ISE和双向信任AD配置

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[验证](#)
[故障排除](#)
[验证](#)

简介

本文档介绍ISE上“双向信任”的定义，以及一个简单的配置示例：如何对不在加入ISE的AD中但在另一个AD中存在的用户进行身份验证。

先决条件

要求

思科建议您对以下方面有基本知识：

- ISE 2.x和Active Directory集成。
- ISE上的外部身份验证。

使用的组件

- ISE 2.x。
- 两个活动目录。

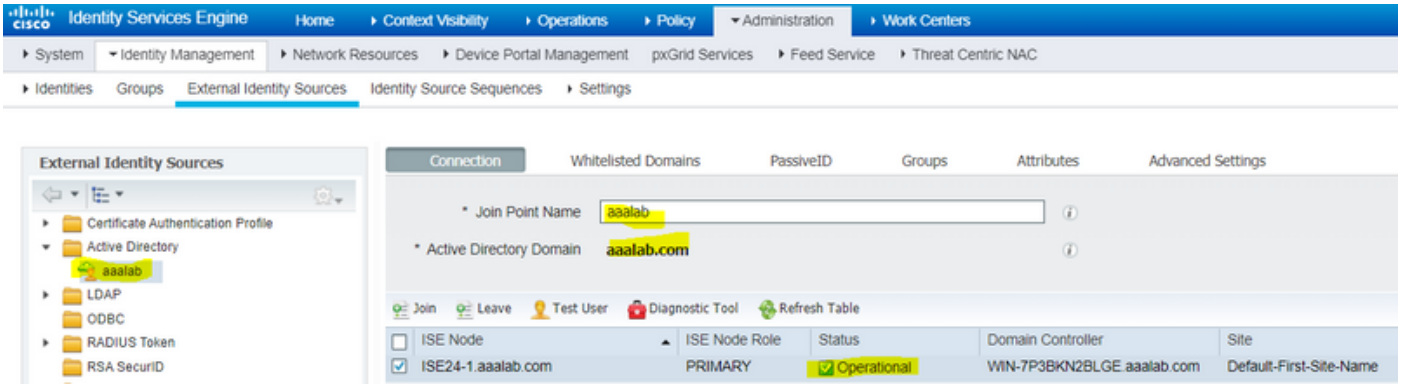
配置

为了扩展您的域，并将其他用户包括在除已加入ISE的域外的其他域中，您有两种方法可以完成此任务：

1. 您可以手动在ISE上单独添加域。通过此操作，您将有两个单独的Active Directories。
2. 加入一个AD到ISE，然后在**此AD和第二个AD**之间配置双向信任，而不将其添加到ISE。这主要是双向信任配置，是在两个或多个Active Directories之间配置的选项。ISE将使用AD连接器自动检测这些受信任域并将其添加到“白名单域”，并将它们视为加入ISE的单独AD。这是您如何在AD“zatar.jo”（未加入ISE）中对用户进行身份验证。

