Dépannage de l'authentification Kerberos dans SWA

Table des matières

Introduction

Ce document décrit les bases de l'authentification Kerberos et les étapes de dépannage de l'authentification Kerberos dans l'appareil Web sécurisé (SWA).

Terminologie

SWA	Appareil Web sécurisé
CLI	Interface de ligne de commande
PUBLICITÉ	Active Directory
CC	Contrôleur de domaine

SPN	Nom principal du service
KDC	Centre de distribution de clés Kerberos
TGT	Ticket d'authentification (Ticket d'octroi de ticket)
TGS	Service De Délivrance De Billets
HA	Haute disponibilité
VRRP	Protocole de redondance de routeur virtuel
TAQUINER	protocole de redondance d’adresses communes
SPN	Nom principal du service
LDAP	protocole allégé d'accès annuaire

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Active Directory et authentification Kerberos.
- Authentification et domaines sur SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Flux réseau Kerberos

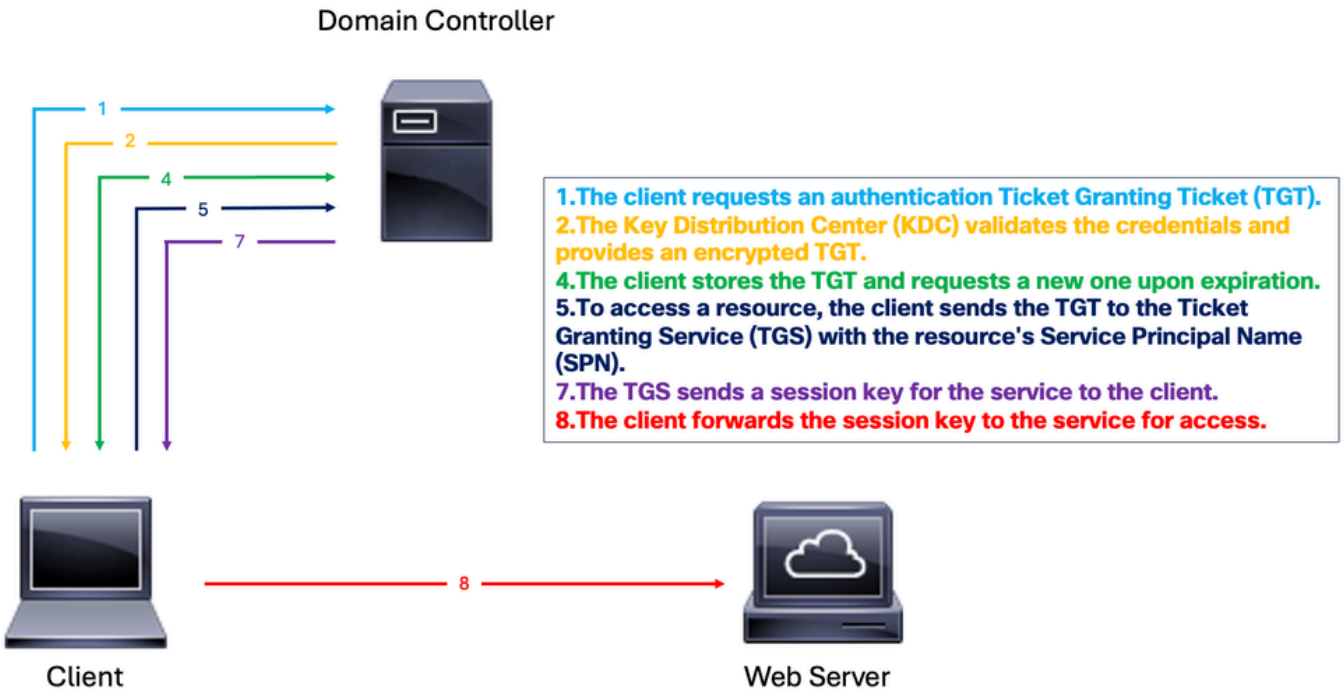


Image : Exemple de flux Kerberos

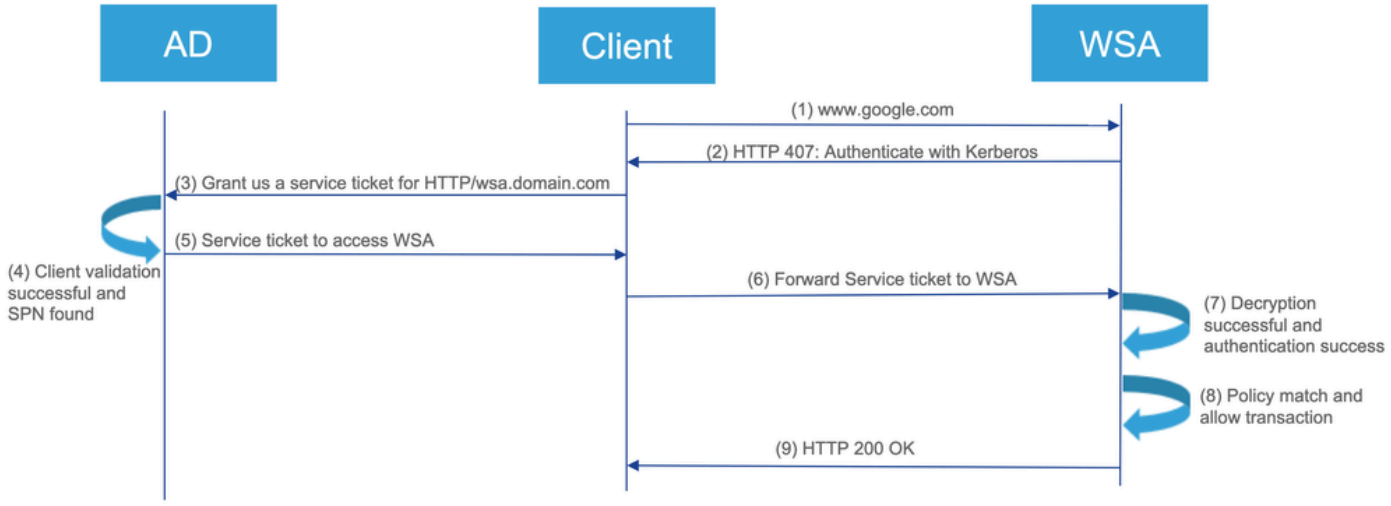
Voici les étapes de base pour l'authentification dans un environnement Kerberized :

1. Le client demande un ticket TGT (Ticket Granting Ticket) au centre de distribution de clés (KDC).
2. Le KDC vérifie les informations d'identification de l'utilisateur de la machine client et renvoie un TGT et une clé de session chiffrés.
