Configuración de ISE y AD de confianza bidireccional

Contenido

Introducción

Este documento describe la definición de "confianza bidireccional" en ISE y un ejemplo de configuración simple : cómo autenticar a un usuario que no está presente en el AD unido a ISE, pero que está presente en otro AD.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre:

- Integración de ISE 2.x y Active Directory .
- Autenticación de identidad externa en ISE.

Componentes Utilizados

- ISE 2.x.
- dos directorios activos.

Configurar

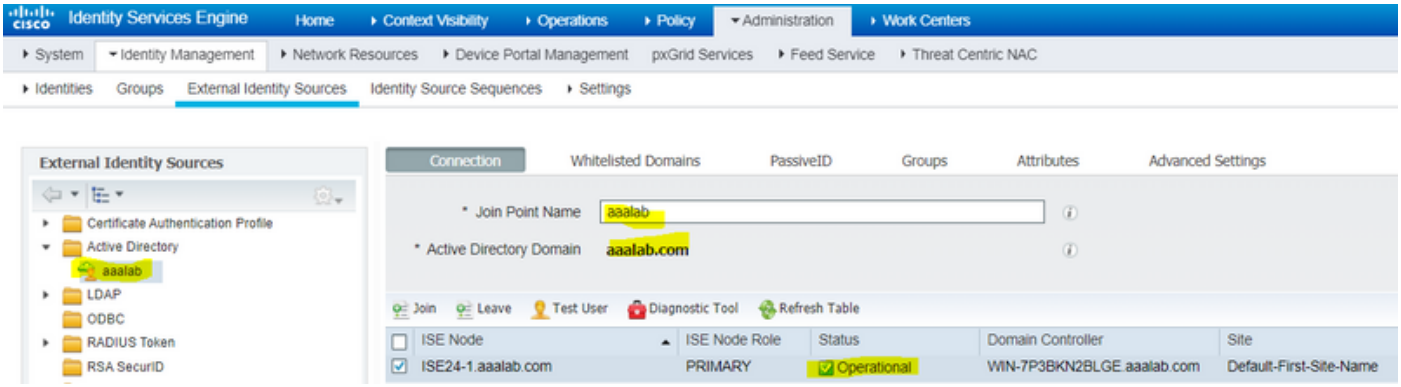
Para expandir su dominio e incluir a otros usuarios en un dominio diferente al que ya está unido a ISE, tiene dos maneras de lograr esto :

1. puede agregar el dominio de forma manual y separada en ISE. con esto, tendría dos directorios activos separados.
2. Únase a un AD en ISE y, a continuación, configure la **confianza bidireccional** entre este AD y el segundo AD, sin agregarlo a ISE. Se trata principalmente de una configuración de confianza bidireccional, es una opción que se configura entre dos o más directorios activos.

ISE detectará automáticamente estos dominios de confianza mediante el conector AD y los agregará a los "dominios de la lista blanca" y los tratará como AD independientes unidos a ISE. Así es como puede autenticar a un usuario en AD "zatar.jo", que no está unido a ISE.

Los siguientes pasos describen el procedimiento de configuración tanto en ISE como en AD:

paso 1. asegúrese de que ISE esté unido a AD; en este ejemplo, tiene el dominio aaalab :

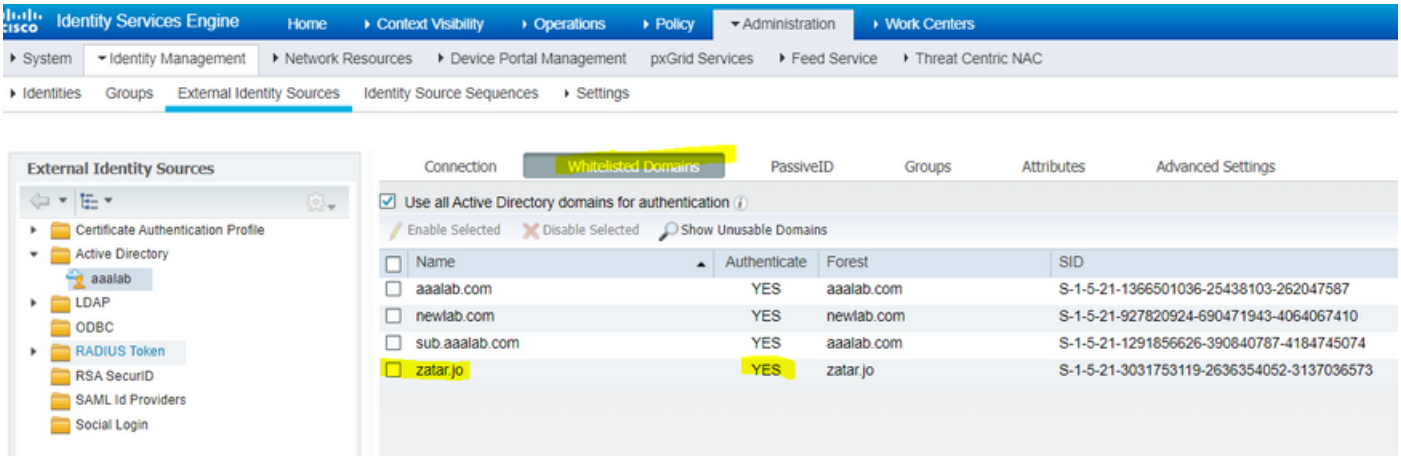


paso 2. asegúrese de que la confianza bidireccional esté habilitada entre ambos directorios activos, como se muestra a continuación :

