

ISE و 2way trust ad configuration

تايوت حمل

[عمدق مل](#)

[ةيساس ال ا تاب ل ط ت مل](#)

[تاب ل ط ت مل](#)

[عمدختس مل ا تانوك مل](#)

[نيوكت ل](#)

[ةحصل مل نم ق قحت ل](#)

[اهالصل او اطاخ ال ا فاش كتس](#)

[ةحصل مل نم ق قحت ل](#)

عمدق مل

ةيفي ك : طيس ب نيوكت ل ا ث م و ISE لى لى "هاجت ال ا ةجود زم ل ا ة ق ث ل ا" في رعت دن ت س م ل ا اذ ه ف ص ي ر خ ا ن ا ل ع ا ي ف د و ج و م ه ن ك ل و ISE ب ل ص ت م ل ن ا ل ع ا ل ا ي ف د و ج و م ر ي غ م د خ ت س م ة ق د ا ص م

ةيساس ال ا تاب ل ط ت مل

تاب ل ط ت مل

: ب ةيساس ا ة فرعم ك يد ل ن ا ب Cisco ي ص و ت

- ISE 2.x و Active Directory ج م د .
- ISE لى لى ة ج ر ا خ ل ا ة ي و ه ل ا ة ق د ا ص م .

عمدختس مل ا تانوك مل

- ISE 2.x .
- ن ي ط ش ن ن ي ل ي ل د .

نيوكت ل

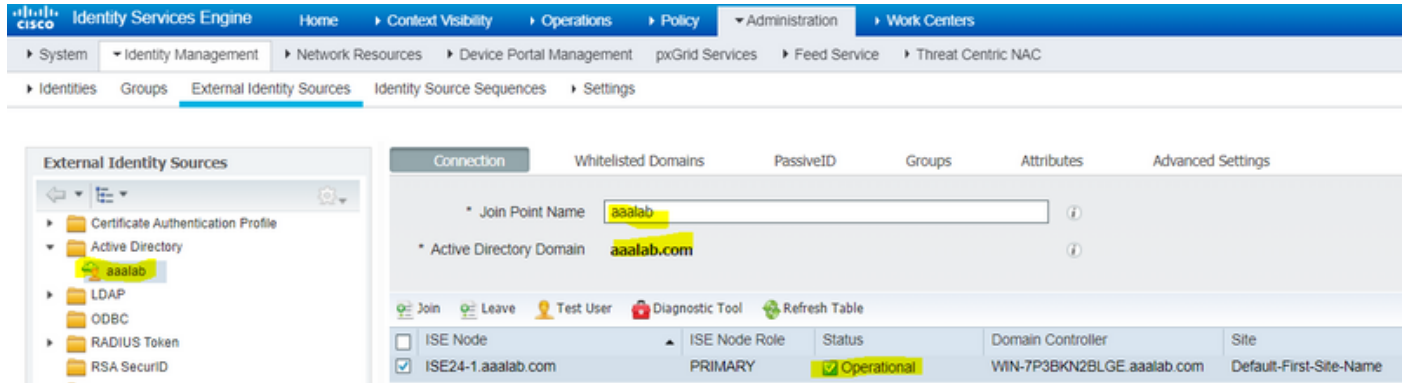
م م ض م ت ي ذ ل ا ل ا ج م ل ن ع ف ل ت خ م ل ا ج م ي ف ن ي ر خ ا ن ي م د خ ت س م ن ي م ض ت و ، ك ل ا ج م ع ي س و ت ل ج ا ن م : ك ل ذ ق ي ق ح ت ل ن ا ت ق ي ر ط ك ي د ل ، ISE لى لى ل ع ف ل ا ب