3. Le TGT est chiffré avec la clé secrète TGS (Ticket Granting Service).
4. Le client stocke le TGT et en demande automatiquement un nouveau lorsqu'il expire.

Pour accéder à un service ou à une ressource :
1. Le client envoie le TGT au TGS avec le nom principal de service (SPN) de la ressource souhaitée.
2. Le KDC vérifie le TGT et les droits d'accès de l'ordinateur client de l'utilisateur.

3. Le TGS envoie une clé de session spécifique au service au client.
4. Le client fournit la clé de session au service pour prouver l'accès, et le service accorde l'accès.

Flux d'authentification Kerberos dans SWA



1. Le client demande l'accès à www.google.com via le SWA.
2. Le SWA répond avec un état "HTTP 407", demandant une authentification.
3. Le client demande un ticket de service du serveur AD pour le service HTTP/SWA.domain.com en utilisant le TGT qu'il obtient lors de la jonction de domaine.
4. Le serveur Active Directory valide le client et émet un ticket de service. S'il réussit et que le SPN (nom principal du service) de SWA est trouvé, il passe à l'étape suivante.
5. Le client envoie ce ticket au SWA.
6. Le SWA déchiffre le ticket et vérifie l'authentification.
7. Si l'authentification réussit, le SWA vérifie les stratégies.
8. Le SWA envoie une réponse « HTTP 200/OK » au client si la transaction est autorisée.

Quel est l'objectif du SPN ?

