ISEおよび双方向の信頼AD設定

内容

概要

このドキュメントでは、ISEでの「双方向の信頼」の定義と、簡単な設定例（ISEの場合）について説明します。ADに存在しないユーザをISEに参加させる方法と、別のADに存在するユーザを認証する方法。

前提条件

要件

次の項目に関する基本的な知識があることが推奨されます。

- ISE 2.xとActive Directoryの統合（Active Directoryの統合）。
- ISEでの外部ID認証。

使用するコンポーネント

- ISE 2.x。
- 2つのActive Directory

設定

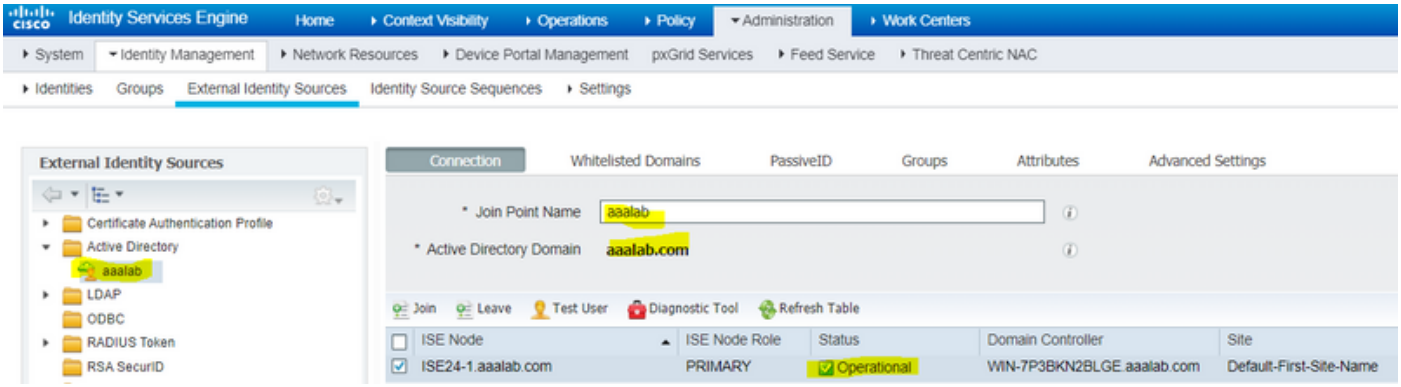
ドメインを拡張し、すでにISEに参加しているドメイン以外の別のドメインに他のユーザを含めるには、次の2つの方法があります。

1. ISEでドメインを手動で個別に追加できます。これにより、2つの別々のActive Directoryが作成されます。
2. 1つのADをISEに結合し、このADと**2つ目のADの間に双方向の信頼**を設定します。ISEに追加する必要はありません。これは主に双方向の信頼設定であり、複数のActive Directory間で設定されるオプションです。ISEは、ADコネクタを使用してこれらの信頼できるドメインを自動的に検出し、「ホワイトリストに登録されたドメイン」に追加し、それらをISEに結合された個別のADとして扱います。これは、ISEに参加していないAD「zatar.jo」でユーザを