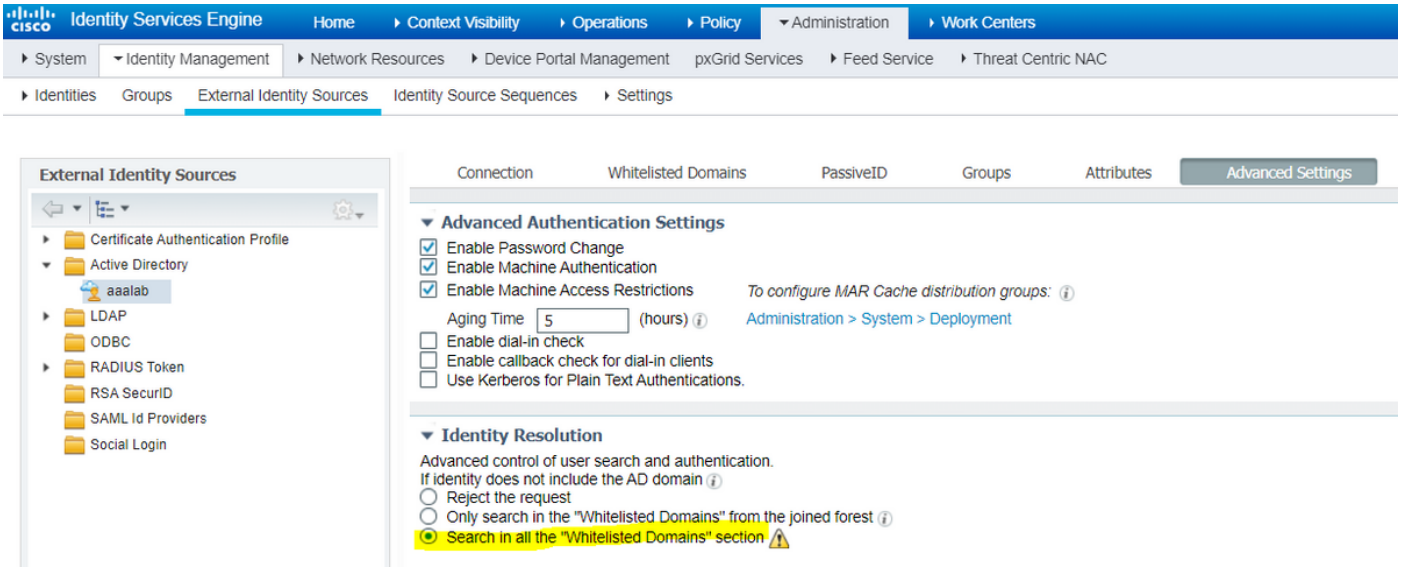
1. Abra el complemento Dominios y confianza de Active Directory.
2. En el panel izquierdo, haga clic con el botón derecho del ratón en el dominio para el que desea agregar una confianza y seleccione Propiedades.
3. Haga clic en la pestaña Confianzas.
4. Haga clic en el botón New Trust (Nueva confianza).
5. Cuando se abra el Asistente para nueva confianza, haga clic en Siguiente.
6. Escriba el nombre DNS del dominio AD y haga clic en Next (Siguiente).
7. Suponiendo que el dominio AD se pudo resolver a través de DNS, en la siguiente pantalla se solicitará la dirección de confianza. Seleccione Two-way (Dos direcciones) y haga clic en Next (Siguiente).
8. En Propiedades de confianza saliente, seleccione todos los recursos que desea autenticar y haga clic en Siguiente.
9. Introduzca y vuelva a escribir la contraseña de confianza y haga clic en Next (Siguiente).
10. Haga clic en Next dos veces.

Nota: La configuración de AD está fuera del ámbito de soporte de Cisco, el soporte de Microsoft se puede utilizar en caso de cualquier problema.

una vez configurado, el ejemplo de AD (aaalab) puede comunicarse con el nuevo AD (zatar.jo) y debería aparecer en la pestaña "dominios en blanco", como se muestra a continuación. si no se muestra, la configuración de confianza bidireccional es incorrecta :



