Fehlerbehebung bei Kerberos-Authentifizierung in SWA

Inhalt

Einleitung

In diesem Dokument werden die Grundlagen der Kerberos-Authentifizierung und die Schritte zur Fehlerbehebung bei der Kerberos-Authentifizierung in einer sicheren Webappliance (SWA) beschrieben.

Terminologie

SWA	Sichere Web-Appliance
CLI	Kommandozeilenschnittstelle
ANZEIGE	Active Directory
RZ	Domänencontroller

SPN	Name des Dienstprinzipals
KDC	Kerberos-Schlüsselverteilungscenter
TGT	Authentifizierungs-Ticket (Ticket zur Kartenerteilung)
TTGS	Dienst für die Ticketgewährung
HA	Hohe Verfügbarkeit
VRRP	Virtual Router Redundancy Protocol
KARBE	Common Address Redundancy Protocol
SPN	Name des Dienstprinzipals
LSAP	Lightweight Directory Access Protocol

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Active Directory- und Kerberos-Authentifizierung.
- Authentifizierung und Realms auf SWA.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Kerberos - Netzwerkablauf

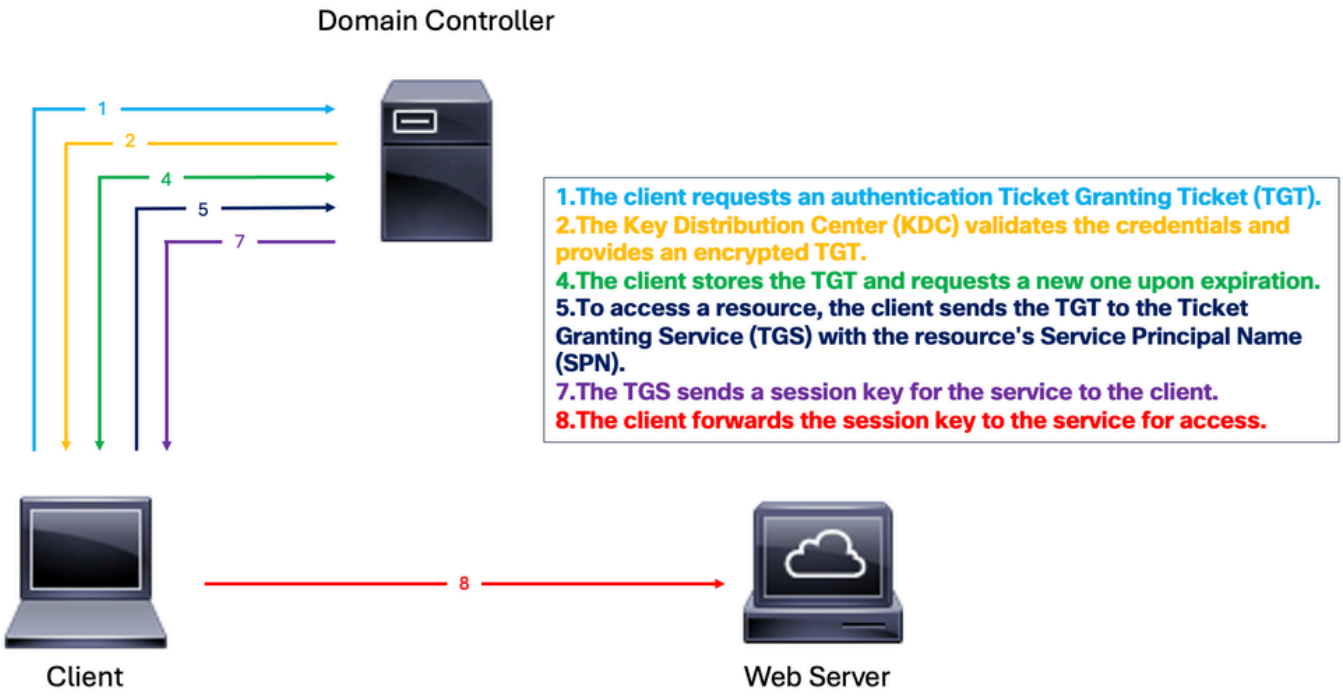


Bild: Kerberos-Beispielablauf

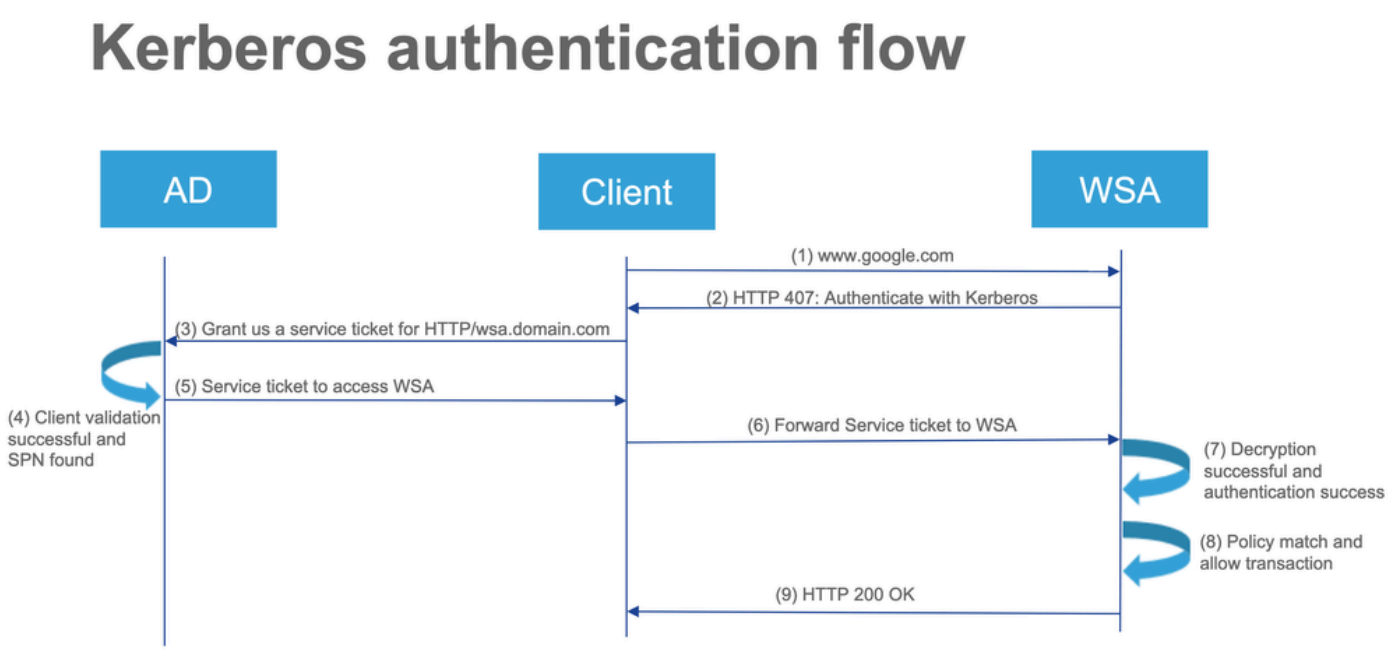
Im Folgenden werden die grundlegenden Schritte für die Authentifizierung in einer Kerberized-Umgebung beschrieben:

1. Der Kunde fordert ein Ticket Granting Ticket (TGT) vom Key Distribution Center (KDC) an.
2. Der KDC überprüft die Anmeldeinformationen des Client-Computerbenutzers und sendet ein verschlüsseltes TGT und einen Sitzungsschlüssel zurück.
3. Der TGT wird mit dem geheimen Schlüssel des Ticket Granting Service (TGS) verschlüsselt.
4. Der Client speichert das TGT und fordert automatisch ein neues an, wenn es abläuft.

Zugriff auf einen Dienst oder eine Ressource:
1. Der Client sendet das TGT zusammen mit dem Service Principal Name (SPN) der gewünschten Ressource an das TGS.
2. Der KDC überprüft das TGT und die Zugriffsrechte des Client-Systems des Benutzers.