認証する方法です。

次の手順では、ISEとADの両方の設定手順について説明します。

ステップ1:ISEがADに参加していることを確認します。この例では、ドメインaaalabが存在することを確認します。

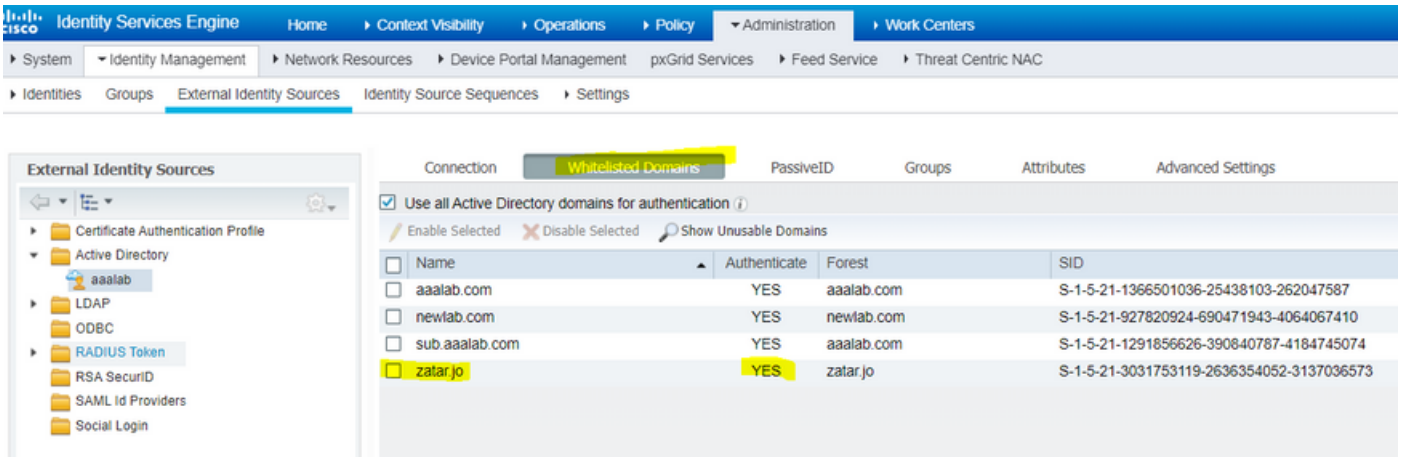


ステップ2：次に示すように、両方のActive Directory間で双方向の信頼が有効になっていることを確認します。

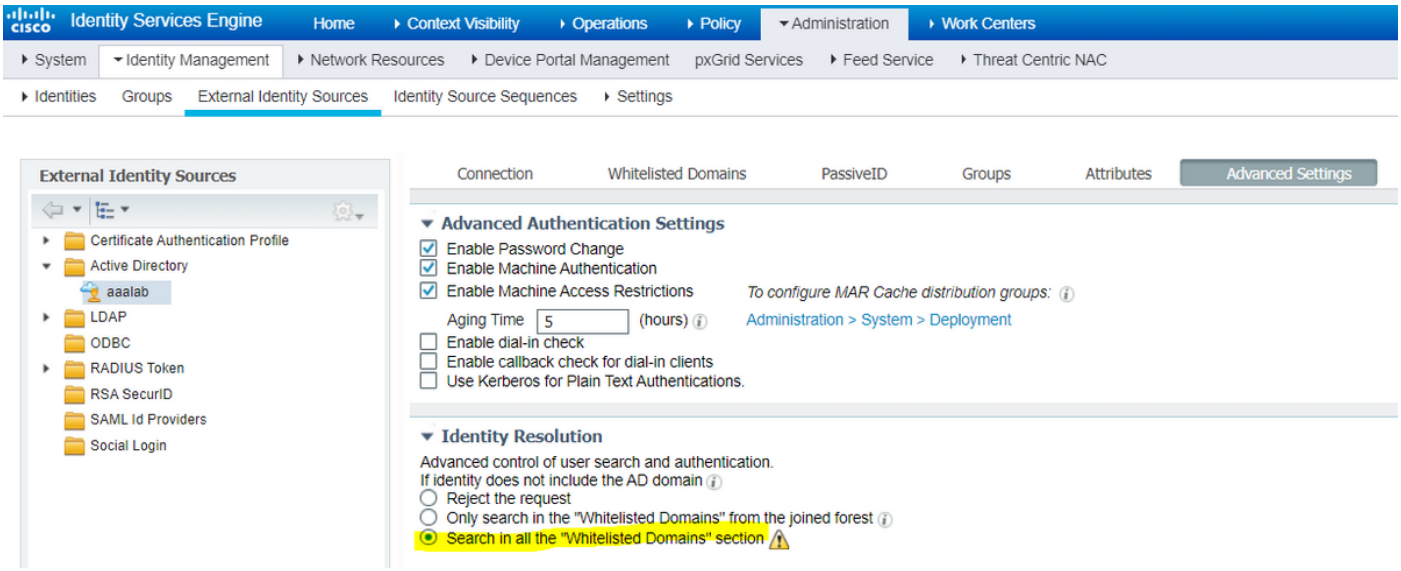
1. [Active Directory Domains and Trusts]スナップインを開きます。
2. 左側のペインで、信頼を追加するドメインを右クリックし、[プロパティ]を選択します。
3. [Trusts]タブをクリックします。
4. [New Trust]ボタンをクリックします。
5. 新しい信頼ウィザードが開いたら、[次へ]をクリックします。
6. ADドメインのDNS名を入力し、[Next]をクリックします。
7. ADドメインがDNS経由で解決できると仮定すると、次の画面で信頼方向を確認します。[Two-way]を選択し、[Next]をクリックします。
8. [Outgoing Trust Properties]で、認証するすべてのリソースを選択し、[Next]をクリックします。
9. 信頼パスワードを入力して再入力し、[Next]をクリックします。
10. [Next] を 2 回クリックします。

注：ADの設定はシスコのサポート範囲を超えており、問題が発生した場合はMicrosoftのサポートに参加できます。

これが設定されると、例のAD(aaalab)は新しいAD(zatar.jo)と通信できるようになり、次のように[whitlasted domains]タブにポップアップ表示されます。表示されない場合は、双方向の信頼設定が正しくありません（図2を参照）。