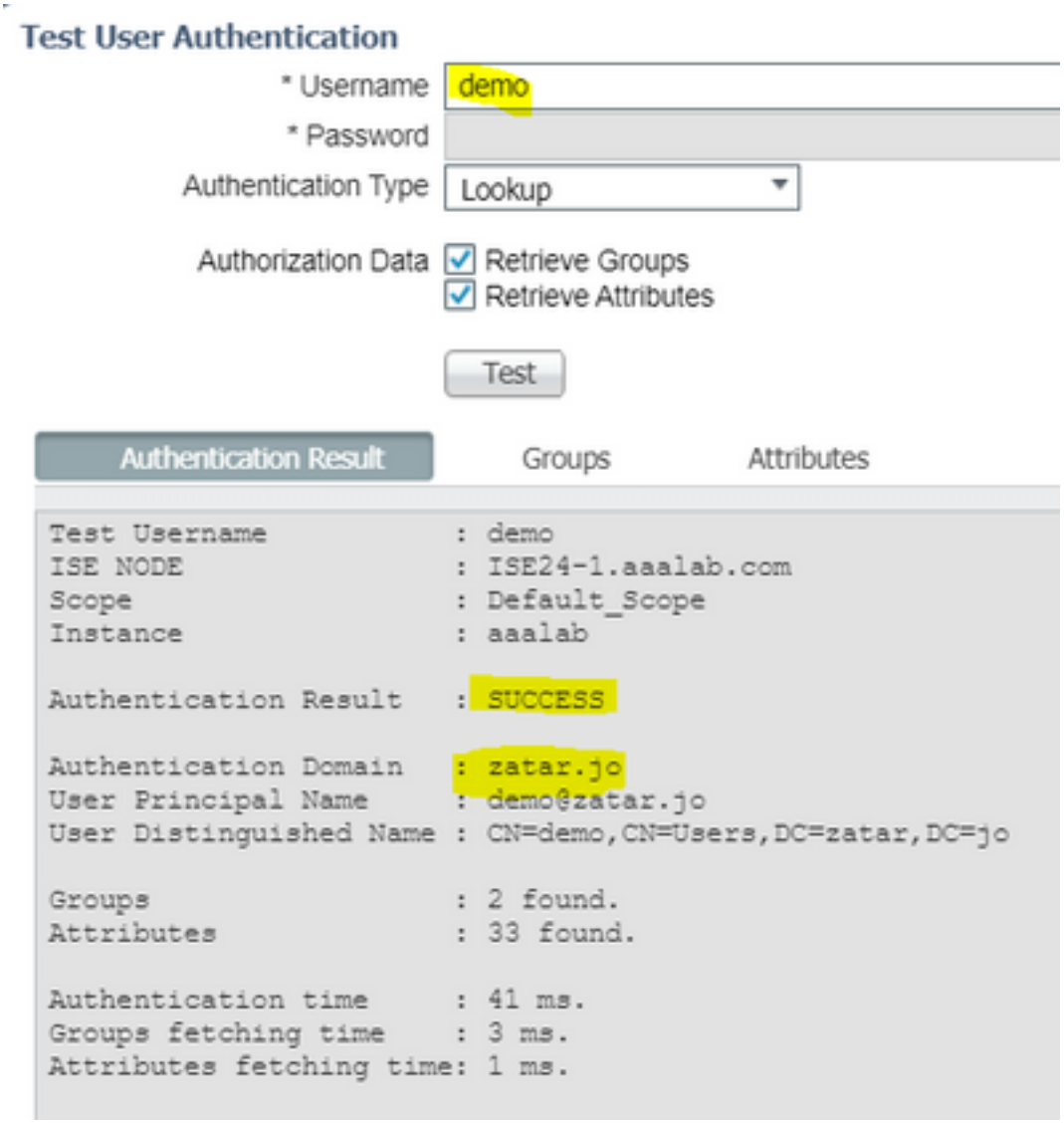
paso 3. Asegúrese de que la **búsqueda** de opciones **en la sección "Dominios anidados"** esté habilitada, como se muestra a continuación. Permitirá la búsqueda en todos los dominios completos, incluidos los dominios de confianza bidireccionales. si la opción **Buscar solamente en los "Dominios de lista blanca" del bosque unido** está habilitada, sólo buscará en los dominios "secundarios" del dominio principal. { ejemplo de dominio secundario: sub.aaalab.com en la captura de pantalla de arriba }.



