ISE和雙向信任AD配置

目錄

簡介

本檔案介紹ISE上「雙向信任」的定義，並舉一個簡單的組態範例：如何驗證加入ISE的AD中不存在但在另一個AD中存在的使用者。

必要條件

需求

思科建議您瞭解以下方面的基本知識：

- ISE 2.x和Active Directory整合。
- ISE上的外部身份身份驗證。

採用元件

- ISE 2.x。
- 兩個Active Directories。

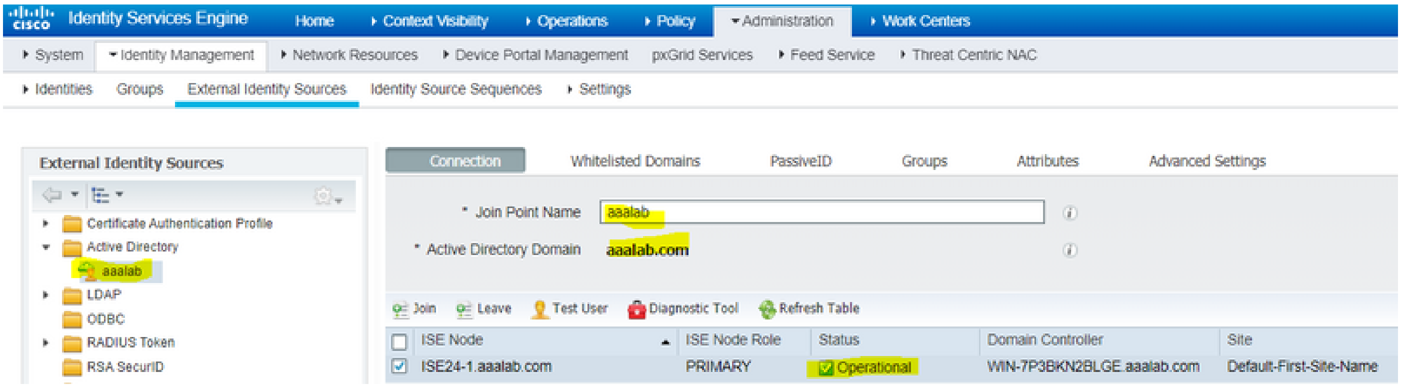
設定

若要擴展您的域，並將其他使用者包括在已加入ISE的其他域以外的其他域中，您有兩種方法：

1. 您可以在ISE上手動和單獨新增域。這樣，您就有兩個單獨的Active Directories。
2. 將一個AD加入ISE，然後配置此AD和第二AD之間的**雙向信任**，而不將其新增到ISE。這主要是雙向信任配置，它是在兩個或多個Active Directories之間配置的選項。ISE將使用AD聯結器自動檢測這些受信任域，並將其新增到「白名單域」，並將它們視為已加入ISE的獨立AD。這是您在AD「zatar.jo」（未加入ISE）中驗證使用者的方法。

以下步驟描述了ISE和AD上的配置過程：

步驟1.確保ISE已加入AD，在本例中，您有一個域aalab：



* Join Point Name: aaalab

* Active Directory Domain: aaalab.com

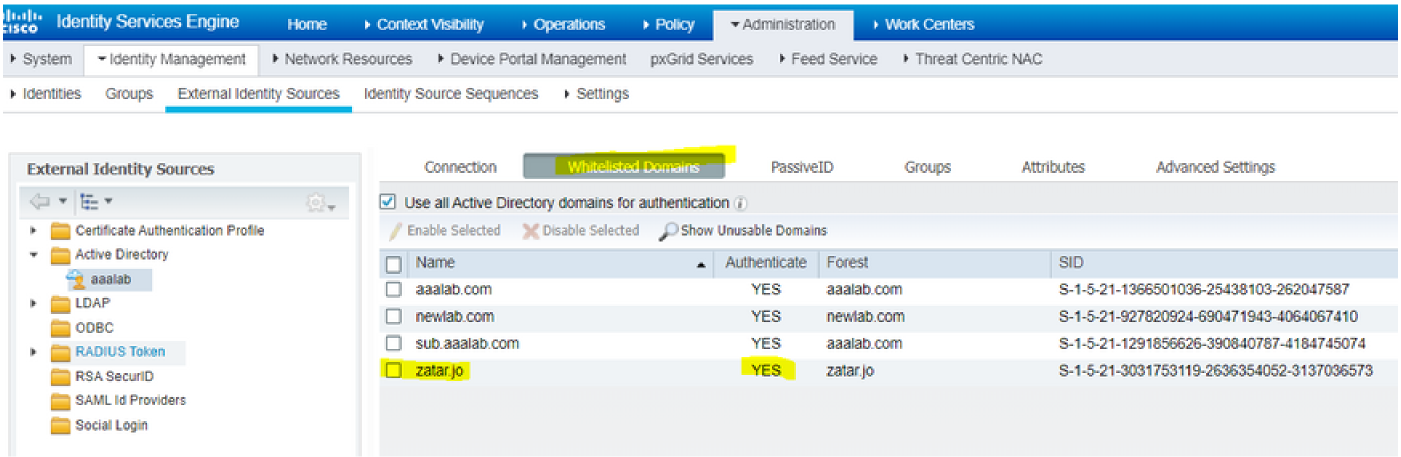
□	ISE Node	ISE Node Role	Status	Domain Controller	Site
☑	ISE24-1.aaalab.com	PRIMARY	✓ Operational	WIN-7P3BKN2BLGE.aaalab.com	Default-First-Site-Name

