Probleemoplossing voor Kerberos-verificatie in SWA

Inhoud

- Inleiding
- Terminologie
- Voorwaarden
  - Vereisten
  - Gebruikte componenten
- Kerberos-netwerkstroom
  - Kerberos-verificatiestroom in SWA
  - Wat is het doel van SPN?
  - Configuratie van Active Directory-server
- Probleemoplossing
  - Problemen oplossen bij Kerberos met SPN-opdrachten
  - Voorbeelden van SPN-opdrachten en -uitvoer
    - Scenario 1: SPN niet gevonden
    - Scenario 2: SPN gevonden
  - Problemen met Kerberos op SWA oplossen
  - Server niet gevonden in Kerberos Database
- Aanvullende informatie en referenties

Inleiding

Dit document beschrijft de basisprincipes van Kerberos-verificatie en de stappen om Kerberos-verificatie in Secure Web Appliance (SWA) op te lossen.

Terminologie

SWA	Secure Web-applicatie
CLI	Opdrachtlijninterface
AD	Active Directory
gelijkstroom	Domeincontroller

CENTRIFUGE	Naam van serviceresources
KDC	Kerberos-sleuteldistributiecentrum
TGT	Verificatiekaart (ticket voor toewijzing)
TGS	Tickettoekenningsservice
HA	Hoge beschikbaarheid
VRRP	Virtueel routerredundantieprotocol
KARPER	Gemeenschappelijk Protocol voor adresredundantie
CENTRIFUGE	Naam van serviceresources
LDAP	Lichtgewicht Directory Access Protocol

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

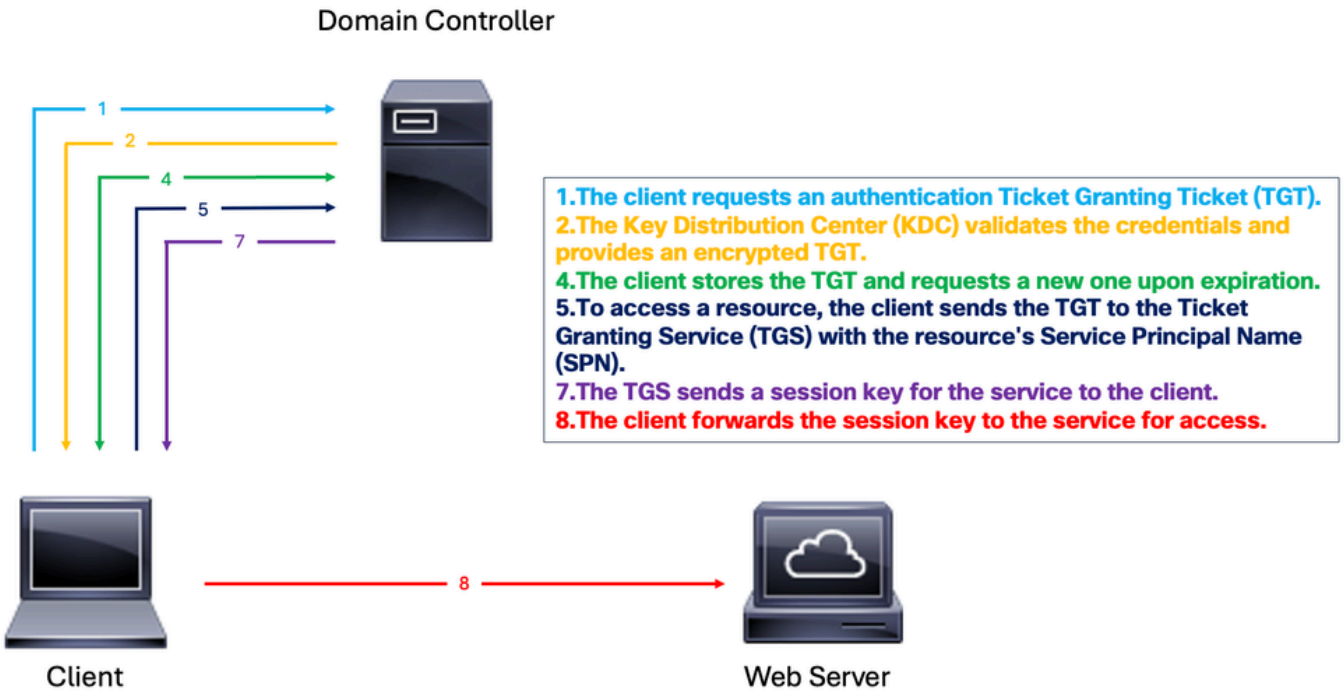
- Active Directory en Kerberos-verificatie.
- Verificatie en domeinen op SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Kerberos-netwerkstroom