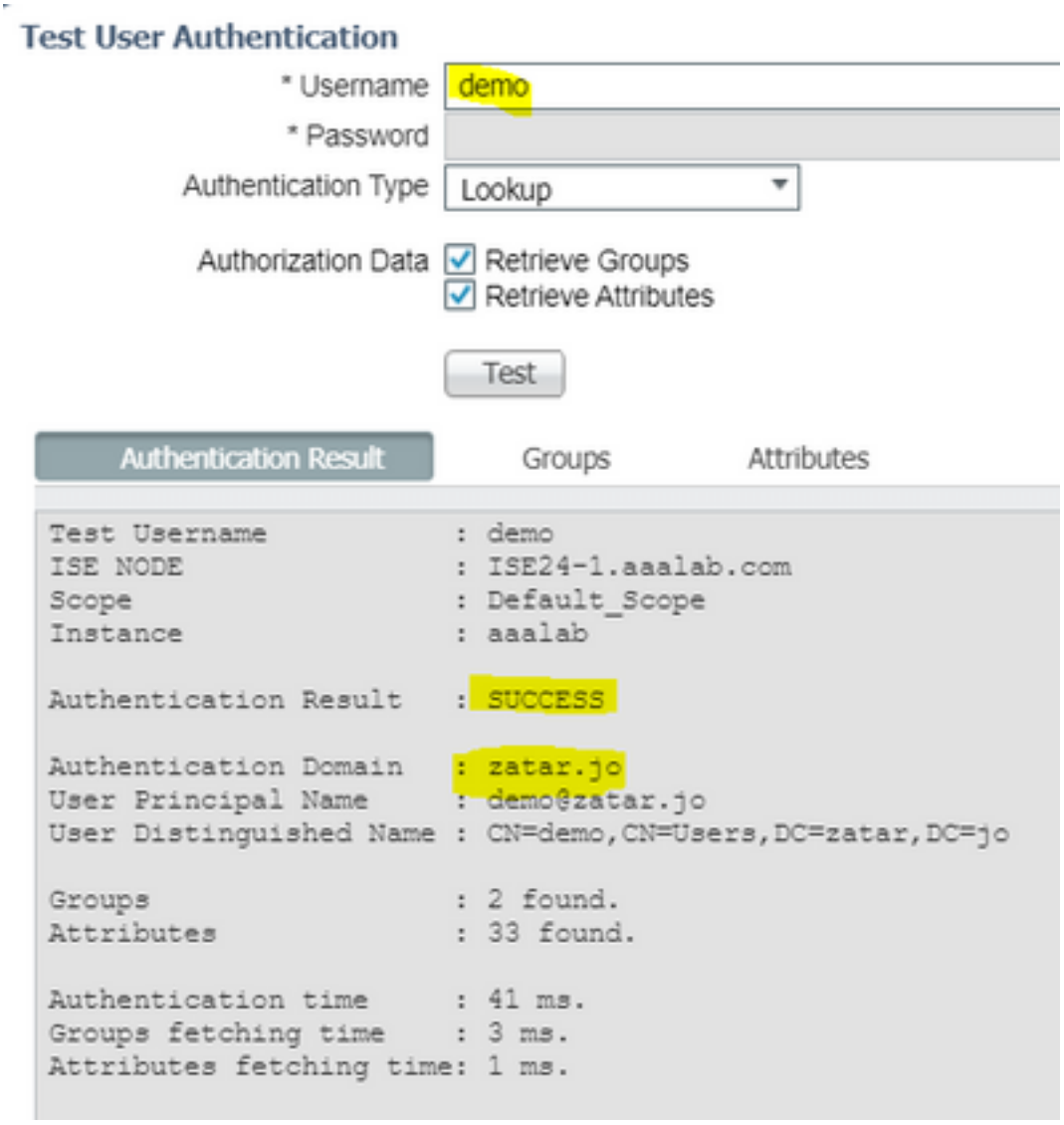
ステップ3:次に示すように、すべての「ホイット**トされたドメイン」セクションのオプション**検索が有効になっていることを確認します。双方向の信頼されたドメインを含むすべての信頼されたドメインを検索できます。[結合されたフォレストからホワイトリストに含まれるドメインのみを検索する]オプションが有効な場合は、メインドメインの"子"ドメインのみを検索します。{ child domain example:上のスクリーンショットのsub.aaalab.com }