1. ن ي ل ي ل د ك ي د ل ن و ك ي س ، ك ل ذ د ن ع . ISE لى لى د ي ر ف ل ك ش ب و ا ي و د ي ل ا ج م ل ا ة ف ا ض ا ك ن ك م ي . ن ي ج ر ف ت م ن ي ط ي ش ن
2. ن ا ل ع ا ل ا اذ ه ن ي ب ه ا ج ت ا ل ا ة ج و د ز م ل ا ة ق ث ل ا ن ي و ك ت ب م ق م ث ، د ح و ISE ن ا ل ع ا لى لى م ض ن ا و ه و ، ن ي ت ق ي ر ط ب ة ق ث ن ي و ك ت و ه س ا س ا ل ا ي ف اذ ه . ISE لى لى ل ا ه ت ف ا ض ا ن و د ، ن ي ن ا ث ل ن ا ل ع ا ل ا و ا ي ا ق ل ت ISE م و ق ي س . ة ط ش ن ل ل لئ ا ل د ل ن م ر ث ك ا و ا ن ي ل ي ل د ن ي ب ه ن ي و ك ت م ت ي ر ا ي خ ت ا ل ا ج م ل ا " لى لى ا ه ت ف ا ض ا و AD ل ص و م م ا د خ ت س ا ب ا ه ب ق و ث و م ل ا ت ا ل ا ج م ل ا ه ذ ه ف ا ش ت ك ا ب ة ق ي ر ط ل ا ي ه ه ذ ه . ISE لى لى ا ه ي لى م ا م ض ن ا ل ا م ت ي ة ل ص ف ن م ت ا ن ا ل ع ا ك ا ه ت ل م ا ع م و " ا ض ا ب ل ا لى لى م ا م ض ن ا م ت ي م ل ي ذ ل ا و ، " AD "zatar.jo" ي ف م د خ ت س م ة ق د ا ص م ا ه ل ا ل خ ن م ك ن ك م ي ي ت ل

ISE.

AD و ISE نم لك ىلع نيوكتلا ءارج اذى لالتا تاوطخل فرصت

aalab لاجملا كيدل ، لاثملا اذى ف ، AD لى ISE مامضنا نم دكأت . 1 ةوطخل

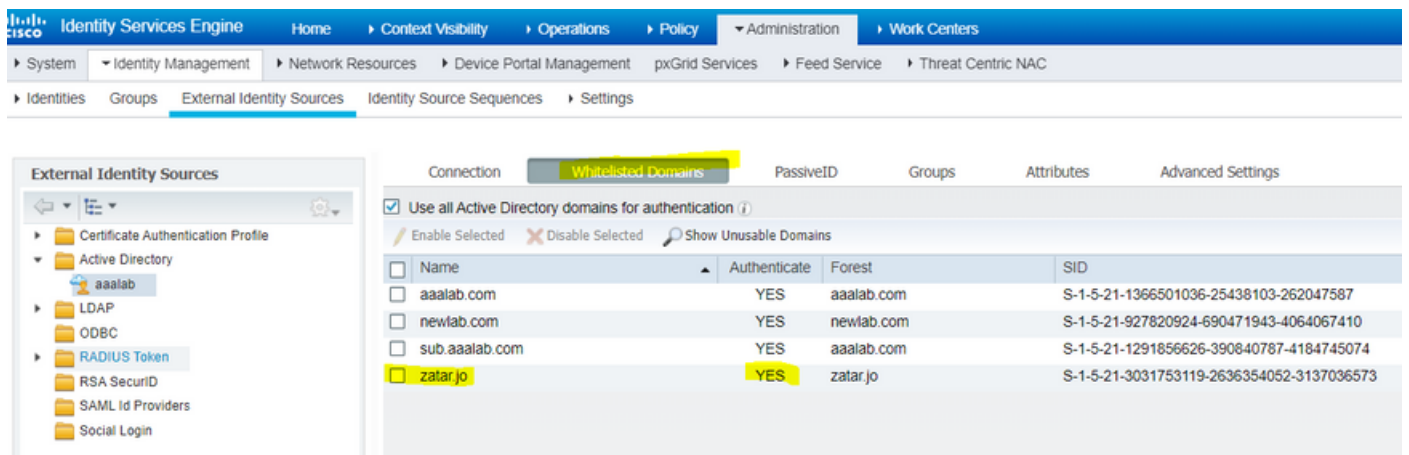


وه امك ، ةطشنلا لئال دل نم لك ني ب هاجتالا ةجودزملا ةقثلا نيكم نم دكأت . 2 ةوطخل
: هاندا حضورم