3. Das TGS sendet einen dienstspezifischen Sitzungsschlüssel an den Client.
4. Der Client stellt den Sitzungsschlüssel für den Dienst bereit, um den Zugriff zu prüfen, und der Dienst gewährt den Zugriff.

Kerberos-Authentifizierungsablauf in SWA



1. Der Client fordert über die SWA Zugriff auf www.google.com an.
2. Der SWA antwortet mit einem "HTTP 407"-Status und bittet um Authentifizierung.
3. Der Client fordert vom AD-Server ein Dienstticket für den Dienst HTTP/SWA.domain.com mit dem TGT an, das er während des Domänenbeitritts erhält.
4. Der AD-Server validiert den Client und stellt ein Service-Ticket aus. Wenn dies erfolgreich ist und der SPN (Service Principal Name) von SWA gefunden wird, wird mit dem nächsten Schritt fortgefahren.
5. Der Kunde sendet dieses Ticket an die SWA.
6. Der SWA entschlüsselt das Ticket und überprüft die Authentifizierung.
7. Wenn die Authentifizierung erfolgreich ist, überprüft der SWA die Richtlinien.
8. Der SWA sendet eine "HTTP 200/OK"-Antwort an den Client, wenn die Transaktion zulässig ist.

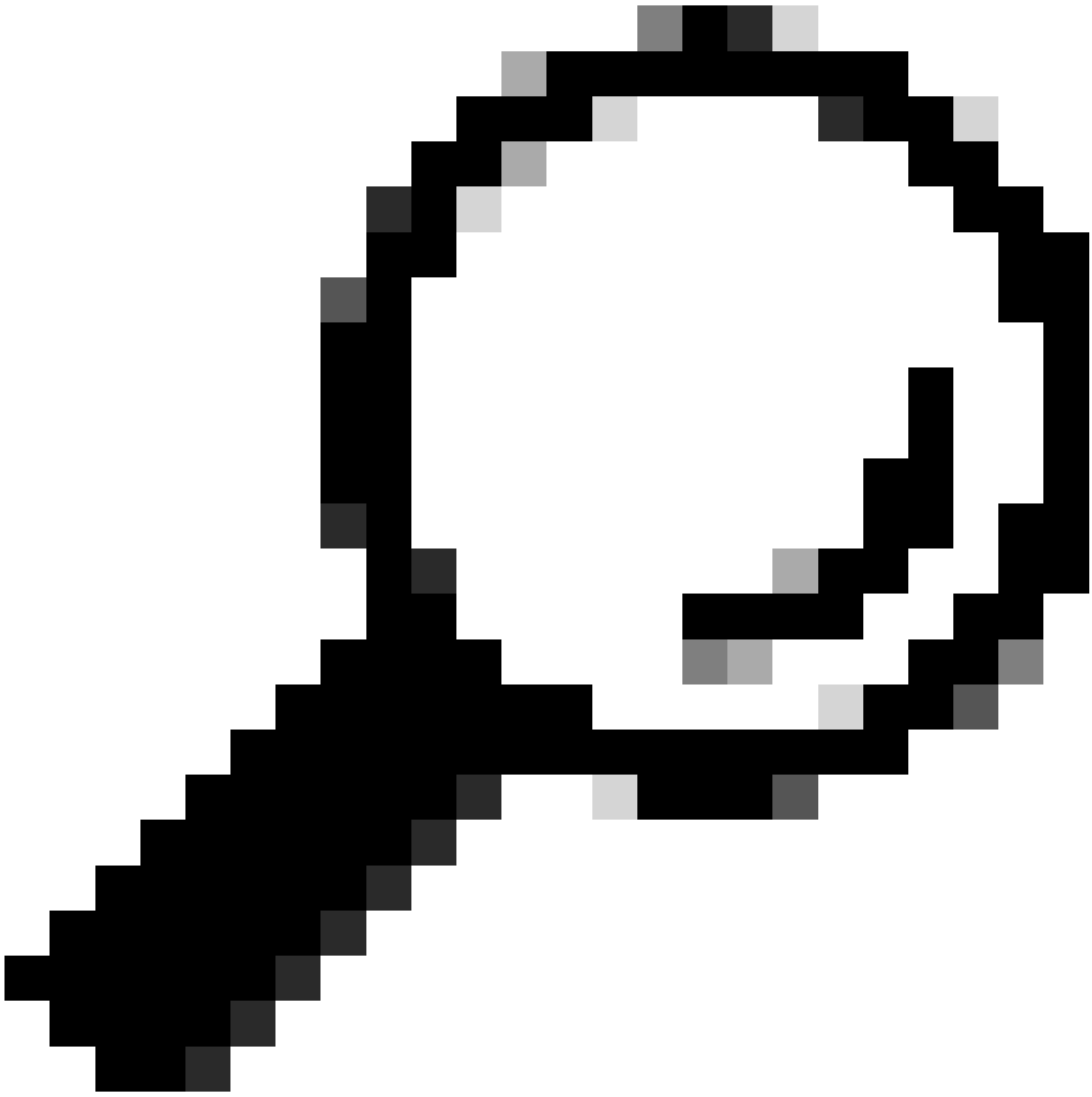
Wozu dient SPN?