步驟2.確保在兩個Active Directories之間啟用雙向信任，如下所示：

1. 開啟Active Directory域和信任管理單元。
2. 在左窗格中，按一下右鍵要新增信任的域，然後選擇「屬性」。
3. 按一下「信任」頁籤。
4. 按一下「新建信任」按鈕。
5. 開啟新建信任嚮導後，按一下下一步。
6. 鍵入AD域的DNS名稱，然後按一下「下一步」。
7. 假設可以通過DNS解析AD域，則下一個螢幕將詢問信任方向。選擇Two-way，然後按一下Next。
8. 對於傳出信任屬性，選擇要進行身份驗證的所有資源，然後按一下下一步。
9. 輸入並再次鍵入信任密碼，然後按一下「下一步」。
10. 按一下兩次下一步。

附註：AD配置超出思科支援範圍，遇到任何問題都可以使用Microsoft支援。

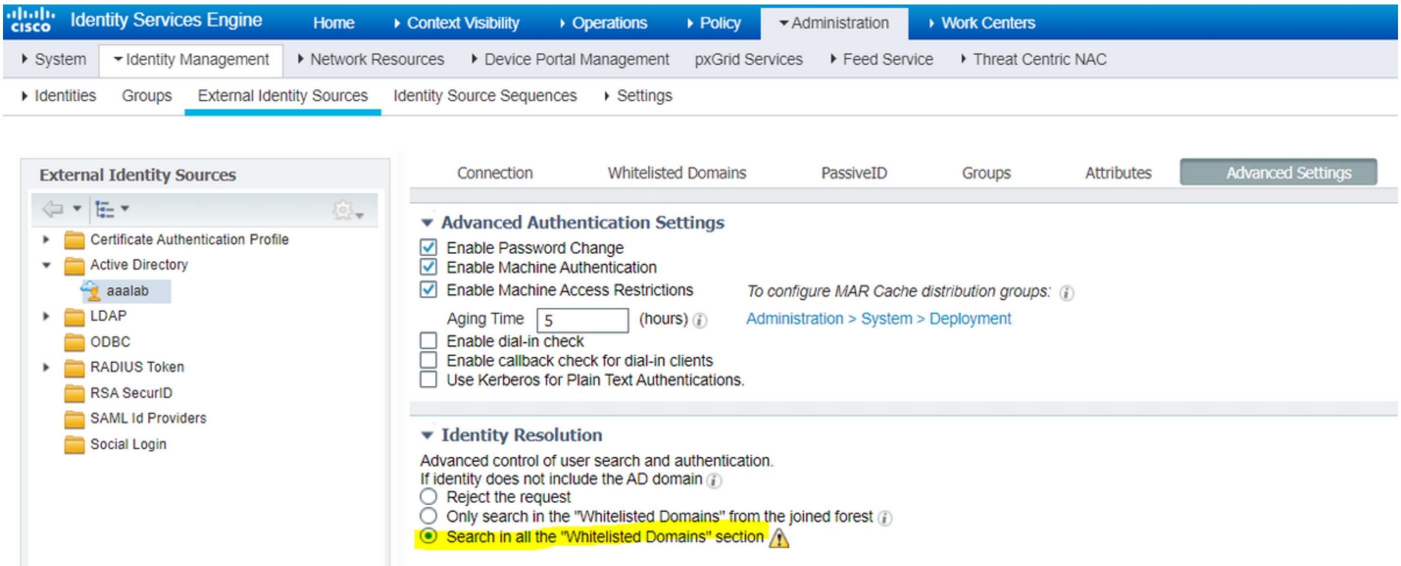
配置好此配置後，示例AD(aalab)可以與新AD(zatar.jo)通訊，它應會彈出「白名單域」頁籤，如下所示。如果未顯示，則雙向信任配置不正確：



☑ Use all Active Directory domains for authentication

□	Name	Authenticate	Forest	SID
□	aaalab.com	YES	aaalab.com	S-1-5-21-1366501036-25438103-262047587
□	newlab.com	YES	newlab.com	S-1-5-21-927820924-690471943-4064067410
□	sub.aaalab.com	YES	aaalab.com	S-1-5-21-1291856626-390840787-4184745074
□	zatar.jo	YES	zatar.jo	S-1-5-21-3031753119-2636354052-3137036573

步驟3.確保啟用所**有「白名單域」部分中的選項**搜尋，如下所示。它將允許在包括雙向受信任域在內的所有自訂域中進行搜尋。如果啟用選項**Only search in the "Whitelisted Domains" from the joined forest**，它將只在主域的「子」域中進行搜尋。{ child domain示例：sub.aaalab.com ，位於上面的螢幕截圖中}。



Advanced Authentication Settings

☑ Enable Password Change

☑ Enable Machine Authentication

☑ Enable Machine Access Restrictions

To configure MAR Cache distribution groups: Administration > System > Deployment

Aging Time 5 (hours)