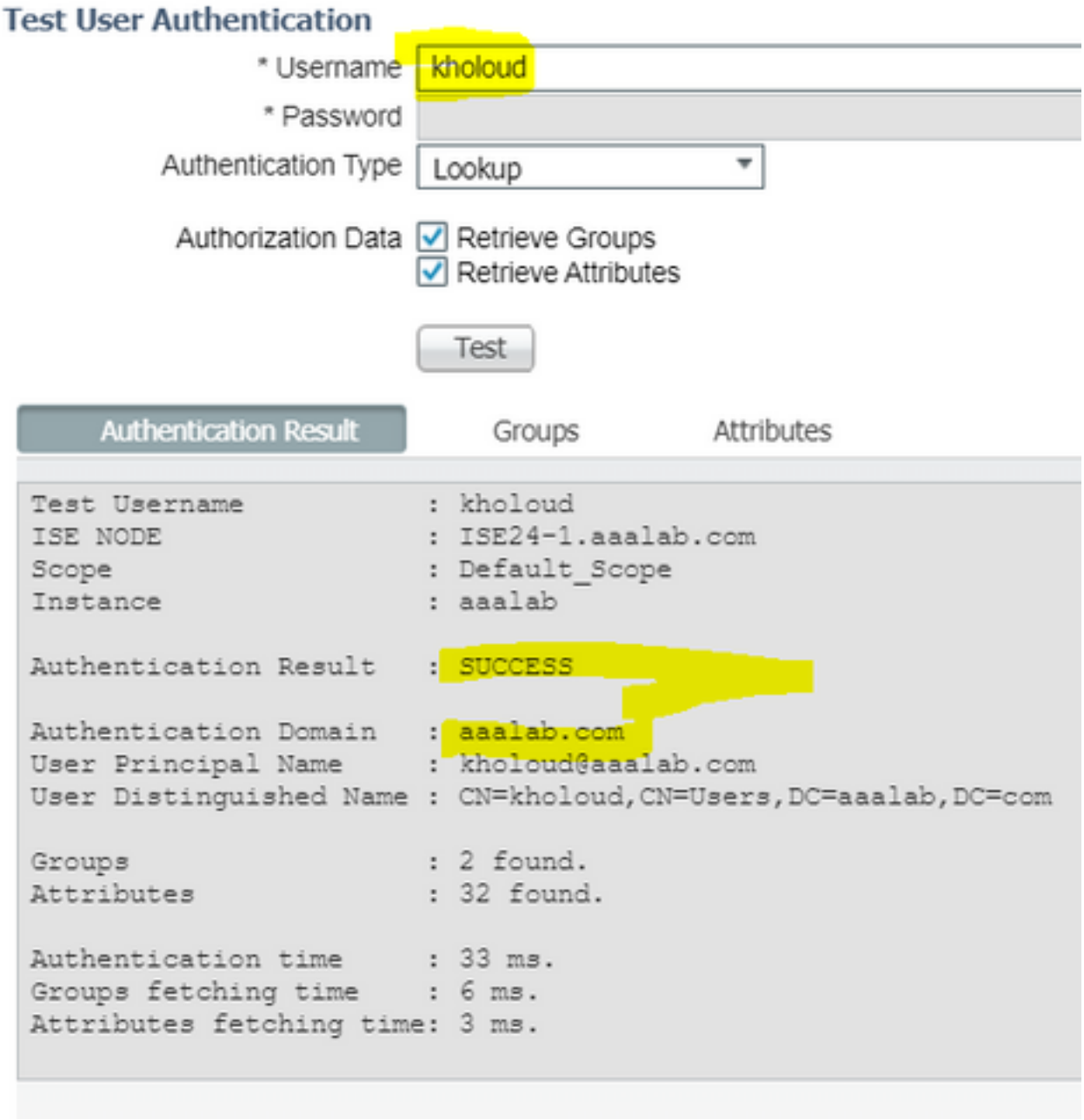
これで、ISEはaaalab.comとzatar.comでユーザを検索できます。

確認

「test user」オプションを使用して動作することを確認し、「zatar.jo」ドメイン内のユーザを使用します（この例では、ユーザ「demo」は「zatar.jo」ドメインにのみ存在し、「aalab.com」には存在しません。テスト結果は次のとおりです）。



aaalab.comのユーザも作業しており、ユーザkhoroudはaaalab.comにあります（ユーザ名はaaalab.comです）。



トラブルシュート

ほとんどのAD/双方向の信頼の問題をトラブルシューティングするには、主に2つの手順があります。ほとんどの外部ID認証(EID)もトラブルシューティングできます。

1. デバッグを有効にしたISEログ（サポートバンドル）の収集このサポートバンドルの特定のフォルダでは、ADでの認証の試みのすべての詳細を確認できます。

2.ISEとAD間のパケットキャプチャを収集します。

ステップ1:ISEログを収集します。

a.デバッグを有効にし、次のデバッグを「trace」に設定します。

- 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.問題を再現し、問題のあるユーザと接続します。

c.サポートバンドルの収集

動作シナリオ「ログ」：

注：認証試行の詳細は、ファイルad_agent.logに記載されています

ad_agent.logファイルから：

zatar two way trust connection verification:

```
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
```

メインドメインaaalabでユーザ「demo」を検索します。

```
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
```

(デモユーザはzatarドメインにあることに注意してください。ただし、iseは最初にaaalabドメインでチェックし、次にnewlab.comなどの「whitlasted」ドメインタブの他のドメインでチェックします。メインドメインでチェックを避け、zatar.joを直接チェックインするには、ISEが検索する場所を認識できるようにUPNサフィックスを使用する必要があります。したがって、ユーザは次の形式でログインする必要があります。demo.zatar.jo)。

zatar.joでユーザ「demo」を検索します。

```
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ドメインで見つかったユーザ「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"
```

ステップ2：キャプチャを収集します。

a.ISEとAD/LDAPの間で交換されるパケットは暗号化されるため、最初に復号化せずにキャプチャを収集すると読み取り可能になりません。

ISEAD

1. ISE[External-ID-Stores] -> [Active Directory] -> [Advanced Tools] -> [Advanced Tuning]
2. ISE
3. [Name]TROUBLESHOOTING(TROUBLESHOOTING.EncryptionOffPeriod
4. [Value]

<>

30

30

5.

