# Comprendre Identity Service Engine (ISE) et Active Directory (AD)

## Table des matières



## Introduction

Ce document décrit comment Identity Service Engine (ISE) et Active Directory (AD) communiquent, les protocoles utilisés, les filtres AD et les flux.

## Conditions préalables

### Exigences

Cisco recommande une connaissance de base des éléments suivants :

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

### Composants utilisés

- ISE 2.x .
- Windows Server (Active Directory).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

# Protocoles AD

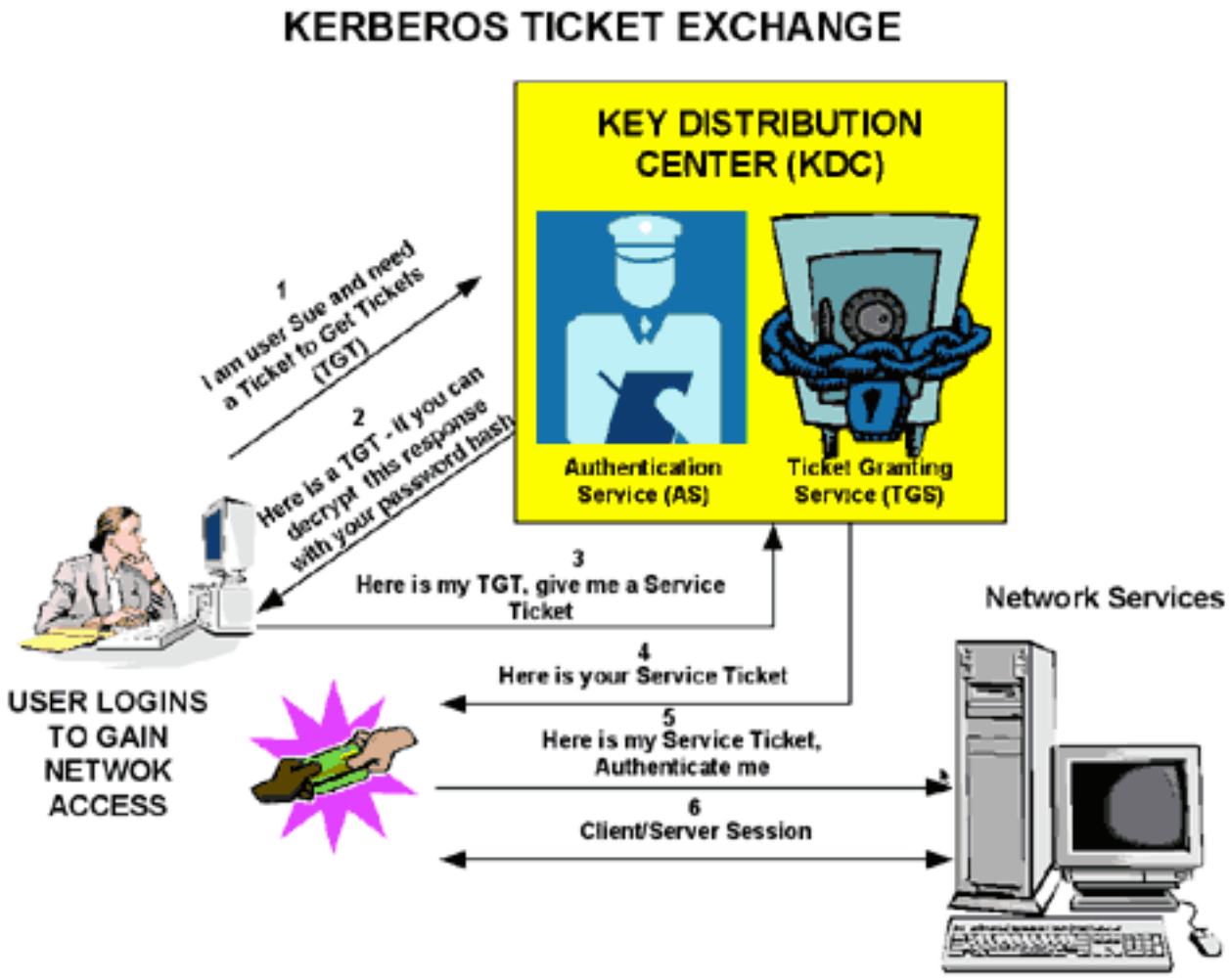
## Protocole Kerberos

Les trois têtes de Kerberos comprennent le centre de distribution de clés (KDC), l'utilisateur client et le serveur auquel accéder.

Le KDC est installé dans le cadre du contrôleur de domaine (DC) et remplit deux fonctions de service : le service d'authentification (AS) et le service d'octroi de tickets (TGS).

Trois échanges sont impliqués lorsque le client accède initialement à une ressource serveur :

1. AS Exchange.
2. Échange TGS.
3. Client/Serveur (CS) Exchange.




- Contrôleur de domaine = KDC (AS + TGS).
- Authentifiez-vous auprès de AS (le portail SSO) avec votre mot de passe.

- Obtenir un ticket d'octroi de ticket (TGT) (un cookie de session).
- Demande de connexion à un service (SRV01).
- SRV01 vous redirige vers KDC.
- Show TGT to KDC - (Je suis déjà authentifié)
- KDC vous donne le TGS pour SRV01.
- Rediriger vers SRV01.
- Afficher le ticket de service pour SRV01.
- SRV01 vérifie/approuve le ticket de service.
- Le ticket de service contient toutes mes informations.
- SRV01 me connecte.

Lors de la connexion initiale à un réseau, les utilisateurs doivent négocier l'accès et fournir un nom et un mot de passe de connexion afin d'être vérifiés par la partie AS d'un KDC au sein de leur domaine.