以下步骤描述ISE和AD上的配置过程：

步骤1.确保ISE已加入AD，在本例中，您有域aaalab：

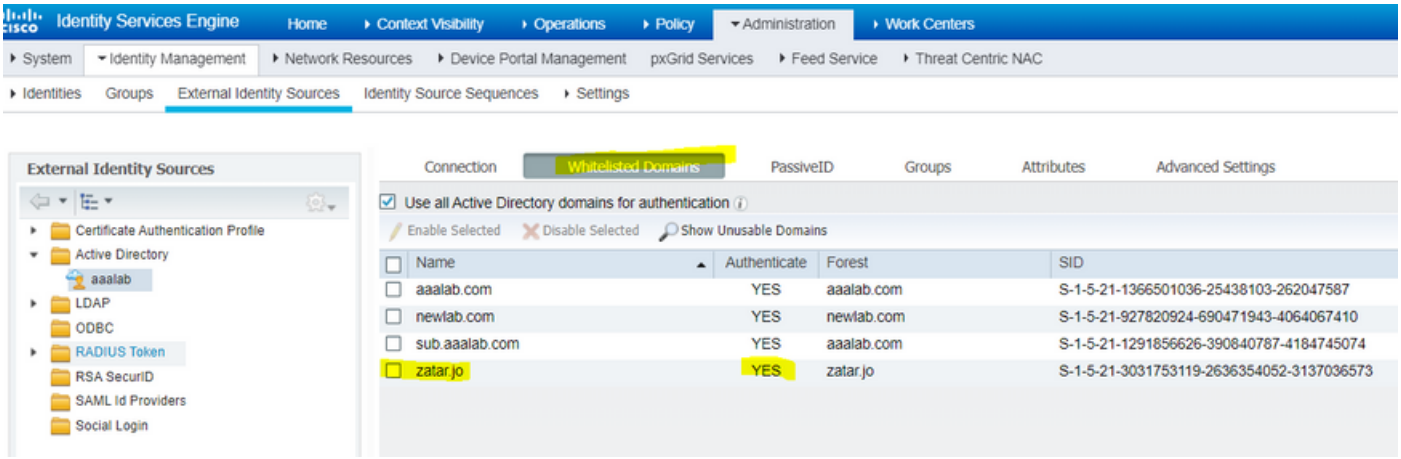


步骤2.确保在两个Active Directories之间启用双向信任，如下所示：

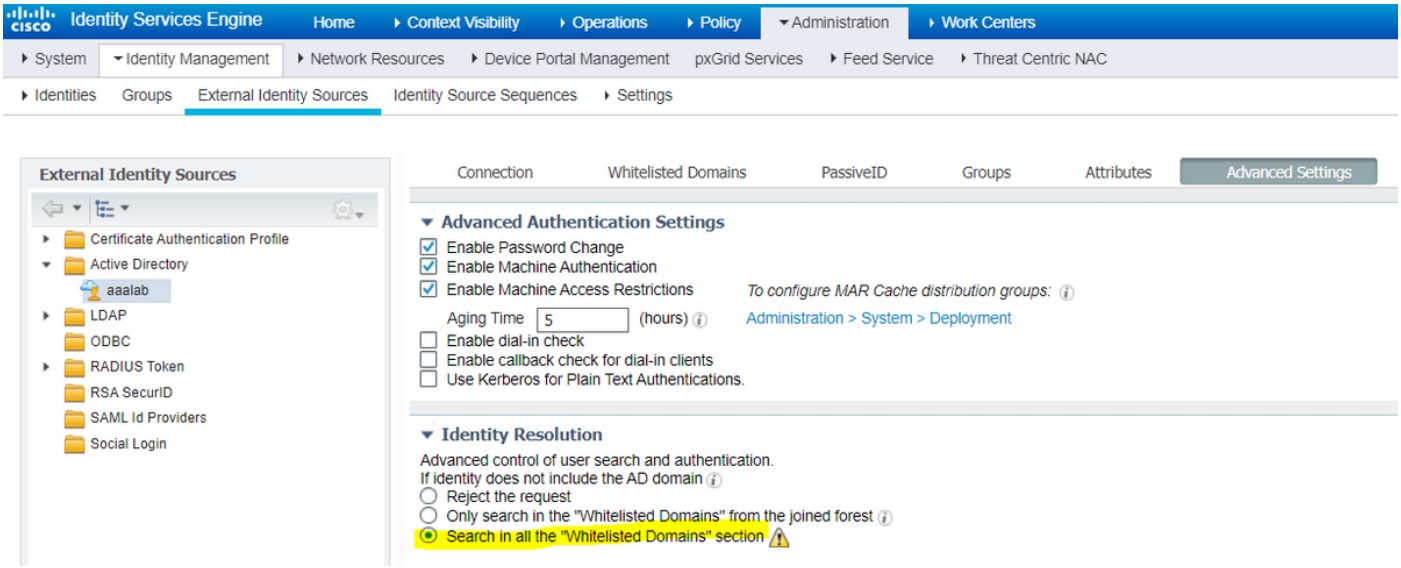
1. 打开Active Directory域和信任管理单元。
2. 在左窗格中，右键单击要添加信任的域，然后选择属性。
3. 点击信任选项卡。
4. 单击“新建信任”按钮。
5. 打开“新建信任向导”后，单击“下一步”。
6. 键入AD域的DNS名称，然后点击Next。
7. 假设AD域可通过DNS解析，则下一屏幕将询问信任方向。选择“双向”，然后单击“下一步”。
8. 对于“传出信任属性”，选择要进行身份验证的所有资源，然后点击“下一步”。
9. 输入并重新键入信任密码，然后点击“下一步”。
10. 单击“下一步”两次。

注意：AD配置不在思科支持范围内，Microsoft支持可在出现任何问题时提供。

配置后，示例AD(aaalab)可以与新AD(zatar.jo)通信，并且它应会弹出到“whitlested domains”选项卡，如下所示。如果未显示，则双向信任配置不正确：