6. [Update Value]

7. [Restart Active Directory Connector]

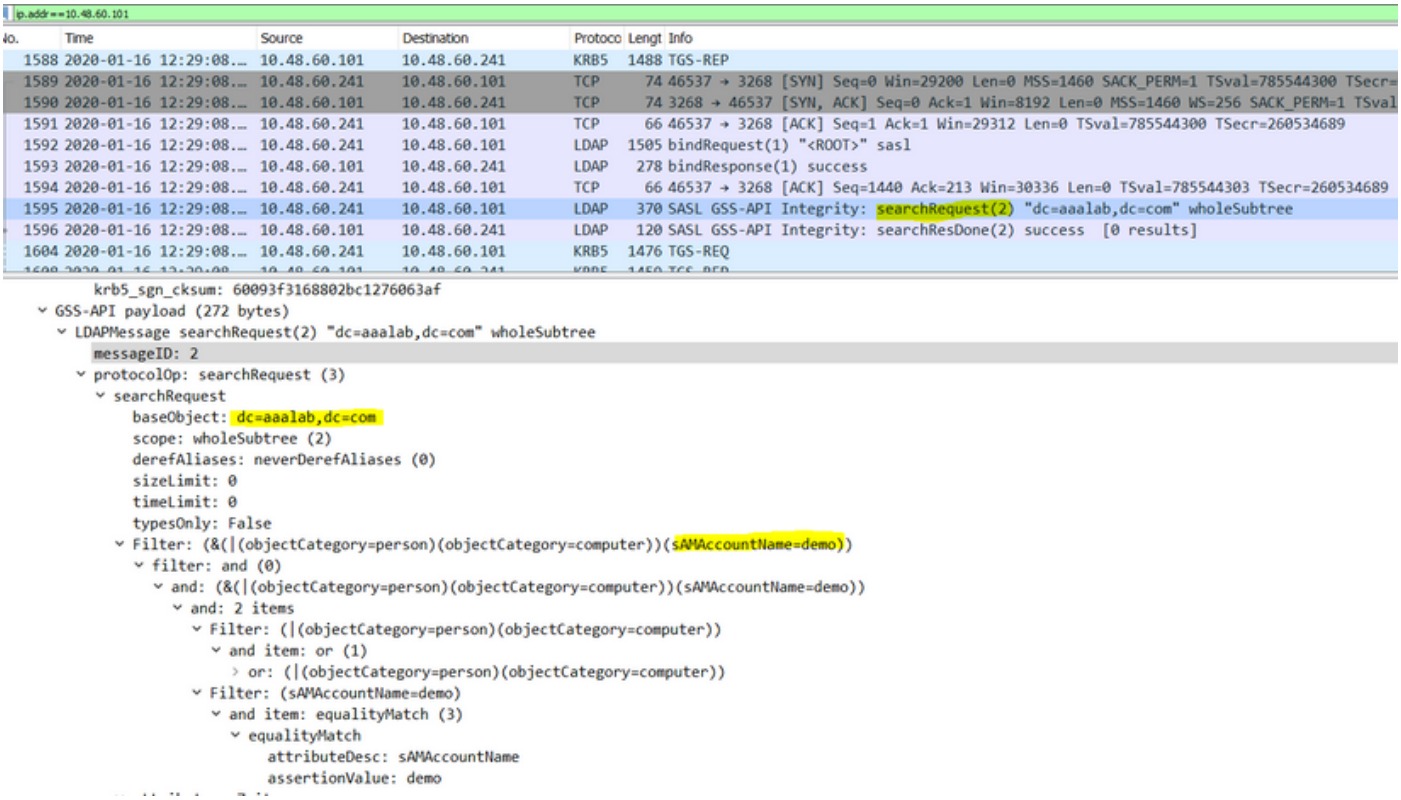
8.1010

b.ISEでキャプチャを開始します。

c.問題を再現します。

d.キャプチャを停止してダウンロードします

動作シナリオ「ログ」：



確認