Le KDC a accès aux informations de compte utilisateur Active Directory. Une fois authentifié, l'utilisateur se voit accorder un ticket TGT (Ticket Granting Ticket) valide pour le domaine local.

Le TGT a une durée de vie par défaut de 10 heures et est renouvelé tout au long de la session d'ouverture de session de l'utilisateur sans que l'utilisateur n'ait besoin de saisir à nouveau son mot de passe.

Le TGT est mis en cache sur la machine locale dans l'espace mémoire volatile et est utilisé pour demander des sessions avec des services sur l'ensemble du réseau.

L'utilisateur présente le TGT à la partie TGS du KDC lorsque l'accès à un service de serveur est nécessaire.

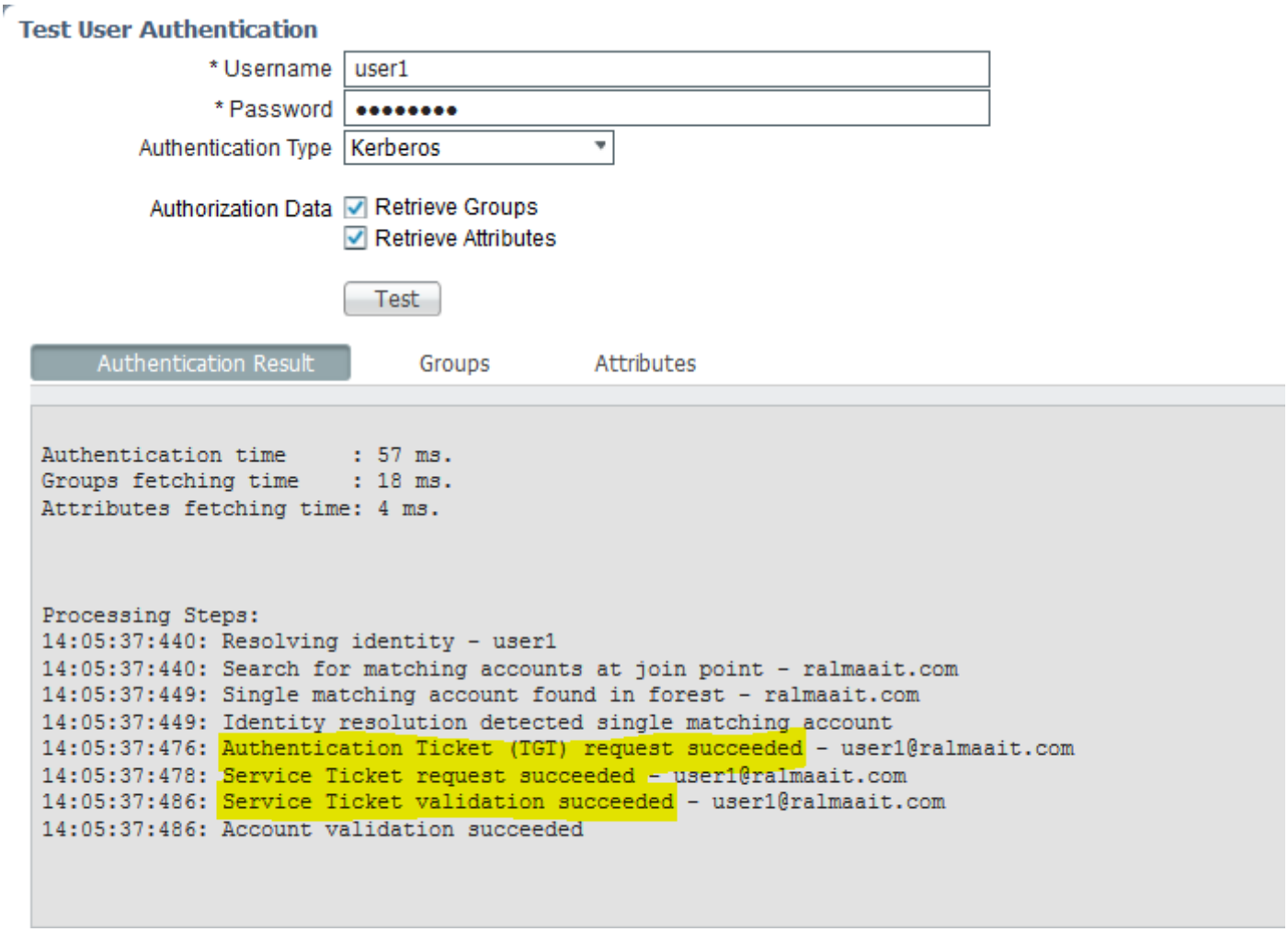
Le TGS du KDC authentifie le TGT de l'utilisateur et crée un ticket et une clé de session pour le client et le serveur distant. Ces informations (le ticket de service) sont ensuite mises en cache localement sur l'ordinateur client.

Le TGS reçoit le TGT client et le lit avec sa propre clé. Si le TGS approuve la demande du client, un ticket de service est généré pour le client et le serveur cible.

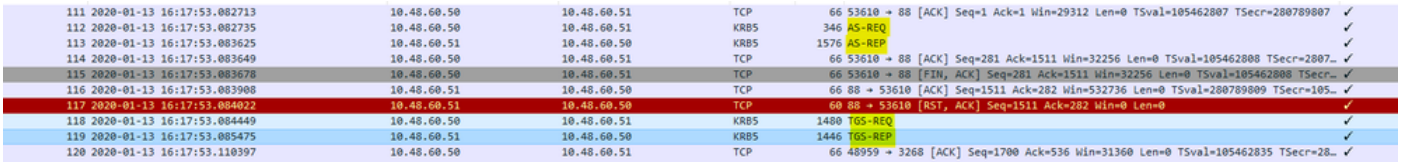
Le client lit sa partie avec la clé de session TGS récupérée précédemment à partir de la réponse AS.