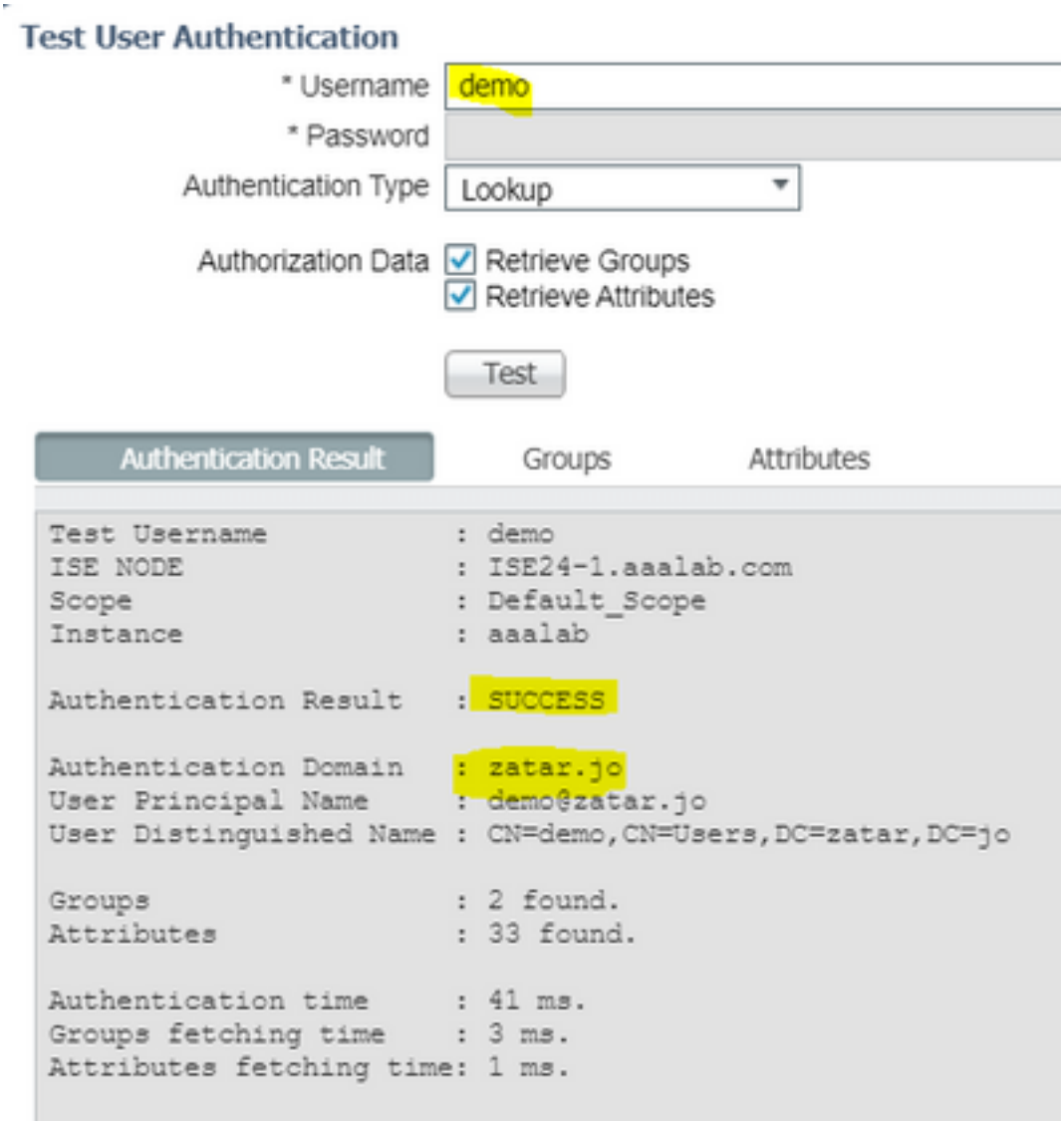
步骤3.确保在所有“**删除的域”部分中启用**了选项搜索，如下所示。它允许在所有情况下搜索包括双向受信任域的域。如果启**用了“仅在已加入林的白名单域”中搜索**选项，则只能在主域的“子域”中搜索。{子域示例：sub.aaalab.com。