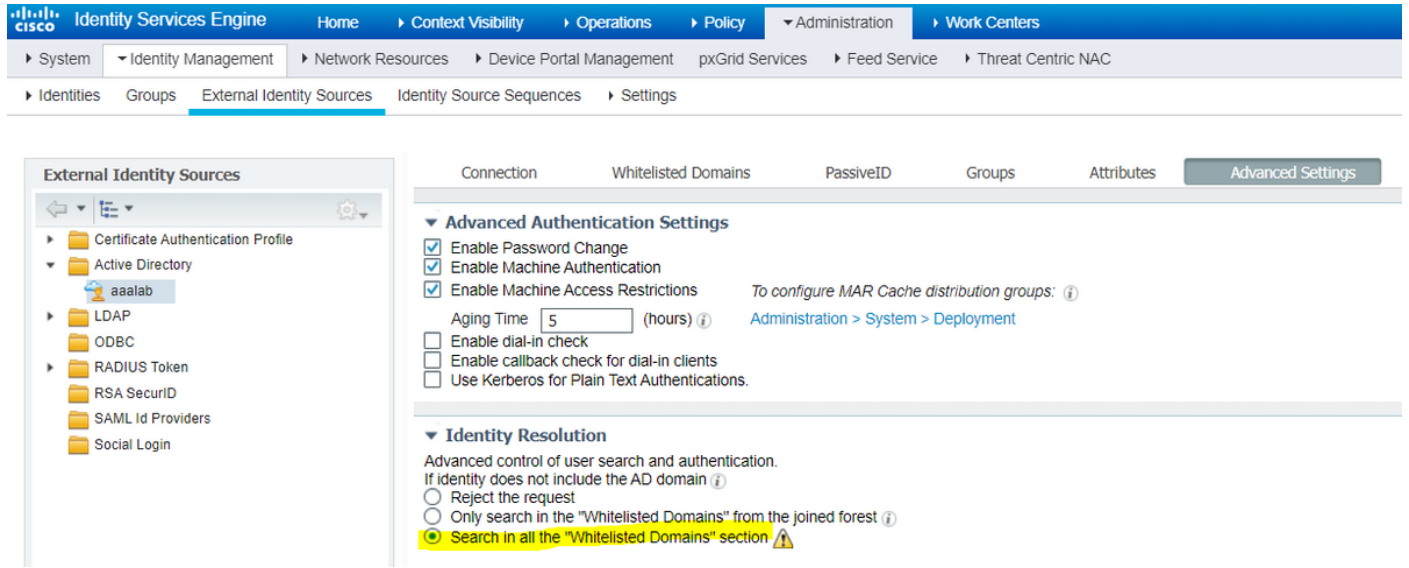
1. ةيفاضالا نامالا ةادأ Active Directory تالاجم حتفا .
2. م ، هل ةقث ةفاضلا ديتر يذلا لاجملا قوف نميالا سواملا رزب رقنا ، رسيالا ءزجلا ي ف "صئاصخ" ددح .
3. Trust ب يوبتلا ةمالع قوف رقنا .
4. ةديج ةقث رزلا قوف رقنا .
5. لالتلا قوف رقنا ، ةديجلا ةقثلا ءلام حتف دعب .
6. لالتلا قوف رقنا و AD لاجملا DNS مسا بتكا .
7. ةقثلا هاجتالا نع ةيالاتلا ءشاشلا لاسنيس ، DNS ربع لجال لباق AD لاجم نأ ضارتاب . لالتلا رقنا و هاجتالا يئانث ددح .
8. لالتلا قوف رقنا و اهتقداصم متيس يتلا دراوملا لك ددح ، ةرداصللا ةقثلا صئاصخل .
9. لالتلا قوف رقنا و اهتباتك دءأ ةقثلا رورم ةملك لخدأ .
10. نيترم لك لذ دعب تقطوط .