□ 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

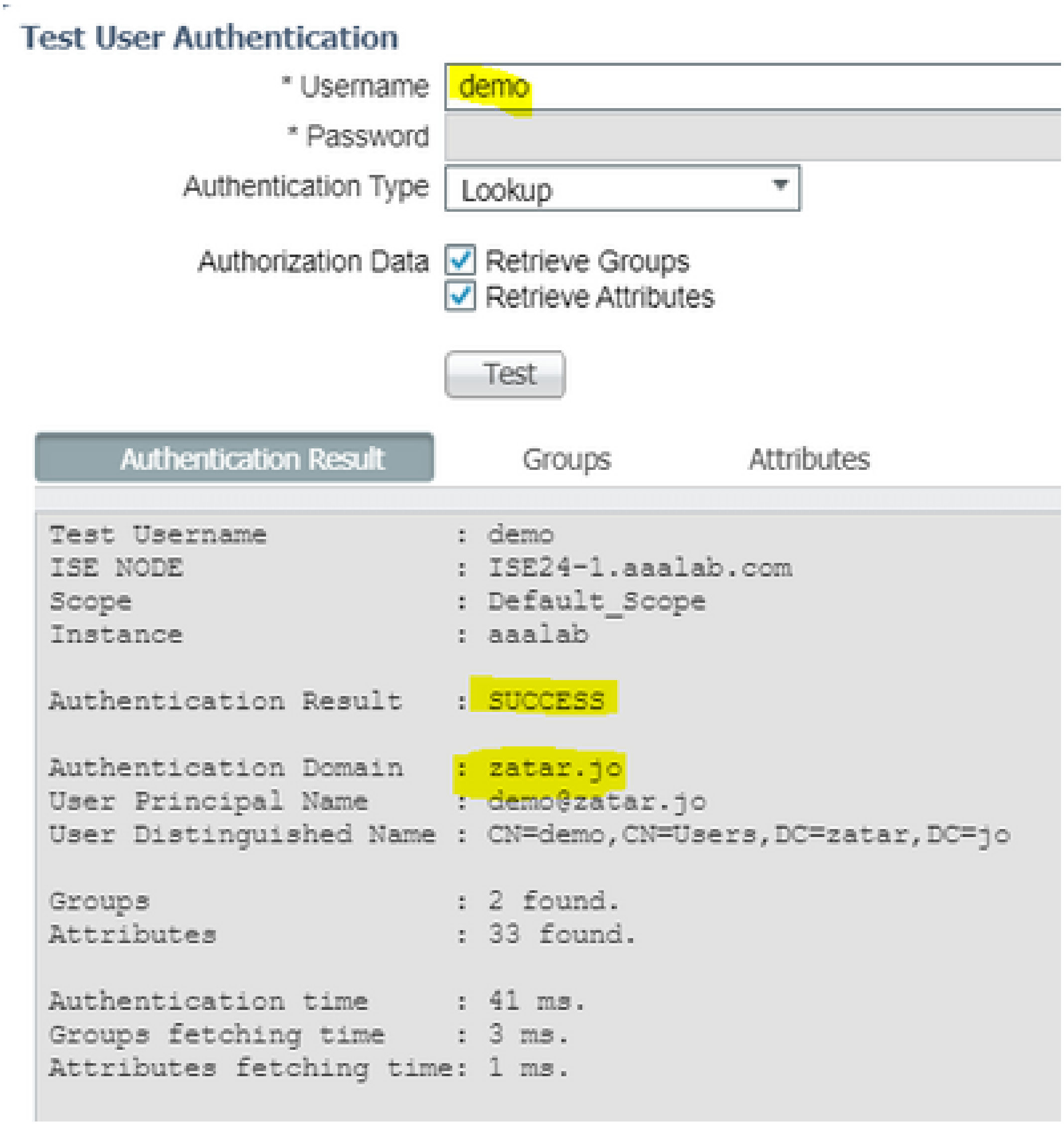
○ Only search in the "Whitelisted Domains" from the joined forest

● Search in all the "Whitelisted Domains" section

現在，ISE可以在aaalab.com和zatar.com中搜尋使用者。

驗證

驗證它是否通過「test user」選項起作用，使用位於「zatar.jo」域中的使用者（在本示例中，使用者「demo」僅存在於「zatar.jo」域中，而不存在於「aaalab.com」中，測試結果如下）：