Ein Dienstprinzipalname (SPN) identifiziert eine Dienstinstanz in der Kerberos-Authentifizierung eindeutig. Sie verknüpft eine Dienstinstanz mit einem Dienstkonto, sodass Clients die Authentifizierung für den Dienst anfordern können, ohne den Kontonamen zu benötigen. Jedes Konto in einer Key Distribution Center (KDC)-Implementierung, z. B. AD oder Open LDAP, verfügt über einen SPN. Während der SPN einen Service streng identifiziert, wird er manchmal fälschlicherweise verwendet, um in Szenarien, in denen der Service auch als Client agiert, auf den Client-Namen (UPN) zu verweisen.

In Kerberos identifiziert ein Service Principal Name (SPN) eine Serviceinstanz innerhalb eines Netzwerks eindeutig. Es ermöglicht Clients, die Authentifizierung für einen bestimmten Dienst anzufordern. Der SPN verknüpft die Dienstinstanz mit ihrem Konto, sodass Kerberos Zugriffsanforderungen für diesen Dienst ordnungsgemäß authentifizieren und autorisieren kann.

Konfiguration des Active Directory-Servers

1. Erstellen Sie ein neues Benutzerkonto, oder wählen Sie ein vorhandenes Benutzerkonto aus.
2. Registrieren Sie den SPN für das ausgewählte Benutzerkonto.
3. Stellen Sie sicher, dass keine doppelten SPNs registriert werden.



Tipp: Was ist bei Kerberos mit SWA hinter dem Load Balancer oder bei einem Traffic Manager/Traffic Shaper anders? Anstatt den SPN für den virtuellen HA-Hostnamen einem Benutzerkonto zuzuordnen, ordnen Sie den SPN für das HTTP-Datenverkehrsumleitungsgerät zu (z. B.: LoadBalancer oder Traffic Manager) mit einem Benutzerkonto auf dem AD.

Best Practices für die Implementierung von Kerberos finden Sie unter:

- Best Practices für sichere Web-Appliances

- Firewall-Ports für SWA-Verbindungen konfigurieren

Fehlerbehebung

Fehlerbehebung bei Kerberos mit SPN-Befehlen

Nachfolgend finden Sie eine Liste nützlicher setspn-Befehle zum Verwalten von Dienstprinzipalnamen (Service Principal Names, SPNs) in einer Kerberos-Umgebung. Diese Befehle werden in der Regel von einer Befehlszeilenschnittstelle mit Administratorberechtigungen in einer Windows-Umgebung ausgeführt.