يا ثودح ءلاح ي ف Microsoft معد كارشلا نكمي ، Cisco معد قاطن جراخ AD نيوكت : **ةظحالم**
لكاشم .

ي ف رهظي نأ بجي و (zatar.jo) ديجال AD ب لاصلتالا (aalab) AD لاثملا نكمي ، اذى نيوكت درجم ب نوكي ذئدنعف ، هضرع متي مل اذى . هاندا حضورم وه امك ، "ءاضيبلا تالاجملا" بيوبتلا ةمالع :
: ححص ريغ ني هاجتاب ةقثلا نيوكت



هاندأ حضورم وه امك ،"اضيف لالاجملا" مسق لك يف راixel شحب نيكمتم نم دكأت 3 ةوطخل تاذ اهب قووم لالاجملا ك لذي يف امب ةلصل تاذ لالاجملا لك يف شحب لالاجملا سيمس م تيس ،ةطبارتملة باغل نم "اضيف لالاجملا" يف طقف شحب لالاجملا نيكمتم مت اذ .نيهاجتالا يف sub.aaalab.com :لف طلالاجم لاثم } .يسير لالاجم لل "عباتلا" تالاجم يف طقف شحب لالاجم لالاعا ةشاشلا ةطلل .



zatar.com و aaalab.com يف مدختسملا نع شحب لالاجم ISE موقوي نأ نكمي ،نألا

ةحصلال نم ققحتلا

لالاجم يف دوجوم لالاجملا مدختسملا مدختسأ ،"مدختسملا رابتخا" راixel ربع لمعي هئا نم ققحت يف سيل وه ،"zatar.jo" لالاجم يف طقف دوجوم "demo" مدختسملا ،لالامل اذه يف ("zatar.jo" : هاندأ رابتخالا ةجيتن نوكت ،"aaalab.com") :

Test User Authentication

* Username

* Password

Authentication Type

Authorization Data Retrieve Groups
 Retrieve Attributes

Authentication Result	Groups	Attributes
Test Username	: demo	
ISE NODE	: ISE24-1.aaalab.com	
Scope	: Default_Scope	
Instance	: aaalab	
Authentication Result	: SUCCESS	
Authentication Domain	: zatar.jo	
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.	

: aaalab.com ف kholoud م دختسم ، اضيأ نولم عي ، aaalab.com ف ني م دختسم ل ا نأ ام لع

- nsf (ise-psc.log)
- nsf-session (ise-psc.log)

يالكشإ مدختسمب لاصتال، ةلكشملاجاتنإ ةداعإ ب.

م.د ةومجم عمج ج.

"تالجمس" لمعلل ويرانيس:

ad_agent.log فللملا يف ةقداصملا تالواجم لىصافت لىل ع روثعلل م تيس: ةظحال

ad_agent.log فلم نم :

هإجتإل لىئانثو راتازب ةقثلا لاصتال نم ققحتل:

```
2020-01-16 12:26:21,210 VERBOSE,140568698918656,LsaDmEngineDiscoverTrustsForDomain: Adding trust info zatar.jo (Other Forest, Two way) in forest zatar.jo,LsaDmEngineDiscoverTrustsForDomain(),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
```

aalab : يسيس لىل لاجملا يف "ةببىرت ةخسن" مدختسملا نع ثحبلا

```
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
```

