Configuration d'ISE et d'AD de confiance bidirectionnelle

Contenu

Introduction

Ce document décrit la définition de la « confiance bidirectionnelle » sur ISE, ainsi qu'un exemple simple de configuration : comment authentifier un utilisateur qui n'est pas présent dans l'AD joint à ISE, mais présent dans une autre AD.

Conditions préalables

Conditions requises

Cisco vous recommande d'avoir des connaissances de base sur :

- Intégration ISE 2.x et Active Directory .
- Authentification d'identité externe sur ISE.

Components Used

- ISE 2.x .
- deux répertoires actifs.

Configuration

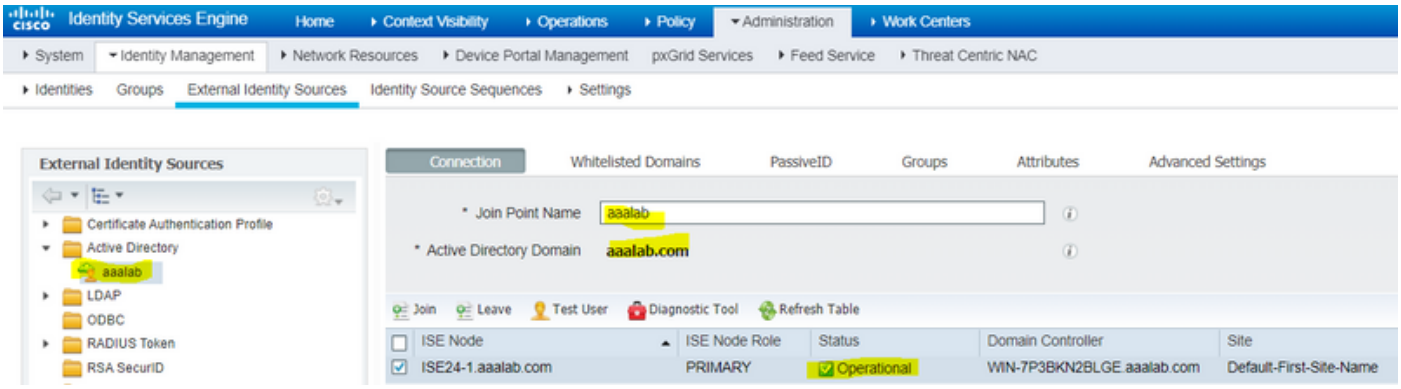
Afin d'étendre votre domaine et d'inclure d'autres utilisateurs dans un domaine différent de celui qui est déjà joint à ISE, vous avez deux façons d'accomplir ceci :

1. vous pouvez ajouter le domaine manuellement et séparément sur ISE. par là, vous auriez deux répertoires Active Directory distincts.
2. Rejoignez une AD à ISE, puis configurez **la confiance bidirectionnelle** entre cette AD et la deuxième AD, sans l'ajouter à ISE. Il s'agit principalement d'une configuration d'approbation bidirectionnelle, c'est une option qui est configurée entre deux ou plusieurs répertoires actifs.

ISE détectera automatiquement ces domaines approuvés à l'aide du connecteur AD et les ajoutera aux domaines “ liste blanche ” et les traitera comme des AD distincts joints à ISE. C'est ainsi que vous pouvez authentifier un utilisateur dans la AD « zatar.jo », qui n'est pas jointe à ISE.

Les étapes suivantes décrivent la procédure de configuration sur ISE et AD :

étape 1. assurez-vous que ISE est joint à AD, dans cet exemple, vous avez l'onglet domaine :

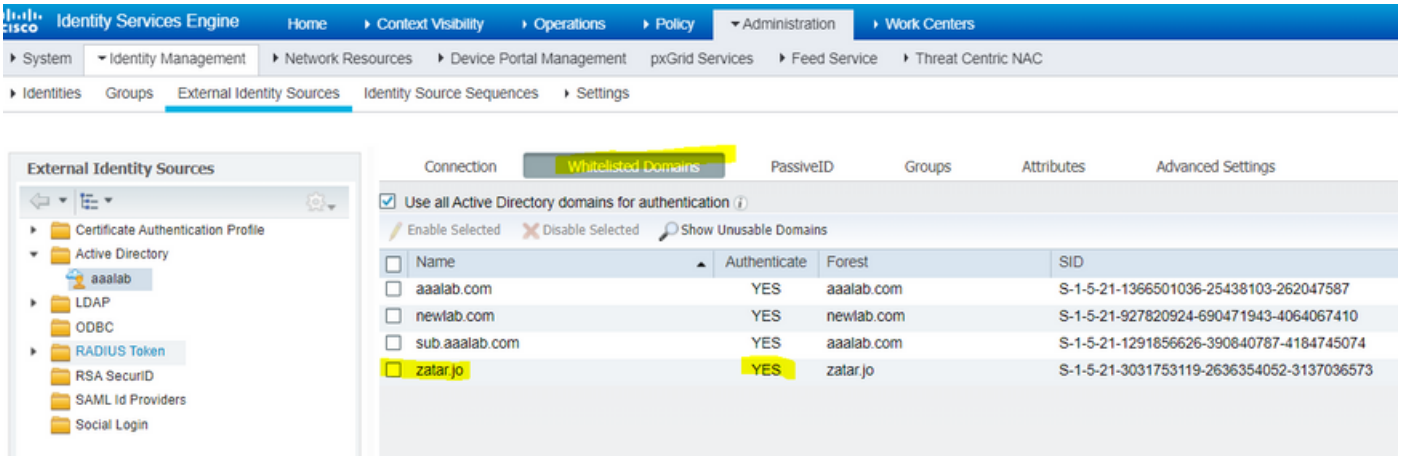


étape 2. assurez-vous que l'approbation bidirectionnelle est activée entre les deux répertoires actifs, comme ci-dessous :

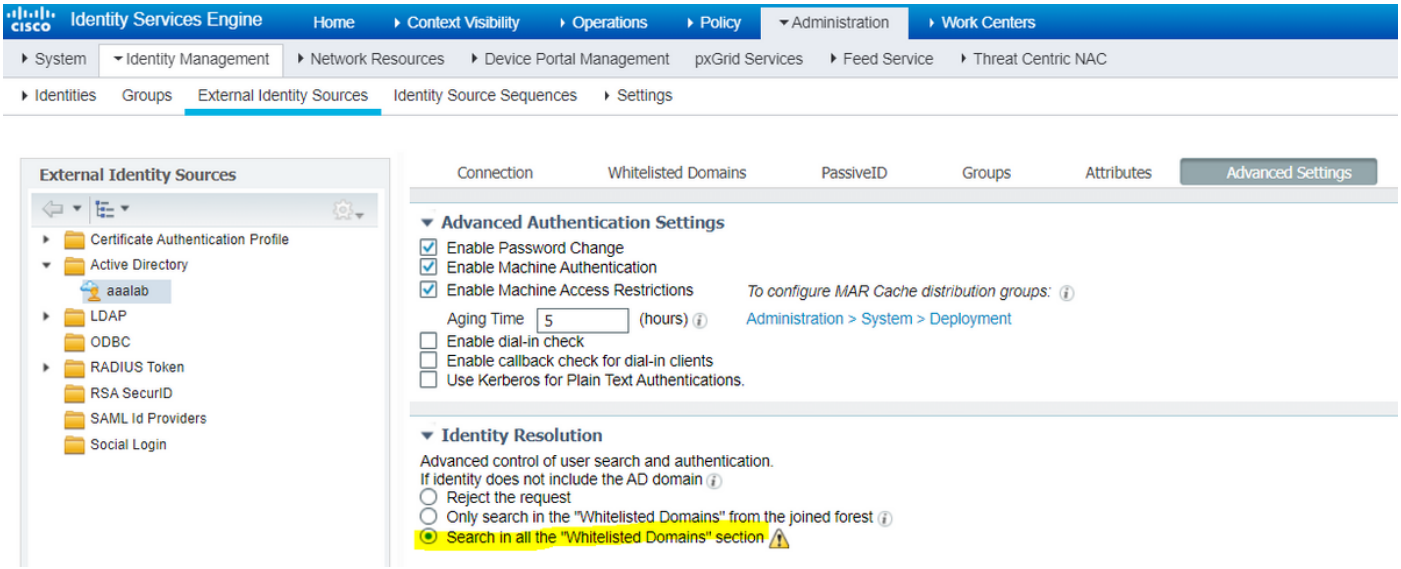
1. Ouvrez le composant logiciel enfichable Domaines et approbations Active Directory.
2. Dans le volet gauche, cliquez avec le bouton droit sur le domaine pour lequel vous voulez ajouter une approbation, puis sélectionnez Propriétés.
3. Cliquez sur l'onglet Fiducies.
4. Cliquez sur le bouton Nouvelle approbation.
5. Une fois l'Assistant Nouvelle approbation ouvert, cliquez sur Suivant.
6. Tapez le nom DNS du domaine AD et cliquez sur Suivant.
7. En supposant que le domaine AD a été résolu via DNS, l'écran suivant demande la direction de la confiance. Sélectionnez Two-way et cliquez sur Next.
8. Pour les propriétés d'approbation sortante, sélectionnez toutes les ressources à authentifier, puis cliquez sur Suivant.
9. Saisissez et retapez le mot de passe d'approbation, puis cliquez sur Suivant.
10. Cliquez deux fois sur Suivant.

Note: La configuration AD n'est pas prise en charge par Cisco, l'assistance Microsoft peut être engagée en cas de problème.

une fois configuré, l'exemple AD (aalab) peut communiquer avec la nouvelle AD (zatar.jo) et devrait apparaître dans l'onglet « domaines blanchis », comme ci-dessous. si elle n'est pas affichée, la configuration de confiance bidirectionnelle est incorrecte :



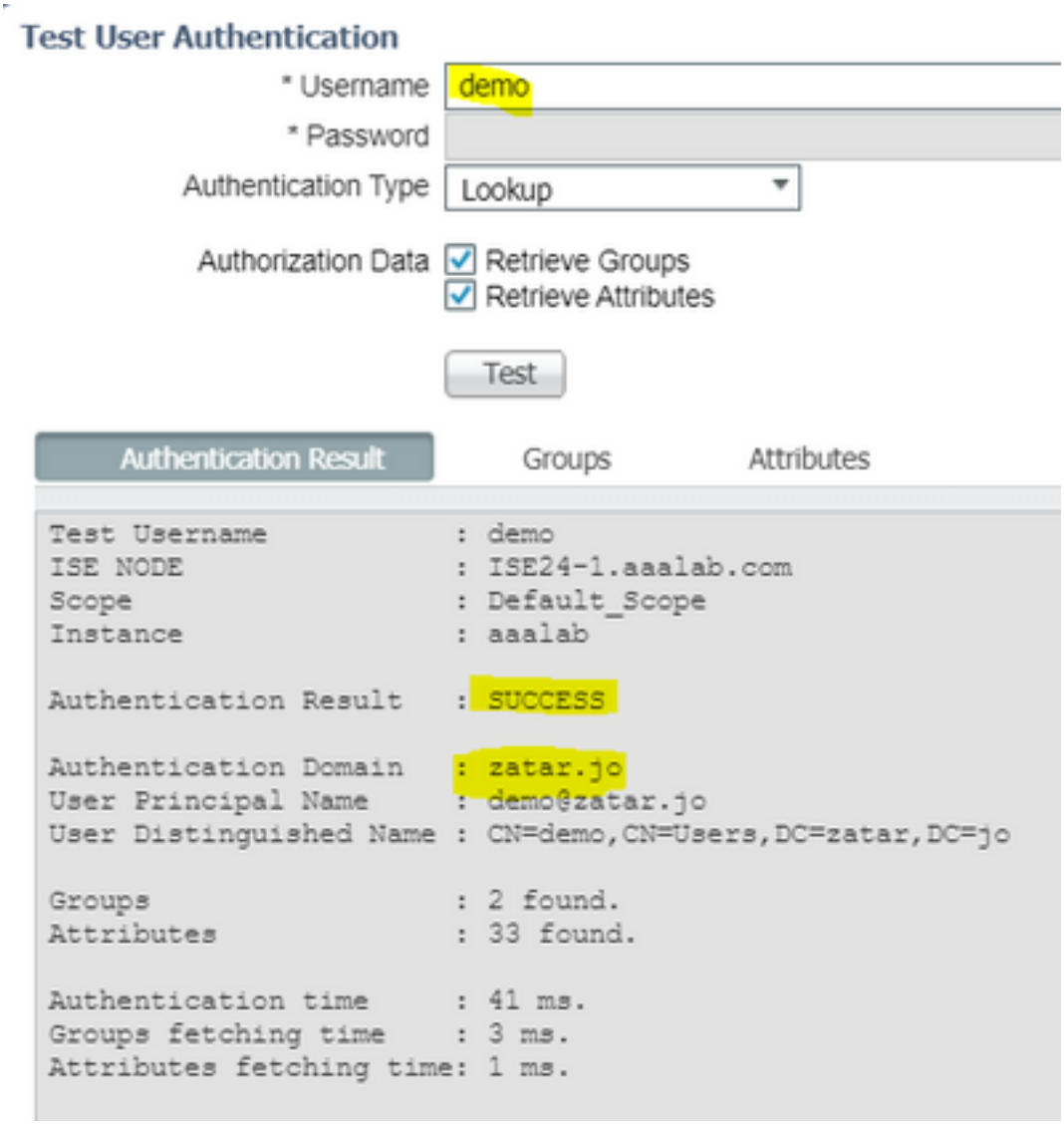
étape 3. Assurez-vous que la **recherche d'**options **dans toutes les sections « Domaines blanchis »** est activée, comme indiqué ci-dessous. Il permet la recherche dans tous les domaines de type parallèle, y compris les domaines de confiance bidirectionnels. si l'option **Recherche uniquement dans les domaines « Whitelisted Domains » de la forêt jointe** est activée, elle recherche uniquement dans les domaines « enfants » du domaine principal. { exemple de domaine enfant : sub.aalab.com dans la capture d'écran ci-dessus }.



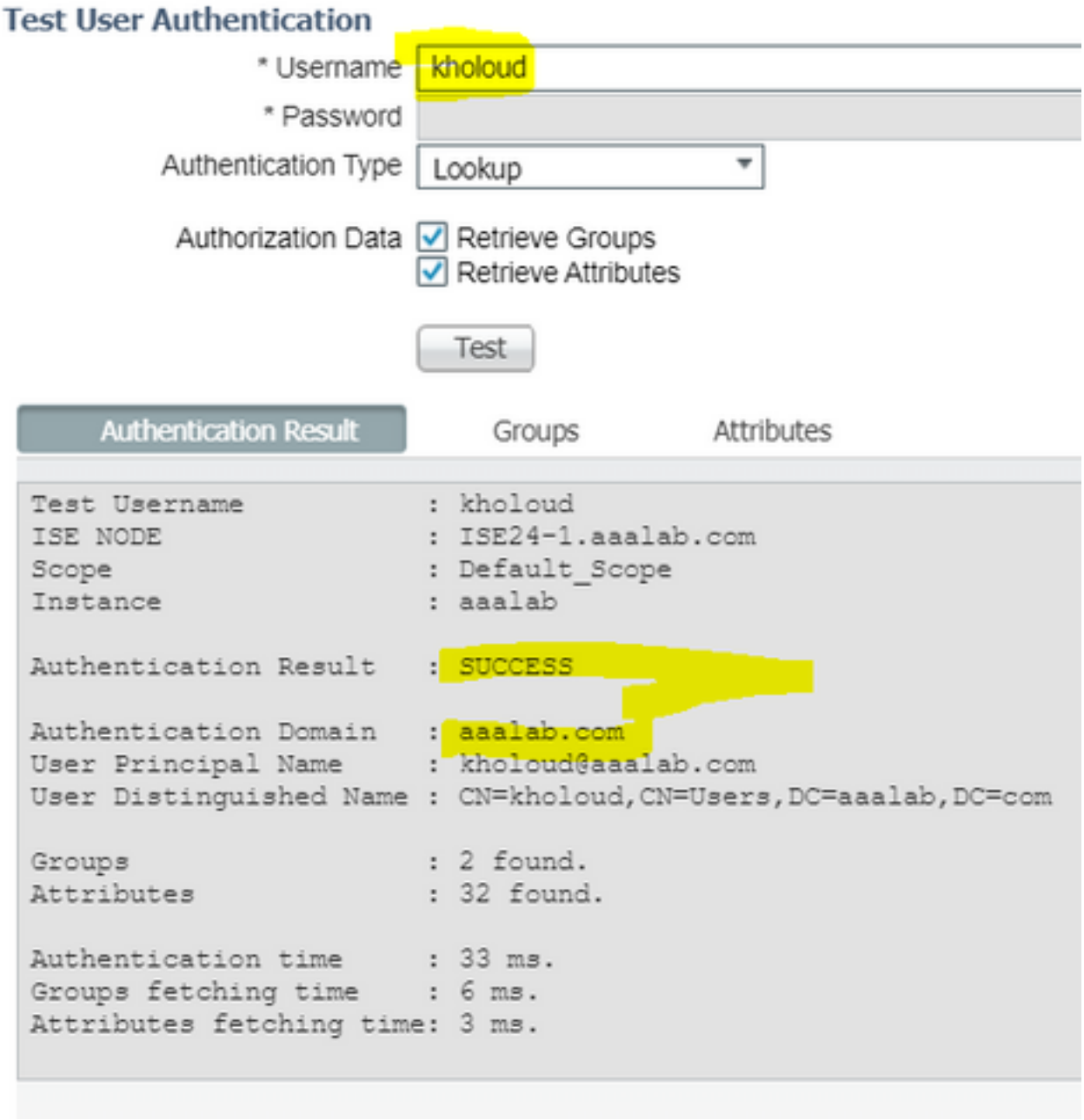
Maintenant, ISE peut rechercher l'utilisateur dans aalab.com et zatar.com.

Vérification

Vérifiez qu'il fonctionne via l'option « utilisateur test », utilisez l'utilisateur qui se trouve dans le domaine « zatar.jo » (dans cet exemple, l'utilisateur « demo » n'existe que dans le domaine « zatar.jo », et il ne se trouve pas dans « aalab.com », le résultat du test est ci-dessous) :



notez que les utilisateurs d'aalab.com fonctionnent également, l'utilisateur kholoud est sur aalab.com :



Dépannage

Il existe deux procédures principales pour résoudre la plupart des problèmes d'approbation AD/bidirectionnelle, même la plupart des authentifications d'identité externe :

1. collecte des journaux ISE (offre de support) avec débogages activés. dans des dossiers spécifiques de cette offre groupée de support, nous pouvons trouver tous les détails de toute tentative d'authentification sur AD.

2. collecte des captures de paquets entre ISE et AD.

étape 1. collecter les journaux ISE :

a. Activez les débogages, définissez les débogages suivants sur « 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. Reproduisez le problème, connectez-vous à un utilisateur problématique.

c. Collectez une offre d'assistance.

Scénario de travail « journaux » :

Note: Les détails des tentatives d'authentification se trouvent dans le fichier ad_agent.log

à partir du fichier ad_agent.log :

vérification de la connexion d'approbation bidirectionnelle 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
```

recherche de l'utilisateur « demo » dans le domaine principal aalab :

```
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
```

(notez que l'utilisateur de la démo est dans le domaine zatar, cependant ise va d'abord le vérifier dans le domaine aalab, puis d'autres domaines dans l'onglet « whitlested » domaines tels que newlab.com. pour éviter de vérifier dans le domaine principal, et pour accéder directement à zatar.jo, vous devez utiliser le suffixe UPN pour que ISE sache où rechercher, de sorte que l'utilisateur doit se connecter au format suivant : demo.zatar.jo).

recherche de l'utilisateur « demo » dans 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
```

utilisateur « demo » trouvé dans le domaine 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"
```

étape2. Collecter les captures :

a. Les paquets échangés entre ISE et AD/LDAP sont chiffrés et ne peuvent donc pas être lus si nous collectons les captures sans les déchiffrer d'abord.

Pour déchiffrer les paquets entre ISE et AD (cette étape doit être appliquée avant de collecter les captures et d'appliquer la tentative) :

1. Sur ISE, accédez à l'onglet : External-ID-Stores -> Active Directory -> Advanced Tools -> Advanced Tuning
2. Sélectionnez votre noeud ISE.
3. Le champ 'Nom' obtient une chaîne de DÉPANNAGE spécifique : DÉPANNAGE.ChiffrementDésactivéPériode.
4. Le champ 'Valeur' obtient le nombre de minutes pour lesquelles vous souhaitez effectuer le dépannage

‹Entier positif en minutes›

Exemple pour une demi-heure :

30

5. Tapez n'importe quelle description. Obligatoire avant l'étape suivante.

6. Cliquez sur le bouton Mettre à jour la valeur

7. Cliquez sur Redémarrer le connecteur Active Directory.

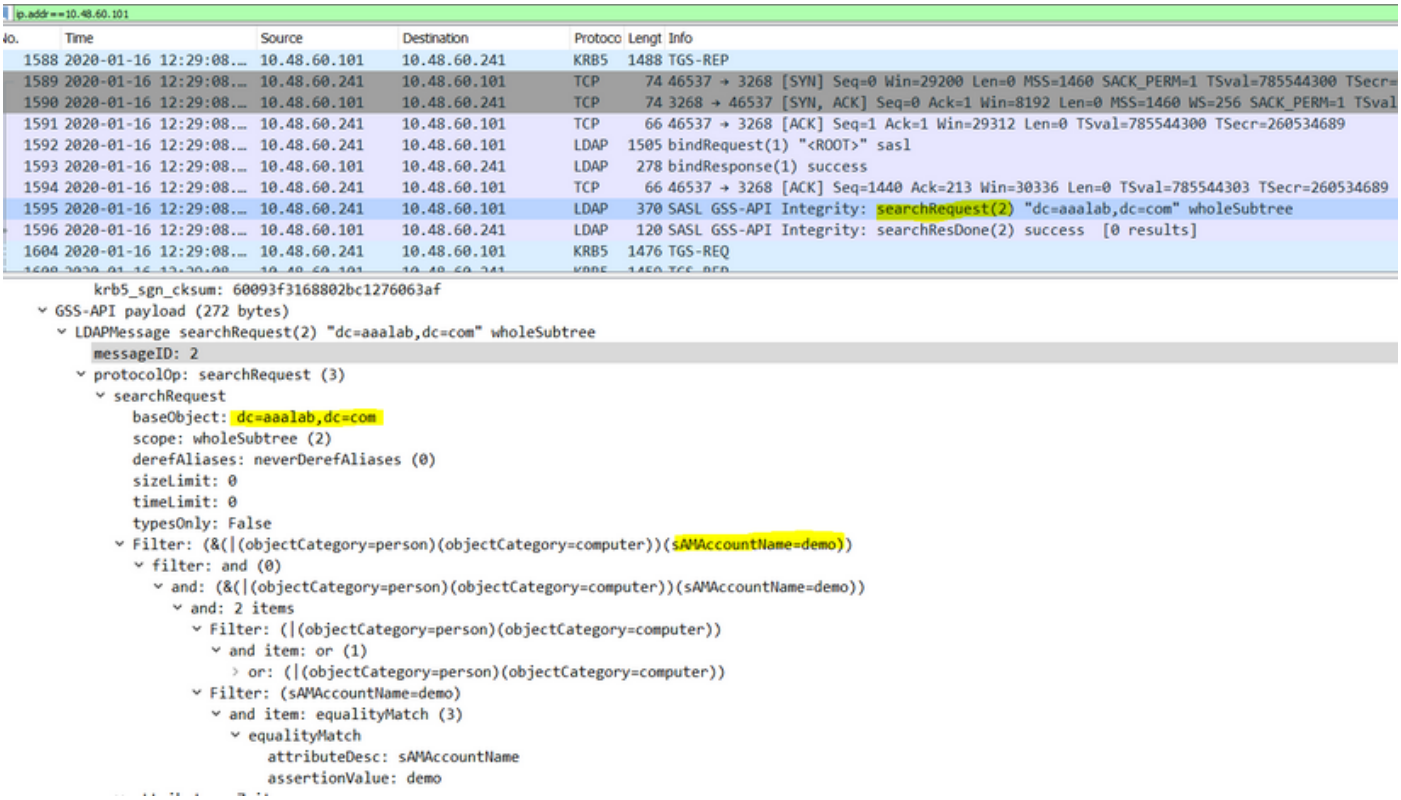
8. attendez 10 minutes pour que le déchiffrement prenne effet.

b. démarrez les captures sur ISE.

c. reproduisez le problème.

d. puis arrêtez et téléchargez la capture

Scénario de travail « journaux » :



Vérification

Voici quelques exemples de situations de travail et de non-travail que vous pourriez rencontrer et les journaux qu'ils produisent.

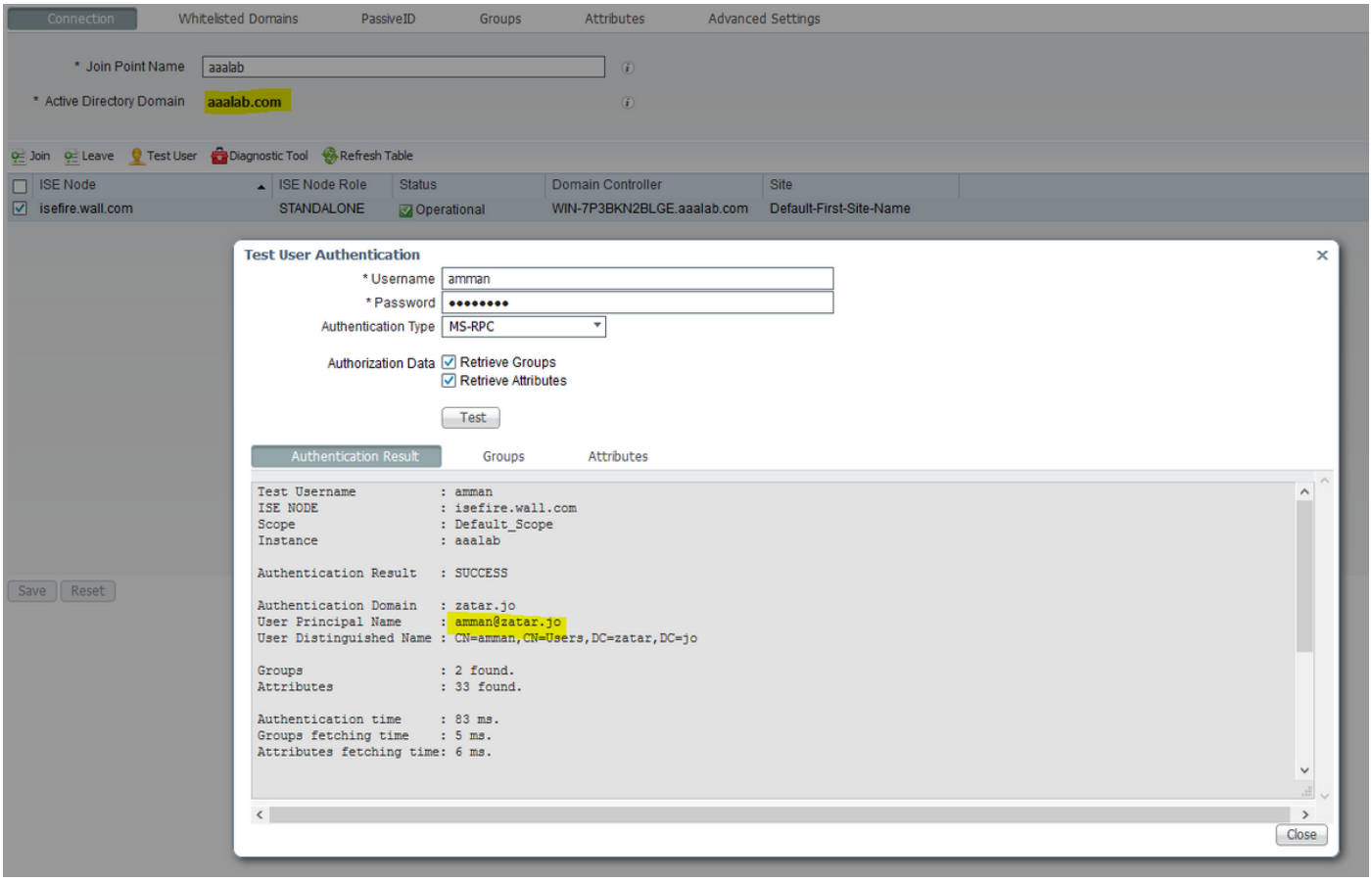
1. Authentification basée sur les groupes AD « zatar.jo » :

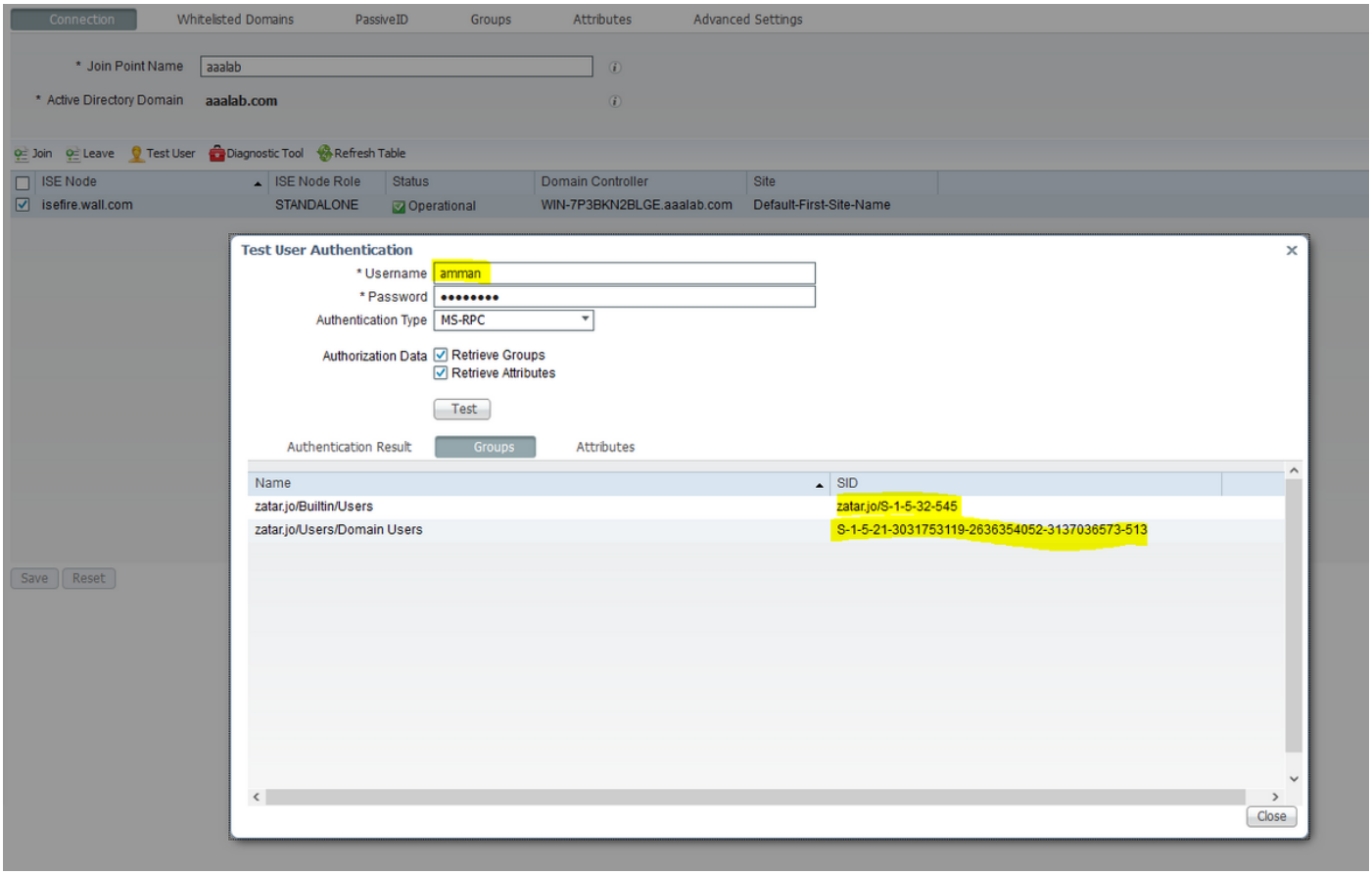
Si le groupe n'a pas été renvoyé de l'onglet de groupe, vous obtiendrez le message suivant :

```
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
```

Nous devons récupérer les groupes dans zatar.jo à partir de l'onglet Groupes.

Vérification des extractions de groupe AD à partir de l'onglet AD :





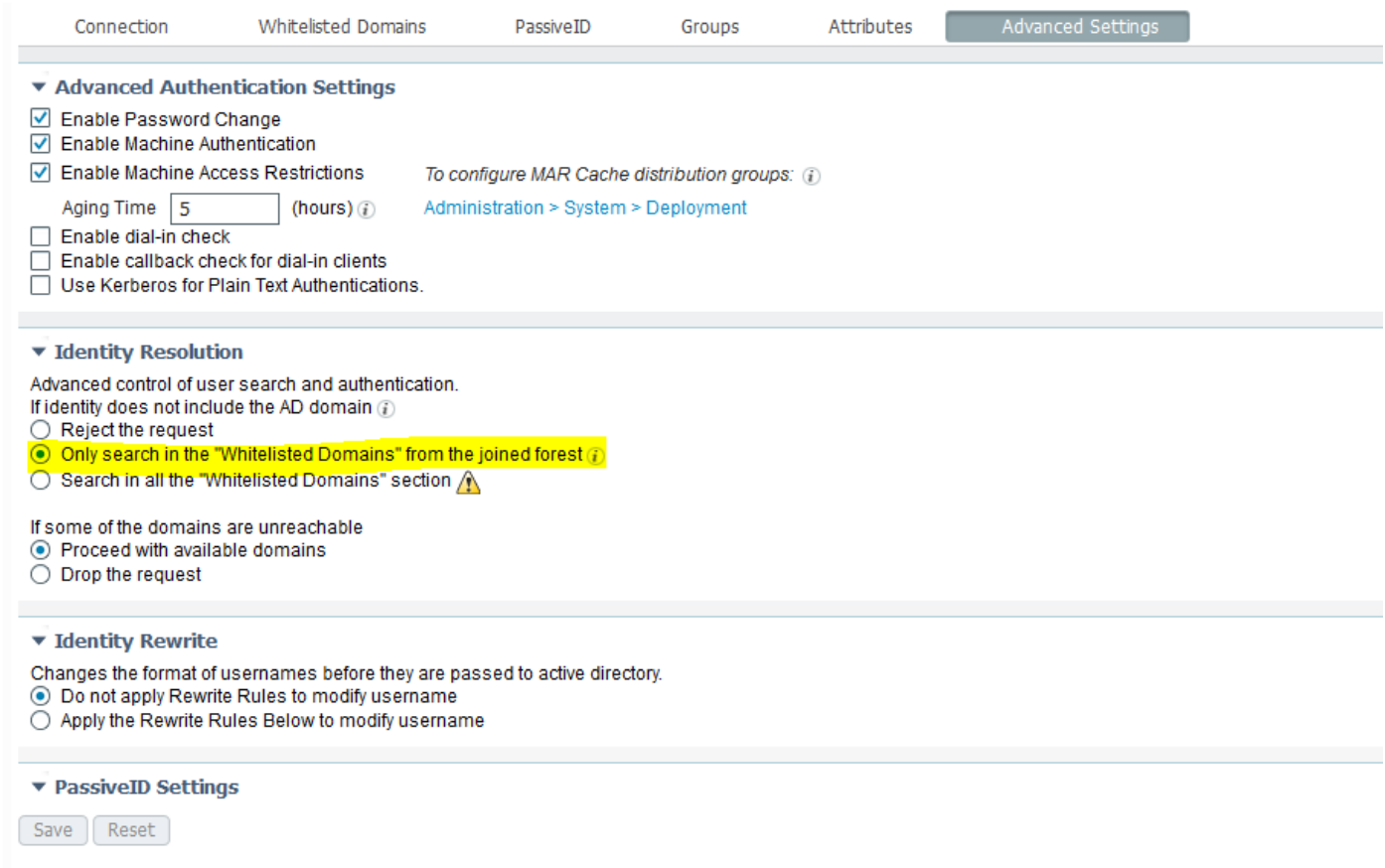
scénario de travail Dans les journaux AD_agent.log :

```
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"
}
}
```

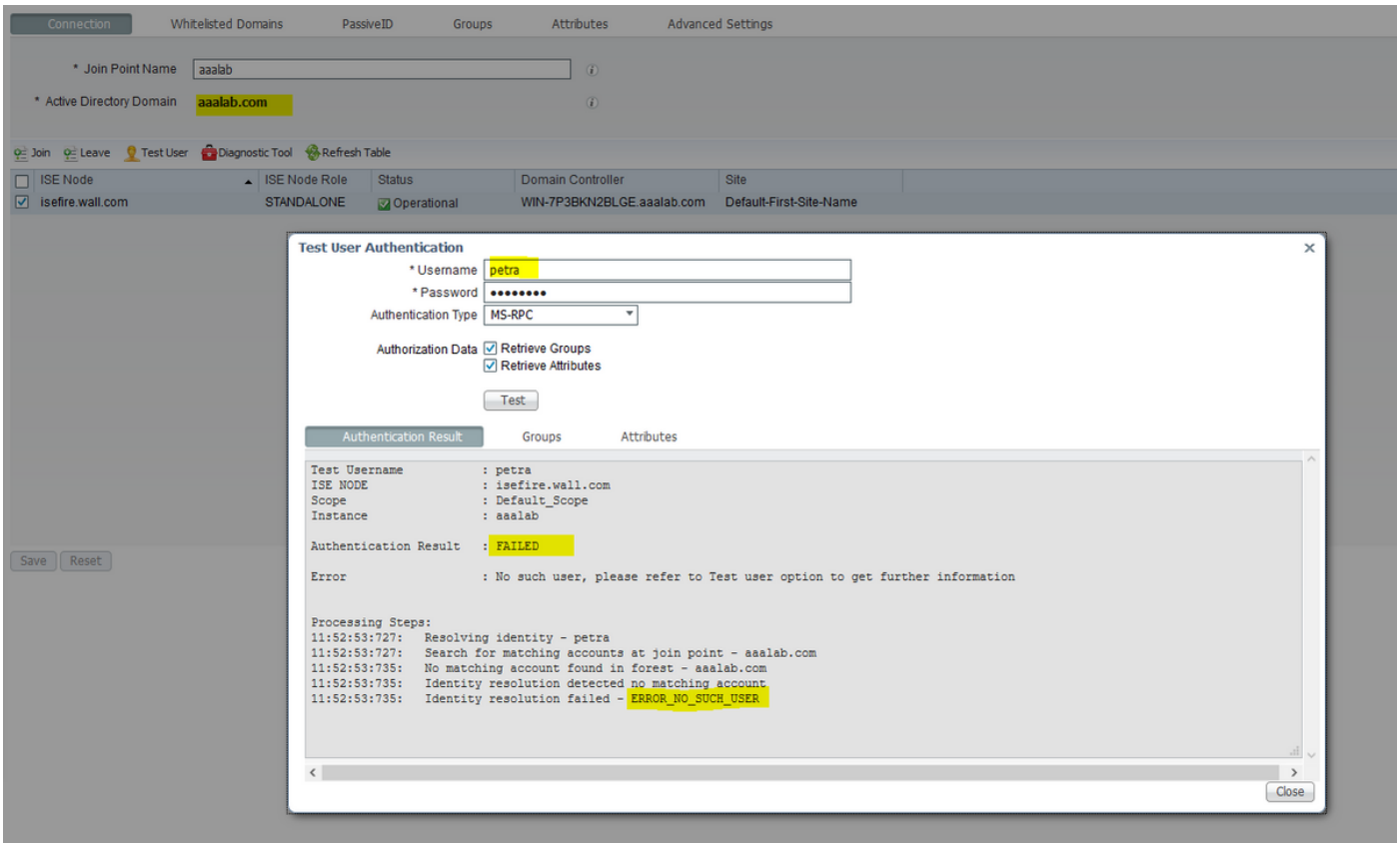
2. Si l'option avancée « Rechercher uniquement dans les « domaines listés » de la forêt jointe » est cochée :



Lorsque vous choisissez l'option « Rechercher uniquement dans les domaines autorisés » de la forêt jointe, l'ISE les a marqués hors connexion :

```
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
```

L'utilisateur « petra » est dans zatar.jo et échouera à l'authentification, comme le montre la capture d'écran ci-dessous :



Dans les journaux :

ISE n'a pas pu accéder à d'autres domaines, en raison de l'option avancée « Rechercher uniquement dans les « domaines listés » à partir de la forêt jointe » :

```
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
```