Le client présente la partie serveur de la réponse TGS au serveur cible lors du prochain échange client/serveur.

Exemple :



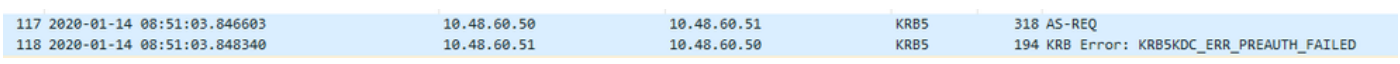

Captures de paquets à partir d'ISE pour un utilisateur authentifié :




AS-REQ contient le nom d'utilisateur. Si le mot de passe est correct, le service AS fournit un TGT chiffré avec le mot de passe utilisateur. Le TGT est ensuite fourni au service TGT pour obtenir un ticket de session.

L'authentification réussit lorsqu'un ticket de session est reçu.

Voici un exemple où le mot de passe donné par le client est incorrect :




Si le mot de passe est incorrect, la requête AS échoue et aucun TGT n'est reçu :

```
Processing Steps:
13:19:55:837:   Resolving Identity - User1
13:19:55:837:   Search For Matching Accounts At Join Point - Ralmaait.com
13:19:55:843:   Single Matching Account Found In Forest - Ralmaait.com
13:19:55:843:   Identity Resolution Detected Single Matching Account
13:19:55:856:   Authentication Ticket (TGT) Request Failed - User1@ralmaait.com,ERROR_PASSWORD_MISMATCH
```

Se connecte au fichier ad_agent.log lorsque le mot de passe est incorrect :

2020-01-14 13:36:05,442 DEBUG ,140574072981248,krb5: Demande envoyée (276 octets) à RALMAAIT.COM,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG,140574072981248,krb5: Erreur reçue de KDC: -1765328360/Echec de la préauthentification, LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG,140574072981248, krb5 : Preauth tryagain input types : 16, 14, 19, 2, LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 WARNING,140574072981248,[LwKrb5GetTgtImpl ../../lwadvapi/threaded/krbtgt.c:329] KRB5 Code d'erreur : -1765328360 (Message : échec de la pré-authentification),LwTranslateKrb5Error(),lwadvapi/threaded/lwkrb5.c:892

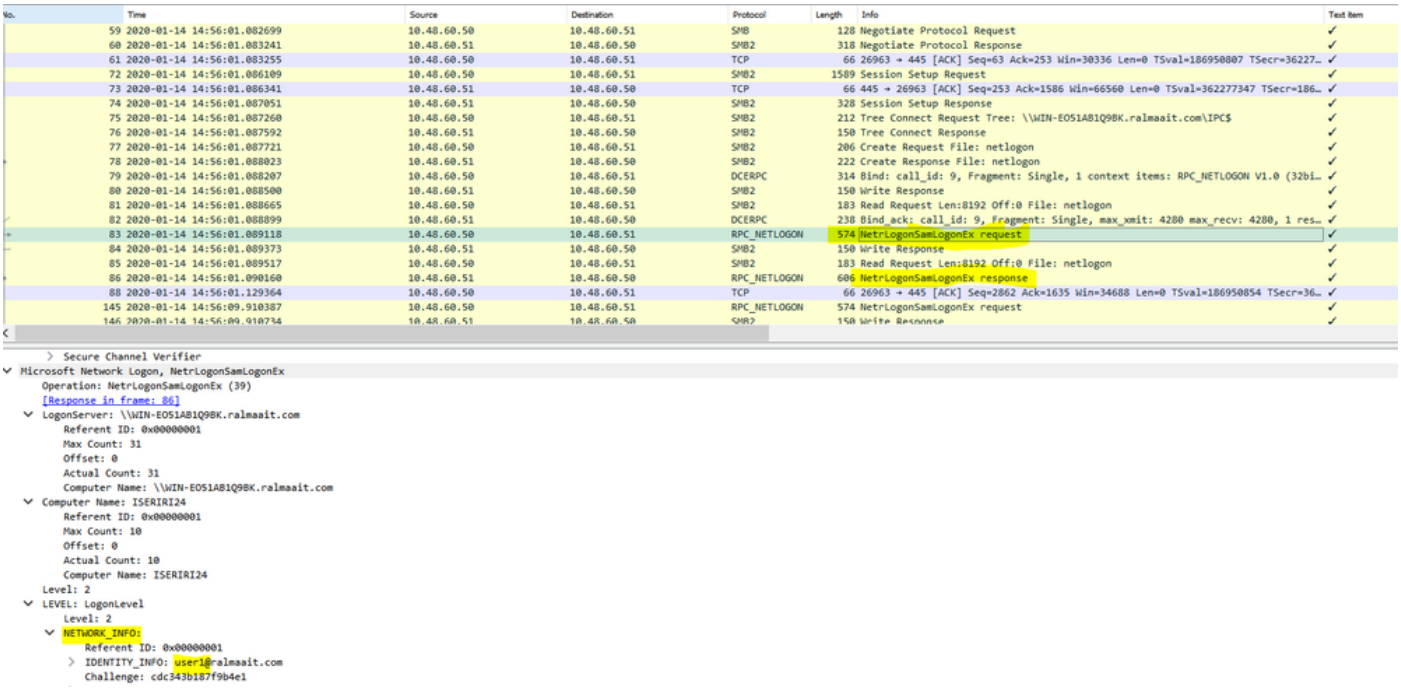
2020-01-14 13:36:05,444 DEBUG,140574072981248,[LwKrb5InitializeUserLoginCredentials()] Code d'erreur : 40022 (symbole : LW_ERROR_PASSWORD_MISMATCH),LwKrb5InitializeUserLoginCredentials(),lwadvapi/threaded/lwkrb

## Protocole MS-RPC

ISE utilise MS-RPC sur SMB, SMB fournit l'authentification et ne nécessite pas de session séparée pour trouver l'emplacement d'un service RPC donné. Il utilise un mécanisme appelé « canal nommé » pour communiquer entre le client et le serveur.

