ist, kann das Beispiel AD (aalab) mit dem neuen AD (zatar.jo) kommunizieren und es sollte in der Registerkarte "Whitlested Domains" (Whitlested Domains) angezeigt werden, wie unten. Wenn sie nicht angezeigt wird, ist die Vertrauenskonfiguration in beide Richtungen falsch:



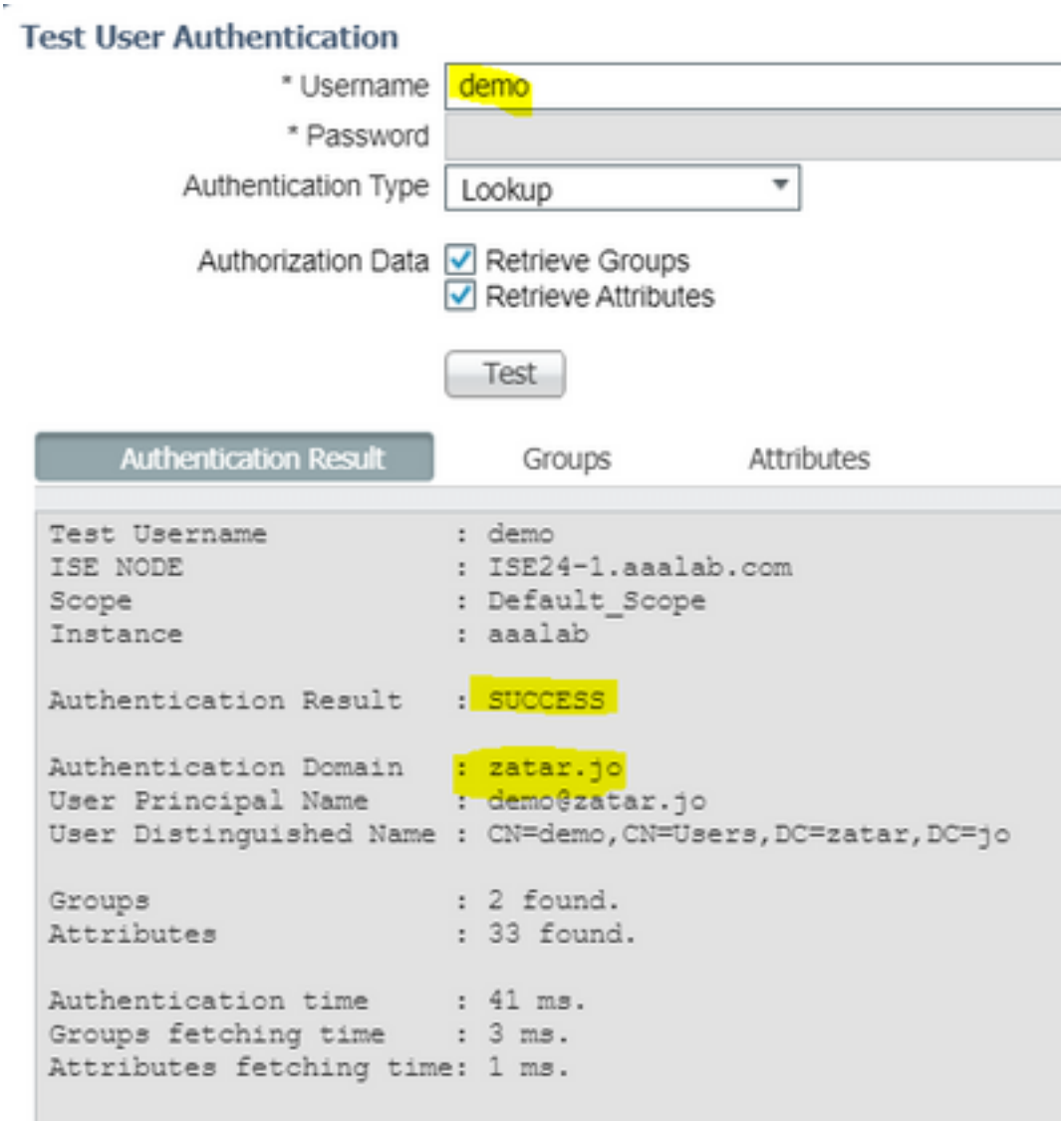
Schritt 3. Stellen Sie sicher, dass die Option **Search in allen "Whitlested Domains" Bereich** aktiviert ist, wie unten gezeigt. Es ermöglicht das Durchsuchen aller gehosteten Domänen, einschließlich bidirektionaler vertrauenswürdiger Domänen. Wenn die Option **Nur in den "Whitelisted Domains" aus dem verbundenen Wald suchen** aktiviert ist, wird nur in den "untergeordneten" Domänen der Hauptdomäne gesucht. Beispiel für eine untergeordnete Domäne: sub.aalab.com im Screenshot oben }.