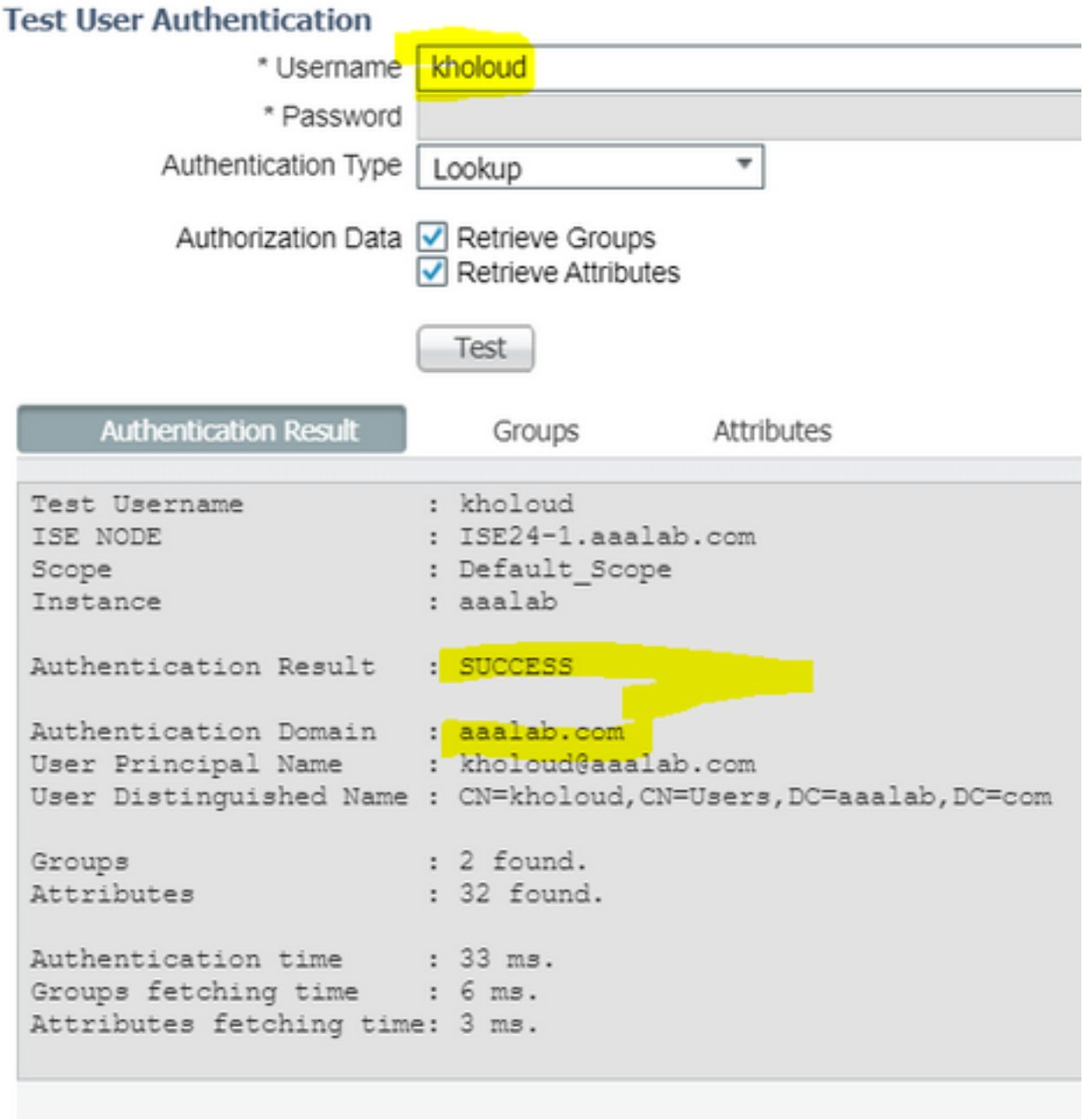
Ahora, ISE puede buscar al usuario en aalab.com y zatar.com.

Verificación

Verifique que funcione a través de la opción "usuario de prueba", use el usuario que está en el dominio "zatar.jo" (en este ejemplo, la "demostración" del usuario existe solamente en el dominio "zatar.jo", y no está en "aaalab.com", el resultado de la prueba está debajo) :



tenga en cuenta que los usuarios de aaalab.com también están trabajando, el usuario kholoud está en aaalab.com :



Troubleshoot

Hay dos procedimientos principales para resolver la mayoría de los problemas de AD/confianza bidireccional, incluso la mayoría de las autenticaciones de identidad externa :

1. recolección de registros ISE (paquete de soporte) con depuraciones activadas. en carpetas específicas de este paquete de soporte, podemos encontrar todos los detalles de cualquier intento de autenticación en AD.

2. recolección de capturas de paquetes entre ISE y AD.

paso 1. recopilar registros de ISE:

a. Habilite las depuraciones, establezca las siguientes depuraciones en "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. Reproduzca el problema y conéctese con un usuario problemático.

c. Recopile un paquete de soporte.

Escenario de trabajo "registros":

> **Nota:** Los detalles de los intentos de autenticación se encontrarán en el archivo ad_agent.log

desde el archivo ad_agent.log:

verificación de la conexión de confianza bidireccional de 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
```

buscando el usuario "demo" en el dominio 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
```

(tenga en cuenta que el usuario de la demostración está en el dominio de zatar; sin embargo, ise lo comprobará primero en el dominio aalab y luego en otros dominios de la ficha de dominios "anidados" como newlab.com. para evitar hacer trampa en el dominio principal, y para proteger zatar.jo directamente, debe utilizar el sufijo UPN para que ISE sepa dónde buscar, de modo que el usuario deba iniciar sesión con este formato : demo.zatar.jo).

buscando el usuario "demo" en 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
```

el usuario "demo" se encontró en el dominio 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"
```

paso 2. Recopilar capturas:

a. Los paquetes intercambiados entre ISE y AD/LDAP, están cifrados de modo que no serían legibles si recopilamos las capturas sin descifrarlas primero.