Afbeelding: Steekproef Kerberos Flow

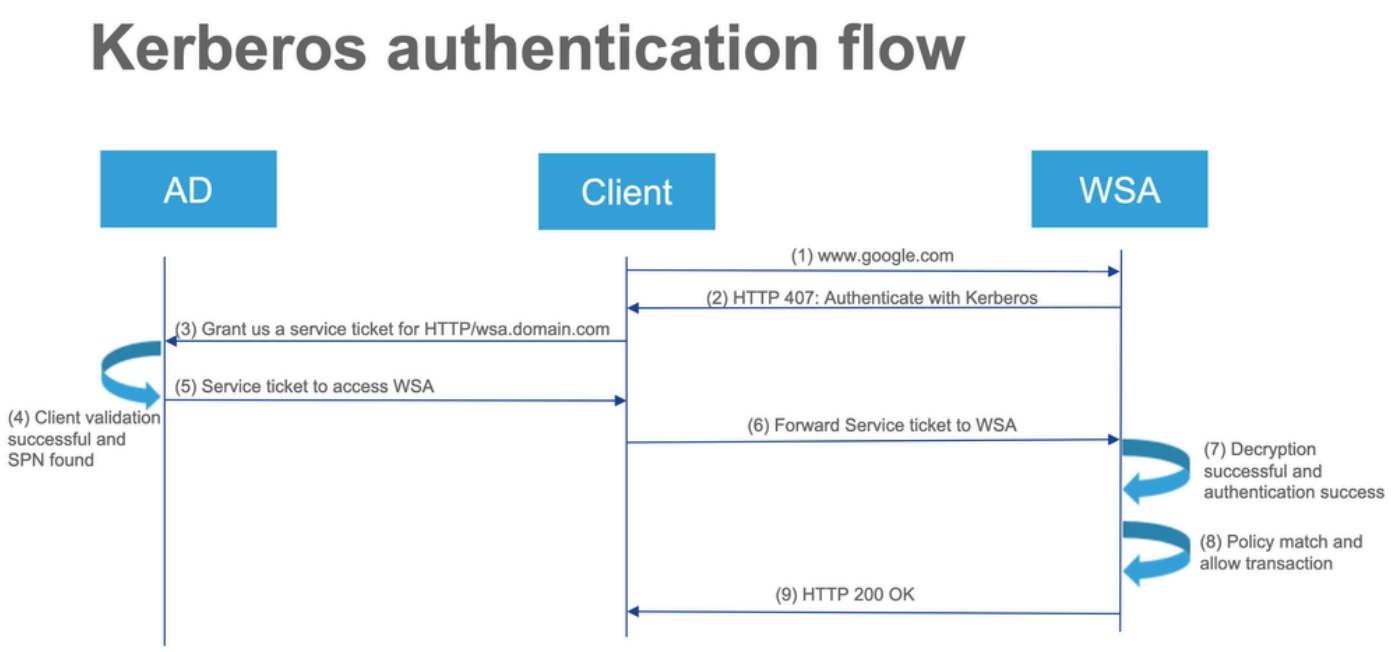
Hier zijn de basisstappen voor verificatie in een Kerberos-omgeving:

1. De klant vraagt een Ticket Granting Ticket (TGT) aan bij het Key Distribution Center (KDC).
2. De KDC verifieert de gebruikersreferenties van de client-machine en stuurt een versleutelde TGT- en sessiesleutel terug.
3. De TGT is versleuteld met de sleutel Ticket Granting Service (TGS).
4. De client slaat de TGT op en vraagt automatisch een nieuwe aan wanneer deze vervalt.

Voor toegang tot een service of bron:
1. De klant stuurt de TGT naar de TGS samen met de Service Principal Name (SPN) van de gewenste bron.
2. De KDC verifieert de TGT en controleert de toegangsrechten van de gebruikersclient.