Listen Sie SPNs für ein bestimmtes Konto auf:	setspn -L <Benutzer-/Computerkontoname> Führt alle SPNs auf, die für das angegebene Konto registriert wurden.
Hinzufügen einer SPN zu einem Konto:	setspn -A <SPN> <Benutzer-/Computerkontoname> Fügt die angegebene SPN dem angegebenen Konto hinzu.
SPN aus einem Konto löschen:	setspn -D <SPN> <Benutzer-/ComputerAccountName> Entfernt die angegebene SPN aus dem angegebenen Konto.
Überprüfen Sie, ob bereits ein SPN registriert wurde:	setspn -Q <SPN> Überprüft, ob der angegebene SPN bereits in der Domäne registriert ist.
Alle SPNs in der Domäne auflisten	setspn -L <Benutzer-/Computerkonto> Führt alle SPNs in der Domäne auf.
Legen Sie einen SPN für ein Computerkonto fest:	setspn -S <SPN> <Benutzer-/Computerkontoname> Fügt einem Computerkonto einen SPN hinzu, um sicherzustellen, dass keine doppelten Einträge vorhanden sind.
SPNs für ein bestimmtes Konto zurücksetzen:	setspn -R <Benutzer-/Computerkontoname> Setzt die SPNs für das angegebene Konto zurück und hilft, doppelte SPN-Probleme zu beheben.

Beispiele für SPN-Befehle und -Ausgaben

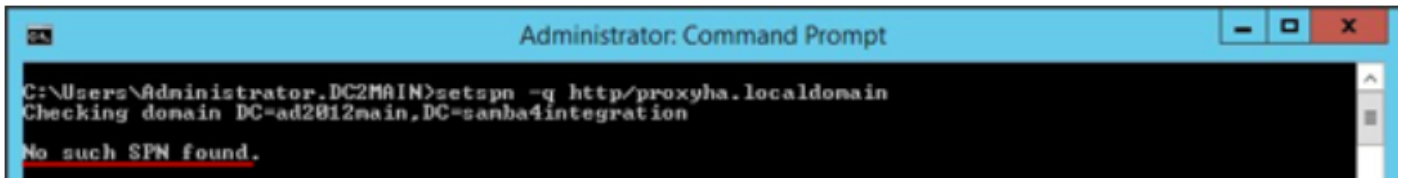
Die angegebenen Beispiele zeigen die Verwendung:

- Benutzer-/Computerkonto: vrrpserviceuser
- SPN: http/WsaHostname.com oder http/proxyha.localdomain

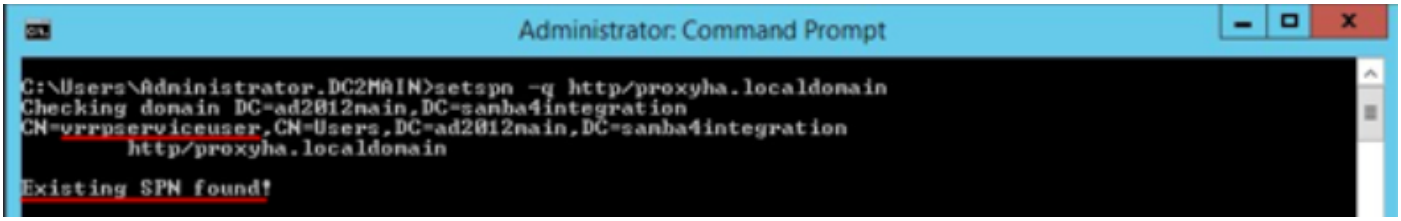
Überprüfen Sie, ob SPN bereits einem Benutzerkonto zugeordnet ist:
setspn -q <SPN>