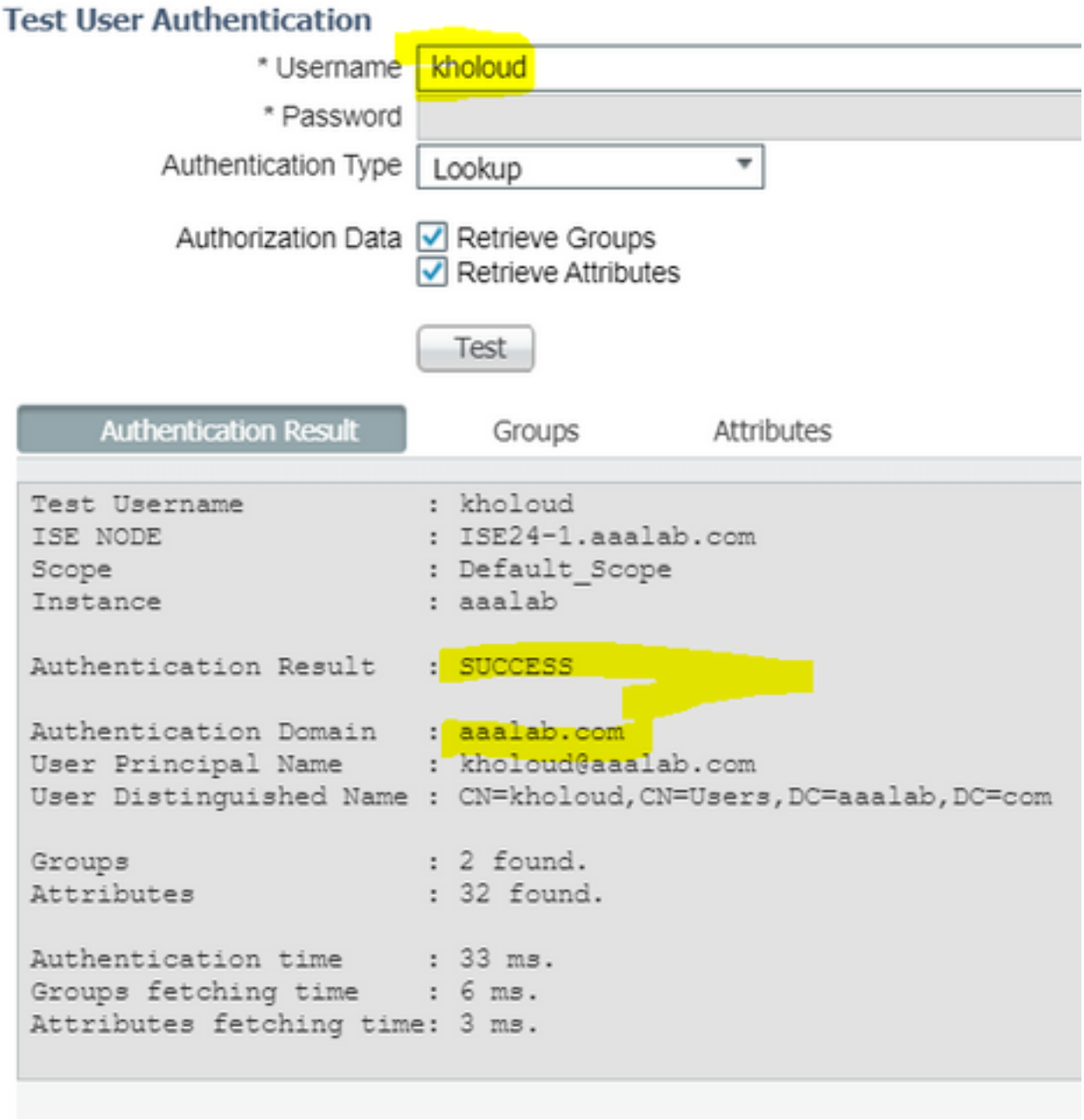
Jetzt kann die ISE in aaalab.com und zatar.com nach dem Benutzer suchen.