Para descifrar paquetes entre ISE y AD (este paso debe aplicarse antes de recopilar las capturas y aplicar el intento):

1. En ISE, ingrese a la pestaña : External-ID-Stores -> Active Directory -> Herramientas avanzadas -> Ajuste avanzado
2. Elija su nodo ISE.
3. El campo 'Nombre' obtiene una cadena específica de RESOLUCIÓN DE PROBLEMAS: RESOLUCIÓN DE PROBLEMAS.EncryptionOffPeriod.
4. El campo 'Valor' obtiene el número de minutos para los que desea resolver problemas

‹Número entero positivo en minutos›

Ejemplo para media hora:

30

5. Escriba cualquier descripción. Obligatorio antes del siguiente paso.

6. Haga clic en el botón "Actualizar valor"

7. Haga clic en 'Reiniciar conector de Active Directory.

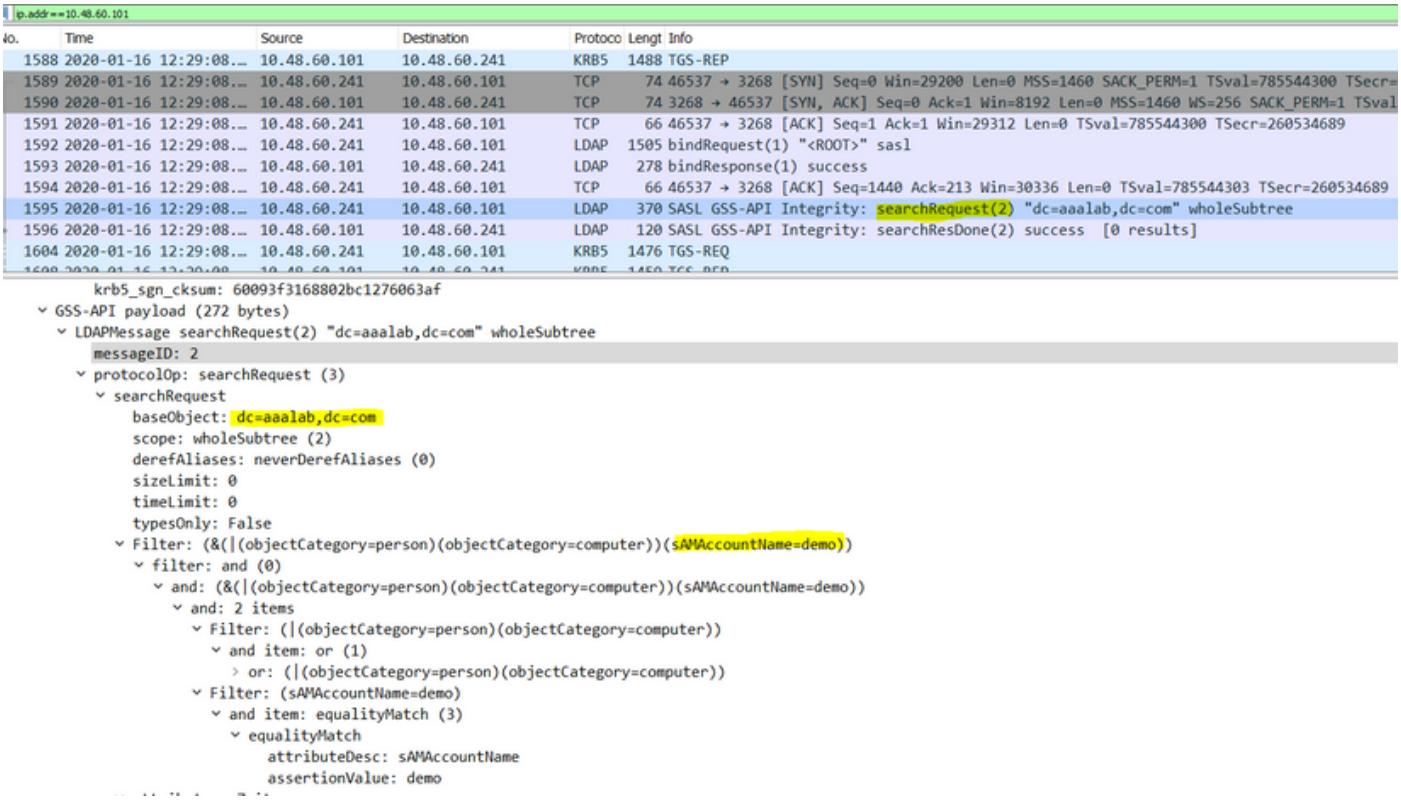
8. espere 10 minutos para que el descifrado afecte .

b. inicie las capturas en ISE.

c. reproduzca el problema.

d. a continuación, detenga y descargue la captura

Escenario de trabajo "registros":



Verificación

A continuación se muestran algunos ejemplos de situaciones laborales y no laborales que puede encontrar y los registros que producen.

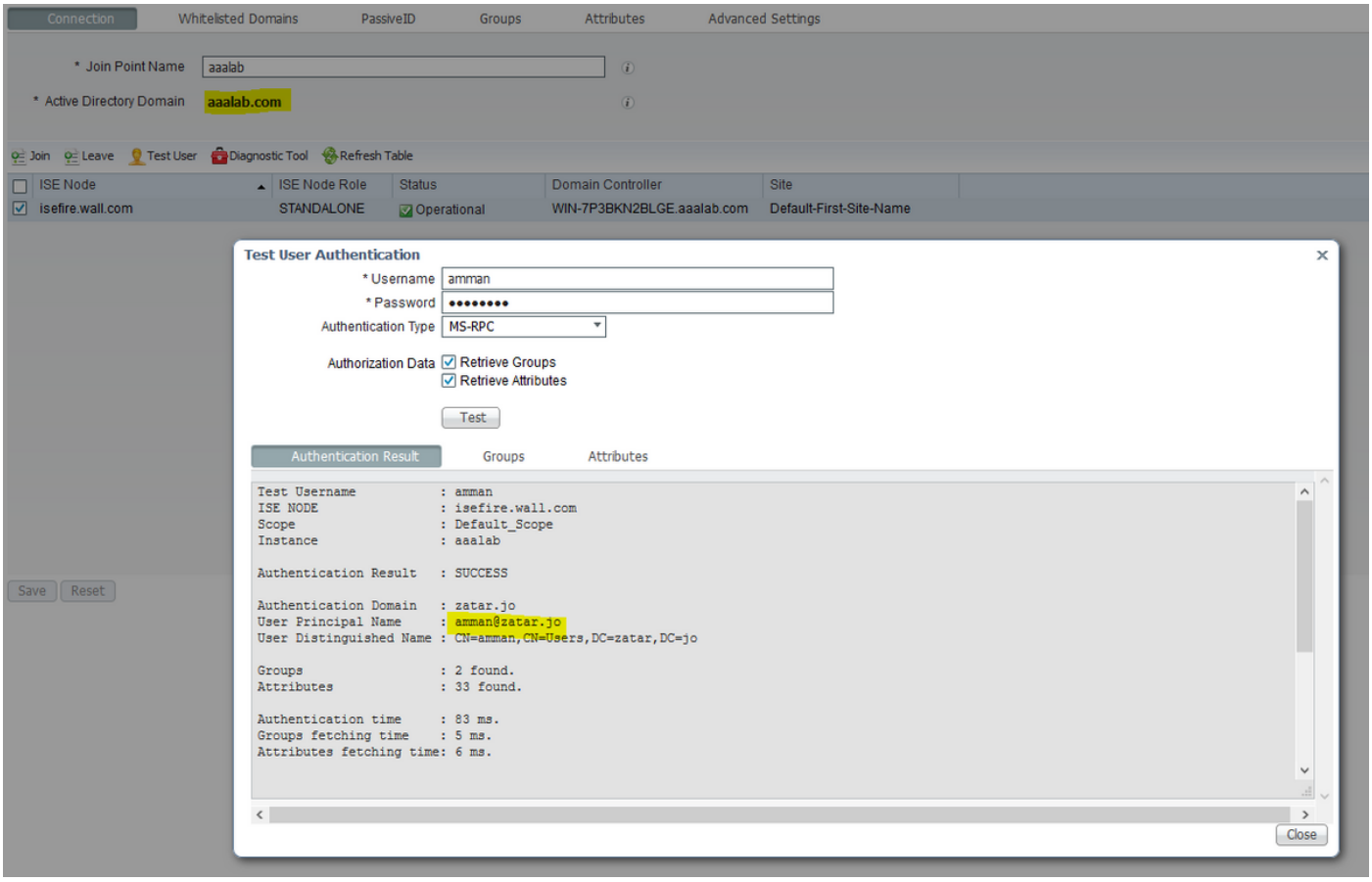
1. Autenticación basada en grupos AD "zatar.jo":

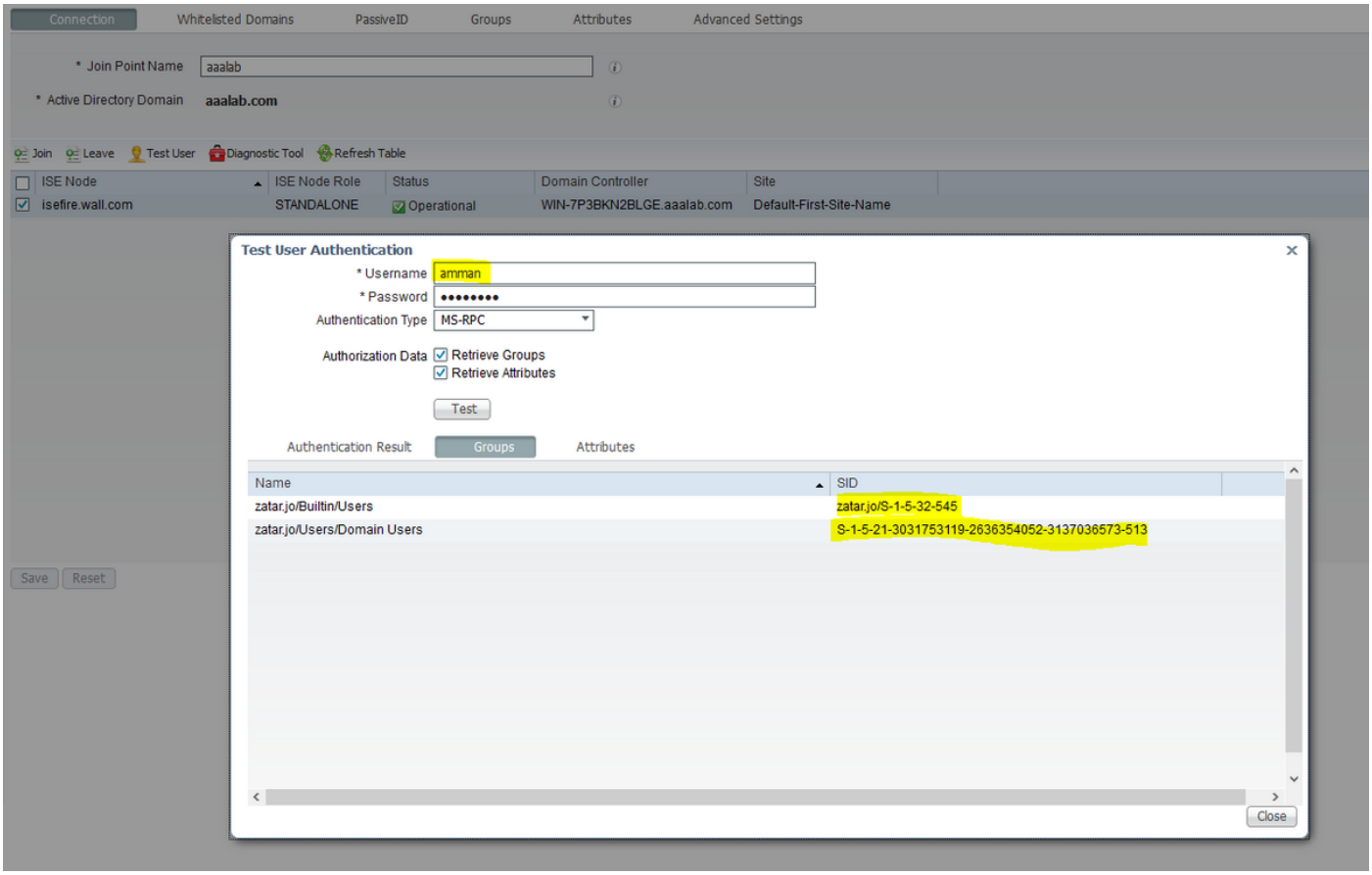
Si el grupo no se recupera de la ficha de grupo, recibirá este mensaje de registro:

```
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
```

Necesitamos recuperar los grupos en zatar.jo de la pestaña Grupos.

Verificación de las recuperaciones de grupos AD de la ficha AD:





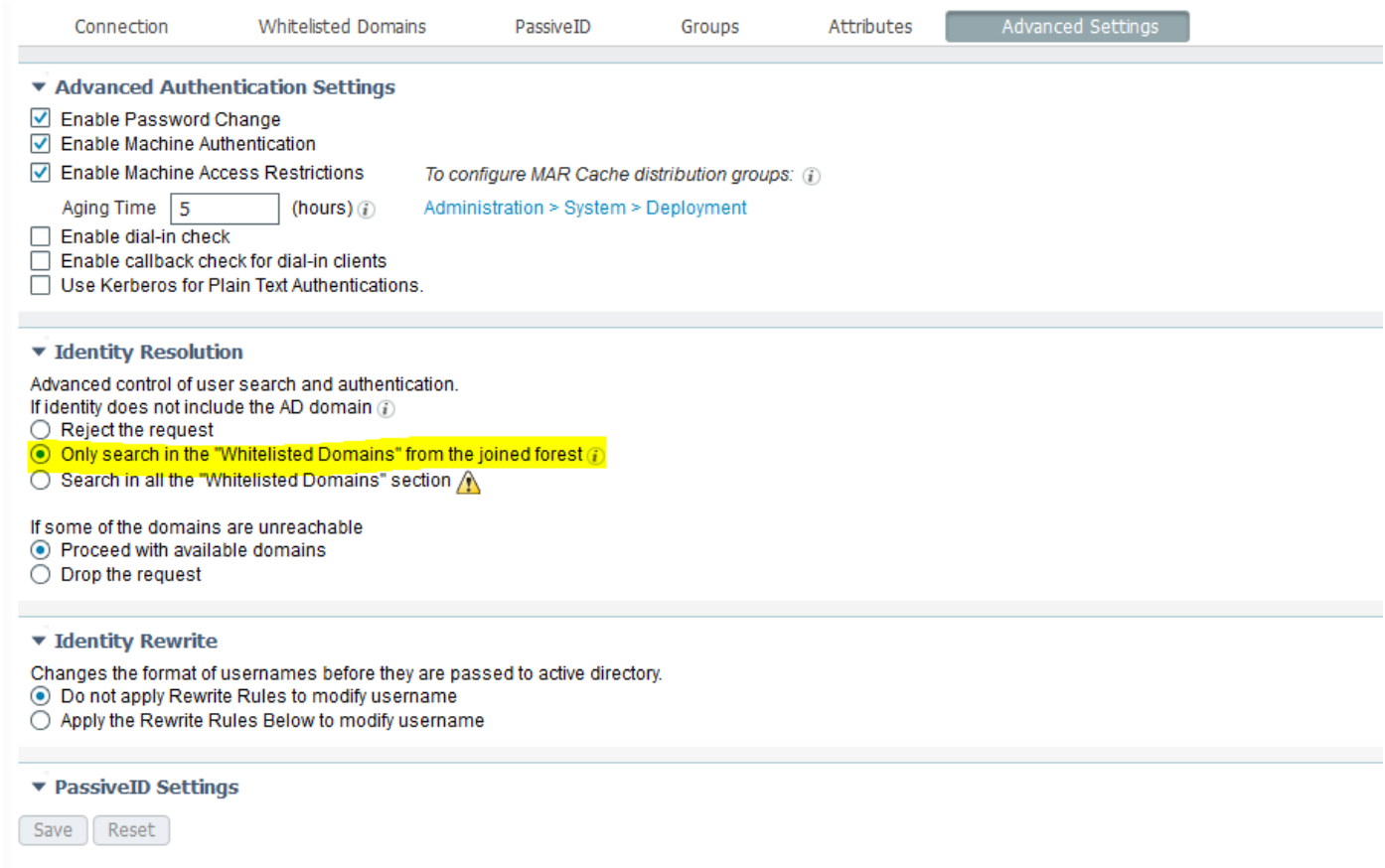
escenario de trabajo De los logs AD_agent.log:

```
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"
}
}
```