ここでは、発生する可能性のある動作状況と非動作状況の例と、それらの口グが生成される口グを示します。

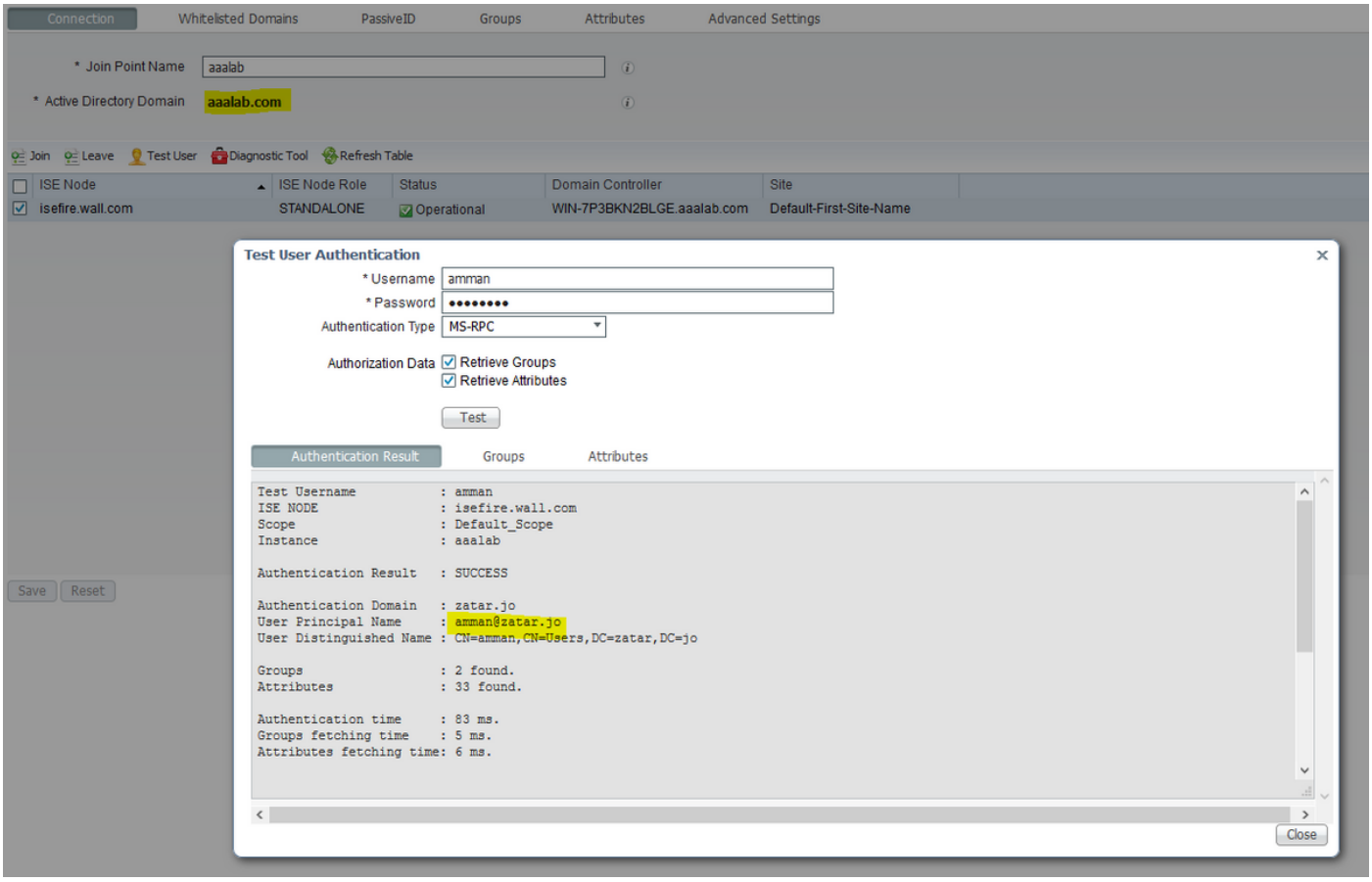
1.AD「zatar.jo」グループに基づく認証：

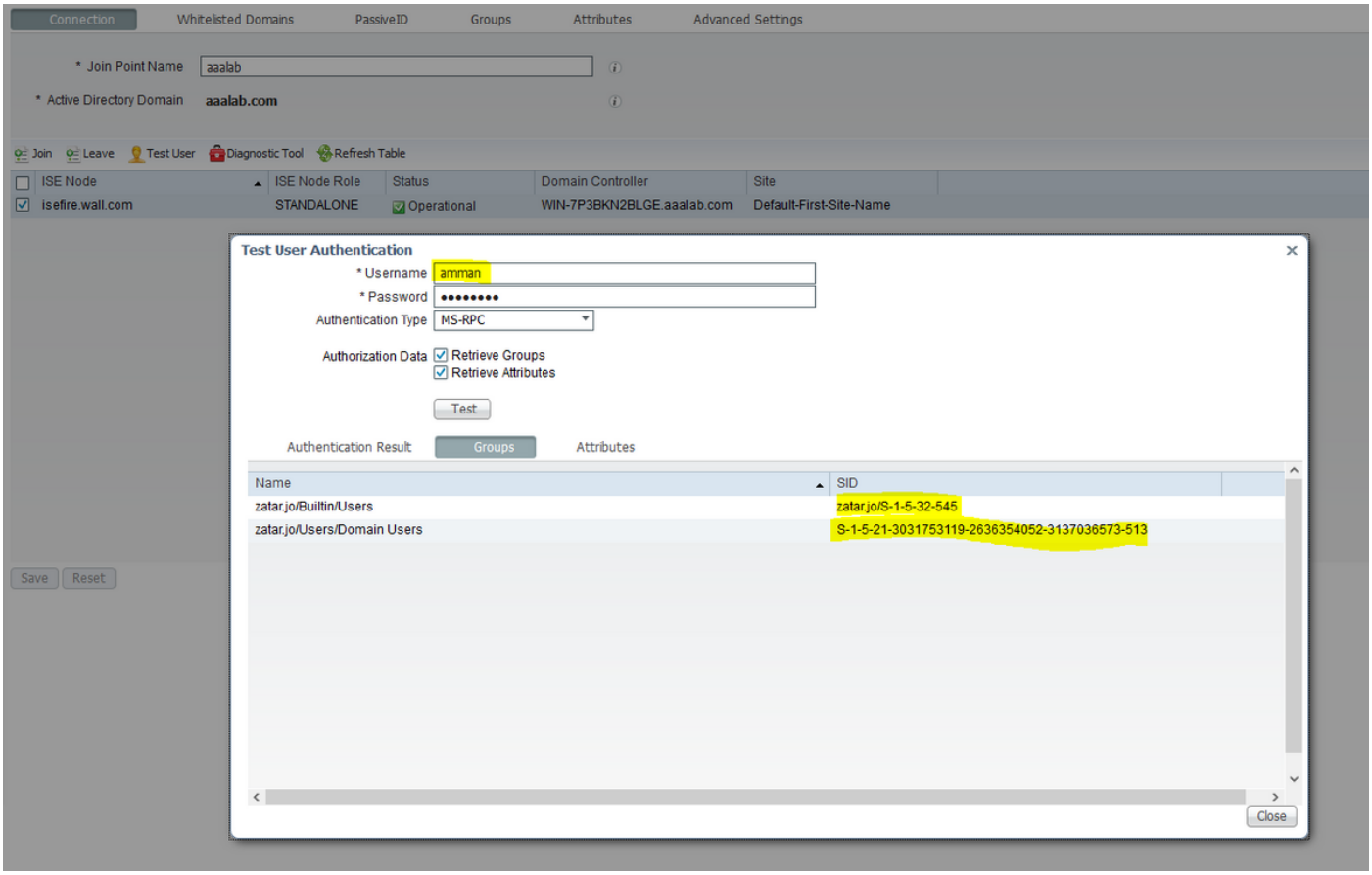
グループが[group]タブから取得されない場合、次の口グメッセージが表示されます。

