ISE e configuração do AD bidirecional

Contents

Introduction

Este documento descreve a definição de "confiança bidirecional" no ISE e um exemplo de configuração simples : como autenticar um usuário que não está presente no AD associado ao ISE, mas presente em outro AD.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico sobre:

- Integração do ISE 2.x e do Ative Diretory .
- Autenticação de identidade externa no ISE.

Componentes Utilizados

- ISE 2.x.
- dois Diretórios ativos.

Configurar

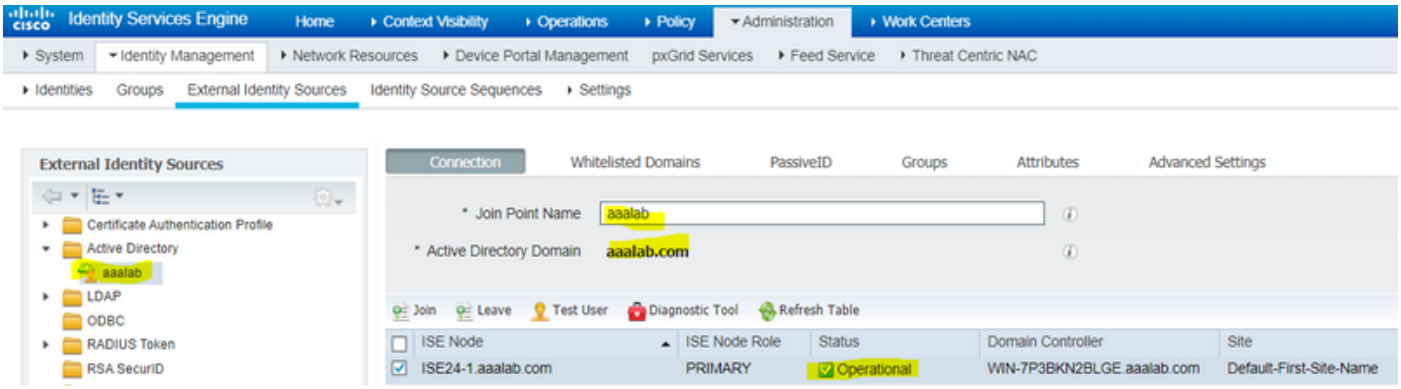
Para expandir seu domínio e incluir outros usuários em um domínio diferente daquele que já está associado ao ISE, você tem duas maneiras de fazer isso:

1. você pode adicionar o domínio manualmente e separadamente no ISE. com isso, você teria dois Ative Diretory separados.
2. Junte-se a um AD ao ISE e, em seguida, configure a **confiança bidirecional** entre este AD e o segundo AD, sem adicioná-lo ao ISE. Essa é principalmente a configuração de confiança de duas vias, é uma opção configurada entre dois ou mais Diretórios ativos. O ISE detectará automaticamente esses domínios confiáveis usando o conector AD e os adicionará aos "domínios listados em branco" e os tratará como ADs separados associados ao ISE. É

assim que você pode autenticar um usuário no AD "zatar.jo", que não está associado ao ISE.

As etapas a seguir descrevem o procedimento de configuração no ISE e no AD:

etapa 1. certifique-se de que o ISE esteja associado ao AD, neste exemplo, você tem o domain aaalab :

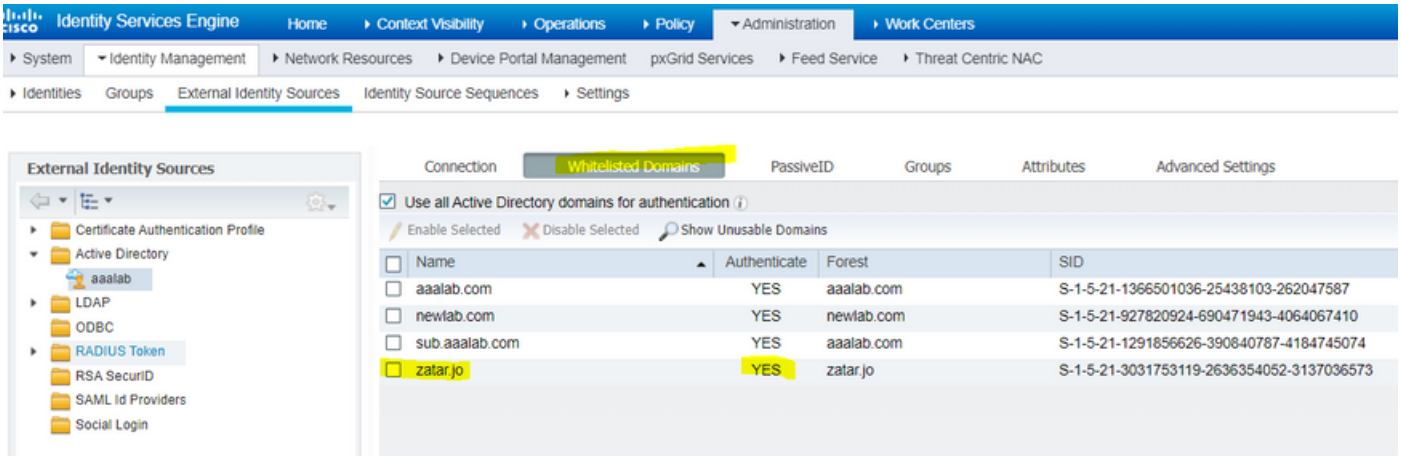


etapa 2. certifique-se de que a confiança bidirecional esteja habilitada entre ambos os Diretórios ativos, conforme abaixo:

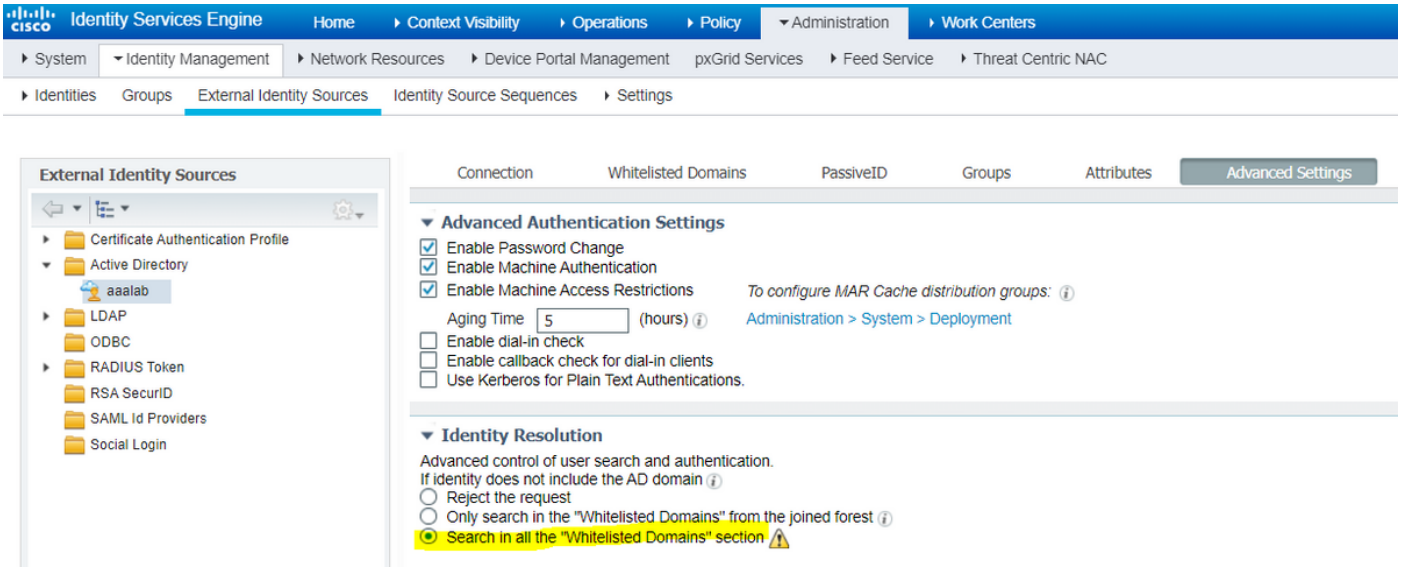
1. Abra o snap-in Domínios e Confianças do Ative Diretory.
2. No painel esquerdo, clique com o botão direito do mouse no domínio para o qual deseja adicionar uma confiança e selecione Propriedades.
3. Clique na guia Confianças.
4. Clique no botão Nova confiança.
5. Depois que o Assistente de nova confiança for aberto, clique em Avançar.
6. Digite o nome DNS do domínio do AD e clique em Avançar.
7. Supondo que o domínio do AD pudesse ser resolvido via DNS, a próxima tela solicitará a Direção de Confiança. Selecione Bidirecional e clique em Avançar.
8. Para Propriedades de Confiança de Saída, selecione todos os recursos a serem autenticados e clique em Avançar.
9. Digite e digite novamente a senha de confiança e clique em Avançar.
10. Clique em Next (Avançar) duas vezes.

Note: A configuração do AD está fora do escopo de suporte da Cisco, o suporte da Microsoft pode ser utilizado em caso de problemas.

uma vez configurado, o exemplo de AD (aaalab) pode se comunicar com o novo AD (zatar.jo) e deve aparecer na guia "domínios com whitlested" (domínios com branco), como abaixo. se não for exibida, a configuração de confiança bidirecional está incorreta:



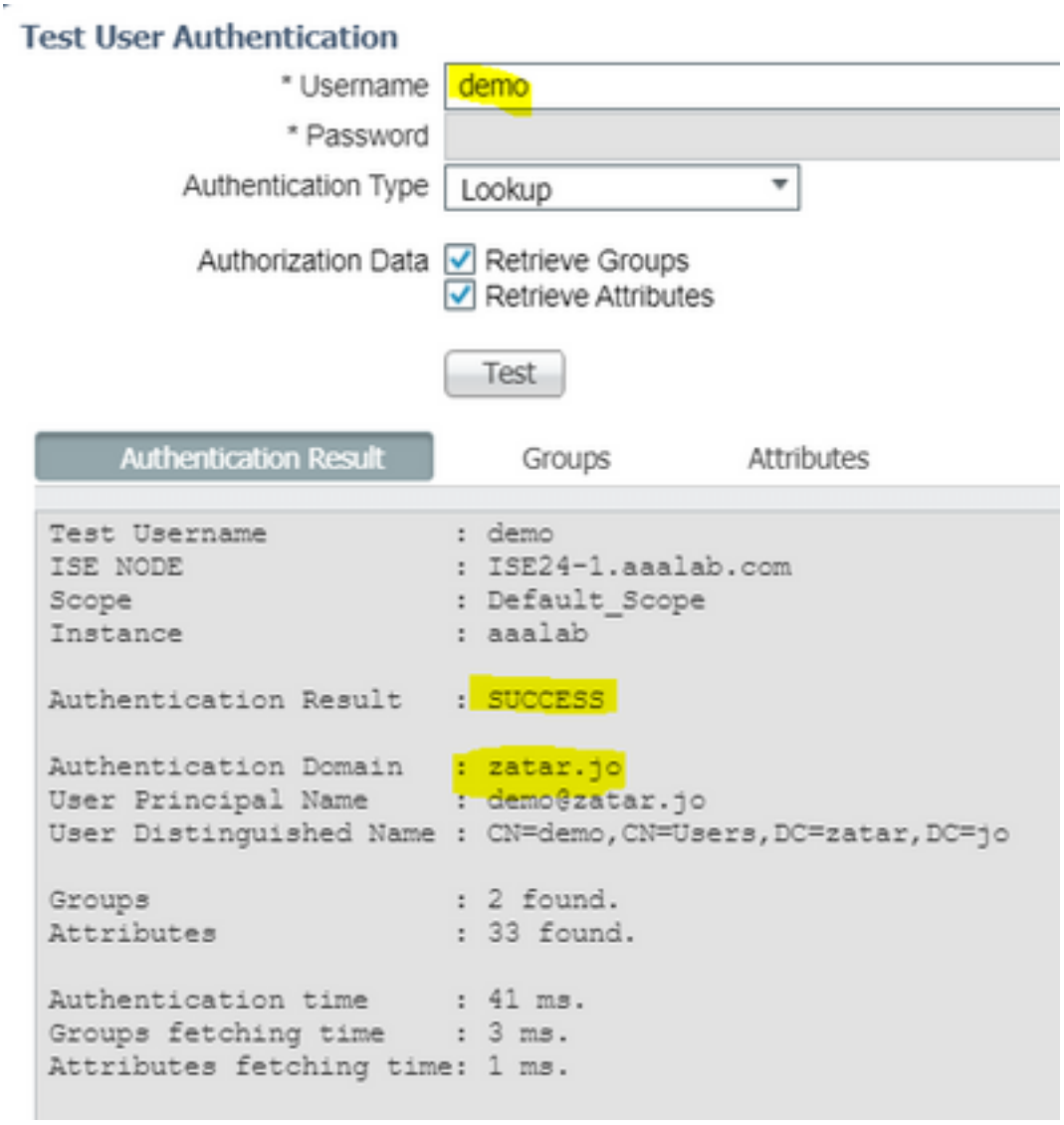
etapa 3. Certifique-se de que a **pesquisa** de opção **em todos os "domínios em branco"** esteja habilitada, como mostrado abaixo. Ele permitirá a pesquisa em todos os domínios em branco, incluindo domínios confiáveis bidirecionais. se a opção **Somente pesquisa nos "Domínios listados" da floresta unida** estiver habilitada, ela pesquisará somente nos domínios "filho" do domínio principal. { exemplo de domínio filho: sub.aaalab.com na captura de tela acima }.