setspn -q http/proxyha.localdomain

Szenario 1: SPN nicht gefunden



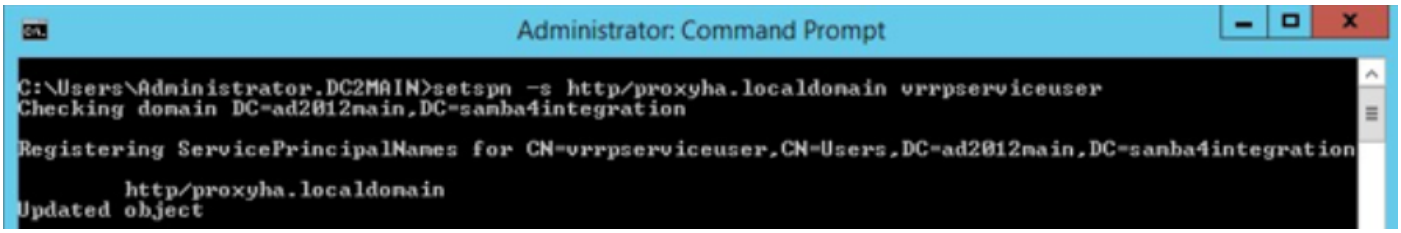
Szenario 2: SPN gefunden



- Ordnen Sie einen SPN einem gültigen Benutzer-/Computerkonto zu:

Syntax: setspn -s <SPN> <Benutzer-/Computerkonto>

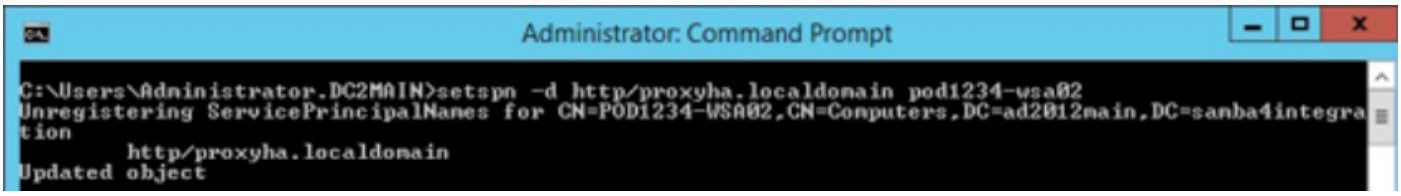
Beispiele: setspn -s http/proxyha.localdomain vrrpserviceuser



- Löschen/Entfernen eines SPN, der bereits mit einem Benutzer- oder Computerkonto verknüpft ist:

Syntax: setspn -d <SPN> <Benutzer-/Computerkonto>

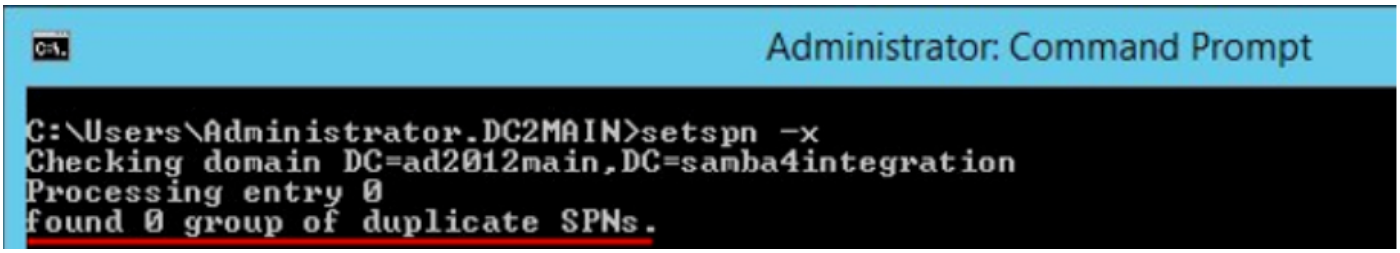
Beispiele: setspn -d http/proxyha.localdomain pod1234-wsa0



Stellen Sie sicher, dass keine doppelten SPNs für den virtuellen HA-Hostnamen vorhanden sind, da Fehler später auftreten können.

- Zu verwendender Befehl: setspn -x

Daher wird das Kerberos Service-Ticket dem Client nicht bereitgestellt, und die Kerberos-Authentifizierung schlägt fehl.