3. De TGS stuurt een servicespecifieke sessiesleutel naar de client.
4. De klant biedt de sessiesleutel aan de dienst om toegang te bewijzen en de dienst verleent toegang.

Kerberos-verificatiestroom in SWA



1. De klant vraagt via de SWA toegang tot www.google.com.
2. De SWA reageert met een status "HTTP 407" en vraagt om verificatie.
3. De klant vraagt een servicekaartje aan bij de AD-server voor HTTP/SWA.domain.com-service met behulp van de TGT die het krijgt tijdens domeindeelname.
4. De AD-server valideert de client en geeft een servicekaartje af, indien geslaagd en de SPN (Service Principal Name) van SWA wordt gevonden, gaat het verder met de volgende stap.
5. De Klant stuurt dit ticket naar de SWA.
6. De SWA decrypteert het ticket en controleert de authenticatie.
7. Als de authentificatie succesvol is, verifieert de SWA beleid.
8. De SWA stuurt een reactie "HTTP 200/OK" naar de client als de transactie is toegestaan.

Wat is het doel van SPN?

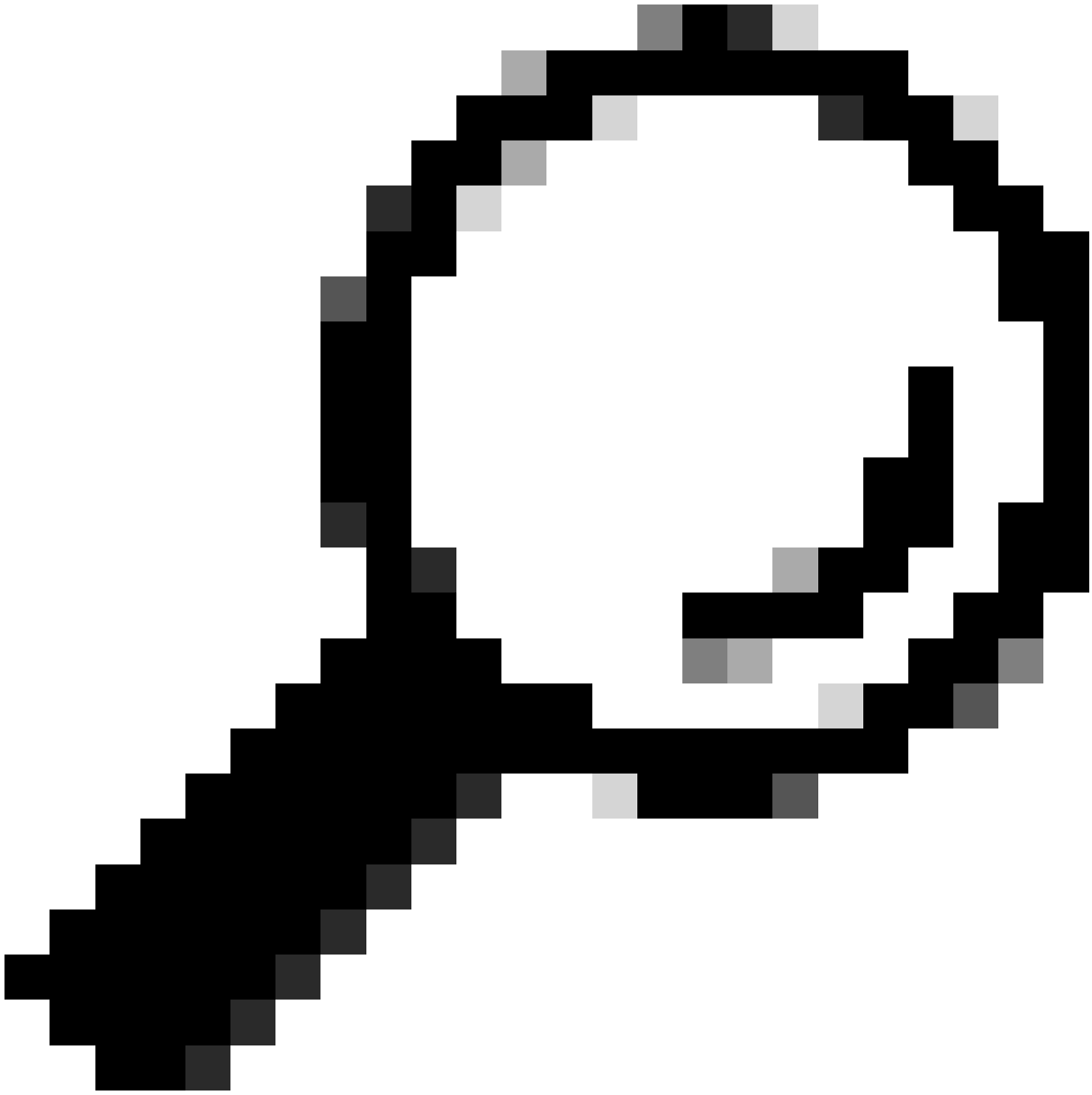
Een Service Principal Name (SPN) identificeert een unieke service instantie in Kerberos-verificatie. Het koppelt een service-instantie aan een service-account, zodat klanten om authenticatie voor de service kunnen vragen zonder de naam van de account te hoeven gebruiken. Elke account in een Key Distribution Center (KDC)-implementatie, zoals AD of Open LDAP, en heeft een SPN. Terwijl de SPN strikt een dienst identificeert, wordt het soms ten onrechte gebruikt om naar de cliëntnaam (UPN) te verwijzen in scenario's waar de dienst ook als een cliënt handelt.