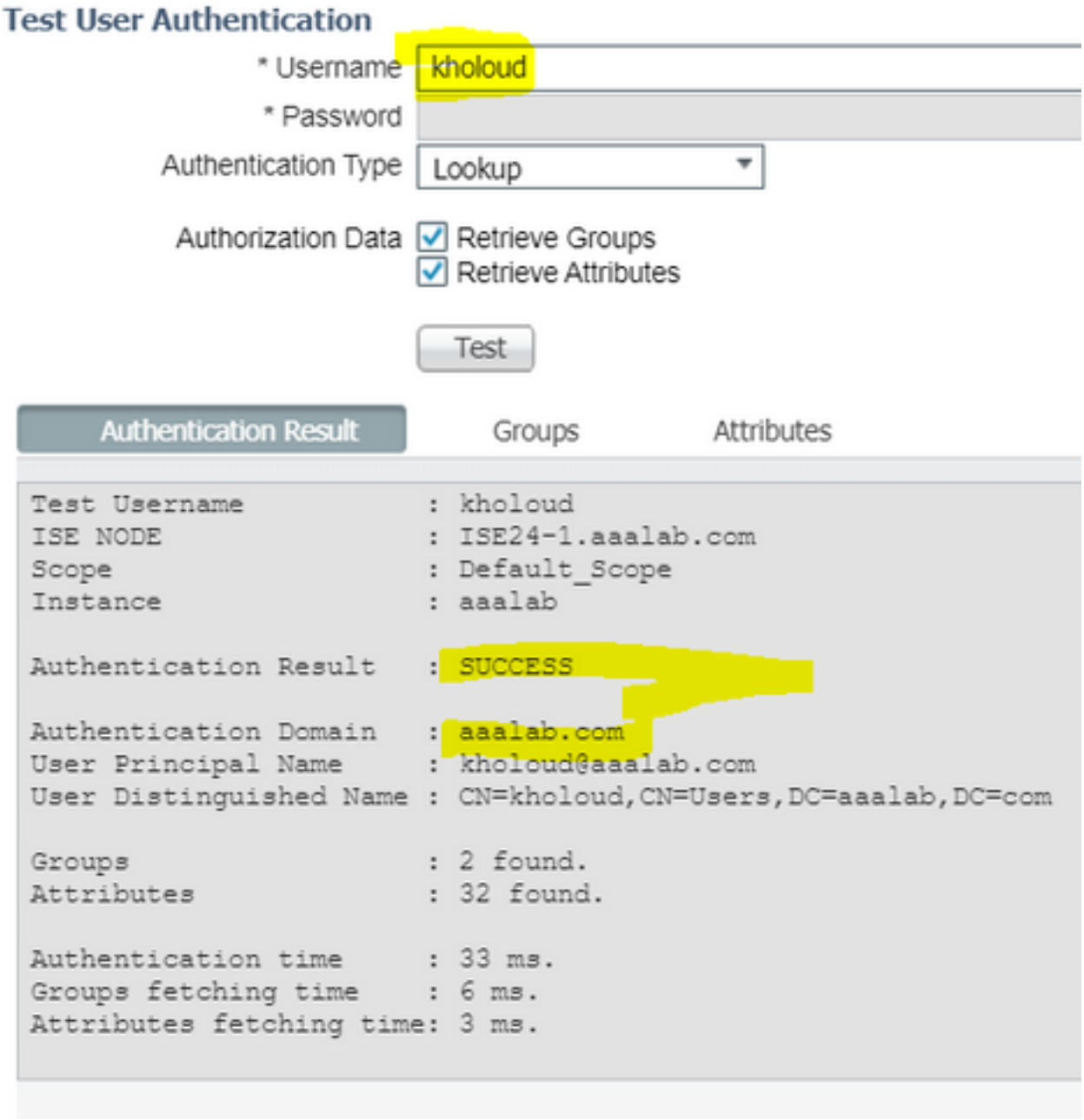
Agora, o ISE pode procurar o usuário em aaalab.com e zatar.com.

Verificar

Verifique se funciona através da opção "usuário de teste", use o usuário que está no domínio "zatar.jo" (neste exemplo, o usuário "demo" existe apenas no domínio "zatar.jo" e não está em "aaalab.com", o resultado do teste está abaixo) :



observe que os usuários do aaalab.com também estão trabalhando, o usuário kholoud está no aaalab.com :



Troubleshoot

Há dois procedimentos principais para solucionar a maioria dos problemas de AD/confiança bidirecional, até mesmo a maioria das autenticações de identidade externa :

1. coletando registros do ISE (pacote de suporte) com depurações habilitadas. em pastas específicas neste pacote de suporte, podemos encontrar todos os detalhes de qualquer tentativa de autenticação no AD.

2. coleta de capturas de pacotes entre o ISE e o AD.

etapa1. coletar registros do ISE:

a. Ative as depurações, defina as seguintes depurações como "trace":

- Ative Diretory (ad_agent.log)
- identity-store-AD (ad_agent.log)

- runtime-AAA (prrt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise-psc.log)

b. Reproduza o problema, conecte-se a um usuário problemático.

c. Colete um pacote de suporte.

"Logs" do cenário de trabalho:

Note: Detalhes das tentativas de autenticação serão encontrados no arquivo ad_agent.log

do arquivo ad_agent.log:

verificação de conexão de confiança bidirecional 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
```

pesquisando a "demonstração" do usuário no domínio principal aaalab :

```
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
```

(observe que o usuário da demonstração está no domínio zatar, no entanto, o ise o verificará primeiro no domínio aaalab, depois em outros domínios na guia domínios "brancos", como newlab.com. para evitar a verificação no domínio principal e para fazer check-in diretamente no zatar.jo, você precisa usar o sufixo UPN para que o ISE saiba onde procurar, então o usuário deve fazer login neste formato: demo.zatar.jo).

procurando o usuário "demo" em 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
```