Überprüfen

Stellen Sie sicher, dass es über "Testbenutzer"-Option funktioniert, verwenden Sie den Benutzer, der sich in der Domäne "zatar.jo" befindet (in diesem Beispiel ist der Benutzer "demo" nur in der Domäne "zatar.jo" vorhanden, und es ist nicht in "aaalab.com", Testergebnis ist unten):



Beachten Sie, dass die Benutzer in aaalab.com auch arbeiten, Benutzer kholoud ist in aaalab.com:



Fehlerbehebung

Es gibt zwei Hauptverfahren zur Fehlerbehebung bei den meisten AD-/Zwei-Wege-Vertrauensproblemen, selbst bei den meisten Authentifizierungen für die externe Identität:

1. Sammeln von ISE-Protokollen (Support-Paket) mit aktiviertem Debugging. in bestimmten Ordnern in diesem Support-Paket finden Sie alle Details zu jedem Authentifizierungsversuch auf AD.

2. Sammeln von Paketerfassungen zwischen ISE und AD.

Schritt 1. Sammeln von ISE-Protokollen:

a) Aktivieren Sie die Debugging, und legen Sie die folgenden Debuggen auf "trace" fest:

- Active Directory (ad_agent.log)
- identity-store-AD (ad_agent.log)

- Runtime-AAA (prt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise-psc.log)

b) Reproduzieren Sie das Problem, und stellen Sie eine Verbindung zu einem problematischen Benutzer her.

c) Sammeln Sie ein Support-Paket.

Arbeitsszenario "Protokolle":

Hinweis: Details zu den Authentifizierungsversuchen finden Sie in der Datei ad_agent.log

aus der Datei ad_agent.log :

Überprüfung der Zwei-Wege-Vertrauenswürdigkeit der Zatar-Verbindung:

```
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
```

Suche nach dem Benutzer "demo" in der Hauptdomäne aalab:

```
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
```

(Hinweis: Demo-Benutzer ist in zatar Domain, wird aber ise überprüfen es zuerst in aalab Domain, dann andere Domänen in der "Whitlested"-Domain-Registerkarte, wie newlab.com. Um zu vermeiden, in der Haupt-Domäne zu wechseln und um zatar.jo direkt einzuchecken, müssen Sie das UPN-Suffix verwenden, damit die ISE weiß, wo gesucht werden soll. Der Benutzer sollte sich also in diesem Format anmelden: demo.zatar.jo).

Suche nach dem Benutzer "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
```

"Demo" des Benutzers in der zatar-Domäne gefunden:

```
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"
```

Schritt 2. Erfassung von Aufnahmen:

a) Die zwischen ISE und AD/LDAP ausgetauschten Pakete werden verschlüsselt, sodass sie nicht lesbar sind, wenn wir die Erfassungen ohne Entschlüsselung zunächst sammeln.

Um Pakete zwischen ISE und AD zu entschlüsseln (dieser Schritt muss vor dem Erfassen und Anwenden des Versuchs angewendet werden):

1. Auf der ISE navigieren Sie zur Registerkarte : External-ID-Stores -> Active Directory -> Advanced Tools -> Advanced Tuning
2. Wählen Sie Ihren ISE-Knoten aus.
3. Das Feld 'Name' erhält eine bestimmte Fehlerbehebungszeichenfolge: FEHLERBEHEBUNG.EncryptionOffPeriod.
4. Das Feld 'Wert' erhält die Anzahl der Minuten, für die Sie eine Fehlerbehebung durchführen möchten.

<positive Ganzzahl in Minuten>

Beispiel für eine halbe Stunde:

30

5. Geben Sie eine beliebige Beschreibung ein. Erforderlich vor dem nächsten Schritt.

6. Klicken Sie auf die Schaltfläche Wert aktualisieren.

7. Klicken Sie auf Active Directory Connector neu starten.

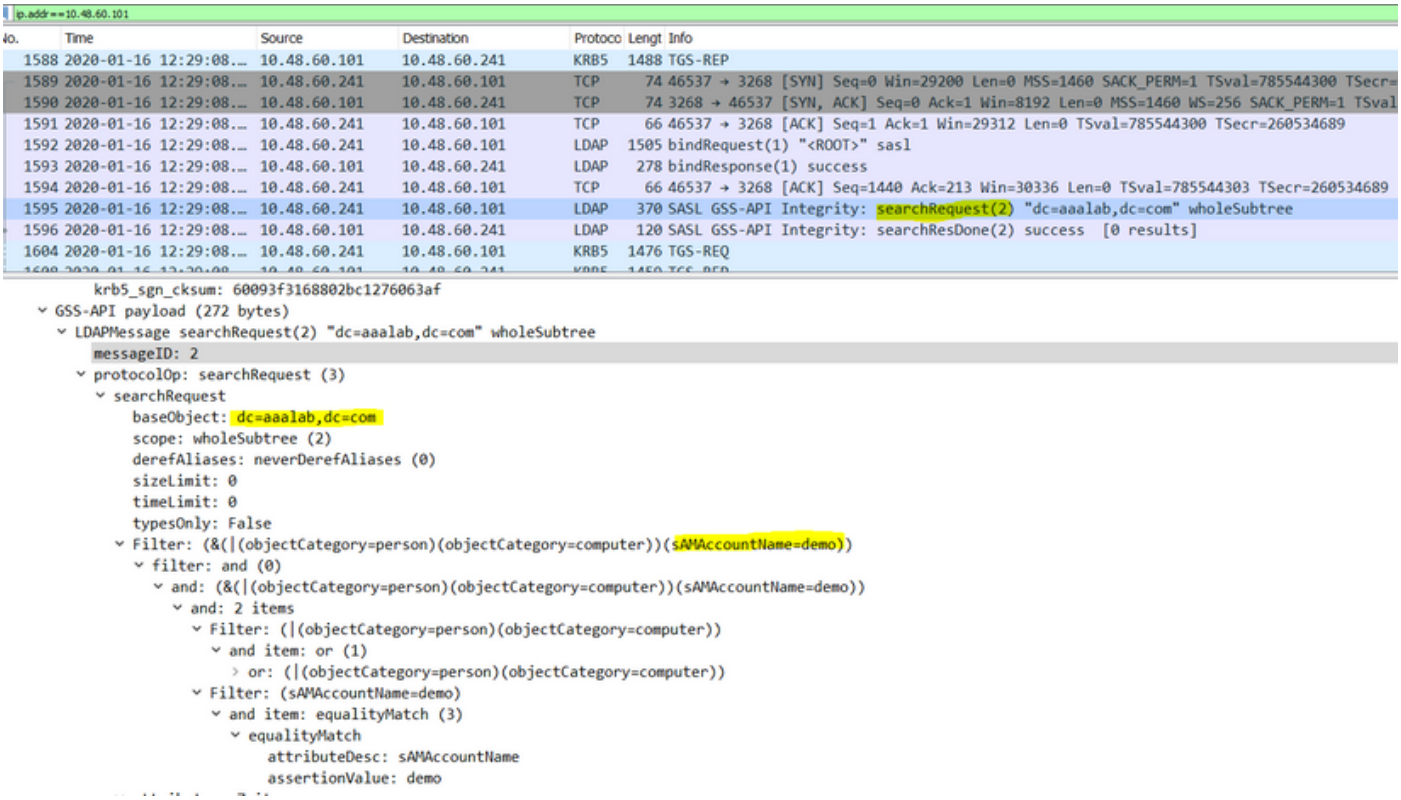
8. Warten Sie 10 Minuten, bis die Entschlüsselung Auswirkungen hat.