In Kerberos identificeert een Service Principal Name (SPN) een unieke service-instantie binnen een netwerk. Hiermee kunnen clients verificatie aanvragen voor een specifieke service. De SPN koppelt de service-instantie naar zijn account, waardoor Kerberos toegangsaanvragen voor die service op de juiste manier kan authenticeren en autoriseren.

Configuratie van Active Directory-server

1. Maak een nieuwe gebruikersaccount of kies een bestaande gebruikersaccount voor gebruik.
2. Registreer de te gebruiken SPN tegen de gekozen gebruikersaccount.

3. Zorg ervoor dat er geen dubbele SPN's zijn geregistreerd.



Tip: Hoe is Kerberos met SWA achter lastverdeler of een Traffic Manager/Traffic Shaper anders? In plaats van de SPN voor HA Virtual hostname te koppelen aan een gebruikersaccount, koppelt u de SPN aan het HTTP-verkeersomleidingsapparaat (bijvoorbeeld: LoadBalancer of Traffic Manager) met een gebruikersaccount op de AD.

De beste praktijken voor het uitvoeren van Kerberos kunnen worden gevonden:

- Best practices voor Secure Web applicatie
- Firewallpoorten voor SWA-verbindingen configureren

Probleemoplossing

Problemen oplossen bij Kerberos met SPN-opdrachten

Hier is een lijst van nuttige setspan commando's voor het beheer van Service Principal Names (SPN's) in een Kerberos-omgeving Deze commando's worden uitgevoerd vanuit een opdrachtregel interface met beheerrechten in een Windows-omgeving.

SPN's voor een specifieke account weergeven:	setspan -L <User/ComputerAccountName> Toont een lijst met alle SPN's die voor de opgegeven account zijn geregistreerd.
Voeg een SPN toe aan een account:	setspan -A <SPN> <User/ComputerAccountName> Voegt de gespecificeerde SPN aan de bepaalde rekening toe.
Een SPN van een account verwijderen:	setspan -D <SPN> <User/ComputerAccountName> Verwijdert de gespecificeerde SPN uit de gegeven account.
Controleer of een SPN al is geregistreerd:	setspan -Q <SPN> Controleert of het opgegeven SPN al is geregistreerd in het domein.
Maak een lijst van alle SPN's in het domein	setspan -L <User/Computer-account> Een lijst van alle SPNs in het domein.
Stel een SPN in voor een computeraccount:	setspan -S <SPN> <User/ComputerAccountName> Voegt een SPN toe aan een computeraccount zonder dubbele vermeldingen.
Reset SPN's voor een specifieke account:	setspan -R <User/ComputerAccountName> Hiermee worden de SPN's voor de opgegeven account hersteld, zodat dubbele SPN-problemen kunnen worden opgelost.

