

# ISE e configuração do AD bidirecional

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificar](#)

[Troubleshoot](#)

[Verificar](#)

## 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 Active Directory .
- Autenticação de identidade externa no ISE.

## Componentes Utilizados

- ISE 2.x.
- dois Diretórios ativos.

## Configurar

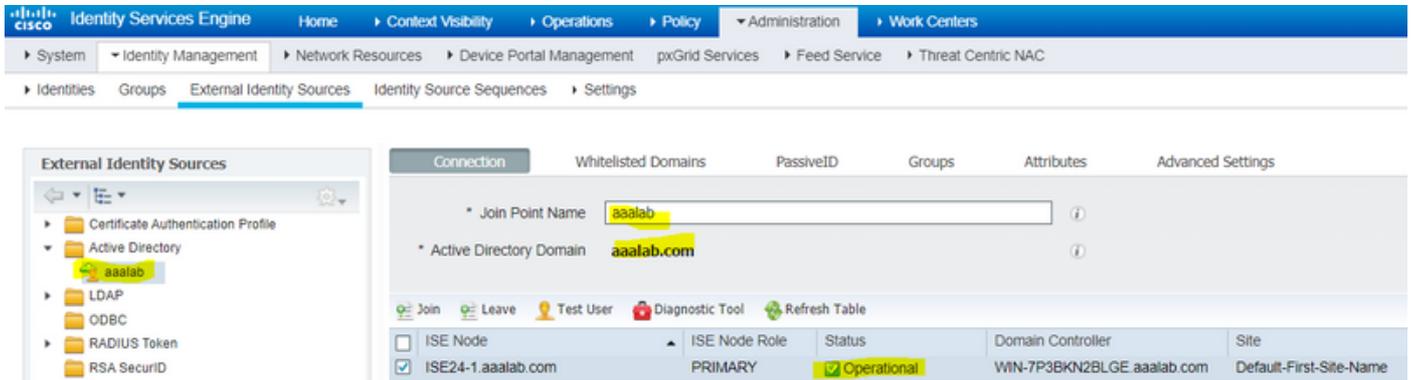
Para expandir seu domínio e incluir outros usuários em um domínio diferente daquele que já está associado ao ISE, você tem duas maneiras de fazer isso:

1. você pode adicionar o domínio manualmente e separadamente no ISE. com isso, você teria dois Active Directory 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:

External Identity Sources

Connection: **Whitelisted Domains** | PassiveID | Groups | Attributes | Advanced Settings

Use all Active Directory domains for authentication ⓘ

Enable Selected | Disable Selected | Show Unusable Domains

Name	Authenticate	Forest	SID
<input type="checkbox"/> aaalab.com	YES	aaalab.com	S-1-5-21-1366501036-25438103-262047587
<input type="checkbox"/> newlab.com	YES	newlab.com	S-1-5-21-927820924-690471943-4064067410
<input type="checkbox"/> sub.aaalab.com	YES	aaalab.com	S-1-5-21-1291856626-390840787-4184745074
<input checked="" type="checkbox"/> zatar.jo	YES	zatar.jo	S-1-5-21-3031753119-2636354052-3137036573

**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 }.

External Identity Sources

Connection | Whitelisted Domains | PassiveID | Groups | Attributes | **Advanced Settings**

**Advanced Authentication Settings**

- Enable Password Change
- Enable Machine Authentication
- Enable Machine Access Restrictions To configure MAR Cache distribution groups: ⓘ

Aging Time:  (hours) ⓘ Administration > System > Deployment

- Enable dial-in check
- Enable callback check for dial-in clients
- Use Kerberos for Plain Text Authentications.

**Identity Resolution**

Advanced control of user search and authentication.  
If identity does not include the AD domain ⓘ

- Reject the request ⓘ
- Only search in the "Whitelisted Domains" from the joined forest ⓘ
- Search in all the "Whitelisted Domains" section ⚠

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 ) :

## Test User Authentication

\* Username

\* Password

Authentication Type

Authorization Data  Retrieve Groups  
 Retrieve Attributes

Authentication Result	Groups	Attributes
Test Username	: demo	
ISE NODE	: ISE24-1.aalab.com	
Scope	: Default_Scope	
Instance	: aalab	
Authentication Result	: <b>SUCCESS</b>	
Authentication Domain	: <b>zatar.jo</b>	
User Principal Name	: demo@zatar.jo	
User Distinguished Name	: CN=demo,CN=Users,DC=zatar,DC=jo	
Groups	: 2 found.	
Attributes	: 33 found.	
Authentication time	: 41 ms.	
Groups fetching time	: 3 ms.	
Attributes fetching time	: 1 ms.	