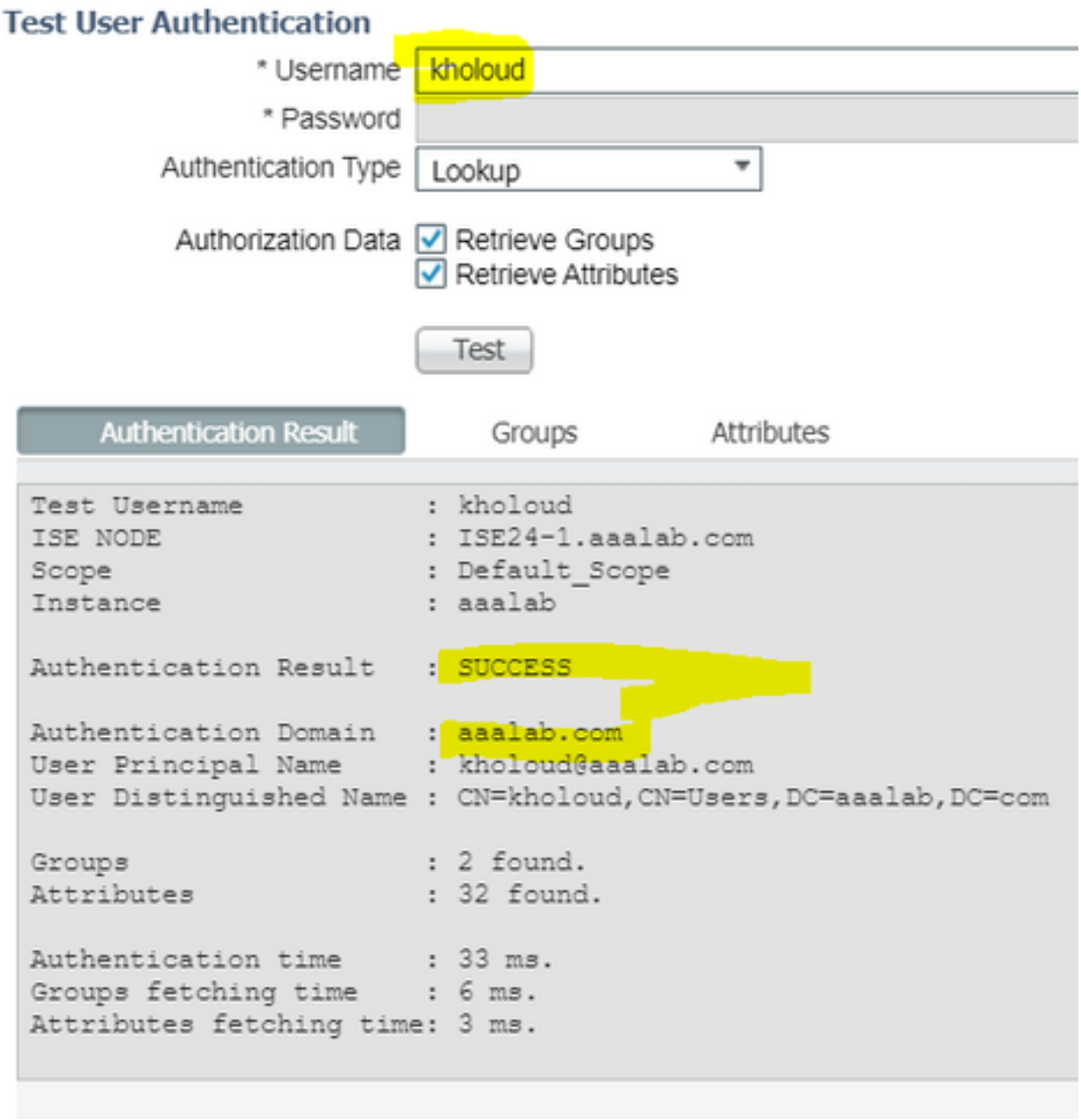
现在，ISE可以在aaalab.com和zatar.com中搜索用户。

验证

验证它是否通过“test user”选项工作，使用“zatar.jo”域中的用户（在本例中，用户“demo”仅存在于“zatar.jo”域中，而不在“aaalab.com”中，测试结果如下）：



请注意，aaalab.com中的用户也在工作，用户kholoud在aaalab.com中：



故障排除

排除大多数AD/双向信任问题（即使大多数外部身份验证）有两个主要步骤：

1.收集启用调试的ISE日志（支持捆绑包）。在此支持捆绑包中的特定文件夹中，我们可以找到AD上任何身份验证尝试的所有详细信息。

2.收集ISE和AD之间的数据包捕获。

步骤1.收集ISE日志：

a.启用调试，将以下调试设置为“trace”：

- 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.重现问题，与有问题的用户连接。

c.收集支持捆绑包。

工作场景"日志"：

注意：身份验证尝试的详细信息将在文件ad_agent.log中找到

从文件ad_agent.log：

zatar双向信任连接验证：

```
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
```

在主域aalab中搜索用户"demo"：

```
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
```

(请注意，演示用户位于zatar域中，但ise将先在aaalab域中检查它，然后在"whitlested"域选项卡中检查其他域，如newlab.com。要避免检查主域，并直接签入zatar.jo，您必须使用UPN后缀，以便ISE知道搜索位置，因此用户应使用此格式登录：demo.zatar.jo)。

在zatar.jo中搜索用户"demo"。

```
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
```