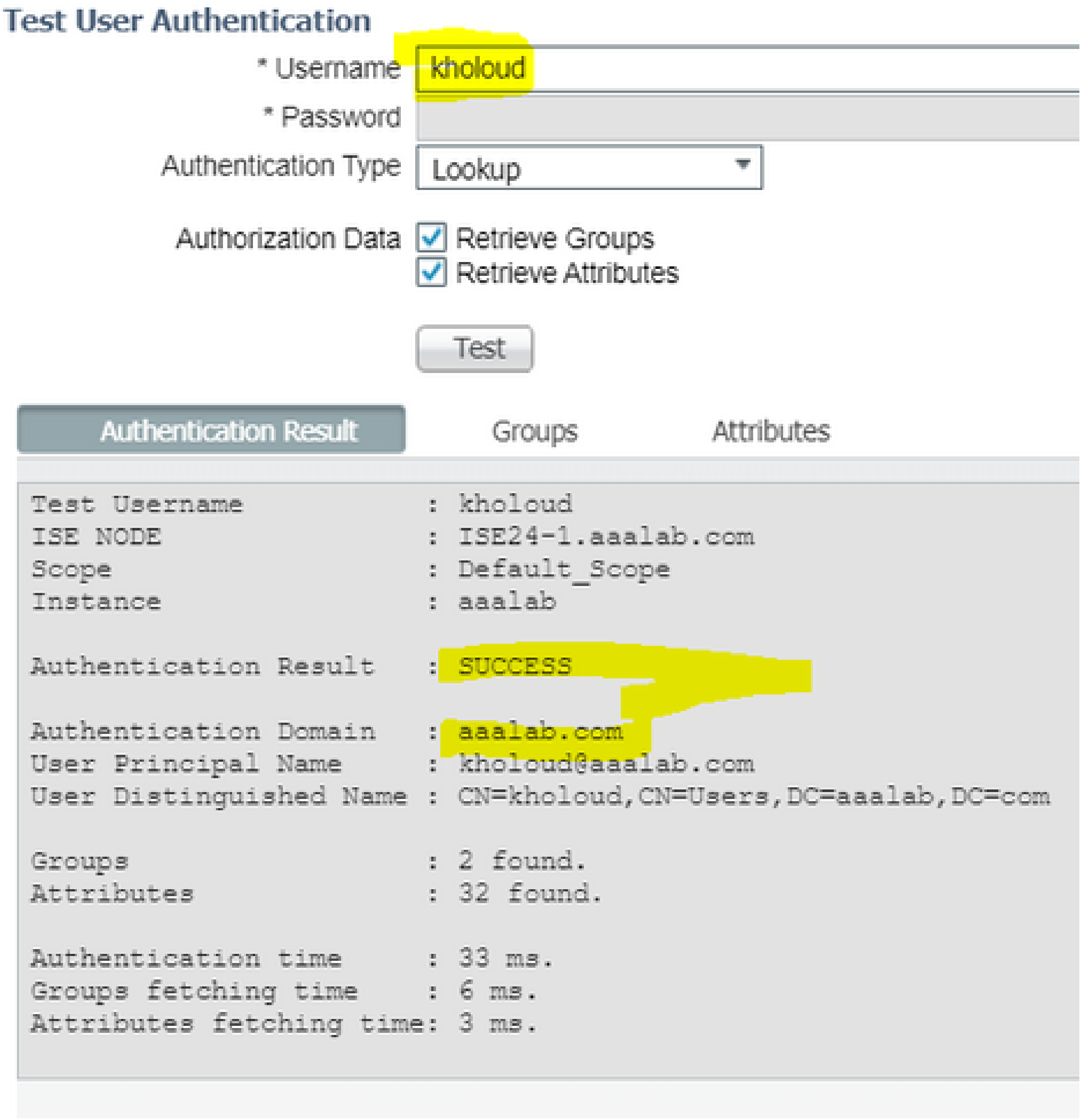


Test User Authentication

* Username	demo
* Password	
Authentication Type	Lookup
Authorization Data	☑ Retrieve Groups ☑ Retrieve 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.
```

請注意，aaalab.com中的使用者也在工作，user kholoud位於aaalab.com:



Test User Authentication

* Username kholoud

* Password

Authentication Type Lookup

Authorization Data ☑ Retrieve Groups
☑ Retrieve 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.
```

疑難排解

排除大多數AD/雙向信任問題（甚至大多數外部身份身份驗證）的主要過程有兩種：

1.收集啟用調試的ISE日誌（支援捆綁包）。在此支援捆綁包中的特定資料夾中，我們可以找到AD上任何身份驗證嘗試的所有詳細資訊。

2.收集ISE和AD之間的資料包捕獲。

步驟1.收集ISE日誌：

a.啟用調試，將以下調試設定為「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.重現問題，與有問題的使用者連線。

c.收集支援捆綁包。

<u>工作場景「日誌」：</u>

附註：身份驗證嘗試的詳細資訊，可在ad_agent.log檔案中找到

在ad_agent.log檔案中：

zatar雙向信任連線驗證：

```
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中搜尋使用者「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
```

(請注意，演示使用者位於zatar域中，但ise將首先在aalab域中檢查它，然後在「白色」域頁籤中的其他域，例如newlab.com。要避免在主域中執行檢查並直接簽入zatar.jo，您必須使用UPN字尾，以便ISE知道搜尋位置，因此使用者應使用以下格式登入：demo.zatar.jo)。

在zatar.jo中搜尋使用者「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
```

zatar域中的使用者「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"
```

步驟2.收集捕獲：

a.在ISE和AD/LDAP之間交換的資料包被加密，因此如果我們收集捕獲但不先解密它們，這些資料包將不可讀。

ISEAD

1. ISEID — > Active Directory -> — >
2. ISE
3. TROUBLESHOOTING.EncryptionOffPeriod
4.

<>

30

5.

6.