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

## Test User Authentication

\* Username

\* Password

Authentication Type

Authorization Data  Retrieve Groups  
 Retrieve Attributes

Authentication Result	Groups	Attributes
Test Username	: kholoud	
ISE NODE	: ISE24-1.aaalab.com	
Scope	: Default_Scope	
Instance	: aaalab	
Authentication Result	: SUCCESS	
Authentication Domain	: aaalab.com	
User Principal Name	: kholoud@aaalab.com	
User Distinguished Name	: CN=kholoud,CN=Users,DC=aaalab,DC=com	
Groups	: 2 found.	
Attributes	: 32 found.	
Authentication time	: 33 ms.	
Groups fetching time	: 6 ms.	
Attributes fetching time	: 3 ms.	

## 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 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. 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 aalab :

```
2020-01-16 12:29:08,579 DEBUG ,140568690480896,AdIdentityResolver::search: do (&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=demo)) search in forest aalab.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 aalab, 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 Directory -> 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 Directory'.

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:**

```

ip.addr==10.48.60.101
No. Time Source Destination Protocol Length Info
1588 2020-01-16 12:29:08... 10.48.60.101 10.48.60.241 KRBS 1488 TGS-REP
1589 2020-01-16 12:29:08... 10.48.60.241 10.48.60.101 TCP 74 46537 → 3268 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=785544300 TSecr=
1590 2020-01-16 12:29:08... 10.48.60.101 10.48.60.241 TCP 74 3268 → 46537 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=
1591 2020-01-16 12:29:08... 10.48.60.241 10.48.60.101 TCP 66 46537 → 3268 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=785544300 TSecr=260534689
1592 2020-01-16 12:29:08... 10.48.60.241 10.48.60.101 LDAP 1505 bindRequest(1) "<ROOT>" sasl
1593 2020-01-16 12:29:08... 10.48.60.101 10.48.60.241 LDAP 278 bindResponse(1) success
1594 2020-01-16 12:29:08... 10.48.60.241 10.48.60.101 TCP 66 46537 → 3268 [ACK] Seq=1440 Ack=213 Win=30336 Len=0 TSval=785544303 TSecr=260534689
1595 2020-01-16 12:29:08... 10.48.60.241 10.48.60.101 LDAP 370 SASL GSS-API Integrity: searchRequest(2) "dc=aaalab,dc=com" wholeSubtree
1596 2020-01-16 12:29:08... 10.48.60.101 10.48.60.241 LDAP 120 SASL GSS-API Integrity: searchResDone(2) success [0 results]
1604 2020-01-16 12:29:08... 10.48.60.241 10.48.60.101 KRBS 1476 TGS-REQ
krb5_sgn_cksum: 60093f3168802bc1276063af
  GSS-API payload (272 bytes)
    LDAPMessage searchRequest(2) "dc=aaalab,dc=com" wholeSubtree
      messageID: 2
        protocolOp: searchRequest (3)
          searchRequest
            baseObject: dc=aaalab,dc=com
            scope: wholeSubtree (2)
            derefAliases: neverDerefAliases (0)
            sizeLimit: 0
            timeLimit: 0
            typesOnly: False
            Filter: (&(|(objectCategory=person)(objectCategory=computer)))(sAMAccountName=demo)
              filter: and (0)
                and: (&(|(objectCategory=person)(objectCategory=computer)))(sAMAccountName=demo)
                  and: 2 items
                    Filter: (|(objectCategory=person)(objectCategory=computer))
                      and item: or (1)
                        or: (|(objectCategory=person)(objectCategory=computer))
                    Filter: (sAMAccountName=demo)
                      and item: equalityMatch (3)
                        equalityMatch
                          attributeDesc: sAMAccountName
                          assertionValue: demo

```

## 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:

Connection | Whitelisted Domains | PassiveID | Groups | Attributes | Advanced Settings

\* Join Point Name:  ⓘ

\* Active Directory Domain: **aaalab.com** ⓘ

Join | Leave | Test User | Diagnostic Tool | Refresh Table

ISE Node	ISE Node Role	Status	Domain Controller	Site
<input checked="" type="checkbox"/> isefire.wall.com	STANDALONE	<input checked="" type="checkbox"/> Operational	WIN-7P3BKN2BLGE.aaalab.com	Default-First-Site-Name

**Test User Authentication**

\* Username:

\* Password:

Authentication Type:

Authorization Data:  Retrieve Groups,  Retrieve Attributes

**Authentication Result** | Groups | Attributes

```

Test Username      : amman
ISE NODE          : isefire.wall.com
Scope             : Default_Scope
Instance          : aaalab

Authentication Result : SUCCESS

Authentication Domain : zatar.jo
User Principal Name  : amman@zatar.jo
User Distinguished Name : CN=amman,CN=Users,DC=zatar,DC=jo

Groups             : 2 found.
Attributes          : 33 found.