- Créez une connexion de session SMB.
- Transport des messages RPC sur le port SMB/CIFS.TCP 445 en tant que transport
- La session SMB identifie le port qu'un service RPC particulier exécute et gère l'authentification des utilisateurs.
- Connectez-vous au partage masqué IPC$ pour la communication entre processus.
- Ouvrez un canal nommé approprié pour la ressource/fonction RPC souhaitée.

Traitez l'échange RPC sur SMB.




Les **negotiate protocol request/response** négocie le dialecte de SMB. Les **session setup request/response** effectue l'authentification.

La requête et la réponse de connexion à l'arborescence se connectent à la ressource demandée. Vous êtes connecté à un partage spécial IPC$.

Ce partage de communication entre processus fournit les moyens de communication entre les hôtes et sert également de transport pour les fonctions MSRPC.

Au niveau du paquet 77 est **Create Request File** et le nom de fichier est le nom du service connecté (le service netlogon dans cet exemple).

Sur les paquets 83 et 86, la demande NetLogonSamLogonEX est l'emplacement où vous envoyez le nom d'utilisateur pour l'authentification client sur ISE à l'AD au champ Network_INFO.

Le paquet de réponse NetLogonSamLogonEX répond avec les résultats.

Quelques valeurs d'indicateur pour la réponse NetLogonSamLogonEX :
0xc000006a est STATUS_WRONG_PASSWORD
0x00000000 est STATUS_SUCCESS
0x00000103 est STATUS_PENDING

## Intégration d'ISE avec Active Directory(AD)

ISE utilise LDAP, KRB et MSRBC pour communiquer avec AD pendant le processus de

jointure/abandon et d'authentification.

Les sections suivantes fournissent les protocoles, le format de recherche et les mécanismes utilisés pour se connecter à un contrôleur de domaine spécifique sur Active Directory et l'authentification des utilisateurs par rapport à ce contrôleur de domaine.

Si le contrôleur de domaine devient hors ligne pour une raison quelconque, ISE bascule vers le contrôleur de domaine disponible suivant et le processus d'authentification n'est pas affecté.

Un serveur de catalogue global est un contrôleur de domaine qui stocke des copies de tous les objets Active Directory dans la forêt.

Il stocke une copie complète de tous les objets dans le répertoire de votre domaine et une copie partielle de tous les objets de tous les autres domaines de forêt.

Ainsi, le catalogue global permet aux utilisateurs et aux applications de trouver des objets dans n'importe quel domaine de la forêt actuelle avec une recherche d'attributs inclus dans le catalogue global.

Le catalogue global contient un jeu d'attributs de base (mais incomplet) pour chaque objet de forêt dans chaque domaine (jeu d'attributs partiel, PAT).

Le catalogue global reçoit des données de toutes les partitions d'annuaire de domaine de la forêt. Ils sont copiés avec le service de réplication AD standard.

## Rejoindre ISE à AD

Prérequis pour l'intégration d'Active Directory et d'ISE

1. Vérifiez que vous disposez des privilèges de super administrateur ou d'administrateur système dans ISE.
2. Utilisez les paramètres du serveur NTP (Network Time Protocol) pour synchroniser l'heure entre le serveur Cisco et Active Directory. La différence de temps maximale autorisée entre ISE et AD est de 5 minutes
3. Le DNS configuré sur ISE doit être capable de répondre aux requêtes SRV pour les DC, les GC et les KDC avec ou sans informations supplémentaires sur le site.
4. Assurez-vous que tous les serveurs DNS peuvent répondre aux requêtes DNS directes et inversées pour n'importe quel domaine DNS Active Directory possible.
5. AD doit avoir au moins un serveur de catalogue global opérationnel et accessible par Cisco, dans le domaine auquel vous rejoignez Cisco.

## Joindre un domaine AD

ISE applique la découverte de domaine pour obtenir des informations sur le domaine joint en trois phases :

1. Requêtes sur les domaines joints : détecte les domaines de sa forêt et les domaines approuvés en externe sur le domaine joint.

2. Interroge les domaines racine dans sa forêt : établit l'approbation avec la forêt.
3. Interroge les domaines racine dans les forêts approuvées : découvre les domaines des forêts approuvées.

En outre, Cisco ISE détecte les noms de domaine DNS (suffixes UPN), les autres suffixes UPN et les noms de domaine NTLM.

ISE applique une détection de contrôleurs de domaine pour obtenir toutes les informations sur les contrôleurs de domaine et les contrôleurs de domaine.

1. Le processus de jointure commence par les informations d'identification d'entrée de super admin sur AD qui existent dans le domaine lui-même. S'il existe dans un domaine ou sous-domaine différent, le nom d'utilisateur doit être noté dans une notation UPN (username@domain).
2. ISE envoie une requête DNS pour tous les enregistrements des contrôleurs de domaine, des contrôleurs de domaine globaux et des contrôleurs de domaine clés. Si la réponse DNS n'en contenait pas, l'intégration échoue avec l'erreur liée au DNS.
3. ISE utilise la requête ping CLDAP pour détecter tous les DC et GC via les requêtes CLDAP envoyées aux DC qui correspondent à leurs priorités dans l'enregistrement SRV. La première réponse CC est utilisée et ISE est alors connecté à ce CC.

Un facteur utilisé pour calculer la priorité du contrôleur de domaine est le temps nécessaire au contrôleur de domaine pour répondre aux requêtes ping LDAP ; une réponse plus rapide reçoit une priorité plus élevée.