7.Active Directory

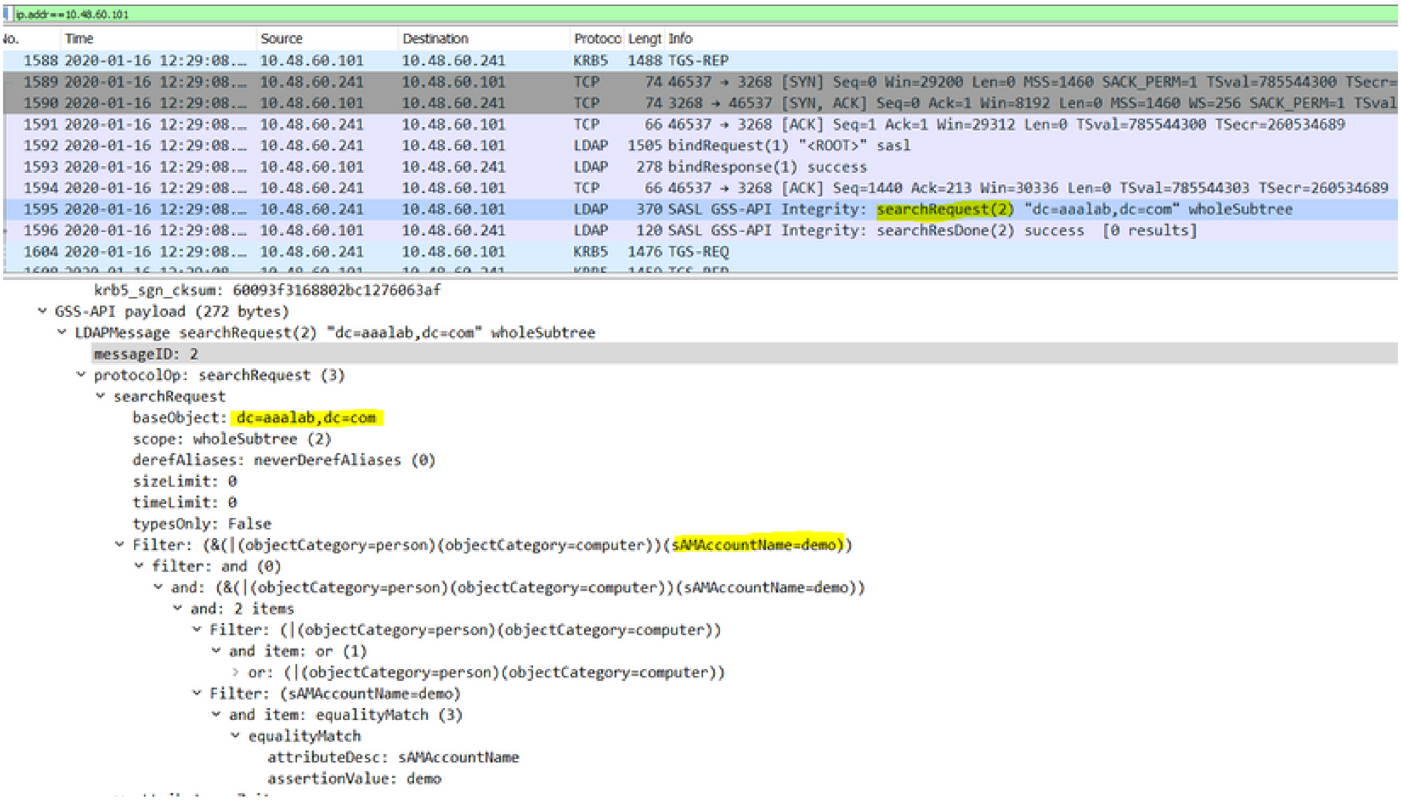
8.10

b.在ISE上啟動捕獲。

c.重現問題。

d.然後停止並下載捕獲

工作場景「日誌」：



```
No.   Time                    Source         Destination    Protoco Lengt Info
 1588 2020-01-16 12:29:08...  10.48.60.101   10.48.60.241   KRB5    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   KRB5    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
```

