Solucionar problemas de autenticación Kerberos en SWA

Contenido

- Introducción
- Terminology
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Flujo de red Kerberos
  - Flujo de autenticación Kerberos en SWA
  - ¿Cuál es el propósito de SPN?
  - Configuración del servidor de directorios activos
- Resolución de problemas
  - Solución de problemas de Kerberos con comandos SPN
  - Ejemplos de Salida y Comandos SPN
    - Escenario 1: SPN no encontrado
    - Escenario 2: SPN encontrado
  - Solución de problemas de Kerberos en SWA
  - No se encontró el servidor en la base de datos Kerberos
- Información adicional y referencias

Introducción

Este documento describe los fundamentos de la autenticación Kerberos y los pasos para resolver problemas de la autenticación Kerberos en el dispositivo web seguro (SWA).

Terminology

SWA	Dispositivo web seguro
CLI	Interfaz de la línea de comandos
ANUNCIO	Directorio activo
CC	Controlador de dominio

SPN	Nombre principal de servicio
KDC	Centro de distribución de claves Kerberos
TGT	Ticket de autenticación (Ticket Grant Ticket)
TGS	Servicio de concesión de entradas
HA	Alta disponibilidad
VRRP	Virtual Router Redundancy Protocol
CARPA	Protocolo de redundancia de dirección común
SPN	Nombre principal de servicio
LDAP	Protocolo ligero de acceso a directorios

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Active Directory y autenticación Kerberos.
- Autenticación y rangos en SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Flujo de red Kerberos

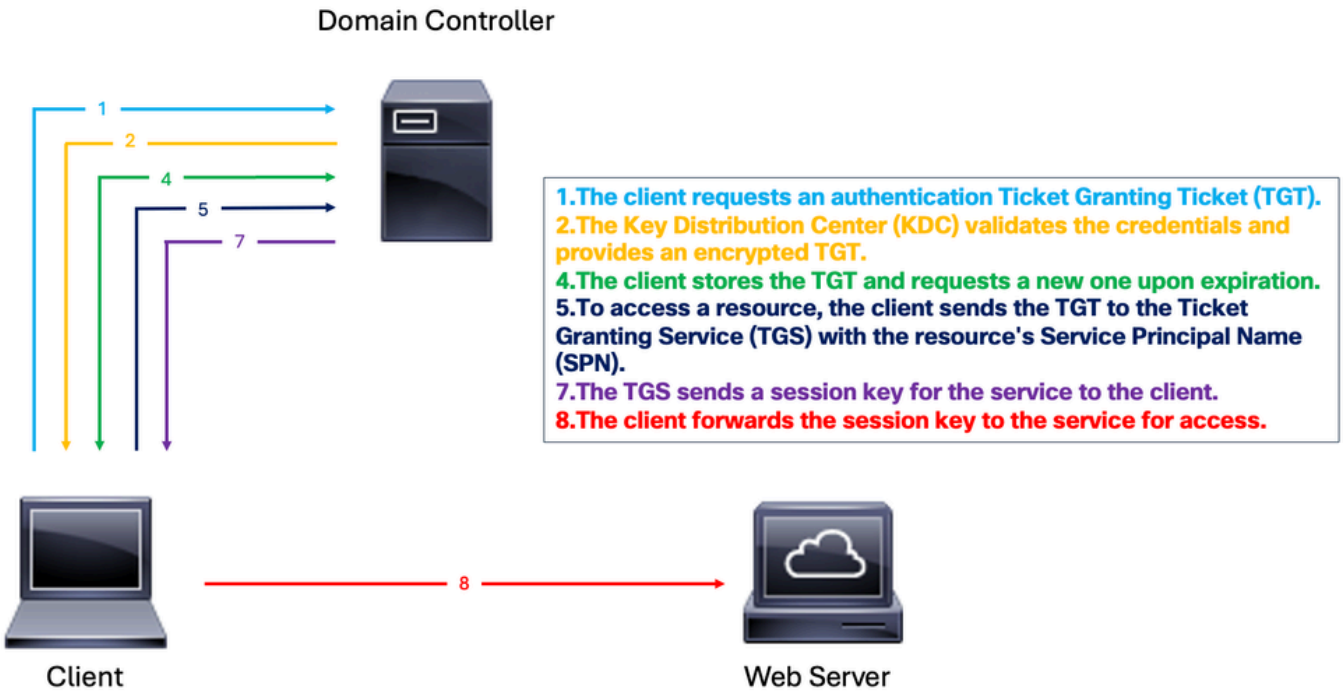


Imagen: Flujo de ejemplo de Kerberos

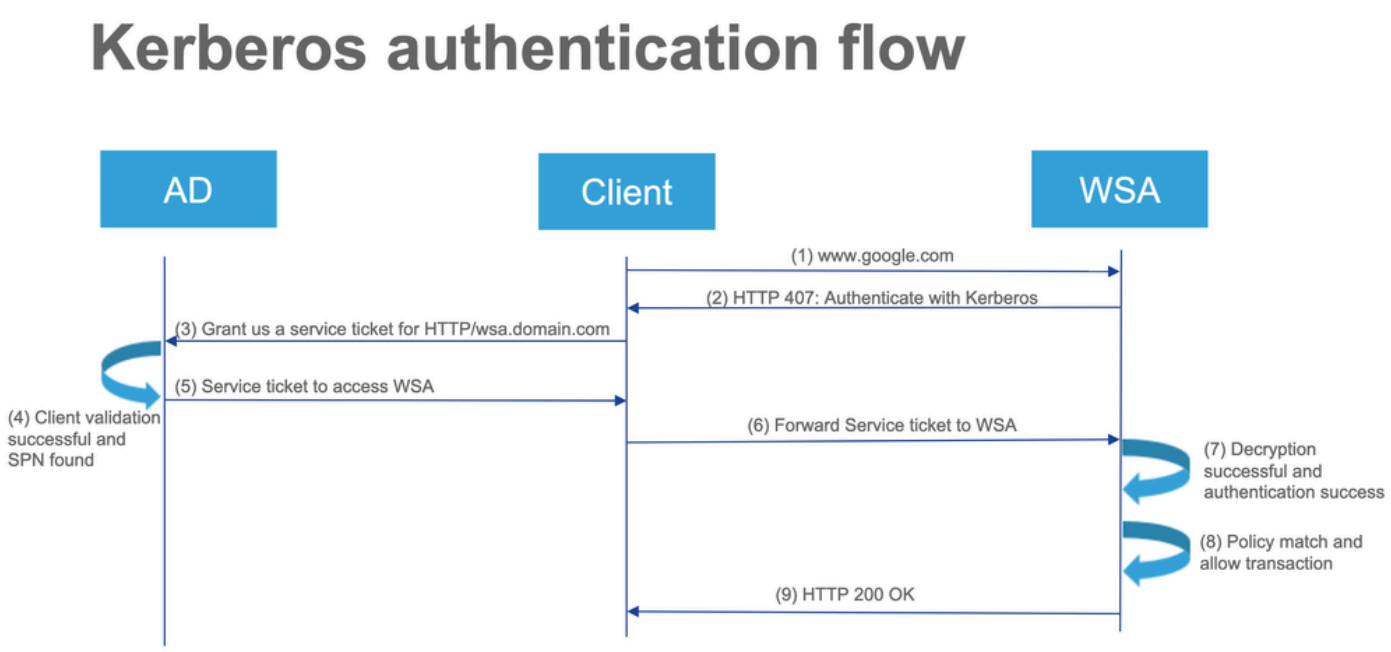
Estos son los pasos básicos para la autenticación en un entorno Kerberizado:

1. El cliente solicita un vale de concesión de vale (TGT) al centro de distribución de claves (KDC).
2. El KDC verifica las credenciales de usuario del equipo cliente y devuelve una TGT cifrada y una clave de sesión.
3. El TGT se cifra con la clave secreta TGS (del inglés Ticket Granting Service, servicio de concesión de notificaciones).
4. El cliente almacena la TGT y solicita automáticamente una nueva cuando caduca.

Para acceder a un servicio o recurso:
1. El cliente envía el TGT al TGS junto con el nombre principal de servicio (SPN) del recurso deseado.
2. El KDC verifica la TGT y verifica los derechos de acceso del equipo cliente del usuario.

3. El TGS envía una clave de sesión específica del servicio al cliente.
4. El cliente proporciona la clave de sesión al servicio para probar el acceso, y el servicio concede el acceso.

Flujo de autenticación Kerberos en SWA



1. El cliente solicita acceso a www.google.com a través de SWA.
2. El SWA responde con un estado "HTTP 407", solicitando autenticación.
3. El cliente solicita un vale de servicio del servidor AD para el servicio HTTP/SWA.domain.com mediante el TGT que obtiene durante la unión al dominio.
4. El servidor de AD valida al cliente y emite un vale de servicio; si se obtiene correctamente y se encuentra el SPN (nombre principal de servicio) de SWA, continúa con el siguiente paso.
5. El cliente envía este ticket al SWA.
6. El SWA descifra el ticket y verifica la autenticación.
7. Si la autenticación es satisfactoria, el SWA verifica las políticas.
8. El SWA envía una respuesta "HTTP 200/OK" al cliente si la transacción está permitida.

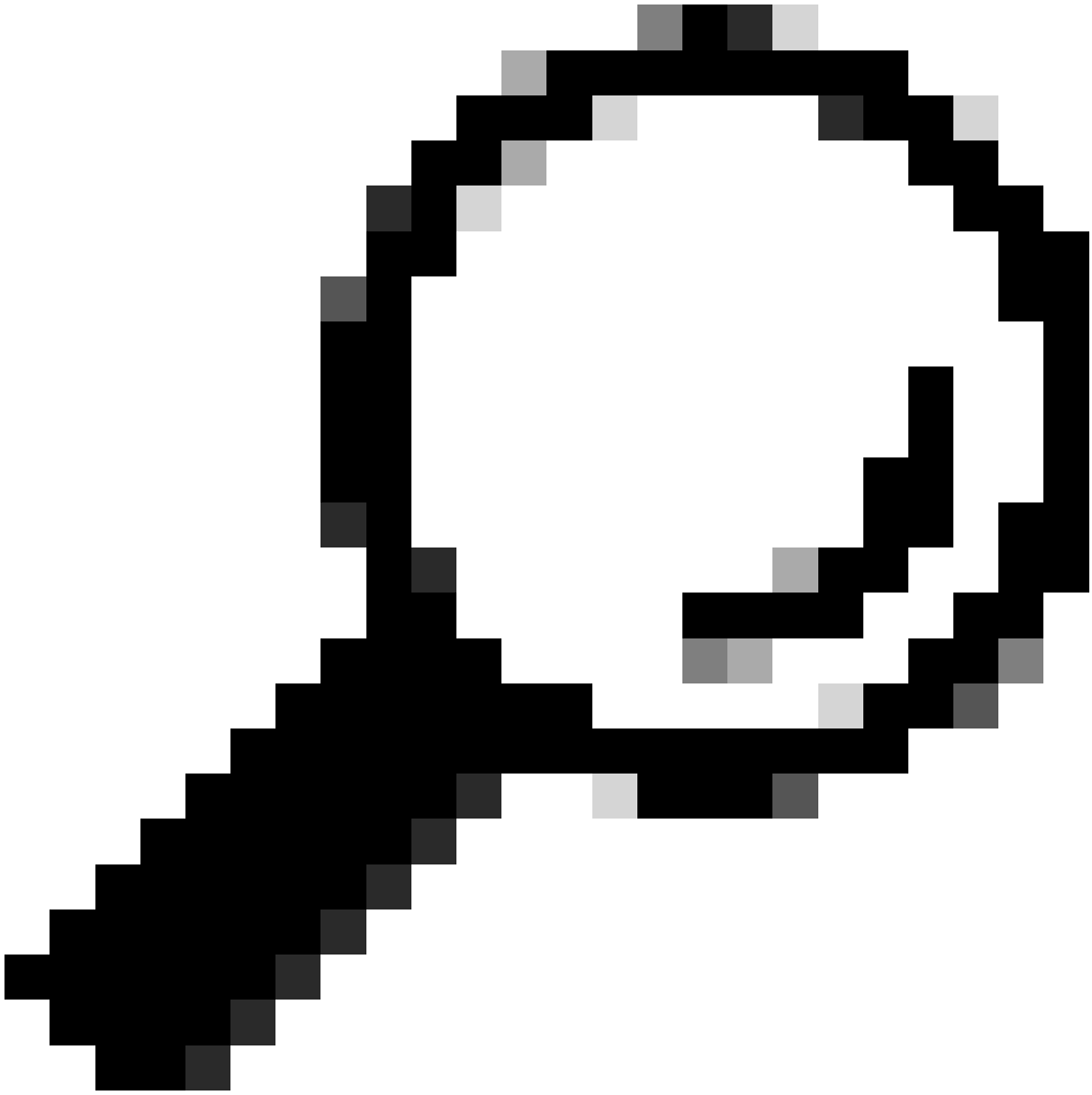
¿Cuál es el propósito de SPN?

Un nombre principal de servicio (SPN) identifica de forma única una instancia de servicio en la autenticación Kerberos. Vincula una instancia de servicio a una cuenta de servicio, lo que permite a los clientes solicitar autenticación para el servicio sin necesidad del nombre de cuenta. Cada cuenta de una implementación de Key Distribution Center (KDC), como AD o Open LDAP, y tiene un SPN. Aunque el SPN identifica estrictamente un servicio, a veces se utiliza erróneamente para referirse al nombre del cliente (UPN) en escenarios donde el servicio también actúa como cliente.

En Kerberos, un nombre principal de servicio (SPN) identifica de forma exclusiva una instancia de servicio dentro de una red. Permite a los clientes solicitar autenticación para un servicio específico. El SPN vincula la instancia de servicio a su cuenta, lo que permite a Kerberos autenticar y autorizar correctamente las solicitudes de acceso a ese servicio.

Configuración del servidor de directorios activos

1. Cree una nueva cuenta de usuario o elija una cuenta de usuario existente para utilizarla.
2. Registre el SPN que se utilizará con la cuenta de usuario seleccionada.
3. Asegúrese de que no se registren SPN duplicados.



Consejo: ¿En qué se diferencia Kerberos con SWA detrás del equilibrador de carga o un Traffic Manager/Traffic Shaper? En lugar de asociar el SPN para el nombre de host virtual de HA a una cuenta de usuario, asocie el SPN para el dispositivo de redirección de tráfico HTTP (por ejemplo: LoadBalancer o Traffic Manager) con una cuenta de usuario en AD.

Se pueden encontrar las mejores prácticas para implementar Kerberos:

- Prácticas recomendadas de Secure Web Appliance
- Configuración de puertos de firewall para conexiones SWA

Resolución de problemas

Solución de problemas de Kerberos con comandos SPN

Esta es una lista de comandos setspan útiles para administrar nombres principales de servicio (SPN) en un entorno Kerberos. Estos comandos se ejecutan normalmente desde una interfaz de línea de comandos con privilegios administrativos en un entorno Windows.

Lista de SPN para una cuenta específica:	setspan -L <User/ComputerAccountName> Enumera todos los SPN registrados para la cuenta especificada.
Agregar un SPN a una cuenta:	setspan -A <SPN> <User/ComputerAccountName> Agrega el SPN especificado a la cuenta dada.
Eliminar un SPN de una cuenta:	setspan -D <SPN> <User/ComputerAccountName> Quita el SPN especificado de la cuenta dada.
Verifique si ya se ha registrado un SPN:	setspan -Q <SPN> Comprueba si el SPN especificado ya está registrado en el dominio.
Lista de todos los SPN del dominio	setspan -L <Cuenta de usuario/equipo> Muestra todos los SPN del dominio.
Establecer un SPN para una cuenta de equipo:	setspan -S <SPN> <User/ComputerAccountName> Agrega un SPN a una cuenta de equipo y garantiza que no haya entradas duplicadas.
Restablecer SPN para una cuenta específica:	setspan -R <User/ComputerAccountName> Restablece los SPN para la cuenta especificada, lo que ayuda a resolver los problemas de SPN duplicados.

Ejemplos de Salida y Comandos SPN

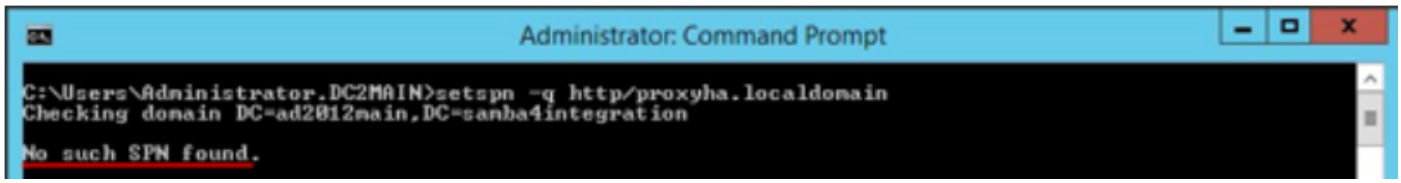
Los ejemplos proporcionados demuestran el uso:

- Cuenta de usuario/equipo: vrpserviceuser
- SPN: http/WsaHostname.com o http/proxyha.localdomain

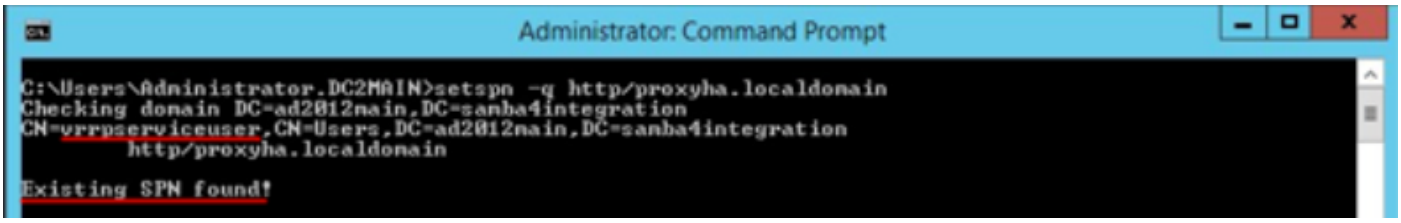
Compruebe si SPN ya está asociado a una cuenta de usuario:
setspan -q <SPN>

setspan -q http/proxyha.localdomain

Escenario 1: SPN no encontrado



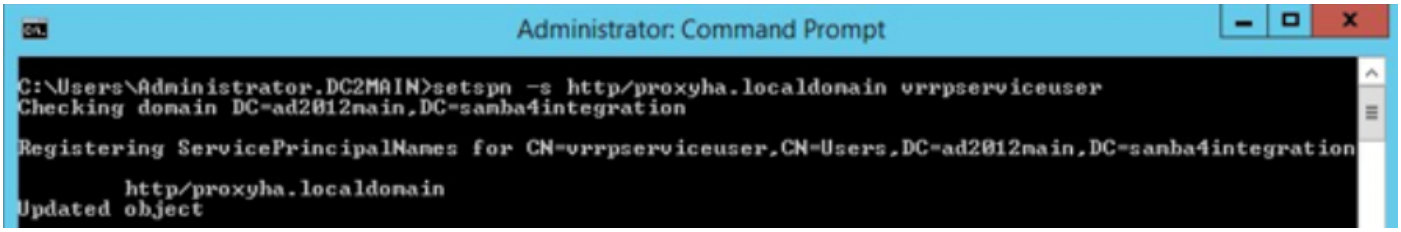
Escenario 2: SPN encontrado



- Asociar un SPN a una cuenta de usuario/equipo válida:

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

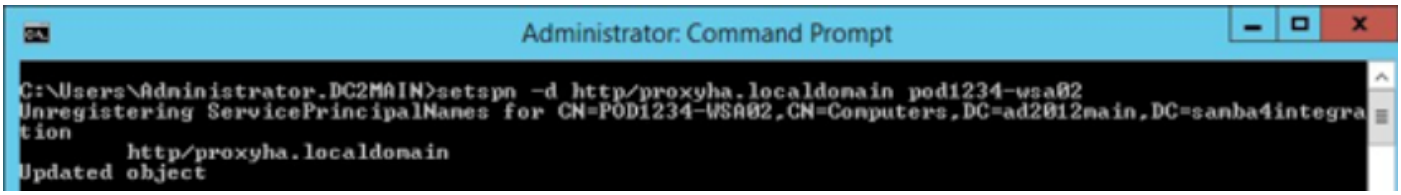
Por ejemplo: setspan -s http/proxyha.localdomain vrrpserviceuser