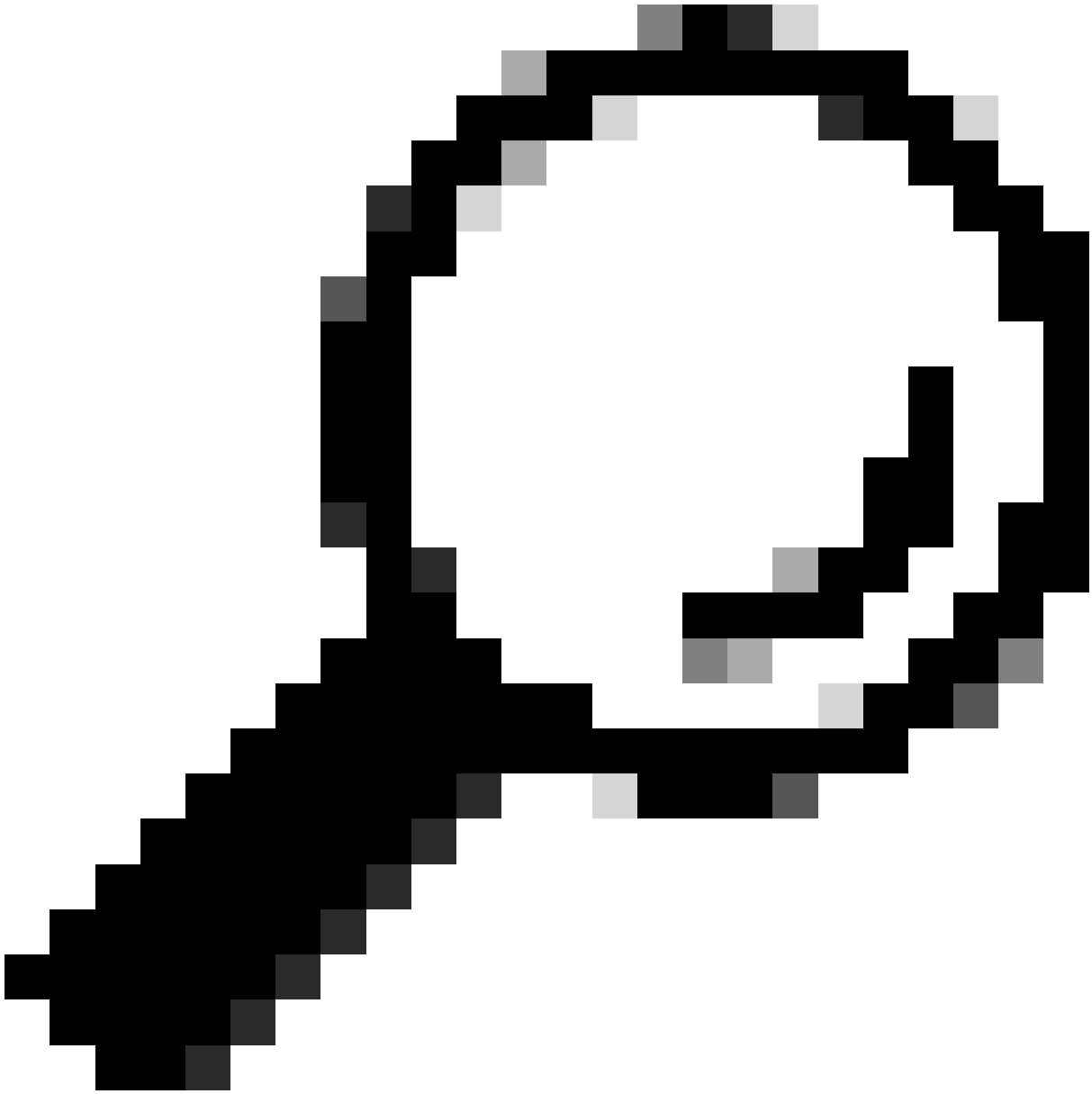
Un nom principal de service (SPN) identifie de manière unique une instance de service dans l'authentification Kerberos. Il relie une instance de service à un compte de service, permettant aux clients de demander l'authentification pour le service sans avoir besoin du nom du compte. Chaque compte d'une implémentation de centre de distribution de clés (KDC), telle qu'AD ou Open LDAP, possède un SPN. Bien que le SPN identifie strictement un service, il est parfois utilisé par erreur pour faire référence au nom du client (UPN) dans des scénarios où le service agit également en tant que client.

Dans Kerberos, un nom principal de service (SPN) identifie de manière unique une instance de service au sein d'un réseau. Il permet aux clients de demander l'authentification pour un service spécifique. Le SPN relie l'instance de service à son compte, ce qui permet à Kerberos d'authentifier et d'autoriser correctement les demandes d'accès à ce service.