在zatar域中找到用户"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"
```

步骤2.收集捕获：

a.在ISE和AD/LDAP之间交换的数据包会被加密，因此如果我们收集捕获而不先解密它们，它们将不可读。

ISEAD

1. ISEID — > Active Directory -> — >
2. ISE
3. “Name”TROUBLESHOOTING.EncryptionOffPeriod
4. “Value”

<>

30

5.

6.“”

7.“Active Directory”

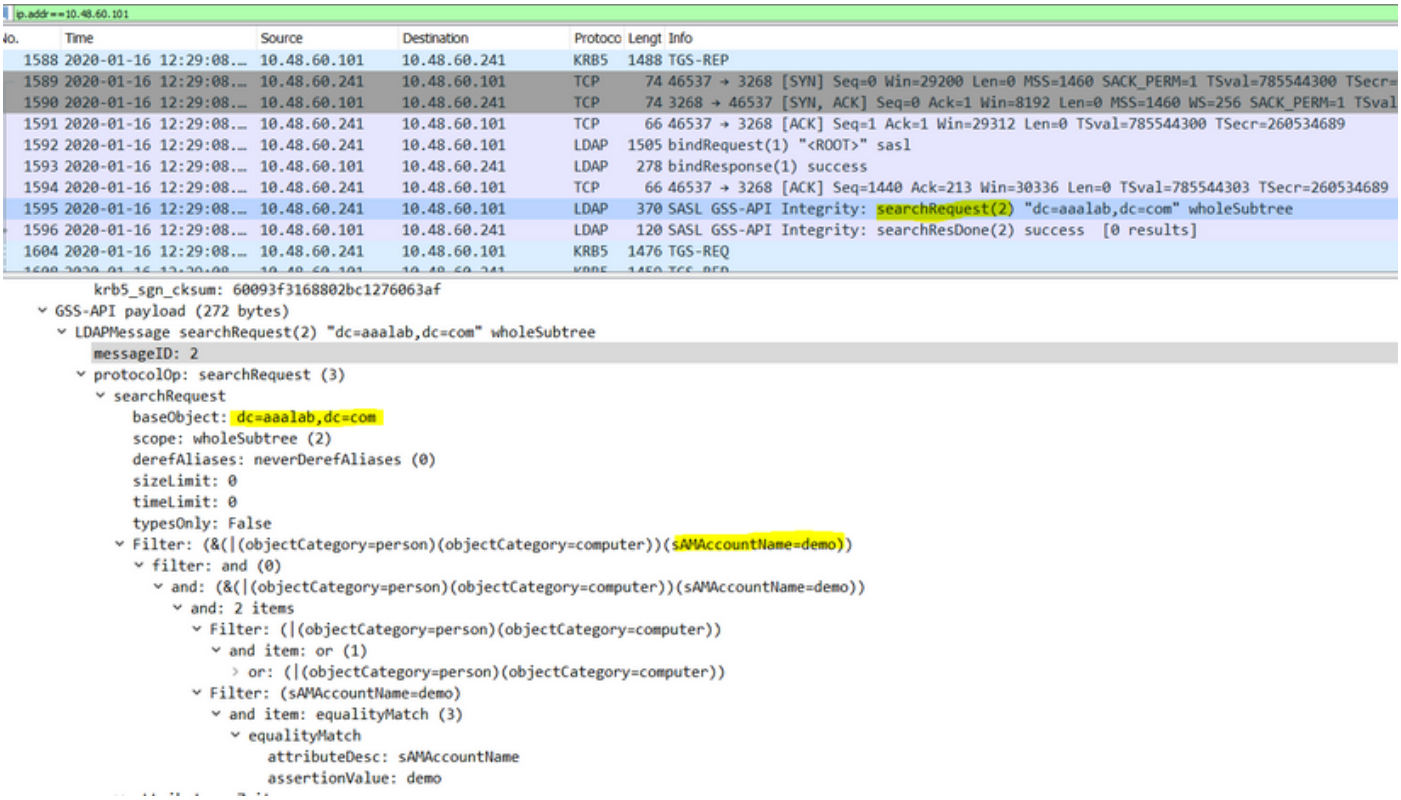
8.10

b.在ISE上启动捕获。

c.重现问题.

d.然后停止并下载捕获

工作场景“日志”：



验证

下面是您可能遇到的工作和非工作情况以及它们生成的日志的几个示例。

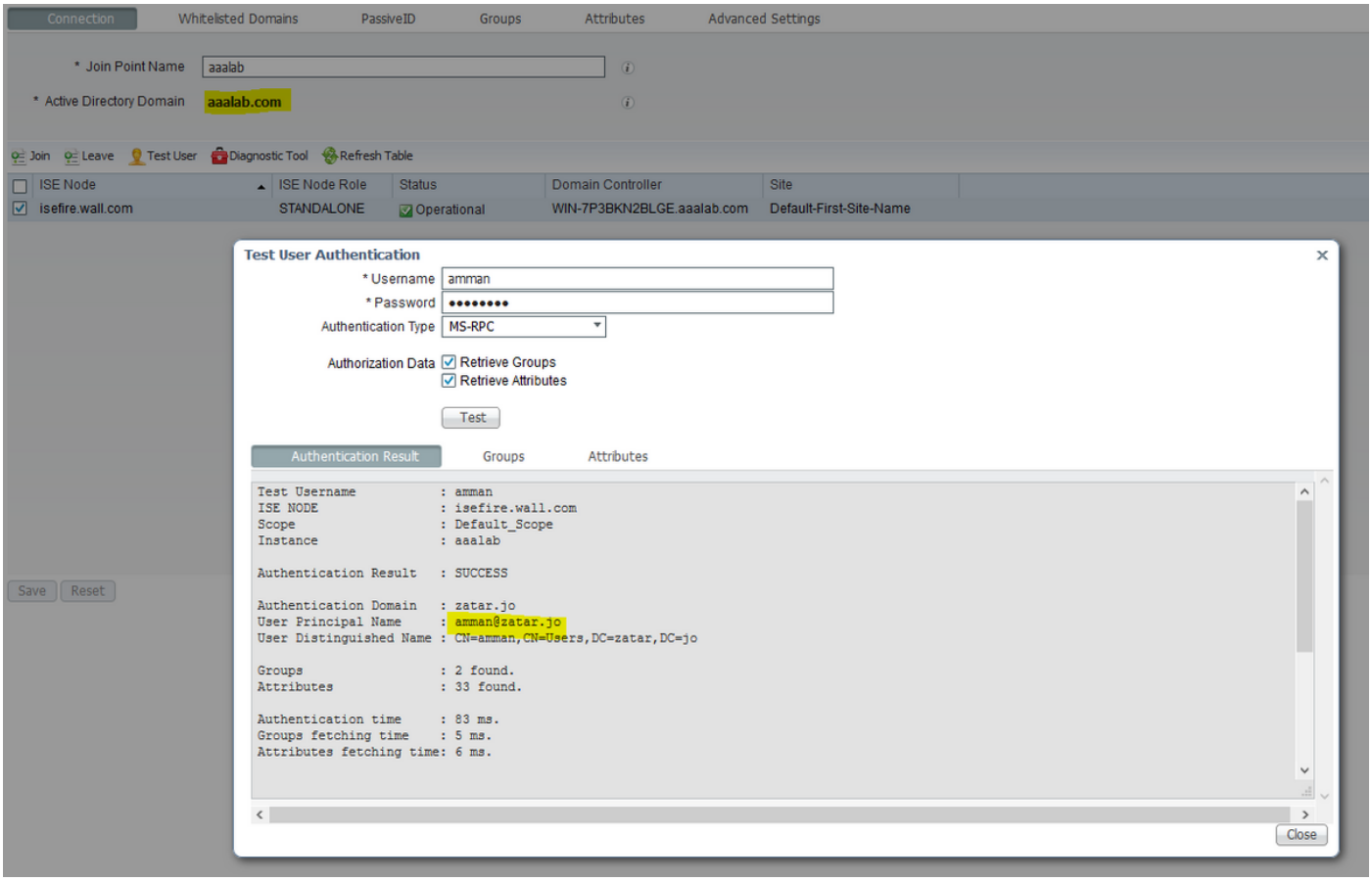
1.基于AD“zatar.jo”组的身份验证：

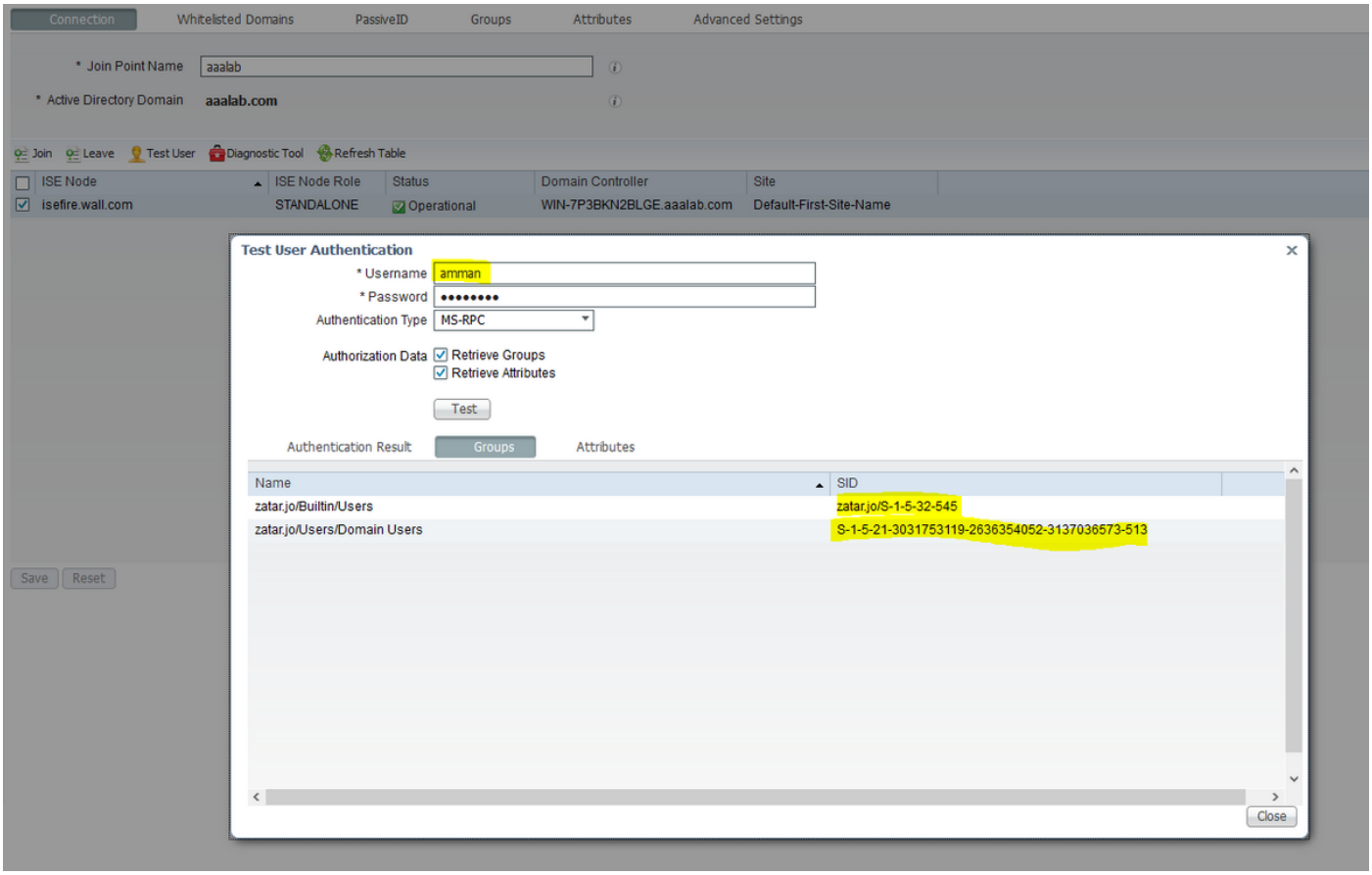
如果组未从组选项卡中恢复，您将收到以下日志消息：