b) die Erfassung auf der ISE starten.

c) das Problem reproduzieren.

d) dann anhalten und die Erfassung herunterladen

Arbeitsszenario "Protokolle":



Überprüfen

Hier sind einige Beispiele für Arbeitssituationen und Arbeitssituationen, auf die Sie stoßen könnten, sowie die Protokolle, die diese Situationen erzeugen.

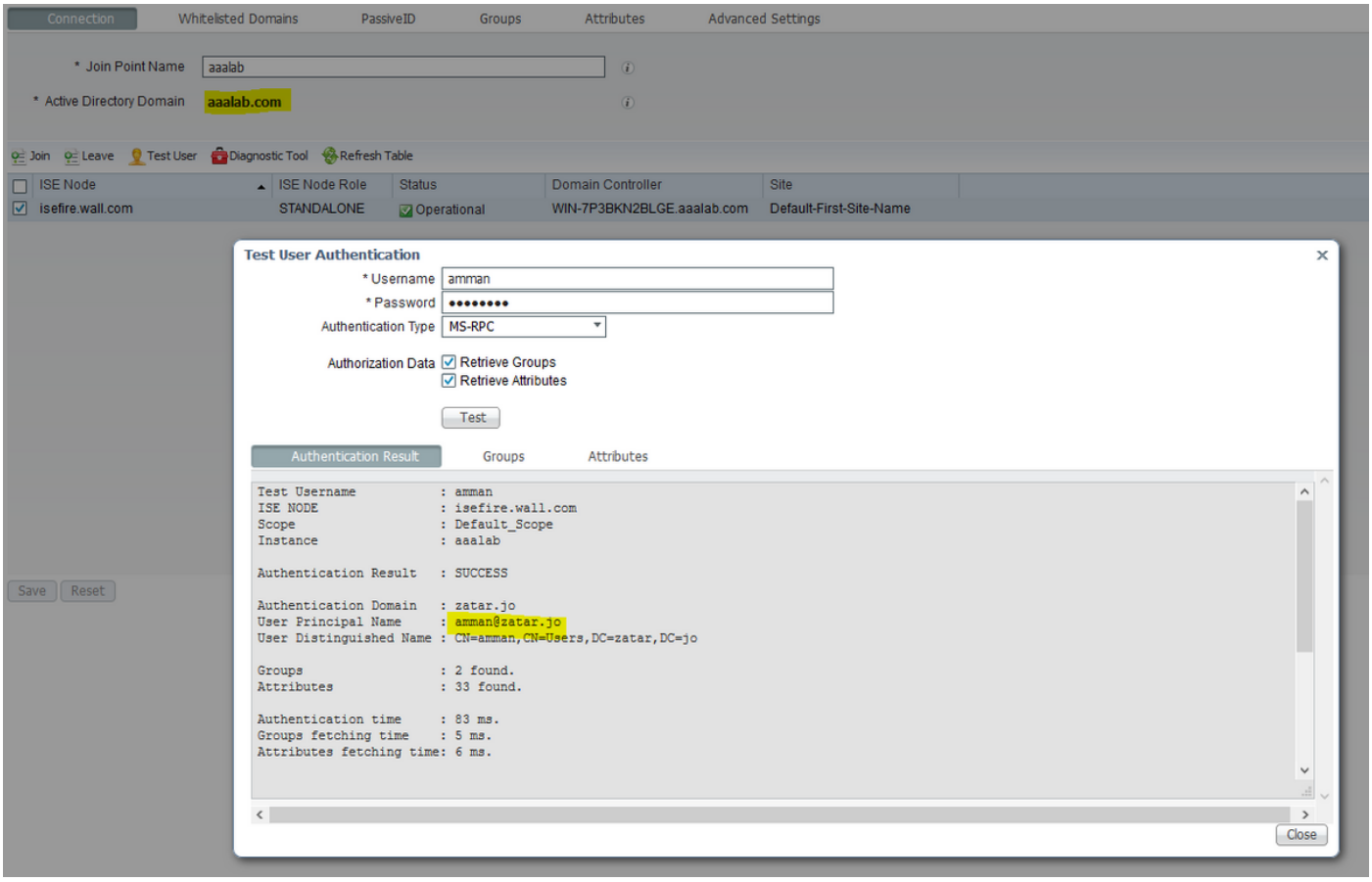
1. Authentifizierung basierend auf AD "zatar.jo"-Gruppen:

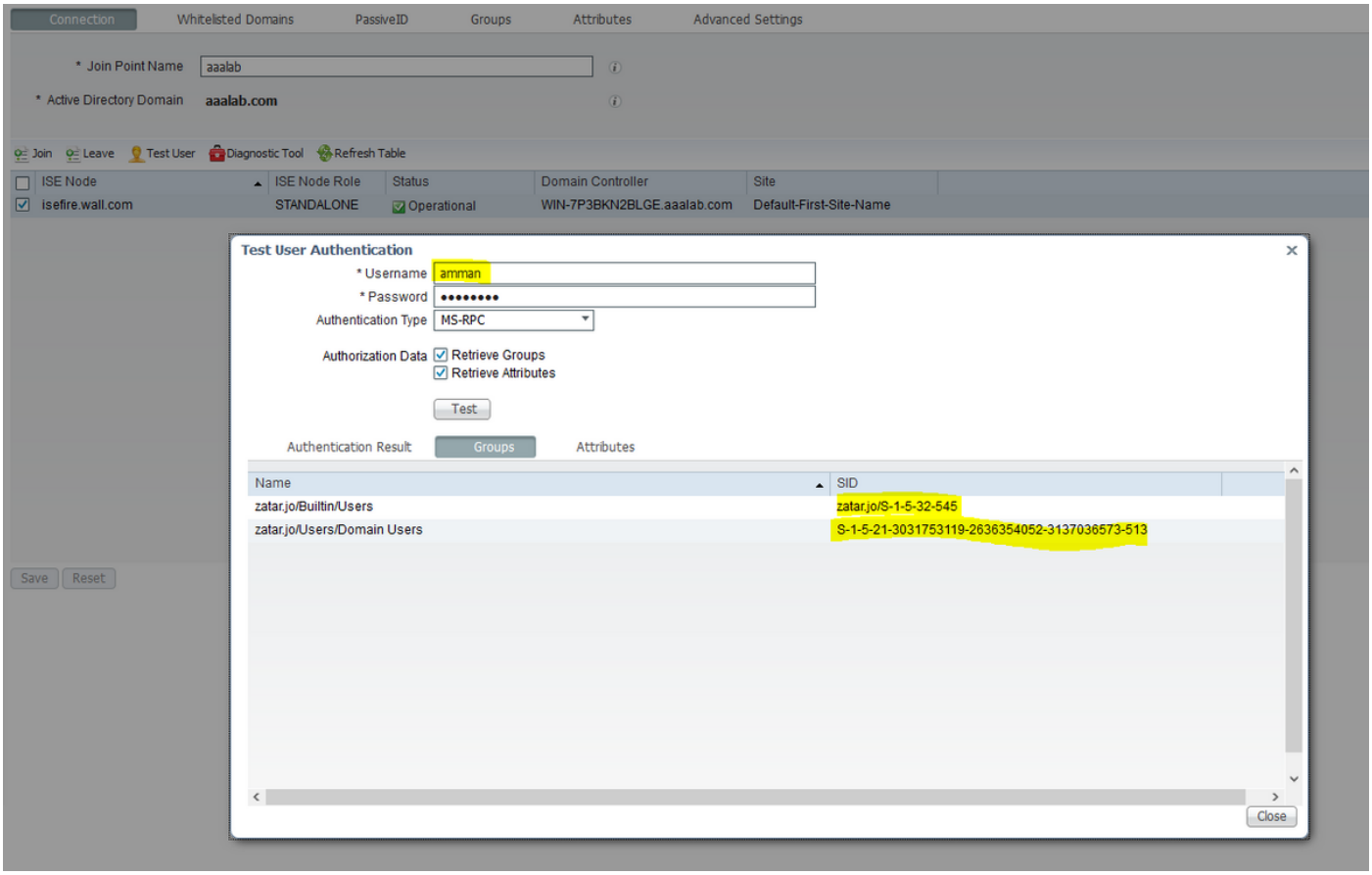
Wenn die Gruppe nicht von der Registerkarte "Gruppe" zurückgerufen wird, erhalten Sie die folgende Protokollmeldung:

```
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
```

Wir müssen die Gruppen in zatar.jo von der Registerkarte Gruppen abrufen.

Überprüfen von AD-Gruppenabrufen von der Registerkarte "AD":





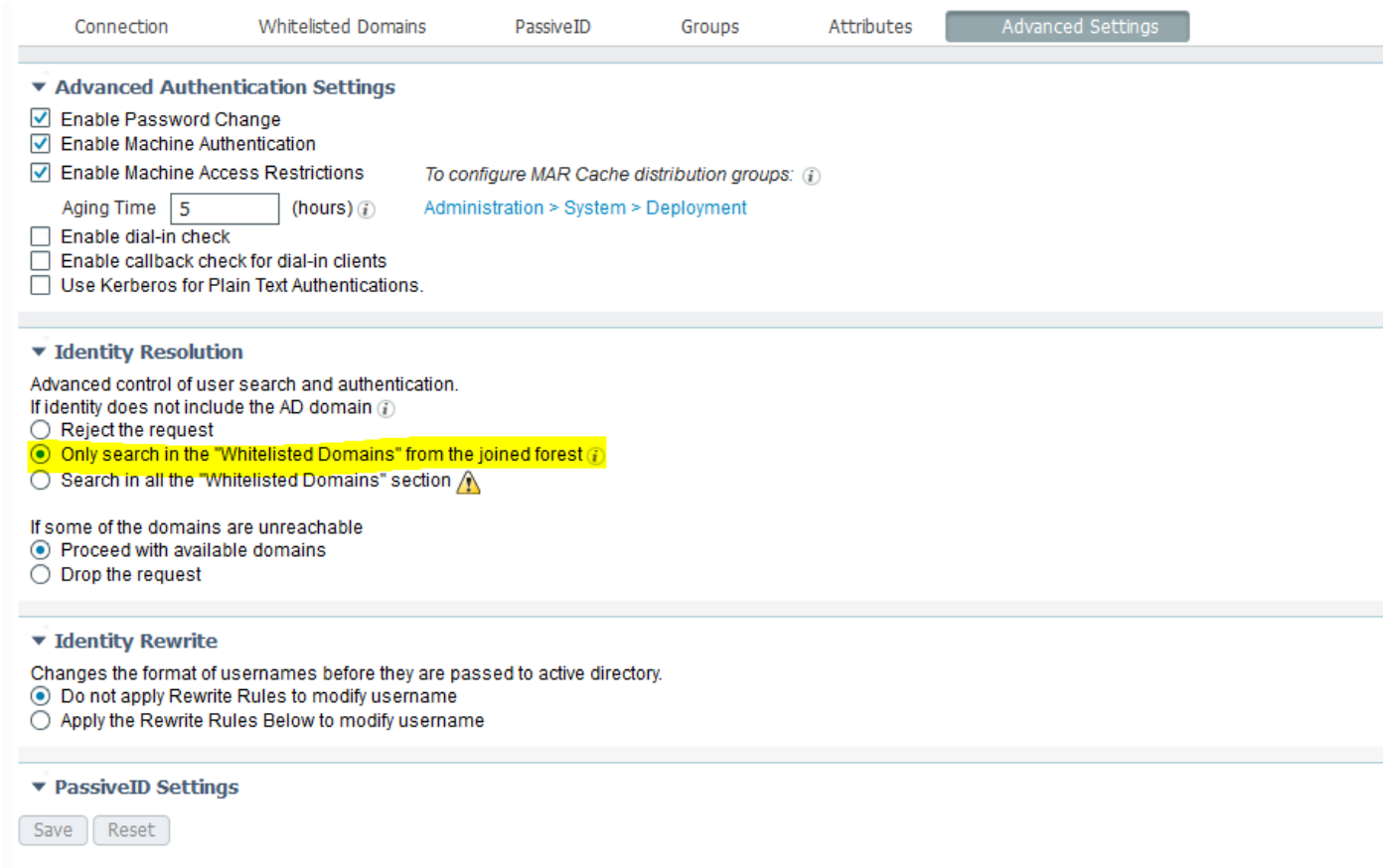
Arbeitsszenario Aus den Protokollen AD_agent.log:

```
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"
}
}
```

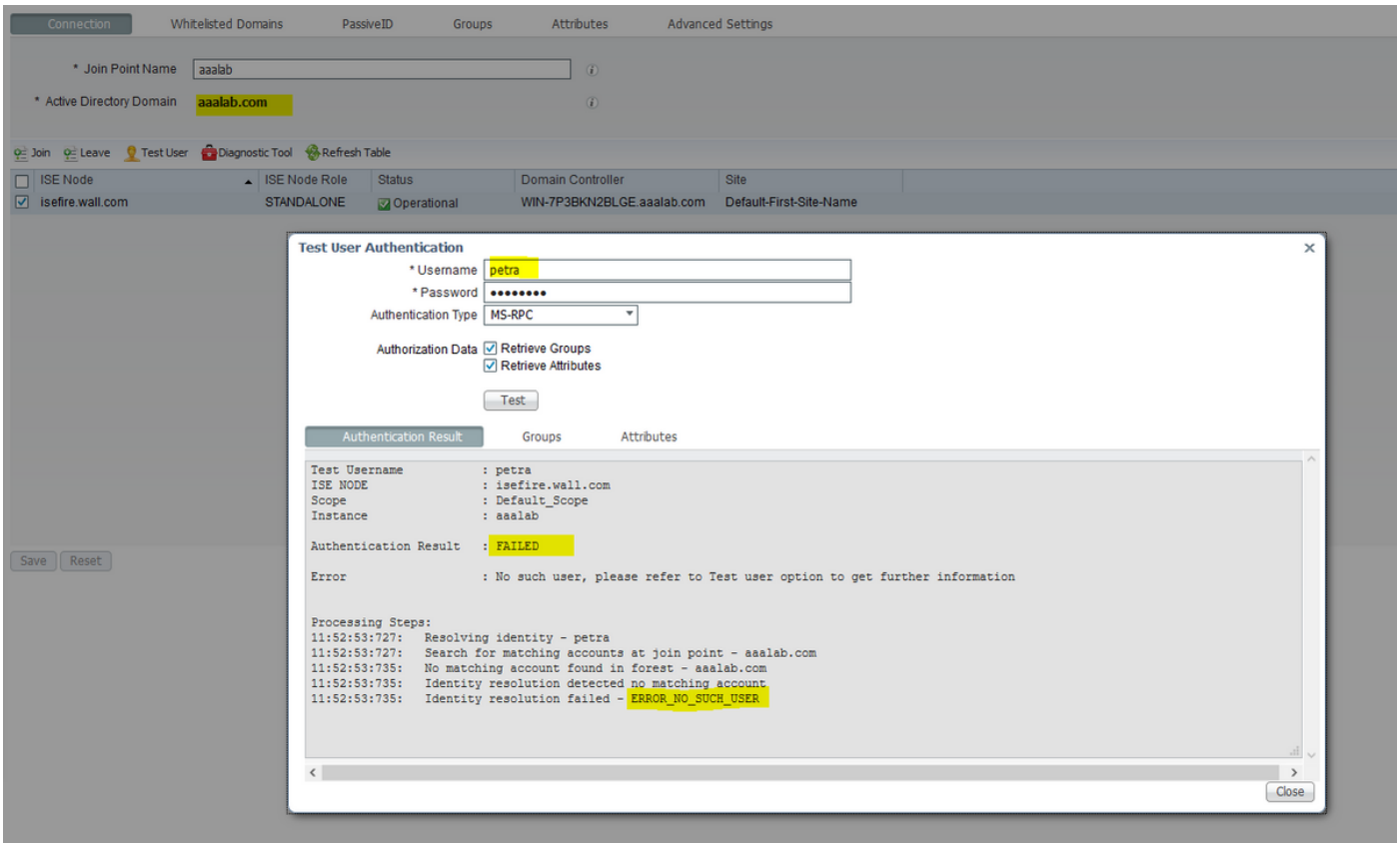
2. Wenn die Vorwärtsoption "Nur in den "Whitelisted Domains" (Whitelisted Domains) aus dem hinzugefügten Wald suchen" aktiviert ist:



Wenn Sie die Option "Nur in den "Whitelisted Domains" (Whitelisted Domains) aus dem hinzugefügten Wald suchen" (nur in Whitelisted Domains suchen) auswählen, markierte die ISE diese 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
```

Der Benutzer "petra" befindet sich in zatar.jo und kann die Authentifizierung nicht durchführen, wie im folgenden Screenshot dargestellt:



In den Protokollen:

Die ISE konnte aufgrund der erweiterten Option "Nur in den "Whitelisted Domains" aus dem verbundenen Wald suchen" keine anderen Domänen erreichen:

```
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
```