```
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]タブからzatar.joのグループを取得する必要があります。

[AD]タブからのADグループ取得を確認しています。





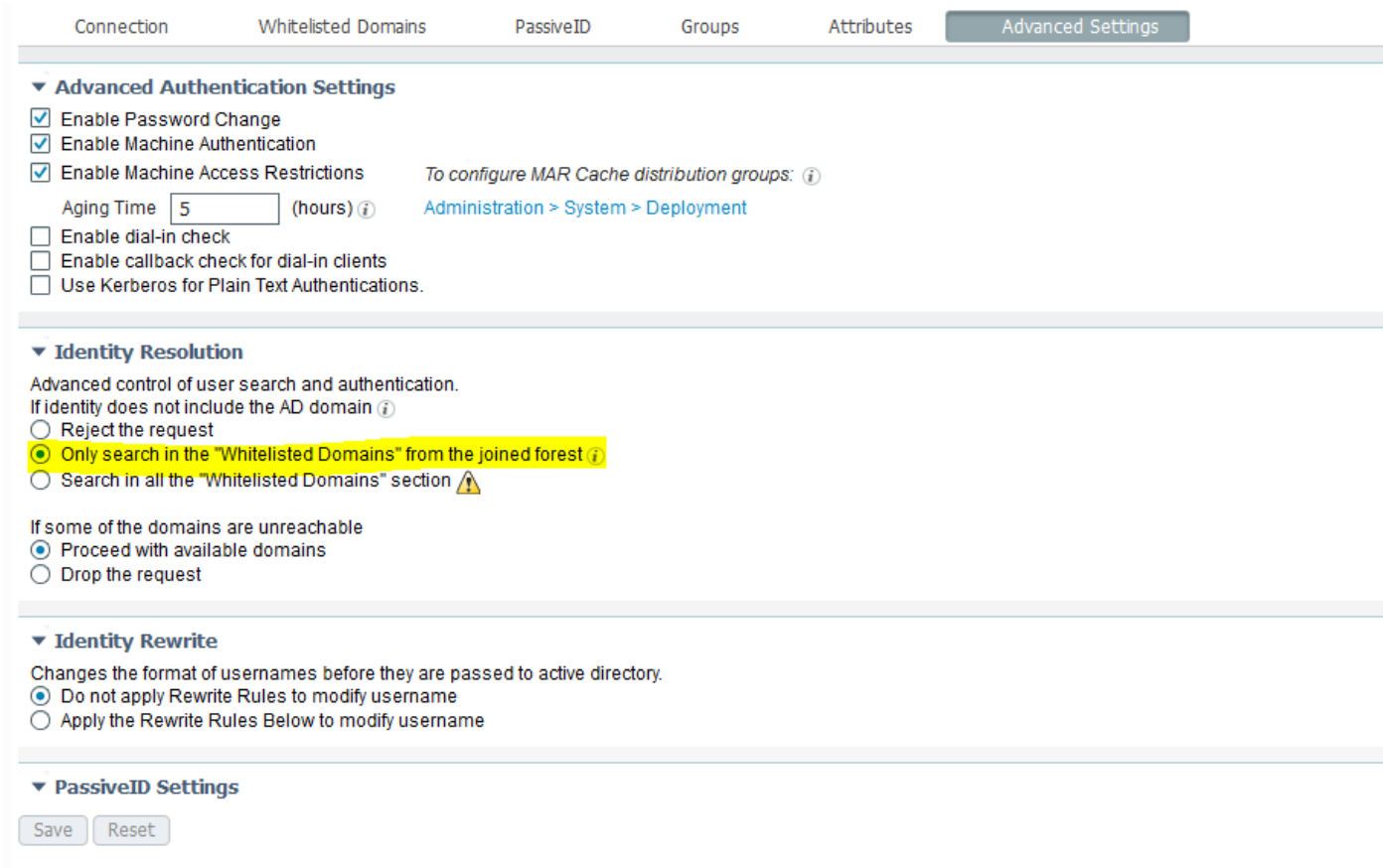
作業シナリオAD_agent.logログから：