```
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
```

我们需要从“组”(Groups)选项卡中检索zatar.jo中的组。

从AD选项卡验证AD组检索：





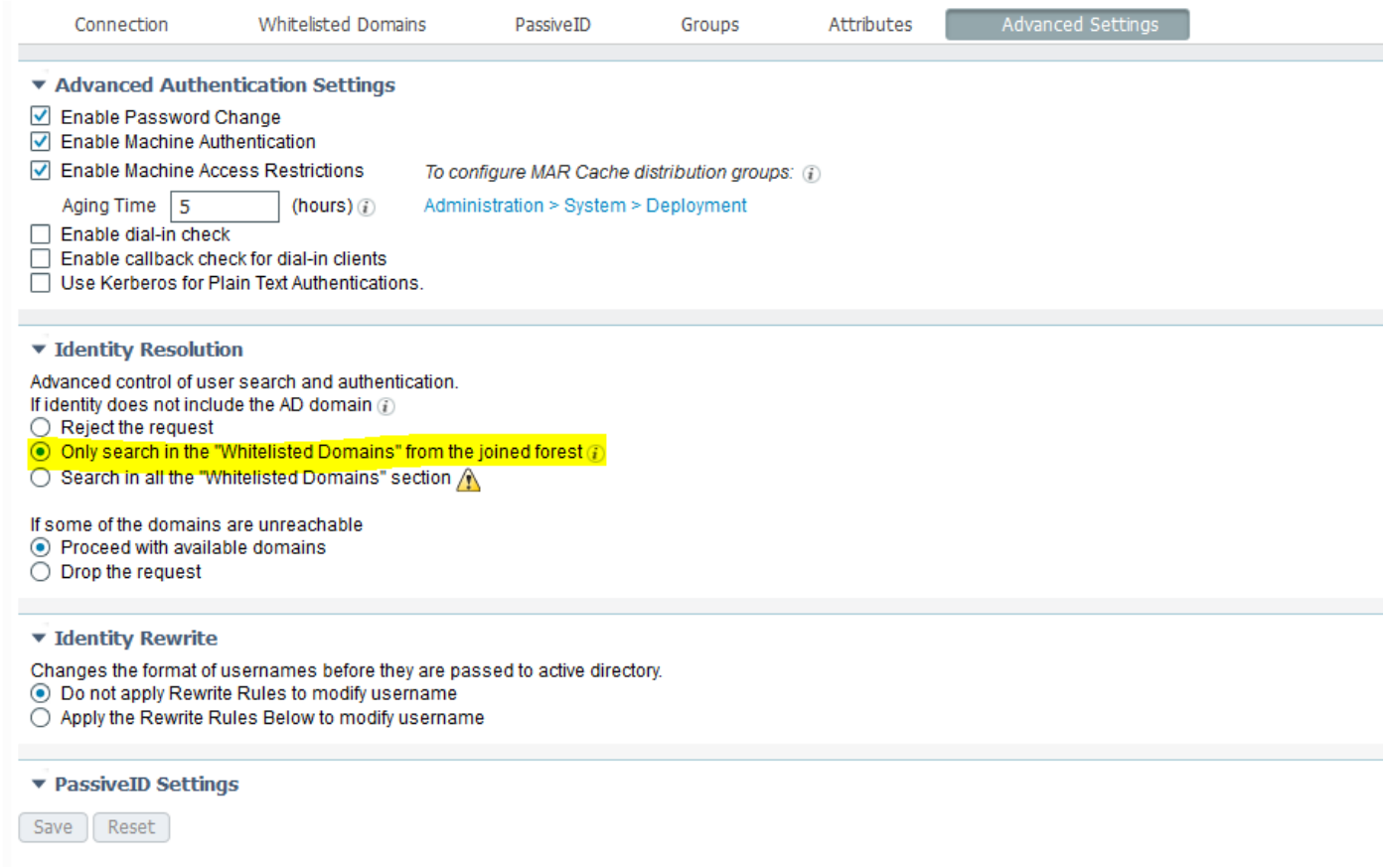
工作场景从日志AD_agent.log:

```
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"
}
}
```

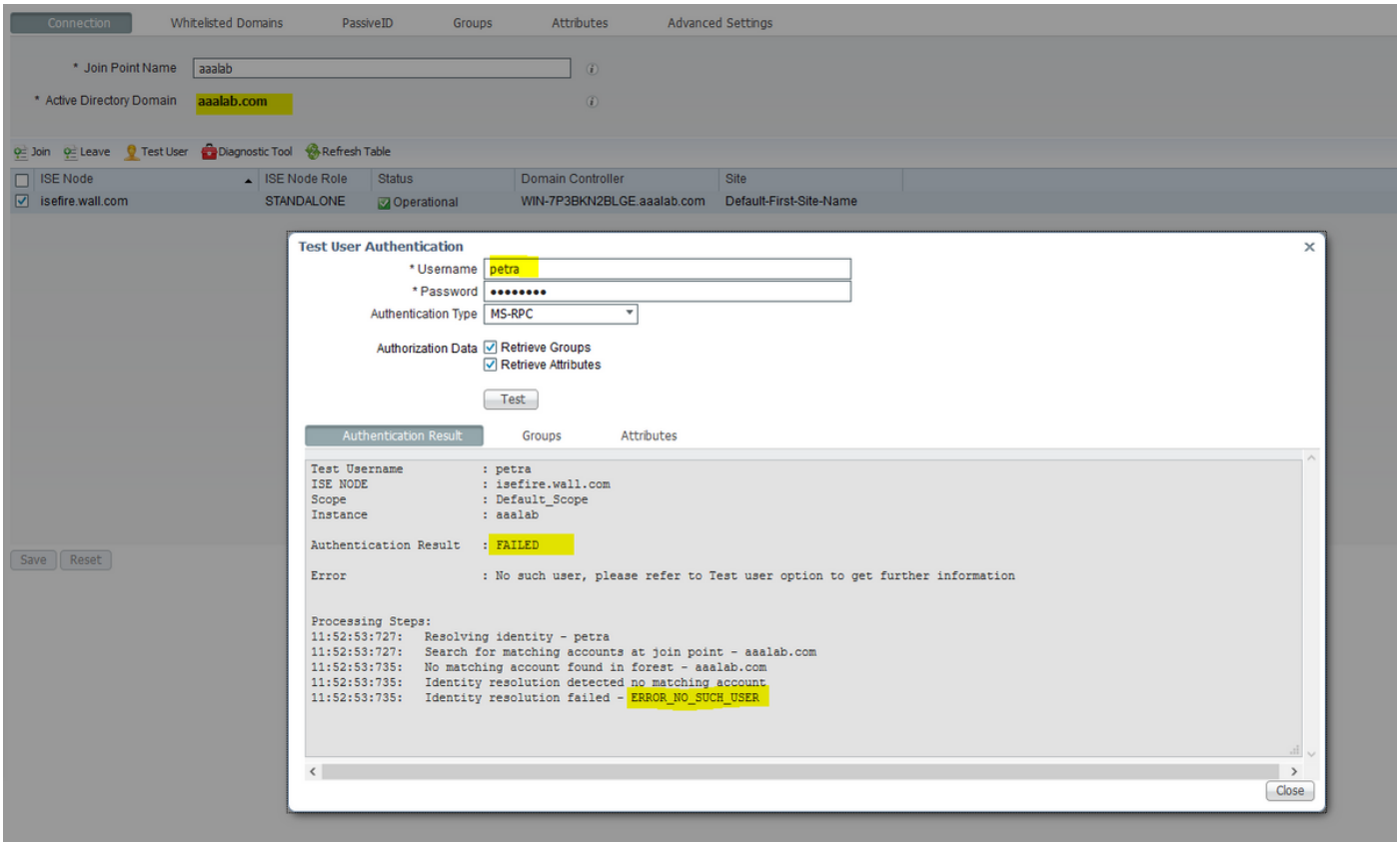
2.如果选中“仅从加入的林中搜索“白名单域”的高级选项：



当您选择“仅在加入的林的“白名单域”中搜索”选项时，ISE会将其标记为脱机：

```
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
```

用户“petra”位于zatar.jo中，身份验证将失败，如下图所示：



在日志中：

由于高级选项“仅从加入的林在“白名单域”中搜索”，ISE无法访问其他域：

```
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
```