驗證

下面是一些您可能會遇到的工作和非工作情況及其生成的日誌的示例。

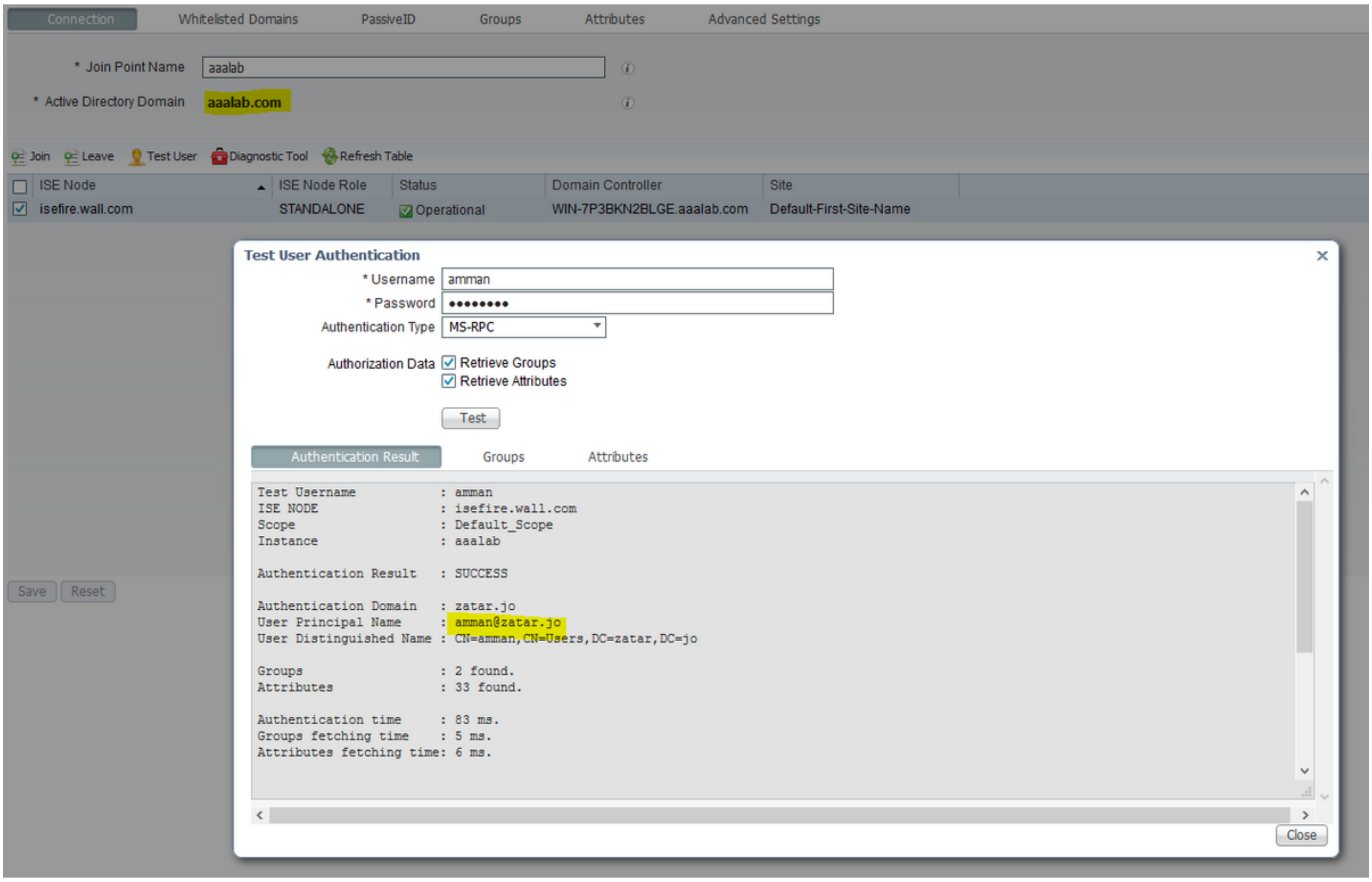
1.基於AD「zatar.jo」組的身份驗證：

如果組未從「組」頁籤中檢索，您將收到以下日誌消息：

```
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
```

我們需要從「組」頁籤檢索zatar.jo中的組。

從AD頁籤驗證AD組檢索：



* Join Point Name: aaalab

* Active Directory Domain: aaalab.com

□	ISE Node	ISE Node Role	Status	Domain Controller	Site
☑	isefire.wall.com	STANDALONE	☑ Operational	WIN-7P3BKN2BLGE.aaalab.com	Default-First-Site-Name