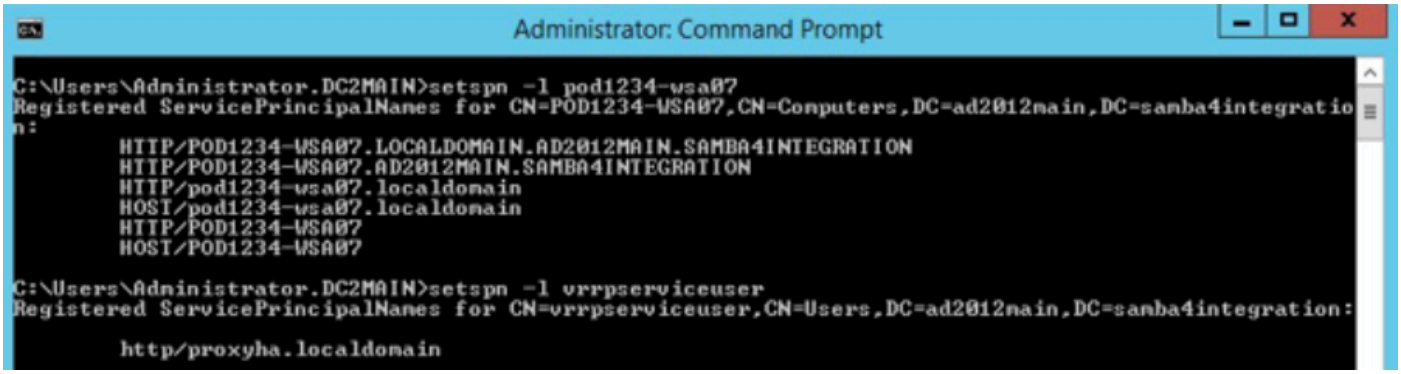


Vorsicht: Wenn Duplikate gefunden werden, entfernen Sie Duplikate mit dem Befehl setspn -d.

- Listen Sie alle SPNs auf, die einem Konto zugeordnet sind:

Syntax: setspn -l <Benutzer-/Computerkonto>

Beispiele: setspn -l vrpserviceuser



Fehlerbehebung bei Kerberos auf SWA

Informationen, die der Cisco Support zur Behebung von Kerberos-Authentifizierungsproblemen erhalten muss:

- Aktuelle Konfigurationsdetails.
- Authentifizierungsprotokolle (Vorzugsweise im Debug- oder Trace-Modus).
- Übernommene Paketerfassungen (mit geeigneten Filtern):