Configuration du serveur Active Directory

1. Créez un nouveau compte d'utilisateur ou choisissez un compte d'utilisateur existant à utiliser.

2. Enregistrez le SPN à utiliser pour le compte d'utilisateur choisi.
3. Assurez-vous qu'aucun SPN dupliqué n'est enregistré.



Conseil : En quoi Kerberos avec SWA derrière l'équilibreur de charge ou un Traffic Manager/Traffic Shaper est-il différent ? Au lieu d'associer le SPN du nom d'hôte virtuel HA à un compte d'utilisateur, associez le SPN du périphérique de redirection du trafic HTTP (par exemple : LoadBalancer ou Traffic Manager) avec un compte d'utilisateur sur AD.

Les Méthodes Recommandées pour la mise en oeuvre de Kerberos sont les suivantes :

- Meilleures pratiques pour les appliances Web sécurisées
- Configuration des ports de pare-feu pour les connexions SWA

Dépannage

Dépannage de Kerberos avec les commandes SPN

Voici une liste de commandes setspn utiles pour la gestion des noms de principal de service (SPN) dans un environnement Kerberos. Ces commandes sont généralement exécutées à partir d'une interface de ligne de commande avec des privilèges d'administration dans un environnement Windows.

Répertorier les SPN d'un compte spécifique :	setspn -L <NomCompteUtilisateur/Ordinateur> Répertorie tous les SPN enregistrés pour le compte spécifié.
Ajouter un SPN à un compte :	setspn -A <SPN> <NomCompteUtilisateur/Ordinateur> Ajoute le SPN spécifié au compte donné.
Supprimer un SPN d'un compte :	setspn -D <SPN> <NomCompteUtilisateur/Ordinateur> Supprime le SPN spécifié du compte donné.
Vérifiez si un SPN est déjà enregistré :	setspn -Q <SPN> Vérifie si le SPN spécifié est déjà enregistré dans le domaine.
Répertorier tous les SPN du domaine	setspn -L <Compte utilisateur/ordinateur> Répertorie tous les SPN du domaine.
Définir un SPN pour un compte d'ordinateur :	setspn -S <SPN> <NomCompteUtilisateur/Ordinateur> Ajoute un SPN à un compte d'ordinateur, ce qui évite les entrées en double.
Réinitialiser les SPN d'un compte spécifique :	setspn -R <NomCompteUtilisateur/Ordinateur> Réinitialise les SPN du compte spécifié, ce qui permet de résoudre les problèmes de SPN en double.

Exemples de commandes et de résultats SPN

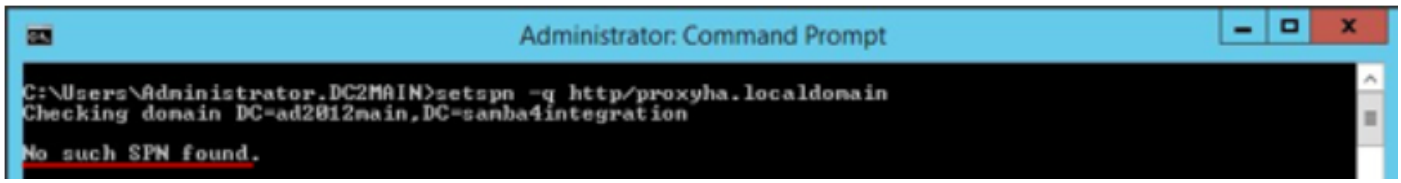
Les exemples fournis illustrent l'utilisation :

- Compte utilisateur/ordinateur : vrrpserviceuser
- SPN : http/WsaHostname.com ou http/proxyha.localdomain

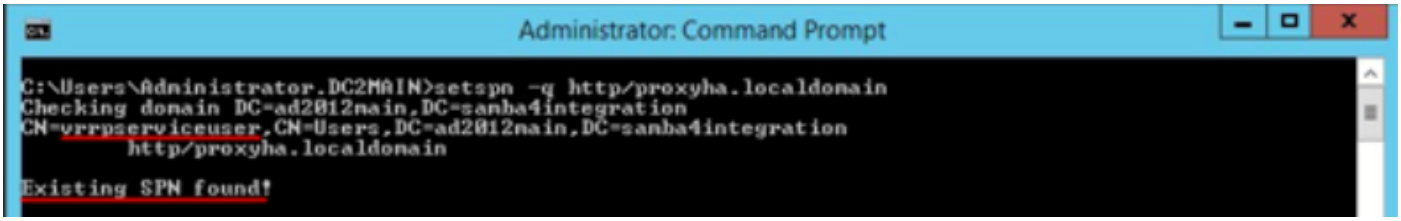
Vérifiez si le SPN est déjà associé à un compte d'utilisateur :
setspn -q <SPN>

setspn -q http/proxyha.localdomain

Scénario 1 : SPN introuvable



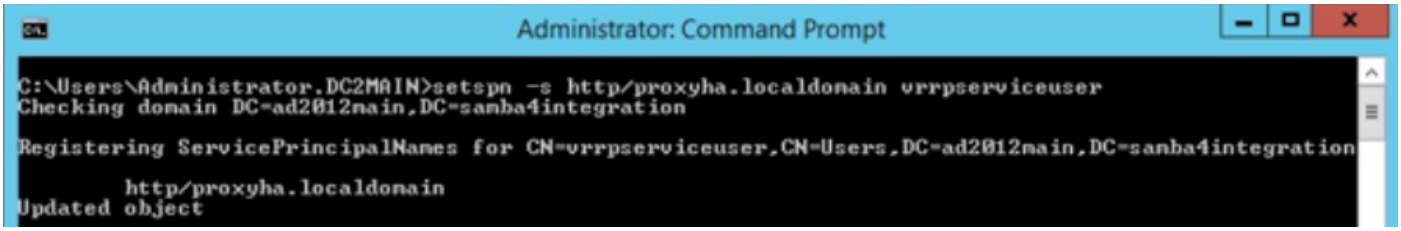
Scénario 2 : SPN détecté



- Associez un SPN à un compte utilisateur/ordinateur valide :

Syntaxe: setspn -s <SPN> <Compte utilisateur/ordinateur>

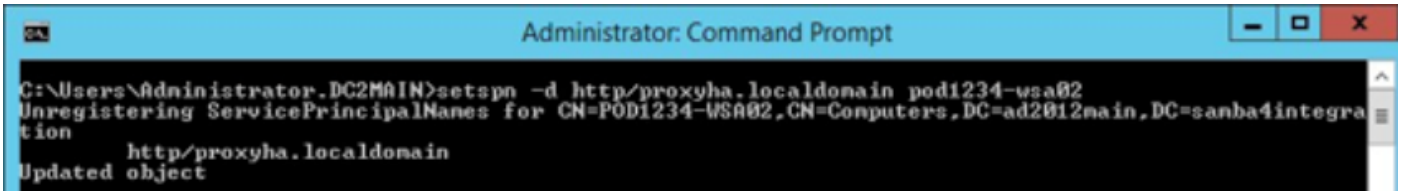
Exemple : setspn -s http/proxyha.localdomain vrrpserviceuser



- Supprimer/Supprimer un SPN déjà associé à un compte d'utilisateur ou d'ordinateur :

Syntaxe: setspn -d <SPN> <Compte utilisateur/ordinateur>

Exemple : setspn -d http/proxyha.localdomain pod1234-wsa0

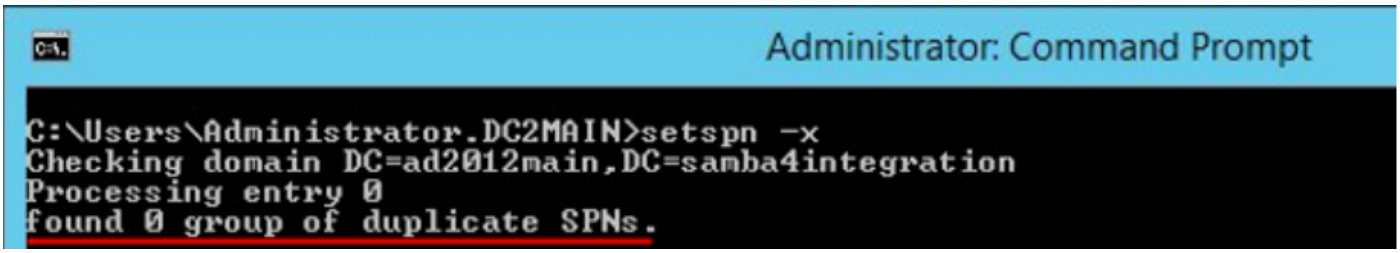


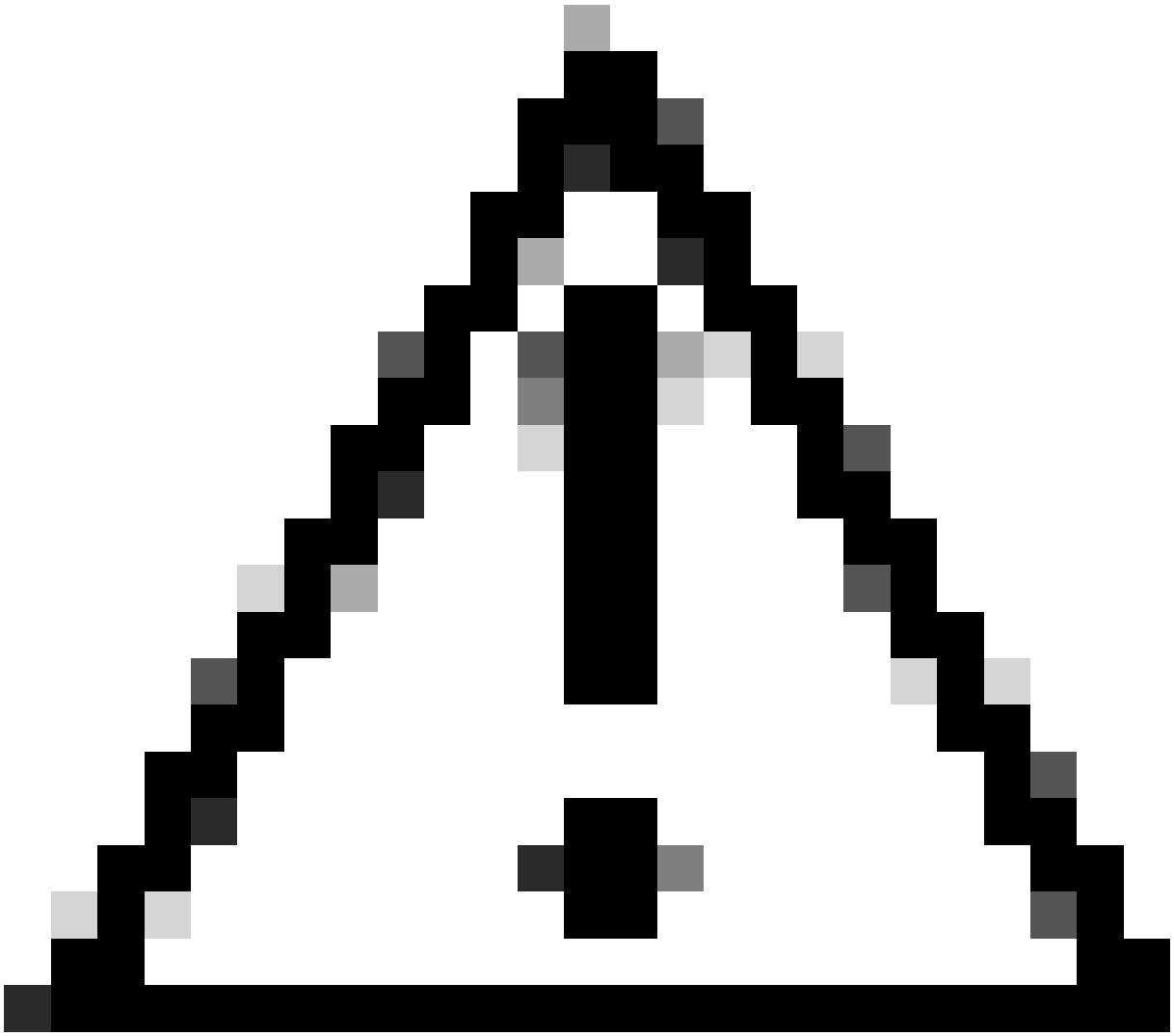
Assurez-vous qu'il n'y a pas de SPN dupliqués pour le nom d'hôte virtuel haute disponibilité, car

des défaillances peuvent se produire ultérieurement.

- Commande à utiliser : setspn -x

Par conséquent, le ticket du service Kerberos n'est pas fourni au client et l'authentification Kerberos échoue.



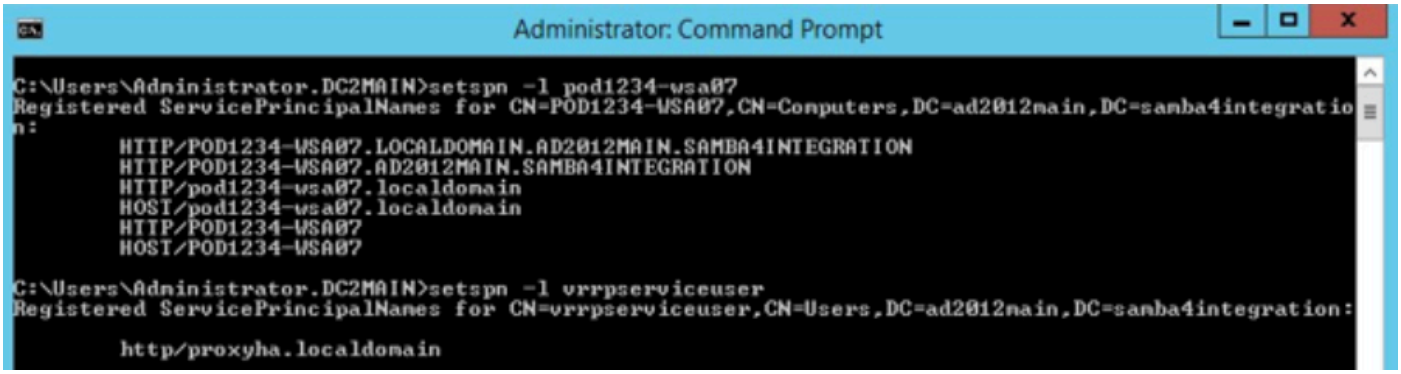


Mise en garde : Si des doublons sont trouvés, veuillez les supprimer à l'aide de la commande setspn -d.

- Répertoriez tous les SPN associés à un compte :

Syntaxe: setspn -l <Compte utilisateur/ordinateur>

Exemple : setspn -l vrrpserviceuser



Dépannage de Kerberos sur SWA

Informations que l'assistance Cisco doit obtenir lors du dépannage des problèmes d'authentification Kerberos :

- Détails de la configuration actuelle.
- Journaux d'authentification (de préférence en mode débogage ou trace).
- Captures de paquets effectuées (avec les filtres appropriés) :