Voorbeelden van SPN-opdrachten en -uitvoer

De verstrekte voorbeelden tonen het gebruik aan:

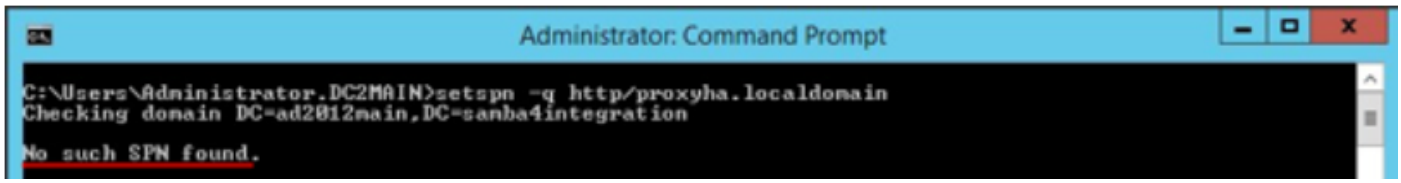
- Gebruikersaccount/computeraccount: vrpreservice-gebruiker

- SPN: http/WsaHostname.com of http/proxyha.localdomain

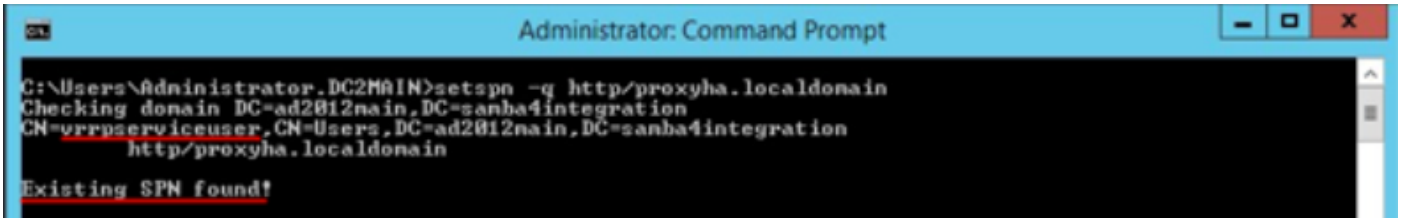
Controleer of SPN al is gekoppeld aan een gebruikersaccount:
setspan -q <SPN>

setspan -q http/proxyha.localdomain

Scenario 1: SPN niet gevonden



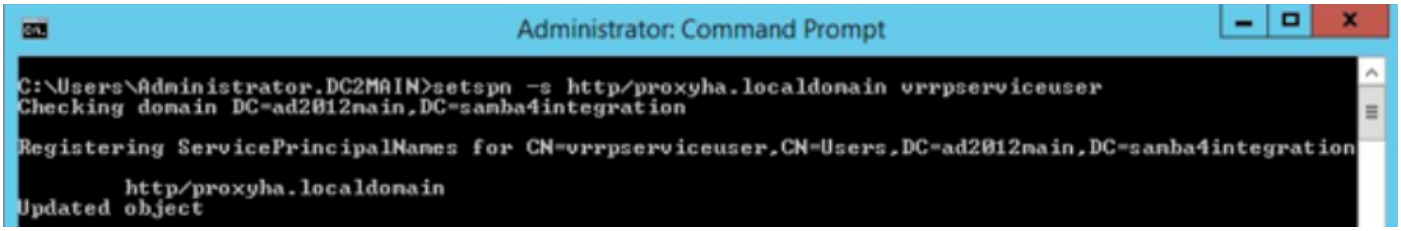
Scenario 2: SPN gevonden



- Koppel een SPN aan een geldig gebruikers-/computeraccount:

Syntaxis: setspan -s <SPN> <User/computer account>

Voorbeeld: setspan -s http/proxyha.localdomain



- Verwijdert/verwijdert een SPN dat al aan een gebruikers- of computeraccount is gekoppeld:

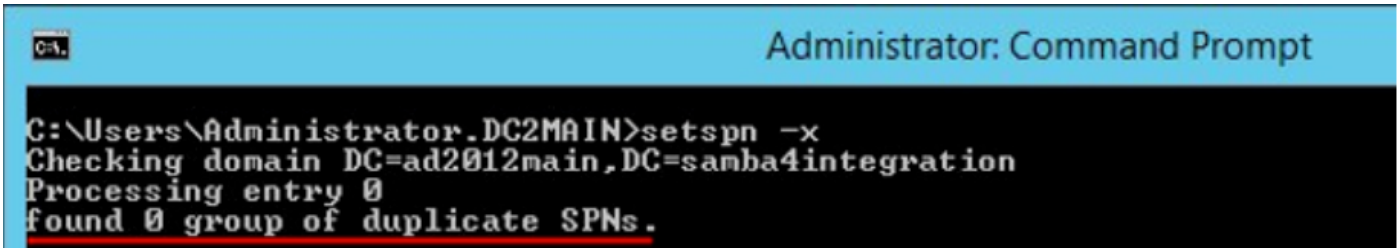
Syntaxis: setspan -d <SPN> <User/computer account>