  a) Client-Gerät

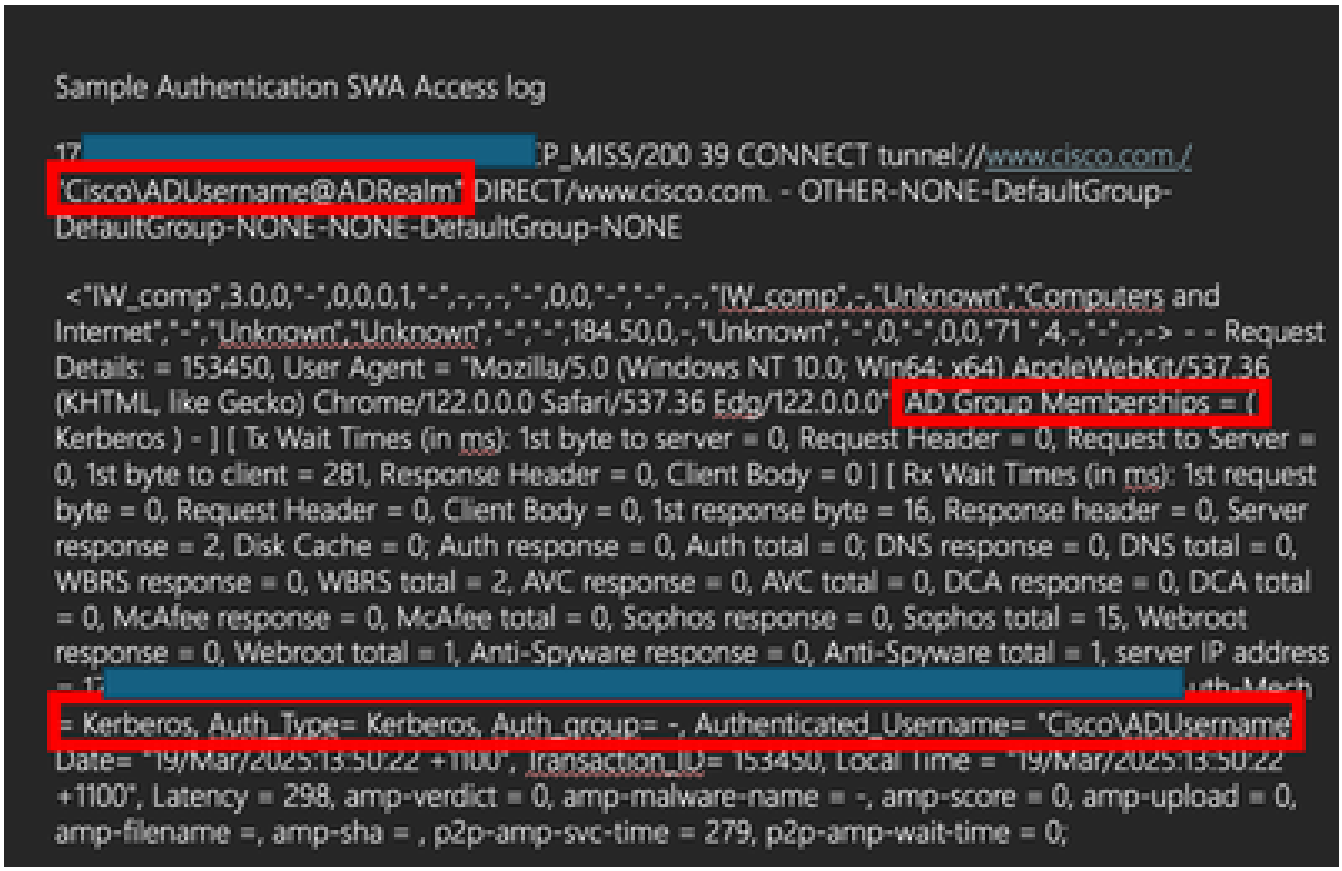
  b) SWA

- Zugriffsprotokolle mit %m aktivierter benutzerdefinierter Formatangabe. Dabei muss der Authentifizierungsmechanismus angezeigt werden, der für eine bestimmte Transaktion verwendet wurde.
- Für detaillierte Authentifizierungsdetails fügen Sie diese benutzerdefinierten Felder den Zugriffsprotokollen auf funktionierenden/nicht funktionierenden Proxys hinzu, um weitere Informationen zu erhalten, oder lesen Sie den Hyperlink Parameter in Zugriffsprotokollen hinzufügen.
- Navigieren Sie in der SWA-GUI zu Systemverwaltung > Protokoll-Abonnement > Zugriffsprotokolle > Benutzerdefinierte Felder > Diese Zeichenfolge für Authentifizierungsprobleme hinzufügen:

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

        a;
```

- SWA-Zugriffsprotokoll für Details zur Benutzerauthentifizierung.
- Cisco SWA zeichnet authentifizierte Benutzernamen im Format Domäne\username@authentication_realm auf:



- Führen Sie die Einstellungen für den Authentifizierungsbereich über die Benutzeroberfläche aus. Navigieren Sie zu Network > Authentication, und klicken Sie dann im Abschnitt Test Current Settings auf den Namen Ihres Realms. Klicken Sie auf Test starten.

Server nicht in Kerberos-Datenbank gefunden

Ein häufiger Fehlerfall sind Web-Anfragen, die mit "Server nicht in der Kerberos-Datenbank gefunden" fehlschlagen:

```
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 diesem Fall zeigt der Fehler an, dass der Dienstprinzipalname, der dem Proxyadressenwert proxyha.local entspricht, nicht auf dem Active Directory-Server registriert ist. Um das Problem zu beheben, muss überprüft werden, ob der SPN http/proxyha.local im AD DC registriert und einem entsprechenden Dienstkonto hinzugefügt wurde.

Weitere Informationen und Referenzen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.