Test User Authentication

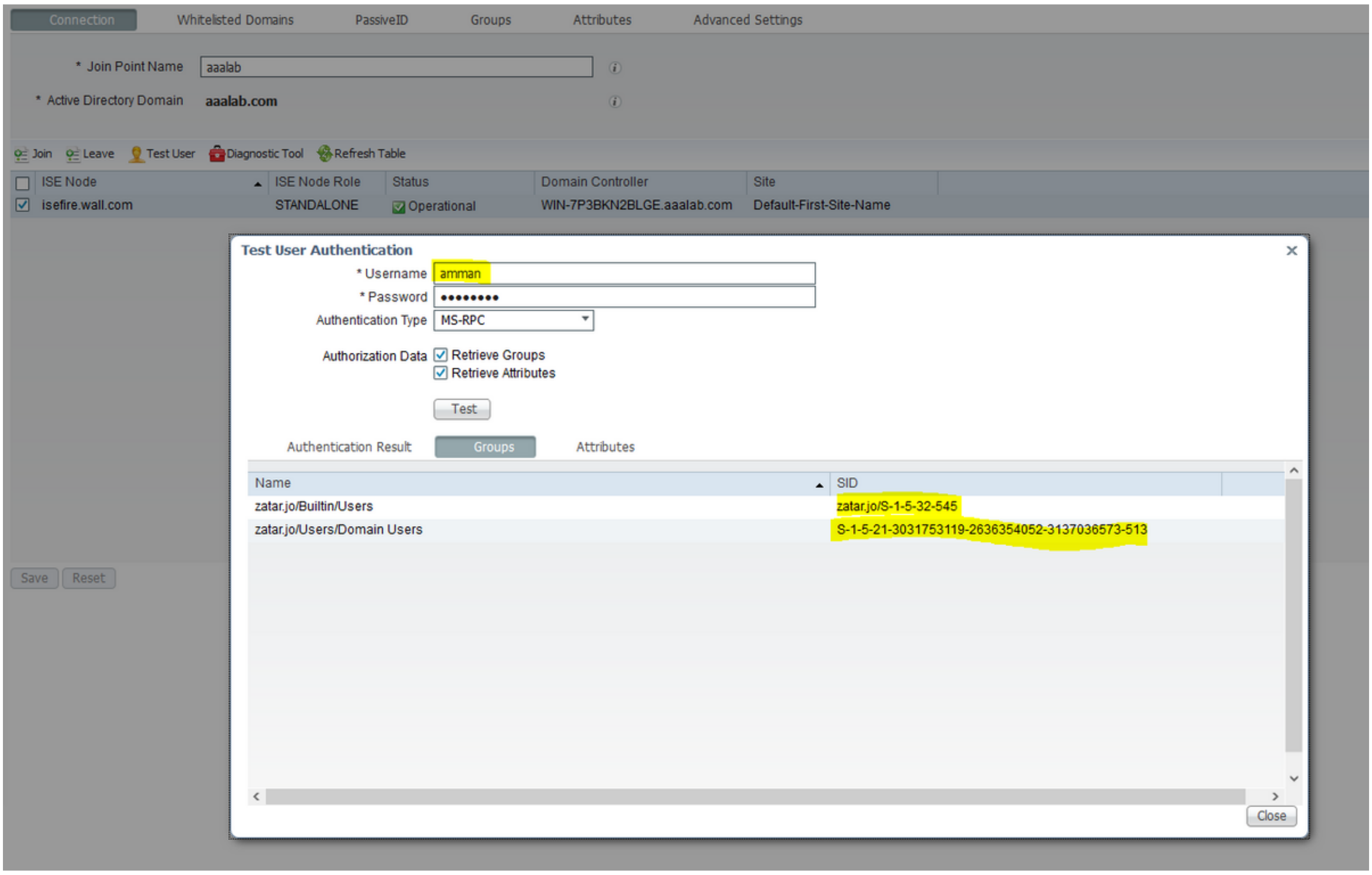
* Username: amman

* Password: ••••••••

Authentication Type: MS-RPC

Authorization Data: ☑ Retrieve Groups ☑ Retrieve 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.
```



* Join Point Name: aaalab

* Active Directory Domain: aaalab.com

□	ISE Node	ISE Node Role	Status	Domain Controller	Site
☑	isefire.wall.com	STANDALONE	☑ Operational	WIN-7P3BKN2BLGE.aaalab.com	Default-First-Site-Name

Test User Authentication

* Username: amman

* Password: ••••••••

Authentication Type: MS-RPC

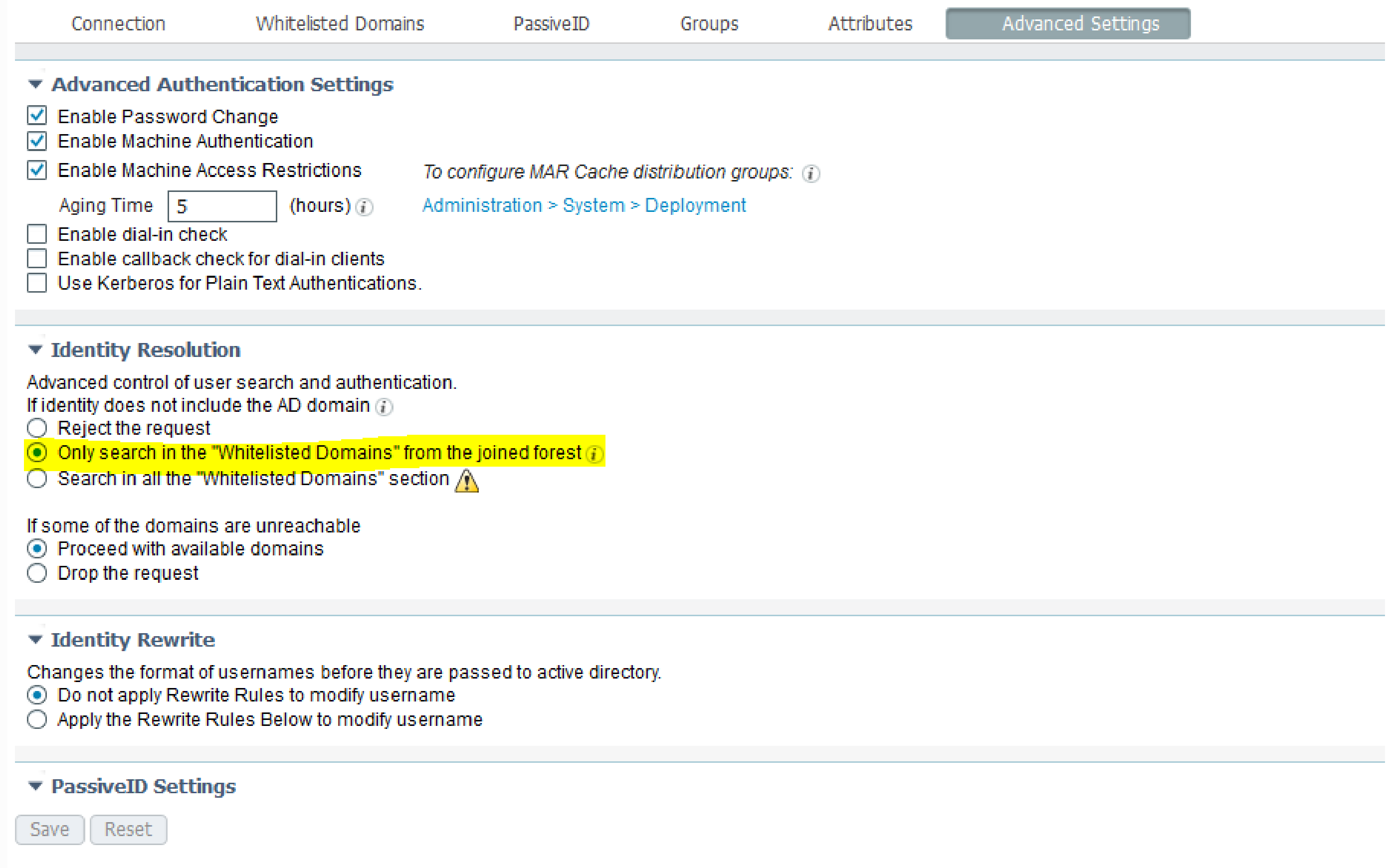
Authorization Data: ☑ Retrieve Groups ☑ Retrieve Attributes

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

工作方案在日誌AD_agent.log中：

```
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.如果選中高級選項「僅搜尋加入林中的「白名單域」：



▾ Advanced Authentication Settings

☑ Enable Password Change
☑ Enable Machine Authentication
☑ Enable Machine Access Restrictions