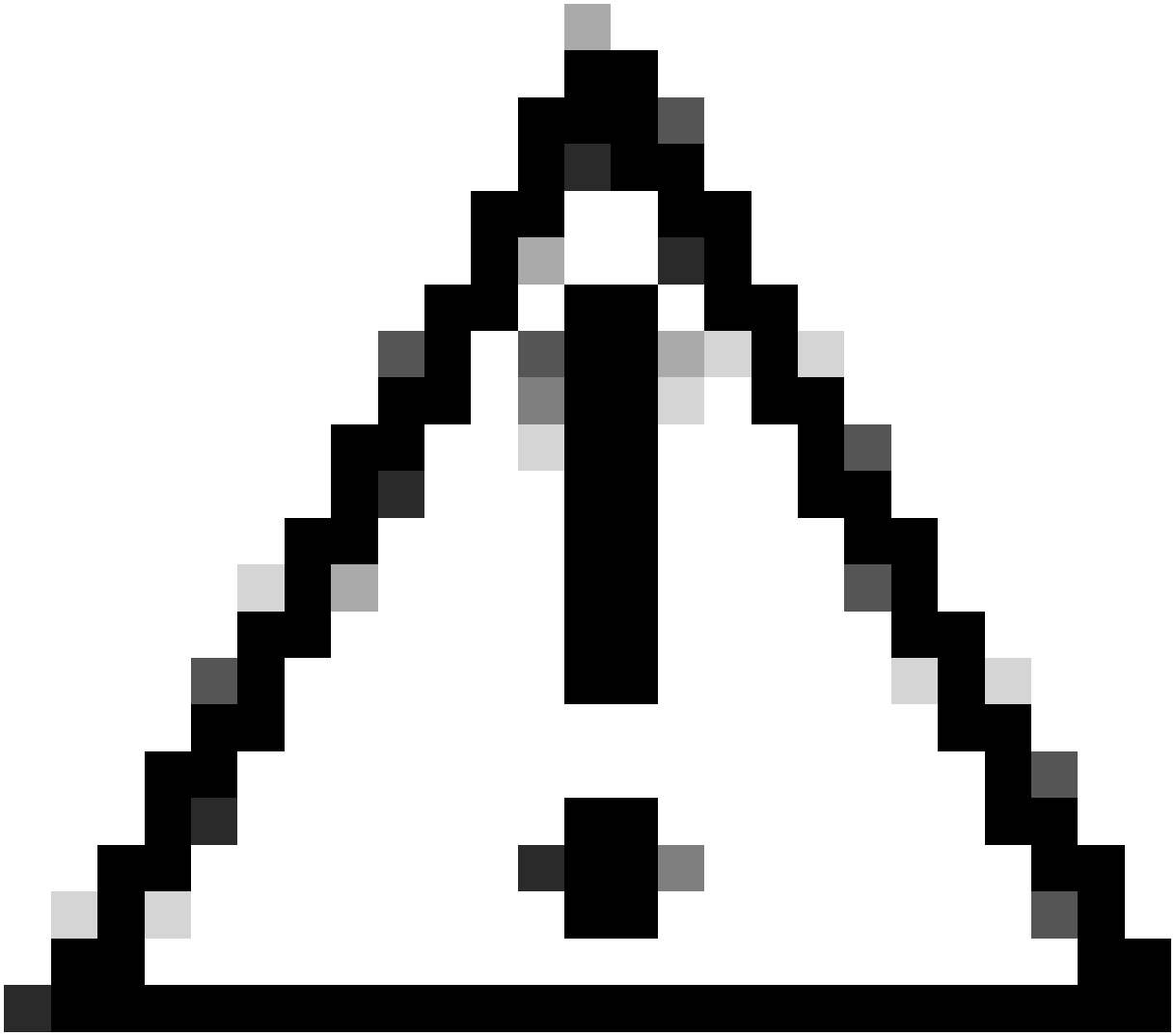
Voorbeeld: setspan -d http/proxyha.localdomain pod1234-wsa0

Zorg ervoor dat er geen dubbele SPN's zijn voor de HA virtuele hostname, aangezien fouten later kunnen optreden.