لاجم يف هصحفب ISE موقيس كلذ عمو، Zatar لاجم يف دوجوم بببىرتل مدختسملا نأ ظحال) Aalab newlab.com لثم "ءاضيب" تالاجملا بببوتل ةمالع يف رخأ تالاجم يف م، الوأ Aalab UPN ةقحال مادختسا بجي، ةرشابم Zatar.jo صحفلو، يسيس لىل لاجملا يف شغلل بئجتل اذهب لوخدلا لىجستب مدختسملا موقى نأ بجي لىلاتلابو، ثحبلا ناكم ISE فرعت ثبب (demo.zatar.jo : قيسنتل).

zatar.jo يف "بببوتل ضرعل" مدختسملا نع ثحبلا نأل م تى

```
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 لاجم يف ةدوجوم "ةببىرت ةخسن" مدختسملا :

```
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"

طاقات لال تاي لمع عي مجت 2. ة و ط خ ل ا

انمق اذ ة عار ق ل ل ة ل باق نوكت ال ى تح ، AD/LDAP و ISE ن ي ب ة ل د اب ت م ل ا مز ح ل ا ر ي ف ش ت م ت ي ا .
ال و ا ه ر ي ف ش ت ك ف ن و د ط ا ق ت ل ل ا ل ت ا ي ل م ع ع ي م ج ت ب

ISE AD ():

1. ISE : " -> Active Directory -> ->
2. ISE .
3. 'Name' : Troubleshooting.EncryptionOffPeriod.
4. ''

< >

:

30

5. . .

6. ''

7. ' Active Directory.

8. 10 .

ب. ISE لى طاق ت ل ا ء د ب .

ج. ة ل ا س م ل ا خ ا س ن ت س ا -

د. ه ل ي ز ن ت و ط ا ق ت ل ل ا ل ف ا ق ي ا ب م ق م ث .