"demonstração" do usuário encontrada no domínio 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"
```

etapa 2. Coletar capturas:

a. Os pacotes trocados entre ISE e AD/LDAP são criptografados de modo que não seriam legíveis se coletássemos as capturas sem descriptografá-las primeiro.

Para descriptografar pacotes entre ISE e AD (esta etapa precisa ser aplicada antes de coletar as capturas e aplicar a tentativa):

1. No ISE, assine até a guia: External-ID-Stores -> Ative Diretory -> Advanced Tools -> Advanced Tuning
2. Escolha seu nó ISE.
3. O campo 'Nome' recebe uma string de identificação e solução de problemas específica: TROUBLESHOOTING.EncryptionOffPeriod.
4. O campo 'Valor' recebe o número de minutos que você gostaria de solucionar para

<Número inteiro positivo em minutos>

Exemplo de meia hora:

30

5. Digite qualquer descrição. Necessário antes da próxima etapa.

6. Clique no botão 'Atualizar valor'

7. Clique em 'Reiniciar conector do Ative Diretory'.

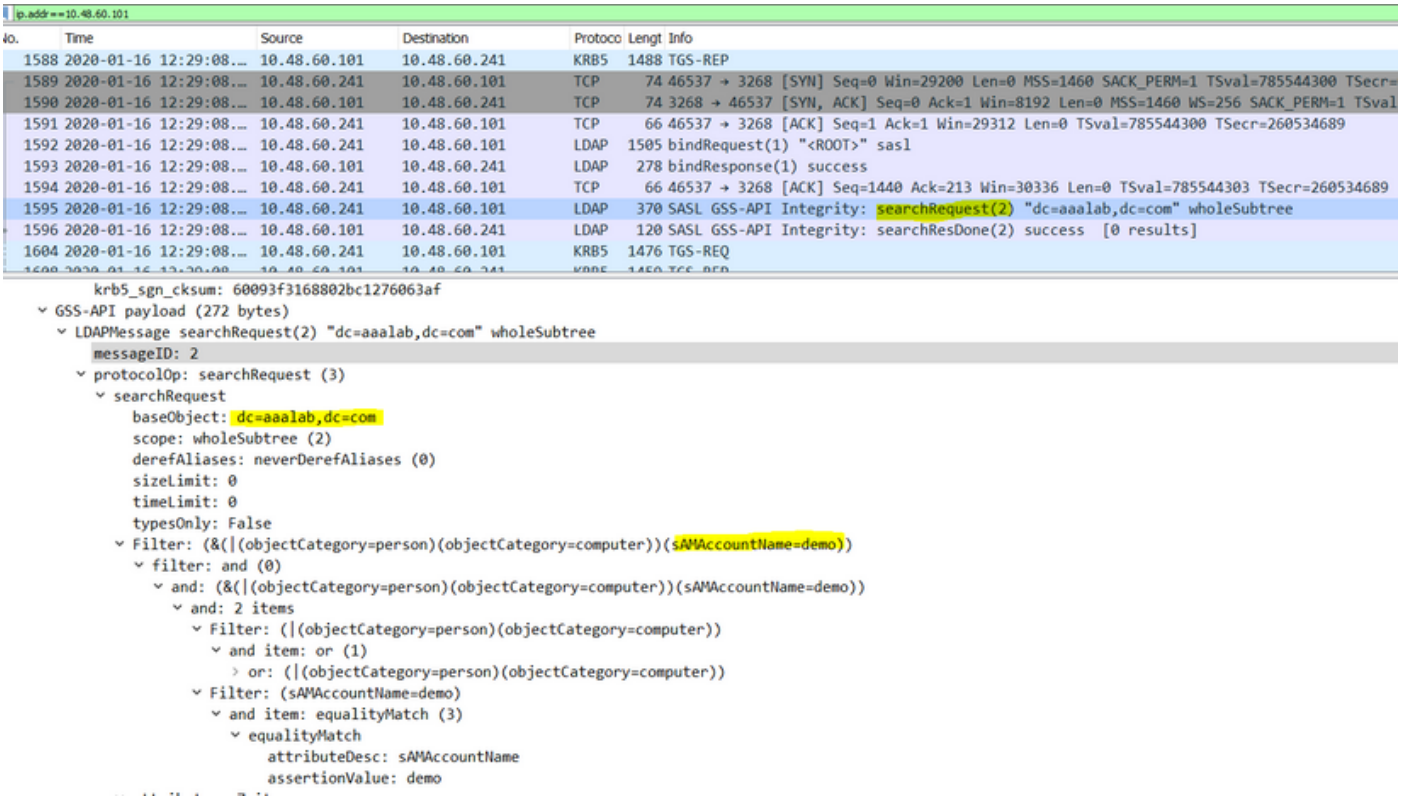
8. aguarde 10 minutos para que a descriptografia entre em vigor .

b. inicie as capturas no ISE.

c. reproduza o problema.

d. em seguida, parar e baixar a captura

"Logs" do cenário de trabalho:



Verificar

Aqui estão alguns exemplos de situações de trabalho e de inatividade que você pode encontrar e os registros que eles produzem.

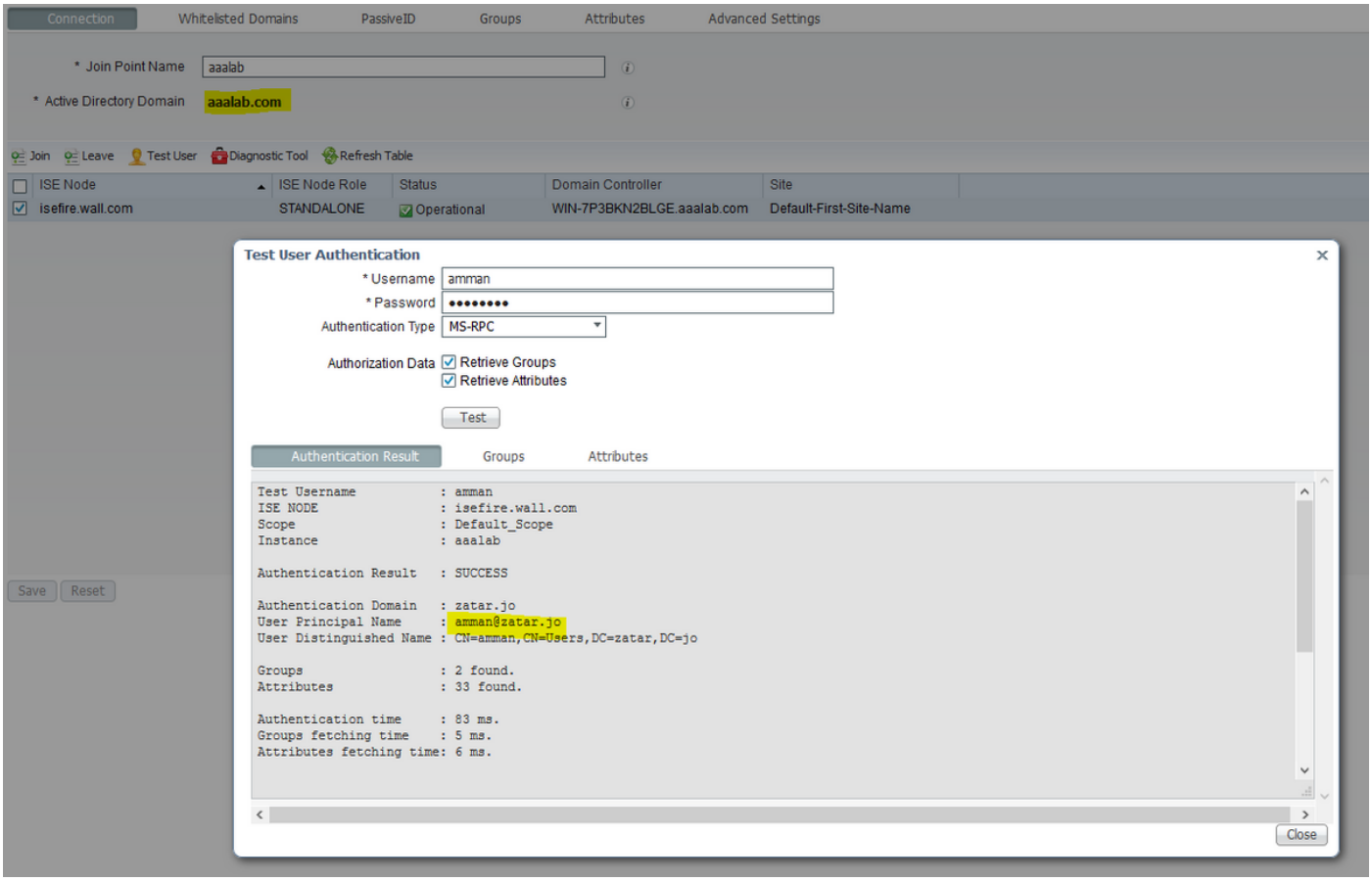
1. Autenticação baseada em grupos AD "zatar.jo":

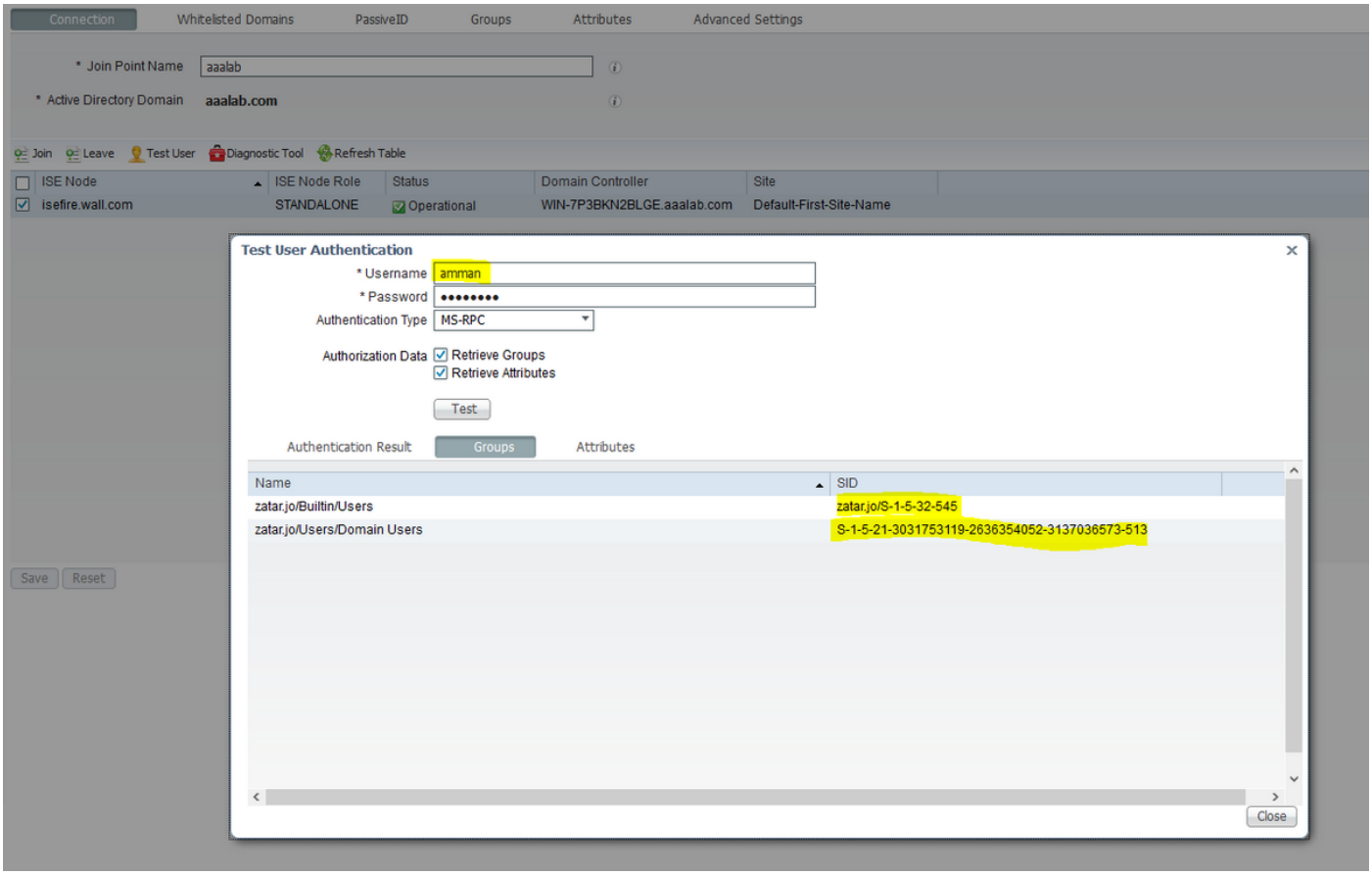
Se o grupo não for recebido da guia Grupo, você receberá esta mensagem de registro:

```
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
```

Precisamos recuperar os grupos em zatar.jo na guia Grupos.

Verificando recuperações de grupo AD na guia AD:





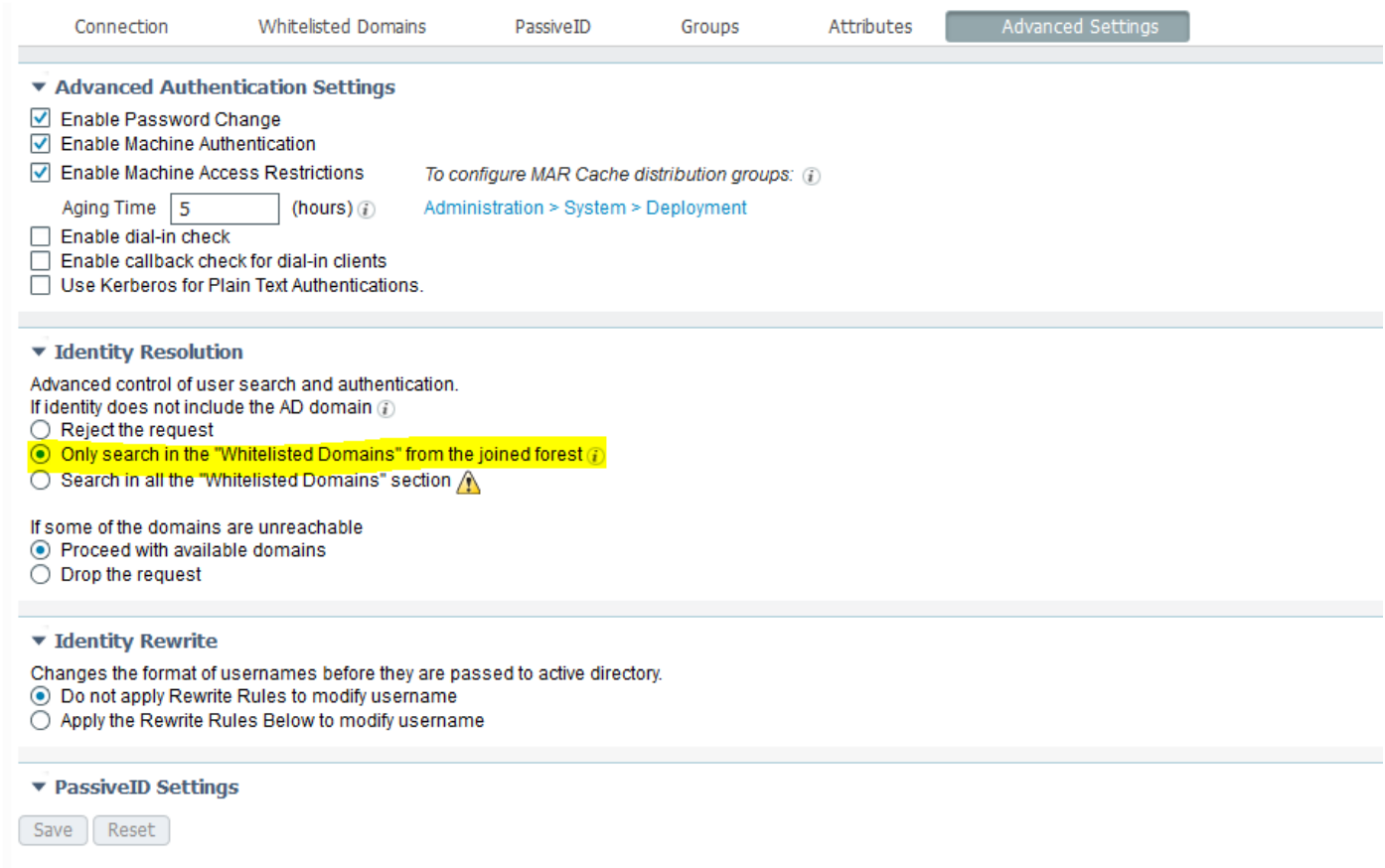
cenário de trabalho dos logs AD_agent.log:

```
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"
}
}
```

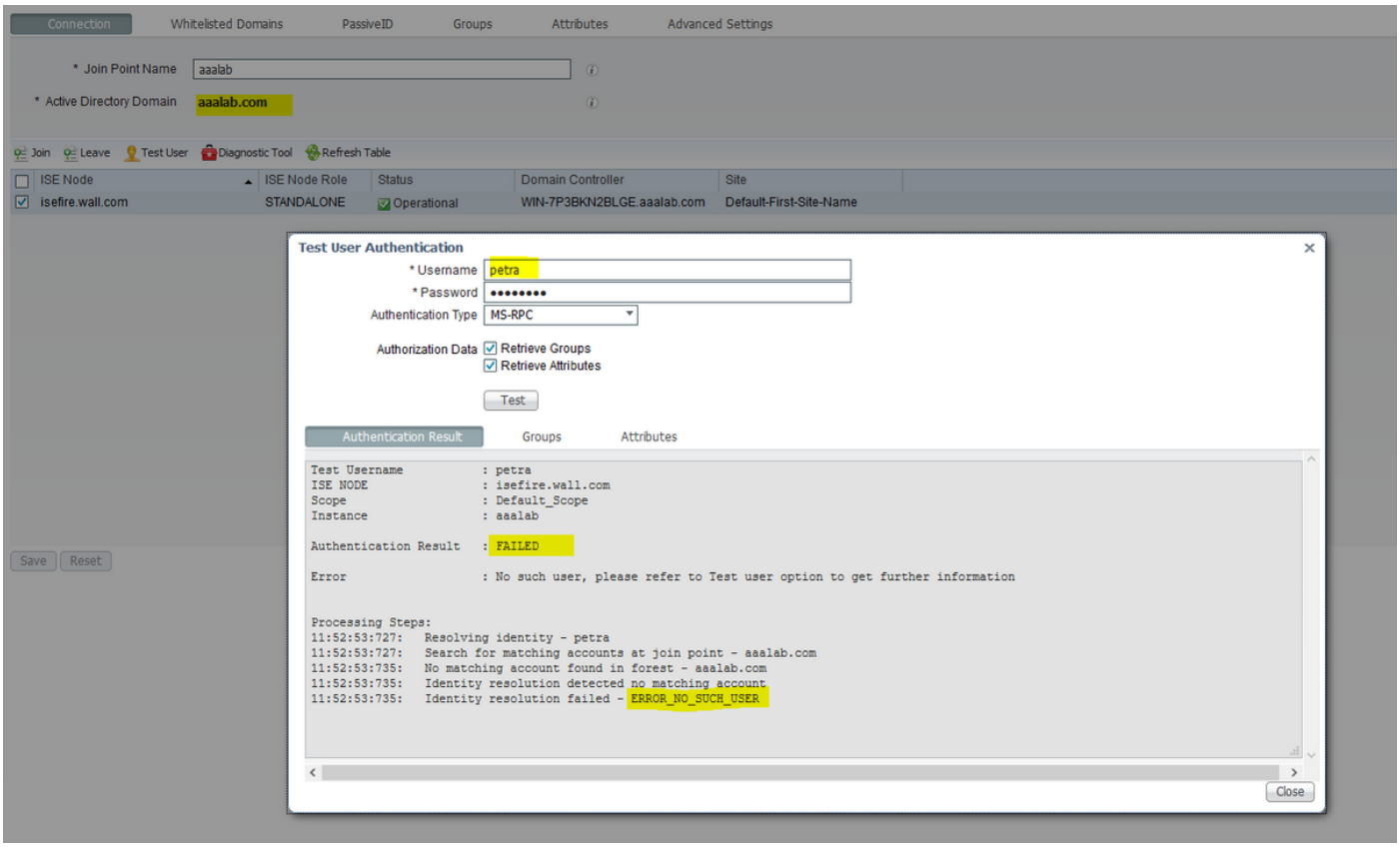
2. Se a opção avançada "Somente pesquisa em "Domínios em branco" da floresta unida" estiver marcada:



Quando você escolhe a opção "Apenas pesquisar em "Domínios em branco" da floresta unida", o ISE os marcou como off-line:

```
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
```

O usuário "petra" está em zatar.jo e falhará na autenticação, como a captura de tela abaixo:



Nos registros:

O ISE não conseguiu alcançar outros domínios, devido à opção avançada "Somente pesquisa nos "Domínios em branco" da floresta unida":

```
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
```