---

Remarque : le protocole CLDAP est le mécanisme utilisé par ISE pour établir et maintenir la connectivité avec les contrôleurs de domaine. Il mesure le temps de réponse jusqu'à la première réponse DC. Il échoue si vous ne voyez aucune réponse du contrôleur de domaine. Avertir si le temps de réponse est supérieur à 2,5 secondes. CLDAP envoie une requête ping à tous les DC du site (si aucun site, tous les DC du domaine). La réponse LDAP contient le site DC et le site client (le site auquel la machine ISE est attribuée).

---

4. ISE reçoit alors le TGT avec les informations d'identification « join user ».
5. Générez le nom du compte de l'ordinateur ISE avec le MSRPC. (SAM et SPN)
6. Rechercher AD par SPN si un compte d'ordinateur ISE existe déjà. Si la machine ISE n'existe pas, ISE en crée une nouvelle.
7. Ouvrez un compte de machine, définissez le mot de passe du compte de machine ISE et vérifiez que le compte de machine ISE est accessible.
8. Définissez les attributs de compte de machine ISE (SPN, dnsHostname, etc.).
9. Obtenez TGT avec les identifiants de machine ISE avec KRB5 et découvrez tous les domaines approuvés.
10. Une fois la jointure terminée, le noeud ISE met à jour ses groupes AD et les SID associés et lance automatiquement le processus de mise à jour des SID. Vérifiez que ce processus peut se terminer du côté Active Directory.

## Quitter le domaine Active Directory

Lorsqu'ISE part, la DA doit tenir compte des éléments suivants :

1. Utilisez un utilisateur administrateur AD complet pour effectuer les processus de congé. Cela permet de vérifier que le compte d'ordinateur ISE est supprimé de la base de données Active Directory.
2. Si la liste de contrôle d'accès est restée sans informations d'identification, le compte ISE n'est pas supprimé de la liste de contrôle d'accès et doit être supprimé manuellement.
3. Lorsque vous réinitialisez la configuration ISE à partir de l'interface de ligne de commande ou que vous restaurez la configuration après une sauvegarde ou une mise à niveau, il effectue une opération de fermeture et déconnecte le noeud ISE du domaine Active Directory. (si joint). Cependant, le compte de noeud ISE n'est pas supprimé du domaine Active Directory.
4. Il est recommandé d'effectuer une opération Leave à partir du portail Admin avec les informations d'identification Active Directory, car le compte de noeud est également supprimé du domaine Active Directory. Cela est également recommandé lorsque vous modifiez le nom d'hôte ISE.

## Basculement de DC

Lorsque le contrôleur de domaine connecté à ISE devient hors ligne ou inaccessible pour une raison quelconque, le basculement du contrôleur de domaine est déclenché automatiquement sur ISE. Le basculement du contrôleur de domaine peut être déclenché par les conditions suivantes :

1. Le connecteur AD détecte que le contrôleur de domaine actuellement sélectionné est devenu indisponible lors d'une tentative de communication LDAP, LDAP, RPC ou Kerberos. Dans ce cas, le connecteur Active Directory lance la sélection du contrôleur de domaine et bascule vers le nouveau contrôleur de domaine sélectionné.
2. Le contrôleur de domaine est actif et répond à la requête ping LDAP, mais le connecteur AD ne peut pas communiquer avec lui pour une raison quelconque (exemples : le port RPC est bloqué, le contrôleur de domaine est en état de « réplication interrompue », le contrôleur de domaine n'a pas été correctement mis hors service).

Dans de tels cas, le connecteur AD initie la sélection de DC avec une liste bloquée (« mauvais » DC est placé dans la liste bloquée) et tente de communiquer avec le DC sélectionné. Le contrôleur de domaine sélectionné dans la liste bloquée n'est pas mis en cache.

Le connecteur AD doit terminer le basculement dans un délai raisonnable (ou échouer si cela n'est pas possible). Pour cette raison, le connecteur AD essaie un nombre limité de contrôleurs de domaine pendant le basculement.

ISE bloque les contrôleurs de domaine Active Directory en cas d'erreur de serveur ou de réseau irrécupérable pour empêcher ISE d'utiliser un contrôleur de domaine défectueux. Le contrôleur de domaine n'est pas ajouté à la liste bloquée s'il ne répond pas aux requêtes ping LDAP. ISE réduit uniquement la priorité du contrôleur de domaine qui ne répond pas.

## Communication ISE-AD via LDAP

ISE recherche un ordinateur ou un utilisateur dans Active Directory avec l'un de ces formats de recherche. Si la recherche portait sur une machine, ISE ajoute « $ » à la fin du nom de la machine. Il s'agit d'une liste de types d'identités utilisée pour identifier un utilisateur dans Active Directory :

- SAM name : nom d'utilisateur ou nom d'ordinateur sans marque de domaine, il s'agit du nom d'ouverture de session utilisateur dans Active Directory. Exemple : sajeda ou sajeda$
- CN : est le nom d'affichage de l'utilisateur sur AD, il ne doit pas être identique au SAM. Exemple : sajeda Ahmed.
- User Principal Name (UPN) : est une combinaison du nom SAM et du nom de domaine (SAM_NAME@domian). Exemple : sajeda@cisco.com ou sajeda$@cisco.com
- Autre UPN : est un suffixe UPN supplémentaire / alternatif qui a été configuré dans AD autre que le nom de domaine. Cette configuration est ajoutée globalement dans AD (non configurée par utilisateur) et il n'est pas nécessaire d'être un suffixe de nom de domaine réel.