- Opdracht voor gebruik: setspan -x

Hierdoor wordt het Kerberos Service-ticket niet aan de client geleverd en mislukt de Kerberos-verificatie.



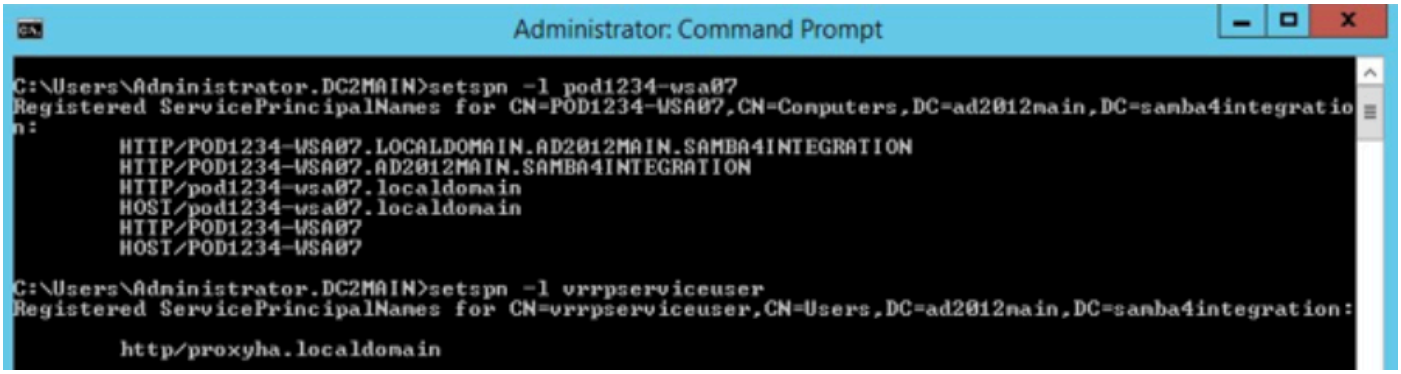


Voorzichtig: Als er duplicaten worden gevonden, verwijdert u deze met de opdracht setspan -d.

- Maak een lijst van alle SPN's die aan een account zijn gekoppeld:

Syntaxis: setspan -l <User/Computer-account>

Voorbeeld: setspan -l vrpserviceuser



Problemen met Kerberos op SWA oplossen

Informatie die Cisco-ondersteuning nodig heeft bij het oplossen van Kerberos-verificatieproblemen:

- Huidige configuratiedetails.
- Verificatielogboeken (bij voorkeur in de debug- of traceermodus).
- Opgenomen pakketopnamen (met geschikte filters):

  a) Clientapparaat

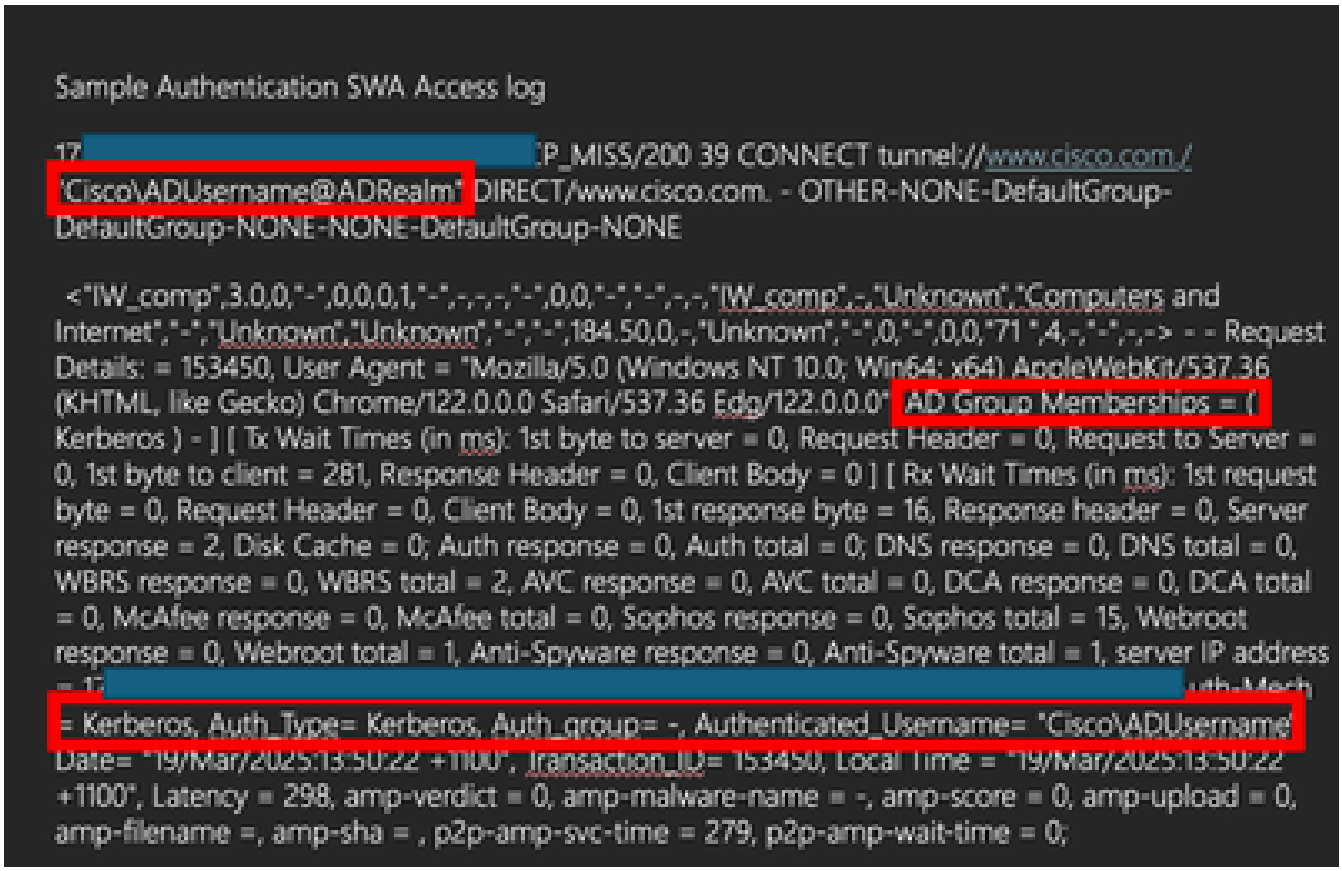
  b) SWA

- Toegangslogboeken met %m speciale indeling ingeschakeld. Dit moet het authenticatiemechanisme tonen dat voor een specifieke transactie is gebruikt.
- Voor gedetailleerde verificatiedetails kunt u deze aangepaste velden toevoegen aan de toegangslogboeken van werkende/niet-werkende proxy's om meer informatie te krijgen of te verwijzen naar hyperlink Parameter toevoegen in toegangslogboeken.
- In de SWA GUI, navigeer naar systeembeheer > Log abonnement > Access logs > Aangepaste velden > Deze tekenreeks toevoegen voor verificatieproblemen:

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

```
a;
```

- SWA-toegangslogboek voor informatie over gebruikersverificatie.
- Cisco SWA-records bevatten geverifieerde gebruikersnamen in de indeling Domain\username@authentication_realm:



- Voer de Verificatieregel-instellingen van de test uit vanuit de GUI. Navigeer naar Netwerk > Verificatie en klik vervolgens op de naam van uw domein in het gedeelte Huidige instellingen testen. Klik op Test starten.

Server niet gevonden in Kerberos Database

Een veel voorkomende fout case zijn webverzoeken die falen met "Server niet gevonden in Kerberos database":

```
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!
```

In dit geval geeft de fout aan dat de Service Principal Name die overeenkomt met de waarde proxyha.local van het proxyadres niet is geregistreerd op de Active Directory-server. Om het probleem op te lossen, moet worden bevestigd dat de SPN http/proxyha.local is geregistreerd op AD DC en wordt toegevoegd aan een juiste service account.

Aanvullende informatie en referenties

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.