"تال ج س" ل م ع ل ا و ي ر ا ن ي س

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

```

تحصيل اسم ققحت ليا

يتل الجسلا لعل واهه جاوت دق يتل لمعل مدع فقاومو لمعل فقاوم لعل ةلثم ال ضع ب انه اهجتت.

1. تاعومجم ليا ةدنتسم ال ةقداصلم ال:

ةلاس ر لعل لصحتس ف ،ةومجم ليا بيوبتل ةم ال ع نم ةومجم ليا نييعت ةداع متي مل اذ هذه تالجسلا

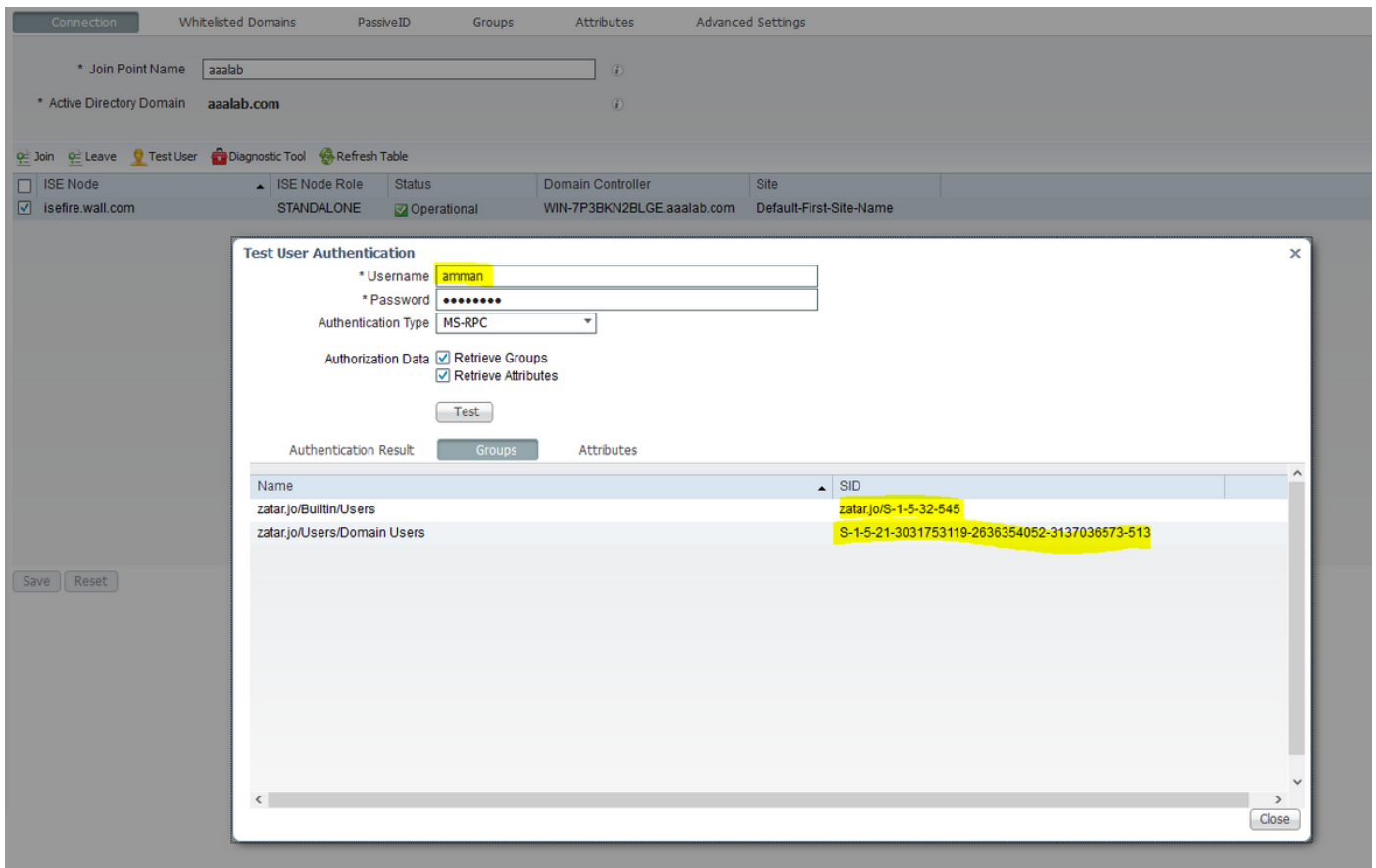
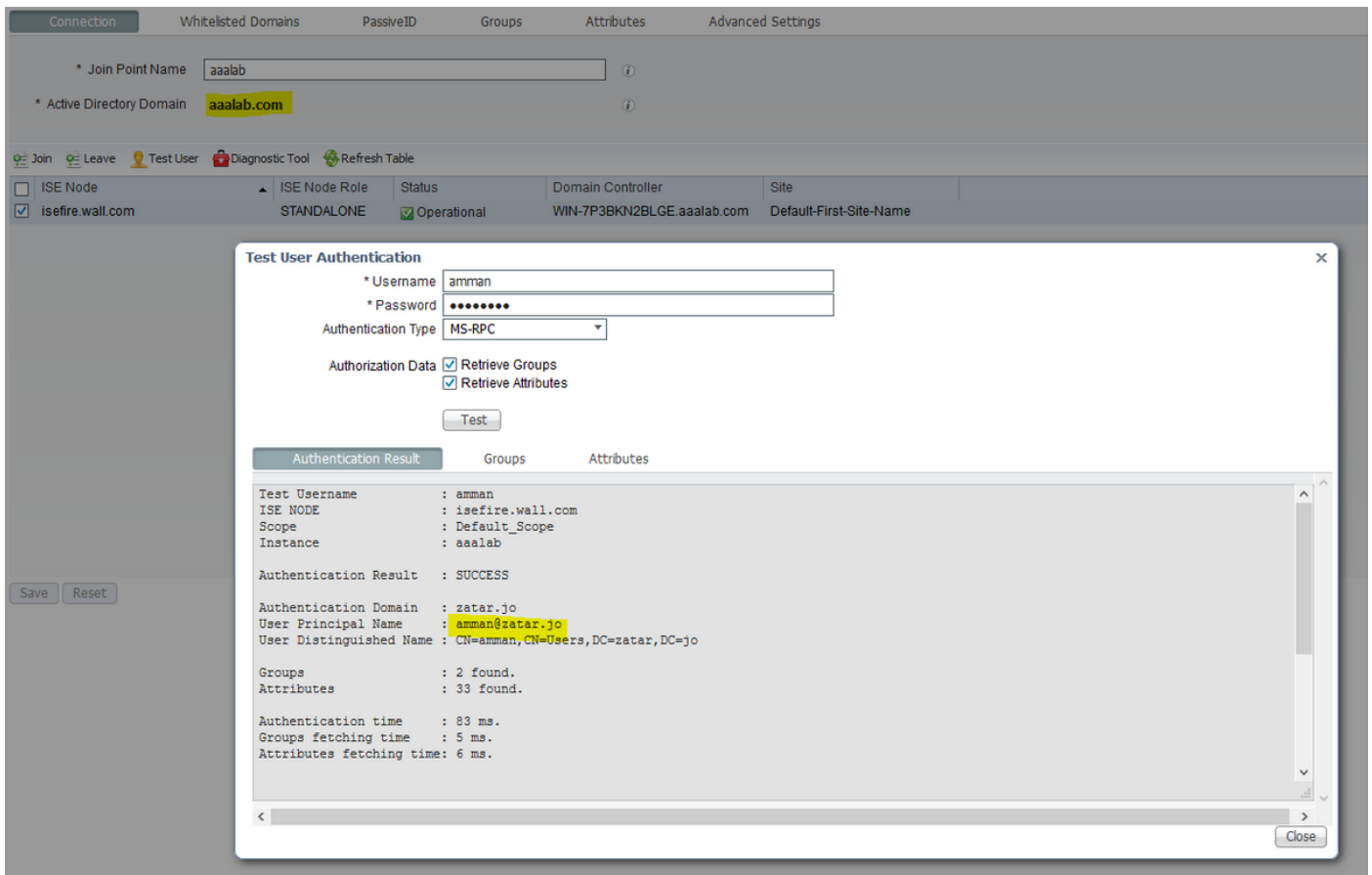
```