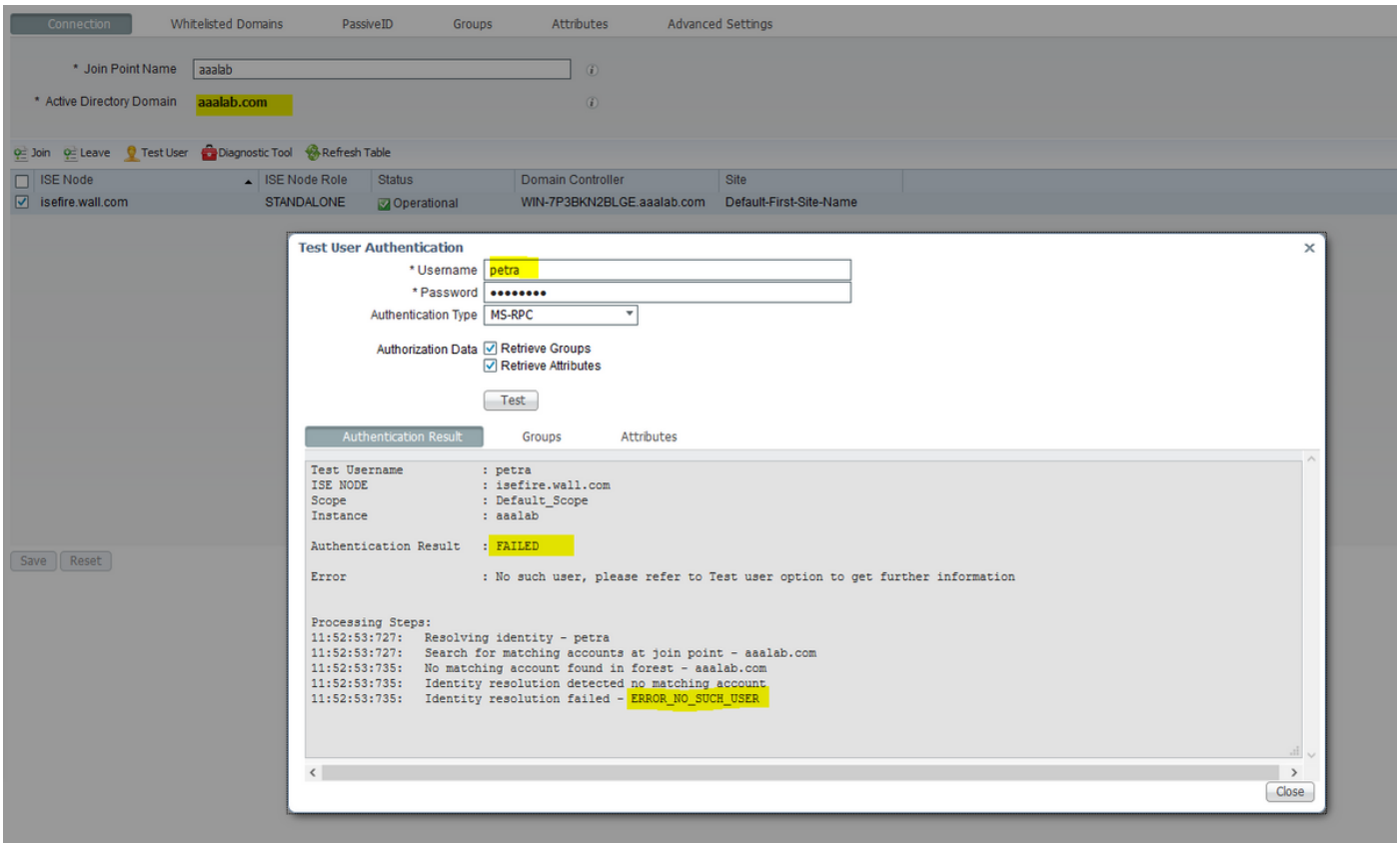
2. Si la opción de avance "Buscar únicamente en los "Dominios con lista blanca" del bosque unido" está activada:



Cuando elige la opción "Buscar sólo en los "dominios con lista blanca" del bosque unido", el ISE los marca desconectados:

```
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
```

El usuario "petra" está en zatar.jo y fallará la autenticación, como se muestra a continuación:



En los registros:

ISE no pudo alcanzar otros dominios, debido a la opción avanzada "Buscar solo en los "dominios de la lista blanca" del bosque unido":

```
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
```