  (a) Périphérique client

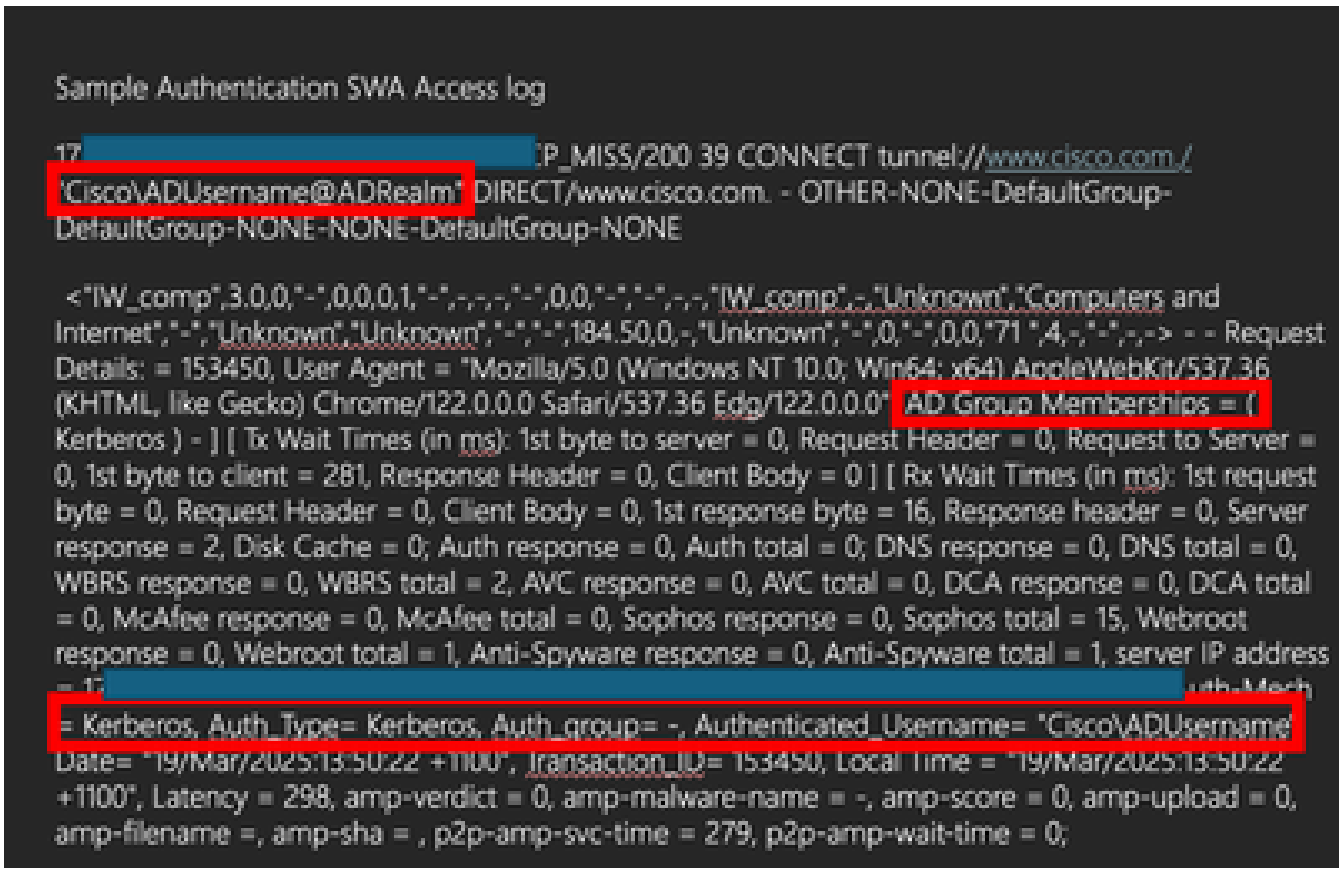
  (b) SWA

- Journaux d'accès avec le spécificateur de format personnalisé %m activé. Ce champ doit indiquer le mécanisme d'authentification qui a été utilisé pour une transaction spécifique.
- Pour obtenir des détails détaillés sur l'authentification, ajoutez ces champs personnalisés aux journaux d'accès sur les proxys actifs/inactifs pour obtenir plus d'informations ou reportez-vous au lien hypertexte Ajout de paramètres dans les journaux d'accès.
- Dans l'interface utilisateur graphique de SWA, accédez à Administration système > Abonnement aux journaux > Journaux d'accès > Champs personnalisés > Ajouter cette chaîne pour les problèmes d'authentification :

```
server IP address = %k, Client IP address= %a, Auth-Mech = %m, Auth_Type= %m, Auth_group= %g, Authentic
```

```
a;
```

- Journal d'accès SWA pour les détails d'authentification utilisateur.
- Cisco SWA enregistre les noms d'utilisateur authentifiés au format Domaine\username@authentication_realm:



- Exécutez Test Authentication Realm Settings à partir de l'interface utilisateur graphique. Accédez à Network > Authentication, puis cliquez sur le nom de votre domaine dans la section Test Current Settings. Cliquez sur Start Test.

Serveur introuvable dans la base de données Kerberos

Les requêtes Web échouant avec « Serveur introuvable dans la base de données Kerberos » constituent un cas d'erreur courant :

```
curl -vx proxyha.local:3128 --proxy-negotiate -u: http://www.cisco.com/
* About to connect() to proxy proxyha.localdomain port 3128 (#0)
* Connected to proxyha.local (10.8.96.30) port 3128 (#0)
< HTTP/1.1 407 Proxy Authentication Required
< Via: 1.1 pod1234-wsa02.local:80 (Cisco-SWA/10.1.2-003)
< Content-Type: text/html
gss_init_sec_context() failed: : Server not found in Kerberos database
< Proxy-Authenticate: Negotiate
< Connection: close
* HTTP/1.1 proxy connection set close!
```

Dans ce cas, l'erreur indique que le nom principal du service correspondant à la valeur d'adresse

proxy proxyha.local n'est pas inscrit sur le serveur Active Directory. Pour résoudre le problème, il est nécessaire de confirmer que le SPN http/proxyha.local est enregistré sur AD DC et ajouté à un compte de service approprié.

Informations supplémentaires et références

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.