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

```

"تاعومجم" بيوبتل ةم ال ع نم zatar.jo في تاعومجم ليا دادرست ليا جاتحن.

AD بيوبتل ةم ال ع نم AD ةومجم ليا دادرست ليا نم ققحت ليا:



AD_AGENT.log: تالچسلا نم لمعالا ويرانيس

```
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"  
}  
}
```

ةباغل نم "ءاضيبل تالاجلم" يف طقف ثحبل" مدقتمل رايلال نم ققحتل مت اذ. 2
ةكرتشملا:

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 ⚠

If some of the domains are unreachable

Proceed with available domains

Drop the request

▼ **Identity Rewrite**

Changes the format of usernames before they are passed to active directory.

Do not apply Rewrite Rules to modify username

Apply the Rewrite Rules Below to modify username

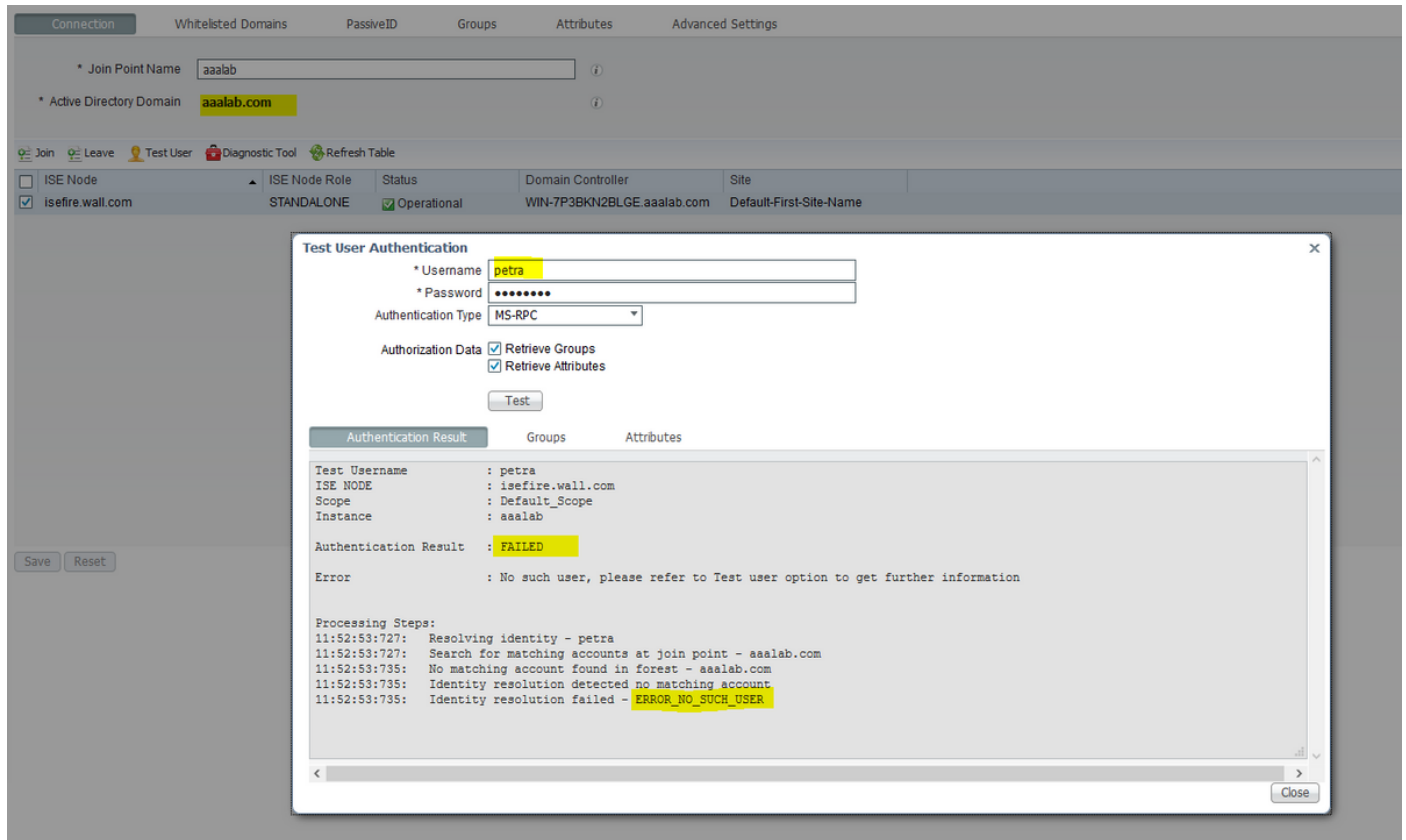
▼ **PassiveID Settings**

Save Reset

ISE ماق، "ةكرتشملا ةباغل نم "ءاضيبل تالاجلم" يف طقف ثحبل" رايلال راتخت ام دنع
لاصتا نود اه لعل ةمالع عوضوب:

```
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
```

هاندأ حضورم وه امك ،ةقداصلملا يف لش فيس و Zatar.jo عقوم يف دجوم "Petra" مدختسمل



تالجالسلا يف

يف طقف ثحبل" مدقتملا رايل ل ببسب ،يرخ تالجالسلا لوصولا نم ISE نكمتي مل
"ةطبترملا ةبالا نم "ءاضيبلا تالجالسلا"

```
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
```

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا