Troubleshoot Kerberos Authentication in SWA

Contents

Introduction

Terminology

Prerequisites

- Requirements
- Components Used

Kerberos Network Flow

- Kerberos Authentication Flow in SWA
- What is the Purpose of SPN?
- Active Directory Server Configuration

Troubleshooting

- Troubleshooting Kerberos with SPN Commands
- Examples of SPN Commands and Output
  - Scenario 1: SPN Not Found
  - Scenario 2: SPN Found
- Troubleshooting Kerberos on SWA
- Server Not Found in Kerberos Database

Additional Information and References

Introduction

This document describes the basics of Kerberos Authentication and steps to troubleshoot Kerberos Authentication in Secure Web Appliance (SWA).

Terminology

SWA	Secure Web Appliance
CLI	Command Line Interface
AD	Active Directory
DC	Domain Controller
SPN	Service Principal Name
KDC	Kerberos Key Distribution Center

TGT	Authentication Ticket (Ticket Granting Ticket)
TGS	Ticket Granting Service
HA	High Availability
VRRP	Virtual Router Redundancy Protocol
CARP	Common Address Redundancy Protocol
SPN	Service Principal Name
LDAP	Lightweight Directory Access Protocol

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Active Directory and Kerberos Authentication.
- Authentication and realms on SWA.

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

Kerberos Network Flow

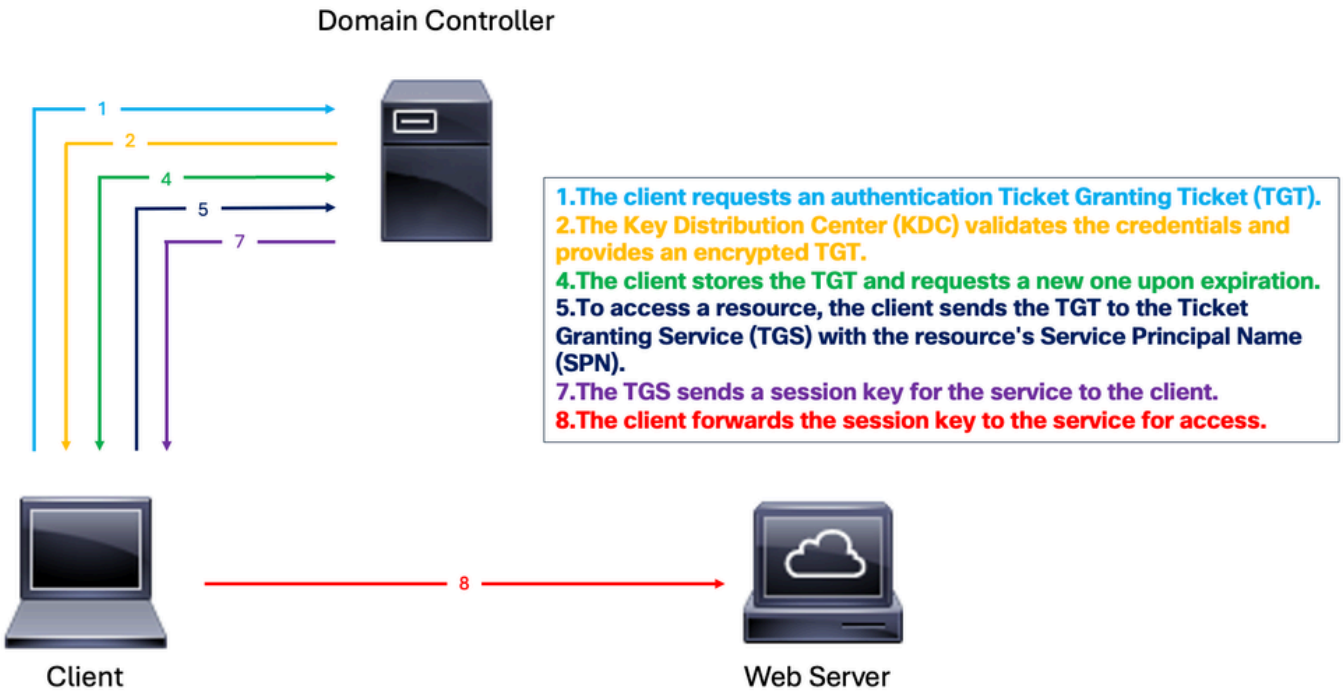


Image: Sample Kerberos Flow

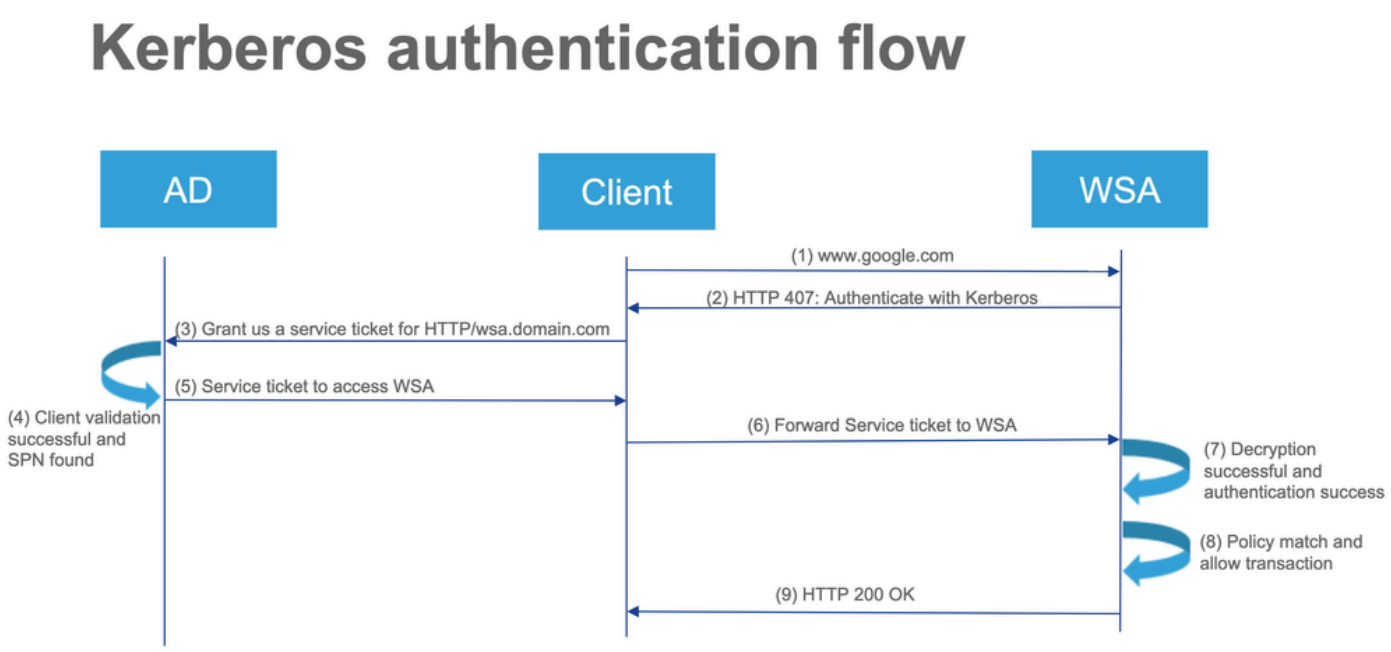
Here are the basic steps for authentication in a Kerberized environment:

1. The client requests a Ticket Granting Ticket (TGT) from the Key Distribution Center (KDC).
2. The KDC verifies the client machine user credentials and sends back an encrypted TGT and session key.
3. The TGT is encrypted with the Ticket Granting Service (TGS) secret key.
4. The client stores the TGT and automatically requests a new one when it expires.

For accessing a service or resource:
1. The client sends the TGT to the TGS along with the Service Principal Name (SPN) of the desired resource.
2. The KDC verifies the TGT and checks the user client machine access rights.

3. The TGS sends a service-specific session key to the client.
4. The client provides the session key to the service to prove access, and the service grants access.

Kerberos Authentication Flow in SWA



1. The Client requests access to www.google.com through the SWA.
2. The SWA responds with an "**HTTP 407**" status, asking for authentication.
3. The Client requests a service ticket from the AD server for **HTTP/SWA.domain.com** service using the TGT that it gets during domain joining.
4. The AD server validates the Client and issues a service ticket, if successful and the SPN (Service Principal Name) of SWA is found, it proceeds to the next step.
5. The Client sends this ticket to the SWA.
6. The SWA decrypts the ticket and checks authentication.
7. If authentication is successful, the SWA verifies policies.
8. The SWA sends an the "**HTTP 200/OK**" response to the client if the transaction is allowed.

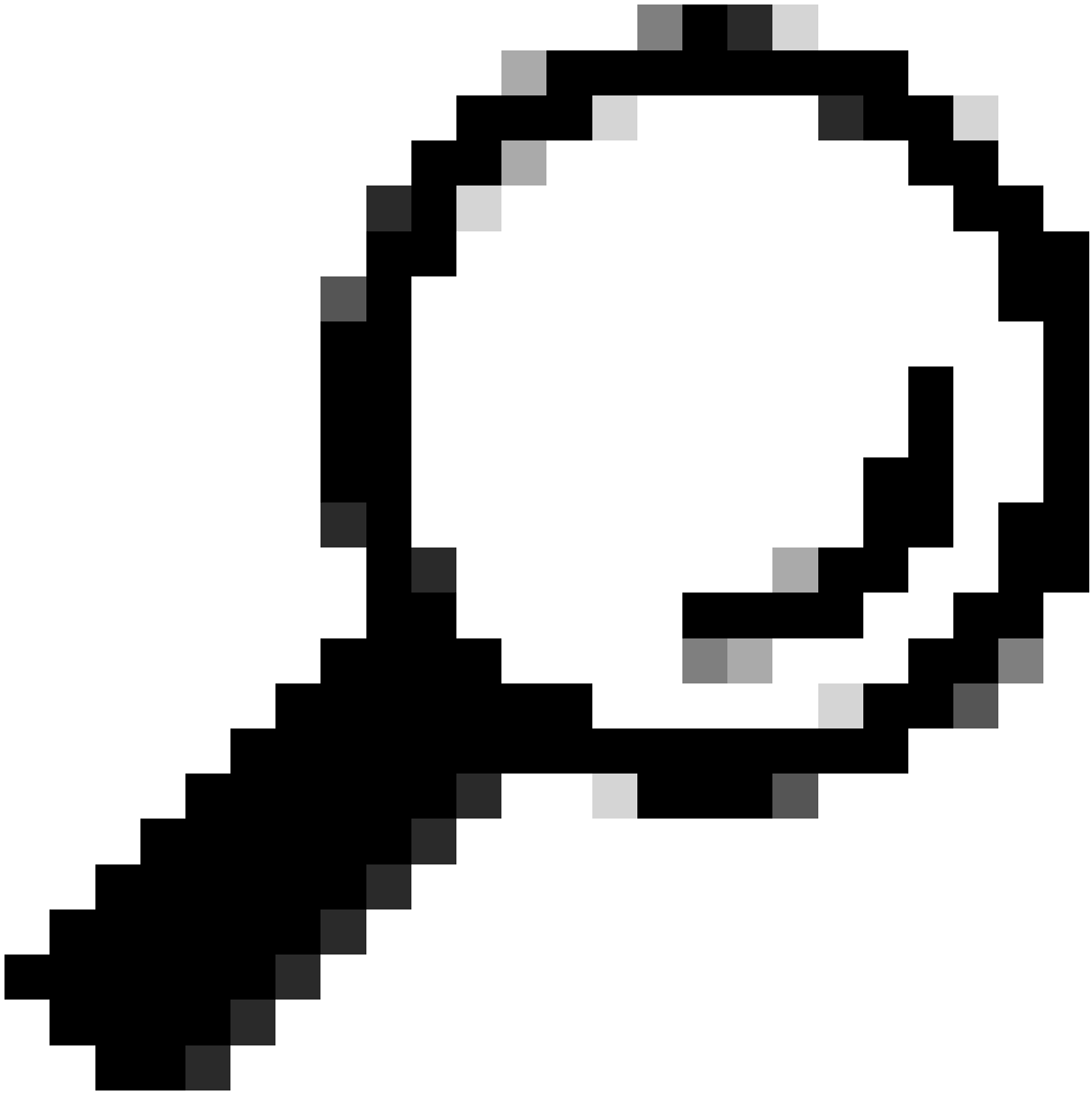
What is the Purpose of SPN?

A Service Principal Name (SPN) uniquely identifies a service instance in Kerberos authentication. It links a service instance to a service account, allowing clients to request authentication for the service without needing the account name. Each account in a Key Distribution Center (KDC) implementation, such as AD or Open LDAP, and has an SPN. While the SPN strictly identifies a service, it is sometimes mistakenly used to refer to the client name (UPN) in scenarios where the service also acts as a client.

In Kerberos, a Service Principal Name (SPN) uniquely identifies a service instance within a network. It allows clients to request authentication for a specific service. The SPN links the service instance to its account, enabling Kerberos to properly authenticate and authorize access requests to that service.

Active Directory Server Configuration

1. Create a new user account or choose an existing user account to use.
2. Register the SPN to be used against the chosen user account.
3. Ensure no duplicate SPNs are registered.



Tip: How is Kerberos with SWA behind load balancer or a Traffic Manager/Traffic Shaper different? Instead of associating the SPN for HA Virtual hostname with a user account, associate the SPN for the HTTP traffic redirection device (for example: LoadBalancer or Traffic Manager) with a user account on the AD.

Best Practices for implementing Kerberos can be found:

- Secure Web Appliance Best Practices
- Configure Firewall Ports For SWA Connections

Troubleshooting

Troubleshooting Kerberos with SPN Commands

Here is a list of useful **setspn** commands for managing Service Principal Names (SPNs) in a Kerberos

environment These commands are typically run from a command-line interface with administrative privileges in a Windows environment.

List SPNs for a specific account:	**setspn -L <User/ComputerAccountName>** Lists all SPNs registered for the specified account.
Add an SPN to an account:	**setspn -A <SPN> <User/ComputerAccountName>** Adds the specified SPN to the given account.
Delete an SPN from an account:	**setspn -D <SPN> <User/ComputerAccountName>** Removes the specified SPN from the given account.
Verify if an SPN is already registered:	**setspn -Q <SPN>** Checks if the specified SPN is already registered in the domain.
List all SPNs in the domain	**setspn -L <User/Computer account>** Lists all SPNs in the domain.
Set an SPN for a computer account:	**setspn -S <SPN> <User/CoumputerAccountName>** Adds an SPN to a computer account, ensuring no duplicate entries.
Reset SPNs for a specific account:	**setspn -R <User/CoumputerAccountName>** Resets the SPNs for the specified account, helping to resolve duplicate SPN issues.

Examples of SPN Commands and Output

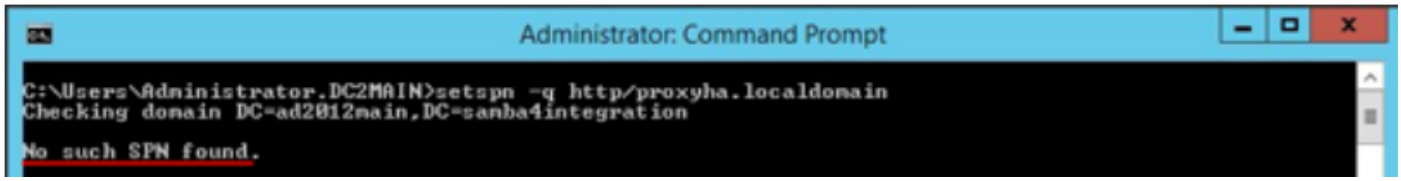
Examples provided demonstrate the use:

- **User/Computer Account: vrrpserviceuser**
- **SPN:** http/WsaHostname.com or http/proxyha.localdomain

Check if SPN is already associated with a user account:
setspn -q <SPN>

setspn -q http/proxyha.localdomain

Scenario 1: SPN Not Found

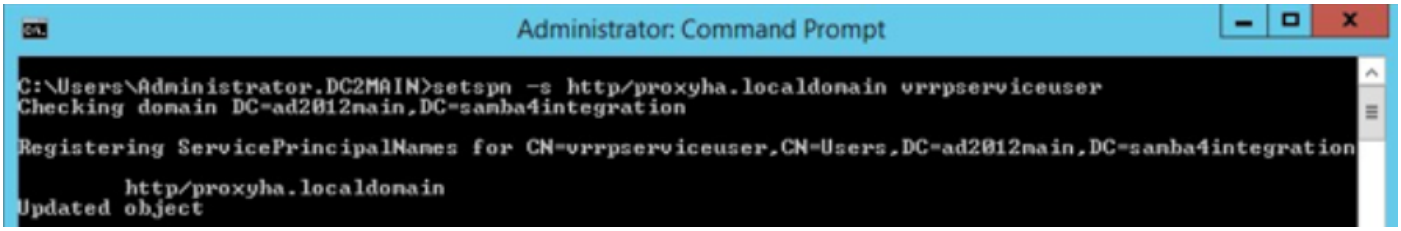


Scenario 2: SPN Found

- Associate an SPN with a valid user/computer account:

Syntax: **setspn -s <SPN> <User/computer account>**

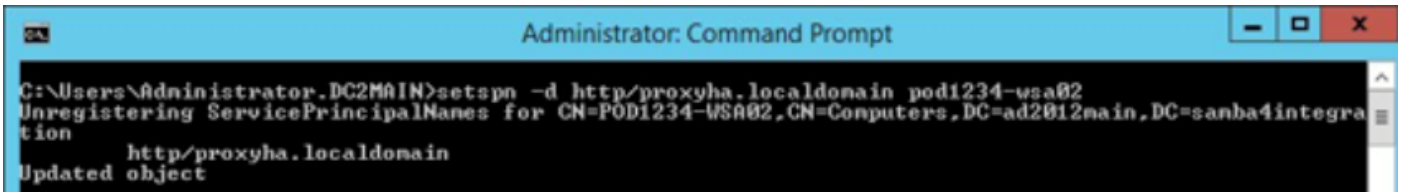
For example: **setspn -s http/proxyha.localdomain vrrpserviceuser**



- **Delete/Remove** an SPN that is already associated with a user or computer account:

Syntax: **setspn -d <SPN> <User/computer account>**

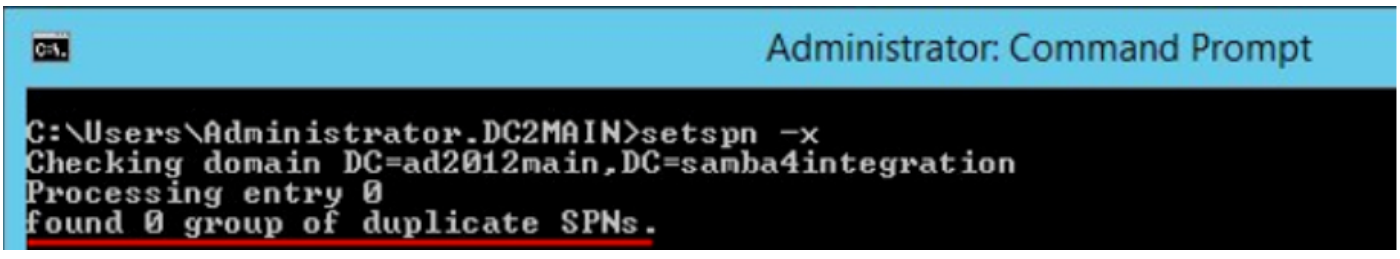
For example: **setspn -d http/proxyha.localdomain pod1234-wsa0**

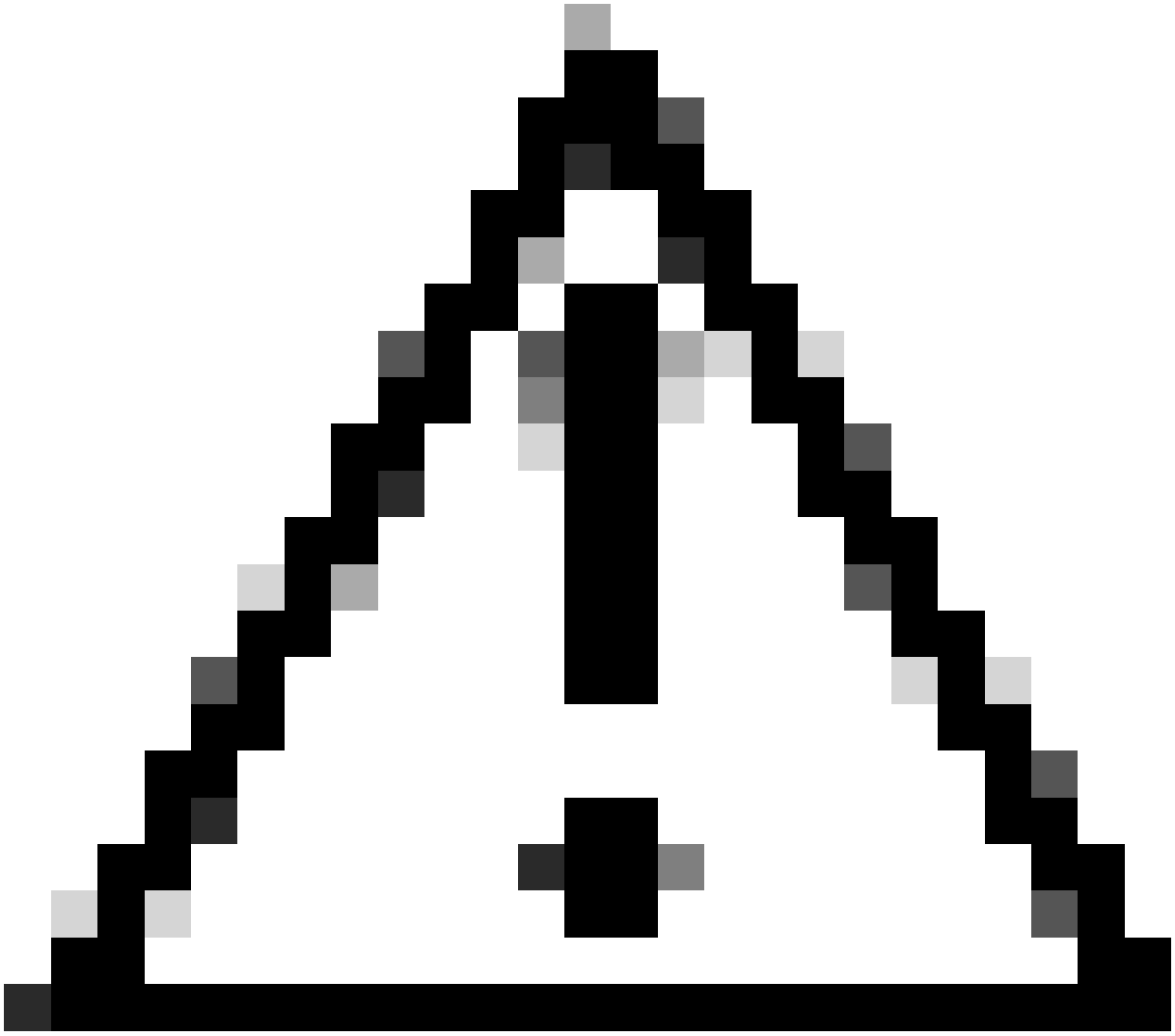


Ensure that there are no duplicate SPNs for the HA virtual hostname, as failures can occur later.

- Command to use: **setspn –x**

As a result, the Kerberos Service ticket is not provided to the client, and Kerberos authentication fails.



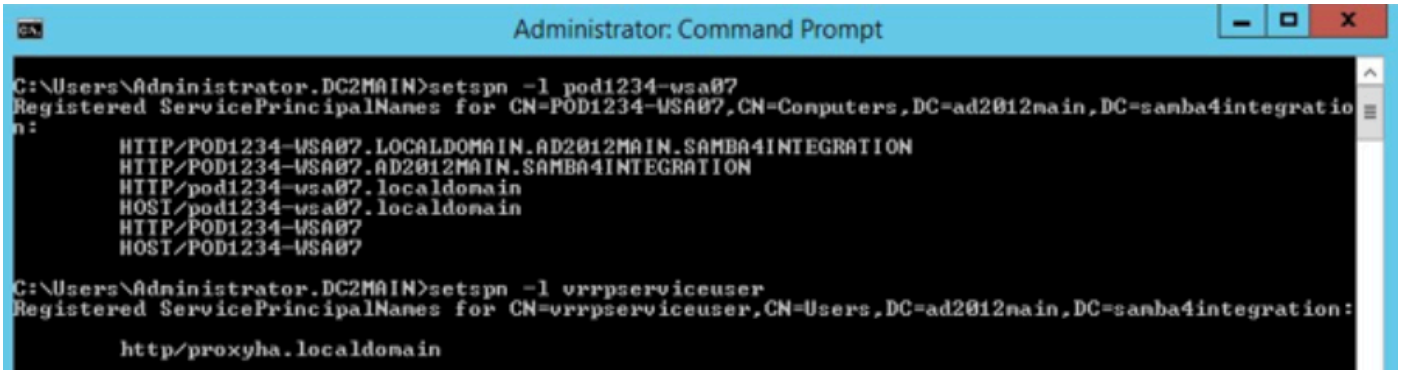


Caution: If duplicates are found, please remove duplicates using the **setspn –d** command.

- List all SPNs associated with an account:

Syntax: **setspn –l <User/Computer account>**

For example: **setspn –l vrrpserviceuser**



Troubleshooting Kerberos on SWA

Information Cisco Support needs to get when troubleshooting Kerberos authentication problems:

- Current configuration details.
- Authentication logs (Preferably in debug or trace mode).
- Packet captures taken on (with appropriate filters):

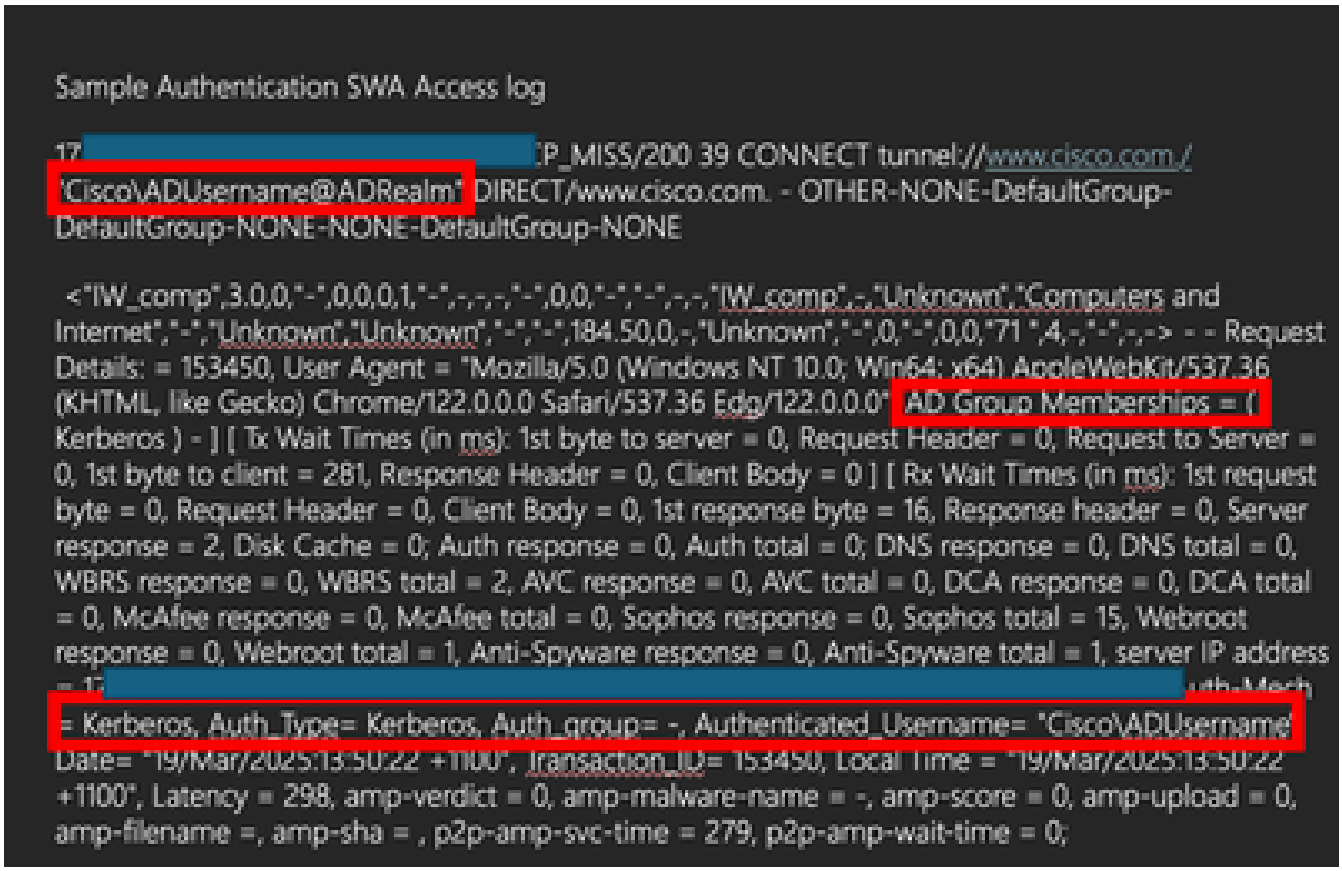
  (a) Client device

  (b) SWA

- Access logs with **%m** custom format specifier enabled. This must show the authentication mechanism that was used for a specific transaction.
- For detailed authentication details, add these custom fields to the access logs on working/non-working proxies to get more information or refer to hyperlink Adding Parameter in Access logs.
- In the SWA GUI, navigate to **System administration > Log subscription > Access logs > Custom fields > Add this string** for authentication issues:

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

- SWA access log for user authentication details.
- Cisco SWA records authenticated usernames in the format Domain\username@authentication_realm:



- Run **Test Authentication Realm Settings** from the GUI. Navigate to **Network > Authentication**, then click on the name of your Realm in the **Test Current Settings** section. Click **Start Test**.

Server Not Found in Kerberos Database

One common error case is web requests failing with “Server not found 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 this case, the error indicates that the Service Principal Name corresponding to proxy address value proxyha.local is not registered on Active Directory server. To resolve the problem, it would be necessary to confirm that the SPN http/proxyha.local is registered on AD DC and added to a proper service account.

Additional Information and References