To configure MAR Cache distribution groups: ⓘ

Aging Time 5 (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

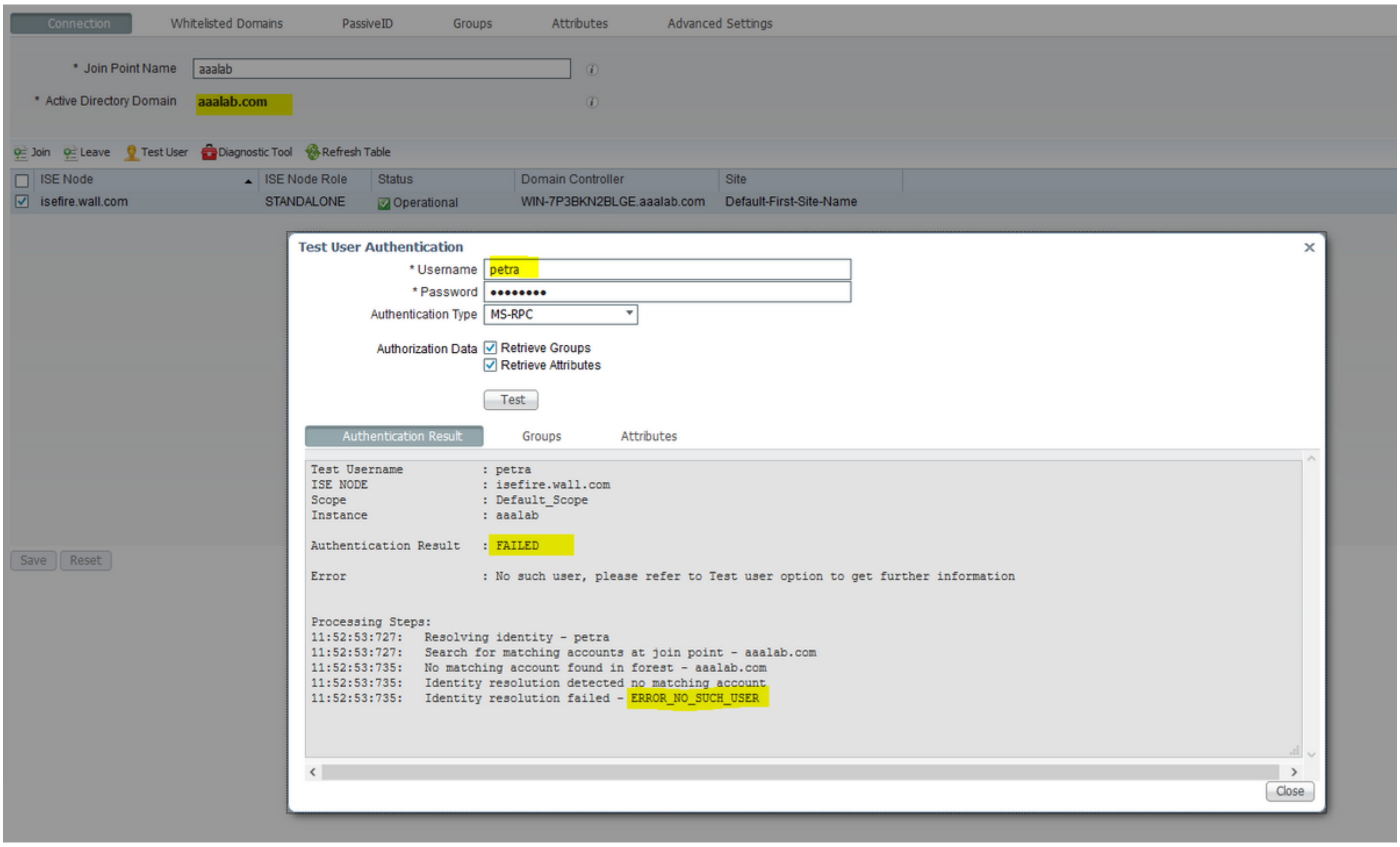
Changes the format of usernames before they are passed to active directory.
● Do not apply Rewrite Rules to modify username
○ Apply the Rewrite Rules Below to modify username

▾ PassiveID Settings

當您選擇「僅在加入林中的「白名單域」中搜尋」選項時，ISE會將其標籤為離線：

```
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
```

使用者「petra」位於zatar.jo中，身份驗證將失敗，如下面的螢幕截圖：



* Join Point Name: aaalab

* Active Directory Domain: aaalab.com

☐ ISE Node	ISE Node Role	Status	Domain Controller	Site
☑ isefire.wall.com	STANDALONE	☑ Operational	WIN-7P3BKN2BLGE.aaalab.com	Default-First-Site-Name

Test User Authentication

* Username: petra

* Password: ••••••••

Authentication Type: MS-RPC

Authorization Data: ☑ Retrieve Groups ☑ Retrieve Attributes

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

Authentication Result : FAILED

Error                 : No such user, please refer to Test user option to get further information


Processing Steps:
11:52:53:727:   Resolving identity - petra
11:52:53:727:   Search for matching accounts at join point - aaalab.com
11:52:53:735:   No matching account found in forest - aaalab.com
11:52:53:735:   Identity resolution detected no matching account
11:52:53:735:   Identity resolution failed - ERROR_NO_SUCH_USER
```

在日誌中：

ISE無法到達其他域，因為高級選項「僅在加入林中的「白名單域」中搜尋」：

```
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
```