Chaque AD peut avoir plusieurs suffixes UPN (@alt1.com,@alt2.com,..., etc). Exemple : UPN principal (sajeda@cisco.com), UPN alternatif :sajeda@domain1 , sajeda@domain2

- Nom préfixe NetBIOS : est le nom de domaine\nom d'utilisateur du nom de l'ordinateur. Exemple : CISCO\sajeda ou CISCO\machine$
- Hôte/préfixe avec ordinateur non qualifié : utilisé pour l'authentification de l'ordinateur lorsque le nom de l'ordinateur est utilisé uniquement, il s'agit du nom de l'hôte/de l'ordinateur uniquement. Exemple : hôte/machine
- Hôte/préfixe avec machine entièrement qualifiée : il est utilisé pour l'authentification de la machine lorsque le nom de domaine complet de la machine est utilisé, généralement en cas d'authentification de certificat, il s'agit de l'hôte/nom de domaine complet de la machine. Exemple : host/machine.cisco.com
- SPN name : nom par lequel un client identifie de manière unique une instance d'un service (par exemple, HTTP, LDAP, SSH) utilisé pour l'ordinateur uniquement.

## Authentification utilisateur par rapport au flux AD :

1. Résolvez l'identité et déterminez le type d'identité - SAM, UPN, SPN. Si ISE reçoit l'identité en tant que nom d'utilisateur uniquement, il recherche un compte SAM associé dans AD. Si ISE reçoit l'identité en tant que username@domain, il recherche un UPN ou un message correspondant dans AD. Dans les deux scénarios, ISE utilise des filtres supplémentaires pour l'ordinateur ou le nom d'utilisateur.
2. Domaine ou forêt de recherche (selon le type d'identité)
3. Conserver les informations sur tous les comptes associés (JP, DN, UPN, domaine)
4. Si aucun compte associé n'est trouvé, AD répond avec l'utilisateur inconnu.
5. Effectuer l'authentification MS-RPC (ou Kerberos) pour chaque compte associé

6. Si un seul compte correspond à l'identité et au mot de passe entrés, l'authentification réussit
7. Si plusieurs comptes correspondent à l'identité entrante, ISE utilise le mot de passe pour résoudre l'ambiguïté de sorte que le compte associé à un mot de passe soit authentifié et que les autres comptes augmentent le compteur de mots de passe incorrects de 1.
8. Si aucun compte ne correspond à l'identité et au mot de passe entrants, AD répond avec un mot de passe incorrect.

## ISE Filtres de recherche

Les filtres sont utilisés pour identifier une entité qui souhaite communiquer avec AD. ISE recherche toujours cette entité dans les groupes d'utilisateurs et d'ordinateurs.

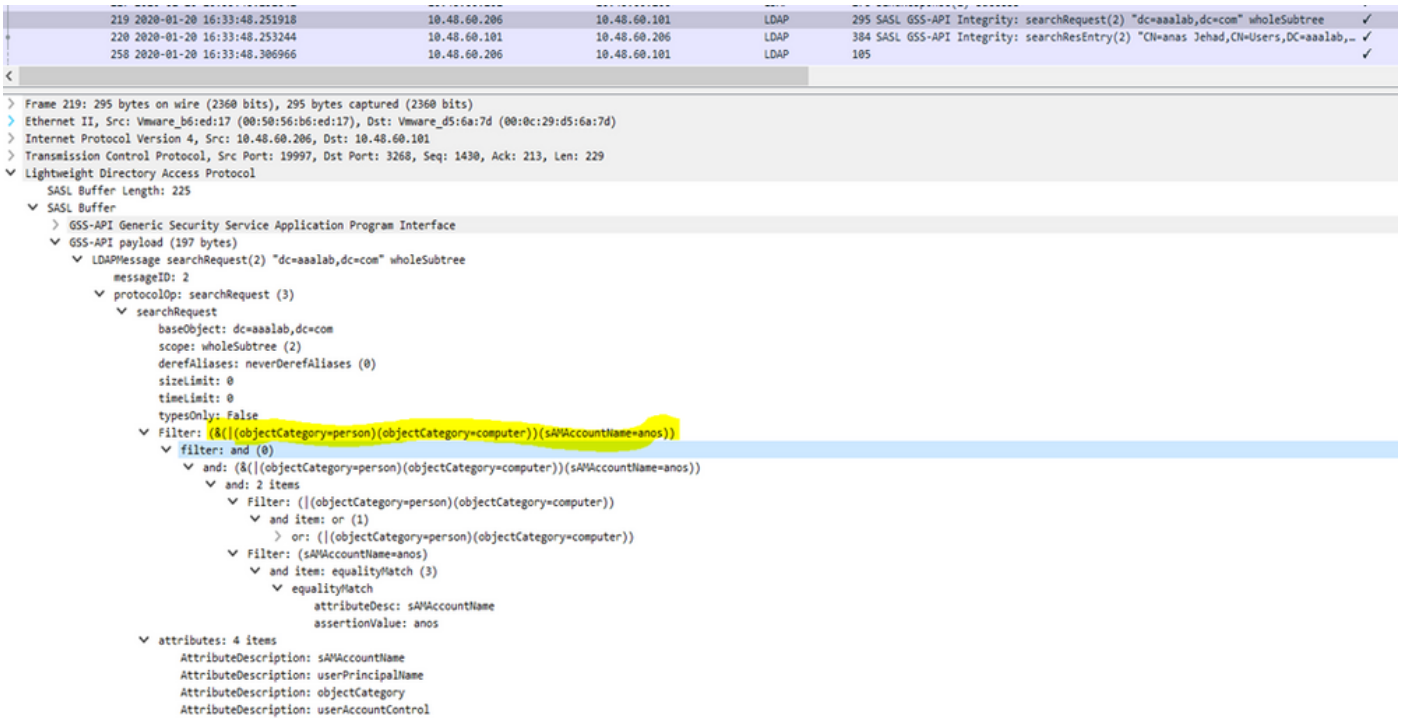
Exemples de filtres de recherche :

1. Recherche SAM : si ISE reçoit une identité en tant que nom d'utilisateur uniquement sans balisage de domaine, ISE traite ce nom d'utilisateur en tant que SAM et recherche dans Active Directory tous les utilisateurs de machine ou les machines qui ont cette identité en tant que nom SAM.