```
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"
}
}
```

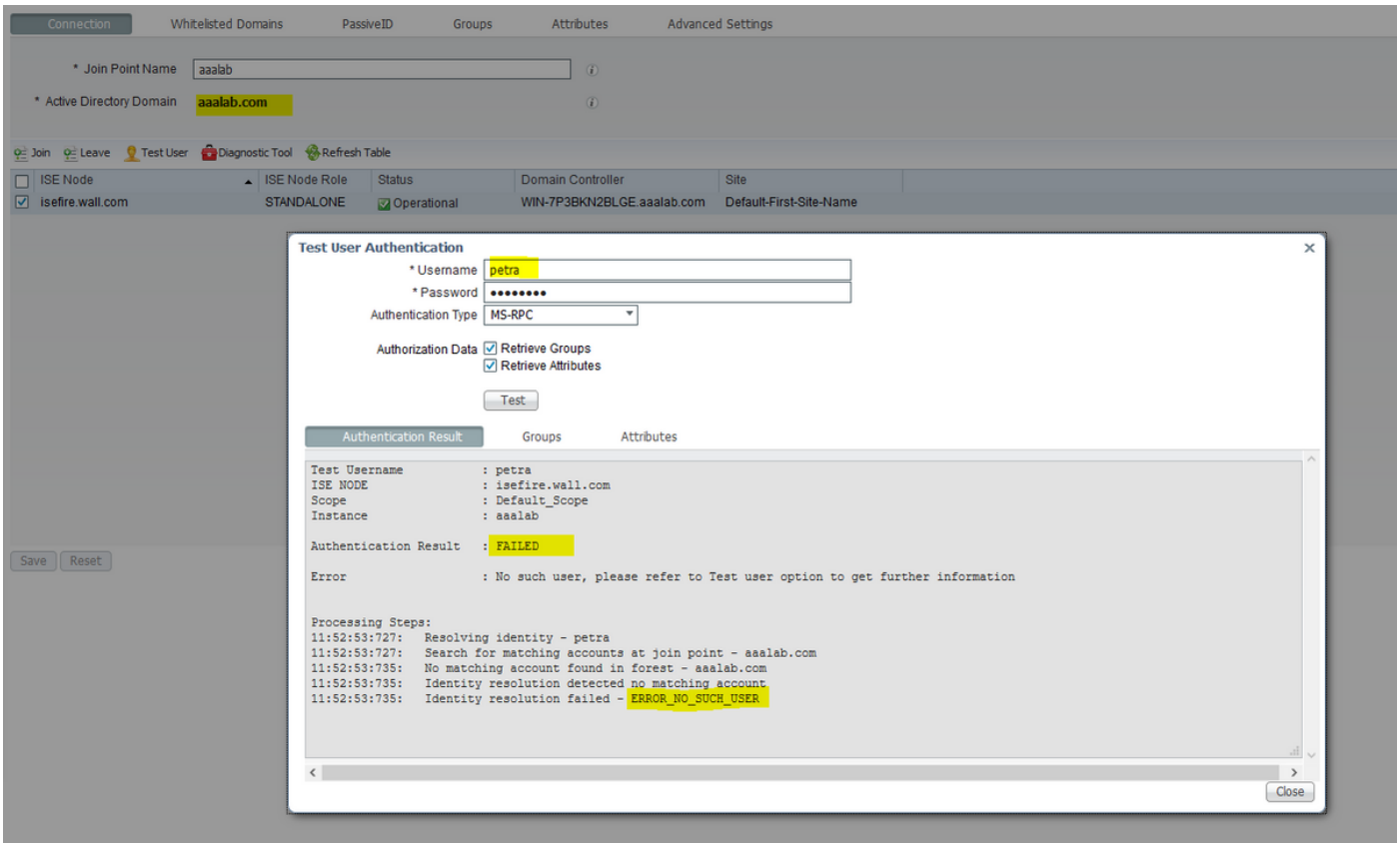
2. [Only search in the "Whitelized Domains from the joined forest"]オプションがオンになっている場合：



[Only search in the "Whitelized Domains from the joined forest"]オプションを選択すると、ISEによってオフラインのマークが付けられます。

```
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
```

ユーザ「petra」はzatar.joにあり、次のスクリーンショットのように認証に失敗します。



ログ：

ISEが他のドメインに到達できませんでした。詳細オプション[Only search in the "Whitelized Domains" from the joined forest]が原因です。

```
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
```