- Eliminar o quitar un SPN que ya está asociado a una cuenta de usuario o de equipo:

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

Por ejemplo: setspan -d http/proxyha.localdomain pod1234-wsa0

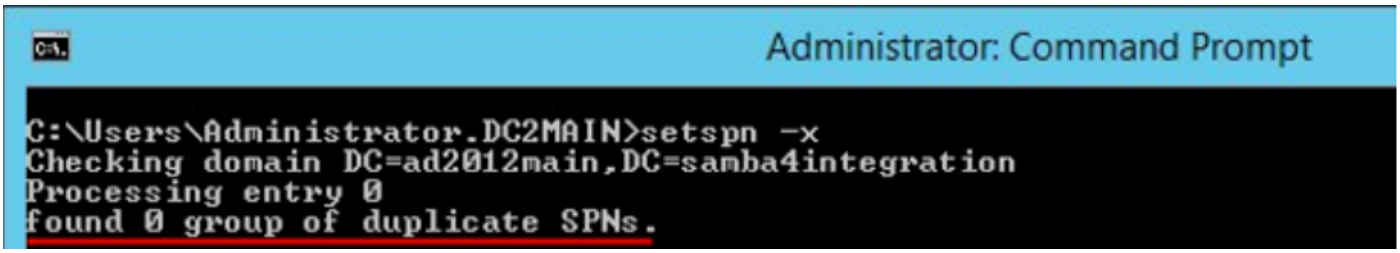


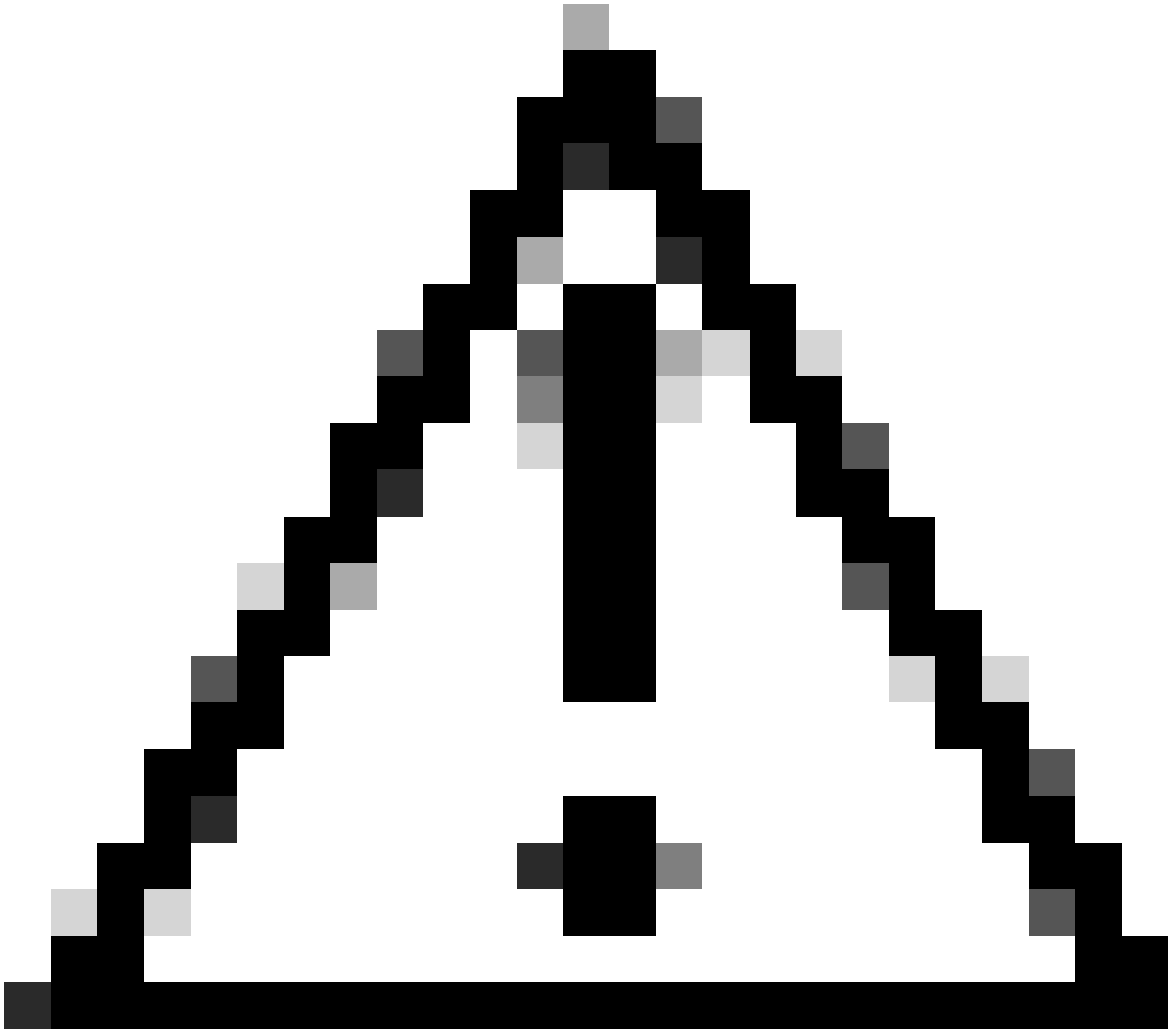
Asegúrese de que no haya SPN duplicados para el nombre de host virtual de HA, ya que las fallas pueden ocurrir más tarde.