Si le nom SAM n'est pas unique, ISE utilise le mot de passe pour différencier les utilisateurs et ISE est configuré pour utiliser un protocole sans mot de passe tel qu'EAP-TLS.

Comme il n'existe aucun autre critère permettant de localiser l'utilisateur approprié, ISE échoue l'authentification avec une erreur « Identité ambiguë ».

Toutefois, si le certificat utilisateur est présent dans Active Directory, Cisco ISE utilise la comparaison binaire pour résoudre l'identité.

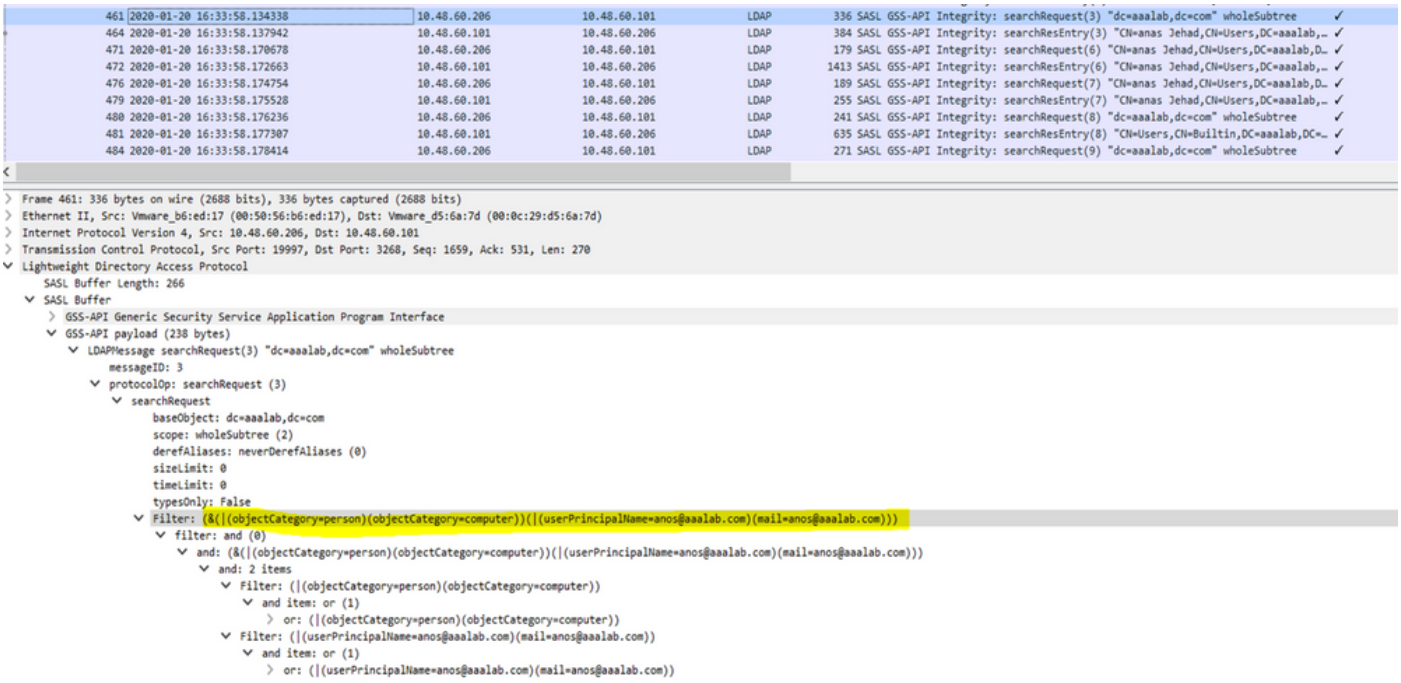



2. Recherche UPN ou MAIL : si ISE reçoit une identité en tant que username@domain, elle recherche dans chaque catalogue global de forêt une correspondance avec cette identité

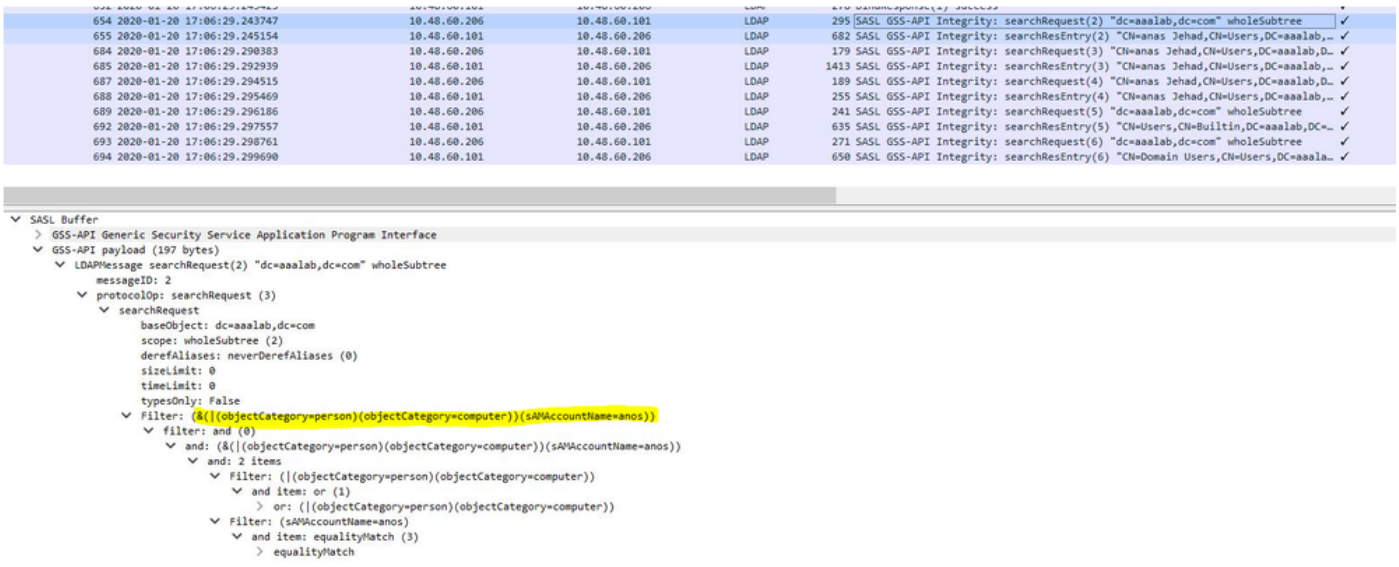
UPN ou identité Mail « identity=match UPN or email ».