Authentication time   : 83 ms.
Groups fetching time  : 5 ms.
Attributes fetching time: 6 ms.

```

Connection | Whitelisted Domains | PassiveID | Groups | Attributes | Advanced Settings

\* Join Point Name:  ⓘ

\* Active Directory Domain: **aaalab.com** ⓘ

Join | Leave | Test User | Diagnostic Tool | Refresh Table

ISE Node	ISE Node Role	Status	Domain Controller	Site
<input checked="" type="checkbox"/> isefire.wall.com	STANDALONE	<input checked="" type="checkbox"/> Operational	WIN-7P3BKN2BLGE.aaalab.com	Default-First-Site-Name

**Test User Authentication**

\* Username:

\* Password:

Authentication Type:

Authorization Data:  Retrieve Groups,  Retrieve Attributes

**Authentication Result** | Groups | Attributes

Name	SID
zatar.jo/Builtin/Users	zatar.jo/S-1-5-32-545
zatar.jo/Users/Domain Users	S-1-5-21-3031753119-2636354052-3137036573-513

### 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"  
}  
}
```

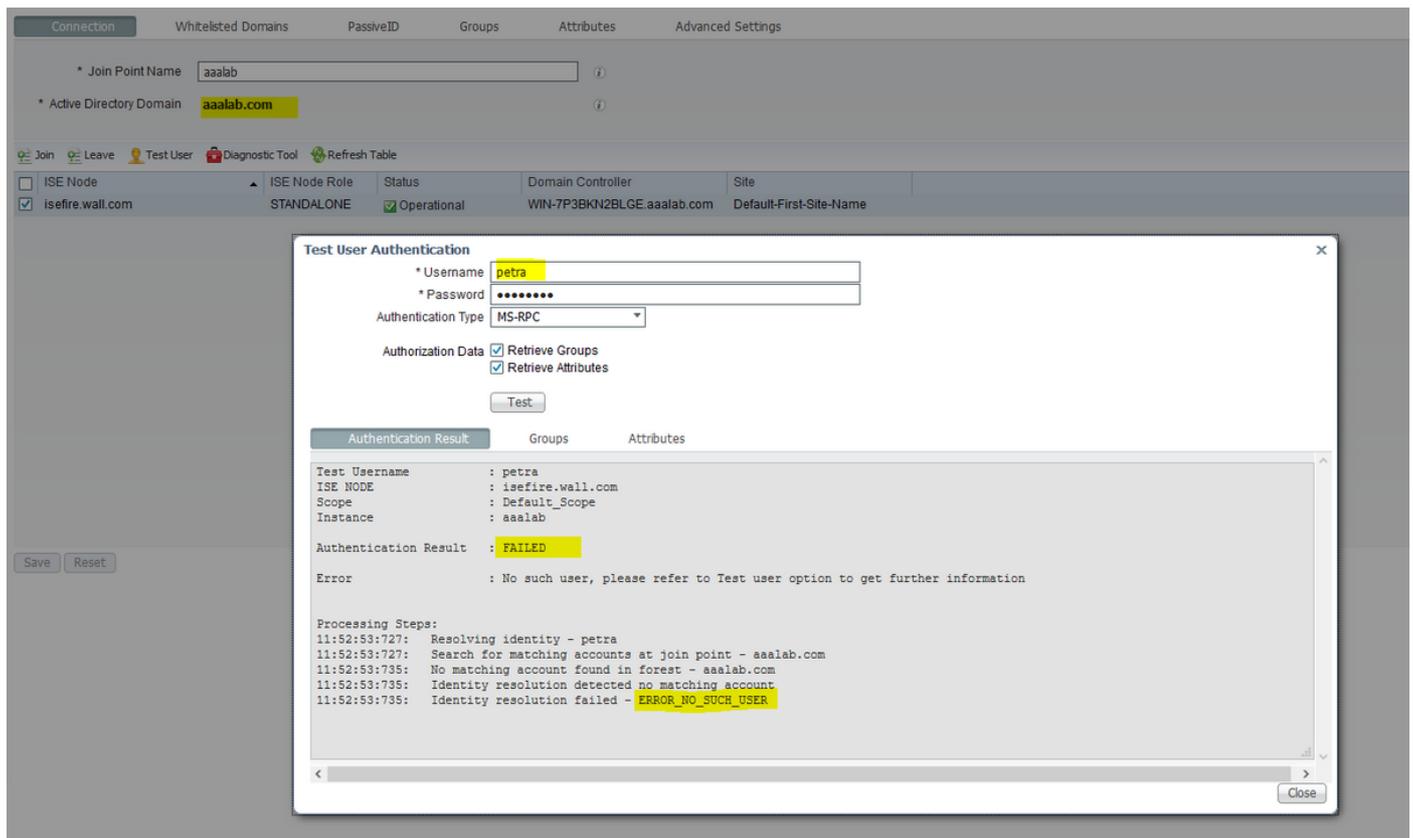
## 2. Se a opção avançada "Somente pesquisa em "Domínios em branco" da floresta unida" estiver marcada:

The screenshot shows the 'Advanced Settings' tab of a configuration interface. The 'Advanced Authentication Settings' section includes options for password change, machine authentication, and machine access restrictions. The 'Identity Resolution' section is highlighted, showing the option 'Only search in the "Whitelisted Domains" from the joined forest' selected. The 'PassiveID Settings' section is also visible at the bottom.

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 aalab.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
```