S'il existe une correspondance unique, Cisco ISE poursuit avec le flux AAA.

S'il existe plusieurs points de jonction avec le même UPN et un mot de passe ou les mêmes UPN et Mail, Cisco ISE échoue l'authentification avec une erreur « Identité ambiguë ».




3. Recherche NetBIOS : si ISE reçoit une identité avec un préfixe de domaine NetBIOS (ex : CISCO\sajedah), alors ISE recherche le domaine NetBIOS dans les forêts. Une fois trouvé, il recherche le nom SAM fourni (sajeda dans notre exemple)

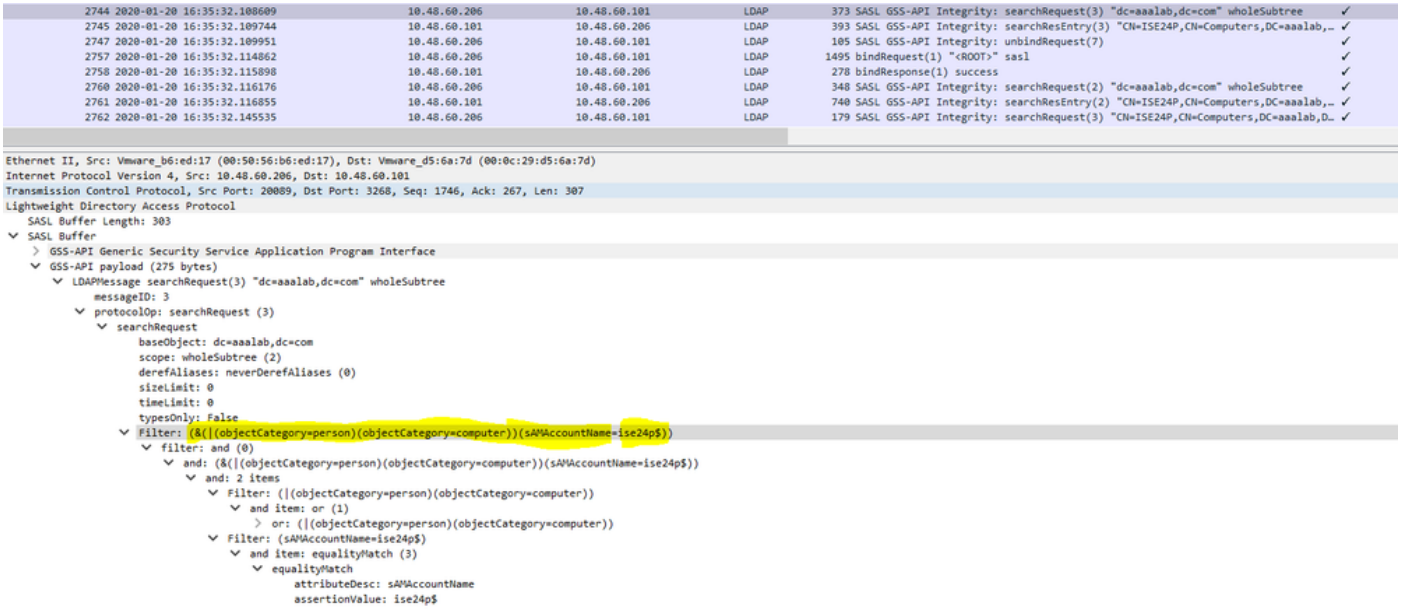



4. Recherche de base de machine : si ISE reçoit une authentification de machine, avec une identité hôte/préfixe, alors ISE recherche dans la forêt un attribut servicePrincipalName correspondant.

Si un suffixe de domaine complet a été spécifié dans l'identité, par exemple host/machine.domain.com, Cisco ISE recherche la forêt où ce domaine existe.

Si l'identité est sous la forme d'hôte/machine, Cisco ISE recherche le nom principal du service dans toutes les forêts.

S'il y a plusieurs correspondances, Cisco ISE échoue l'authentification avec une erreur « Identité ambiguë ».




Remarque : les mêmes filtres sont visibles dans les fichiers ISE ad-agent.log

Remarque : ISE 2.2 patch 4 et versions antérieures et 2.3 patch 1 et versions antérieures ont identifié les utilisateurs avec les attributs SAM, CN ou les deux. Cisco ISE, version 2.2 Patch 5 et ultérieure, et 2.3 Patch 2 et ultérieure, utilisent uniquement l'attribut sAMAccountName comme attribut par défaut.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.