- Comando a utilizar: setspan -x

Como resultado, el vale del servicio Kerberos no se proporciona al cliente y la autenticación

Kerberos falla.



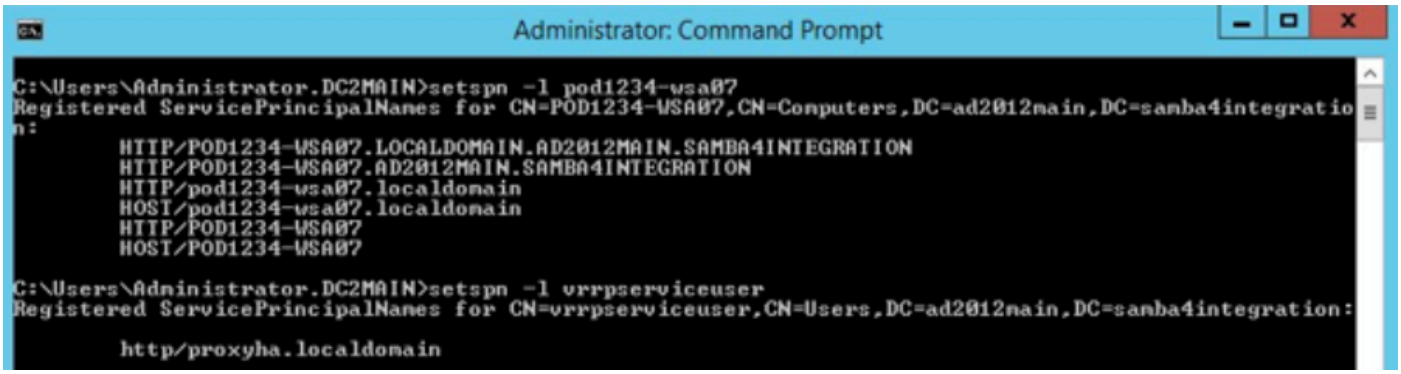


Precaución: Si se encuentran duplicados, elimine los duplicados mediante el comando setspan -d.

- Enumera todos los SPN asociados a una cuenta:

Sintaxis: setspan -l <Cuenta de usuario/equipo>

Por ejemplo: setspan -l vrrpserviceuser



Solución de problemas de Kerberos en SWA

Información que el Soporte Técnico de Cisco debe obtener al resolver problemas de autenticación Kerberos:

- Detalles de la configuración actual.
- Registros de autenticación (preferiblemente en modo de depuración o seguimiento).
- Capturas de paquetes realizadas (con los filtros adecuados):

  (a) Dispositivo cliente

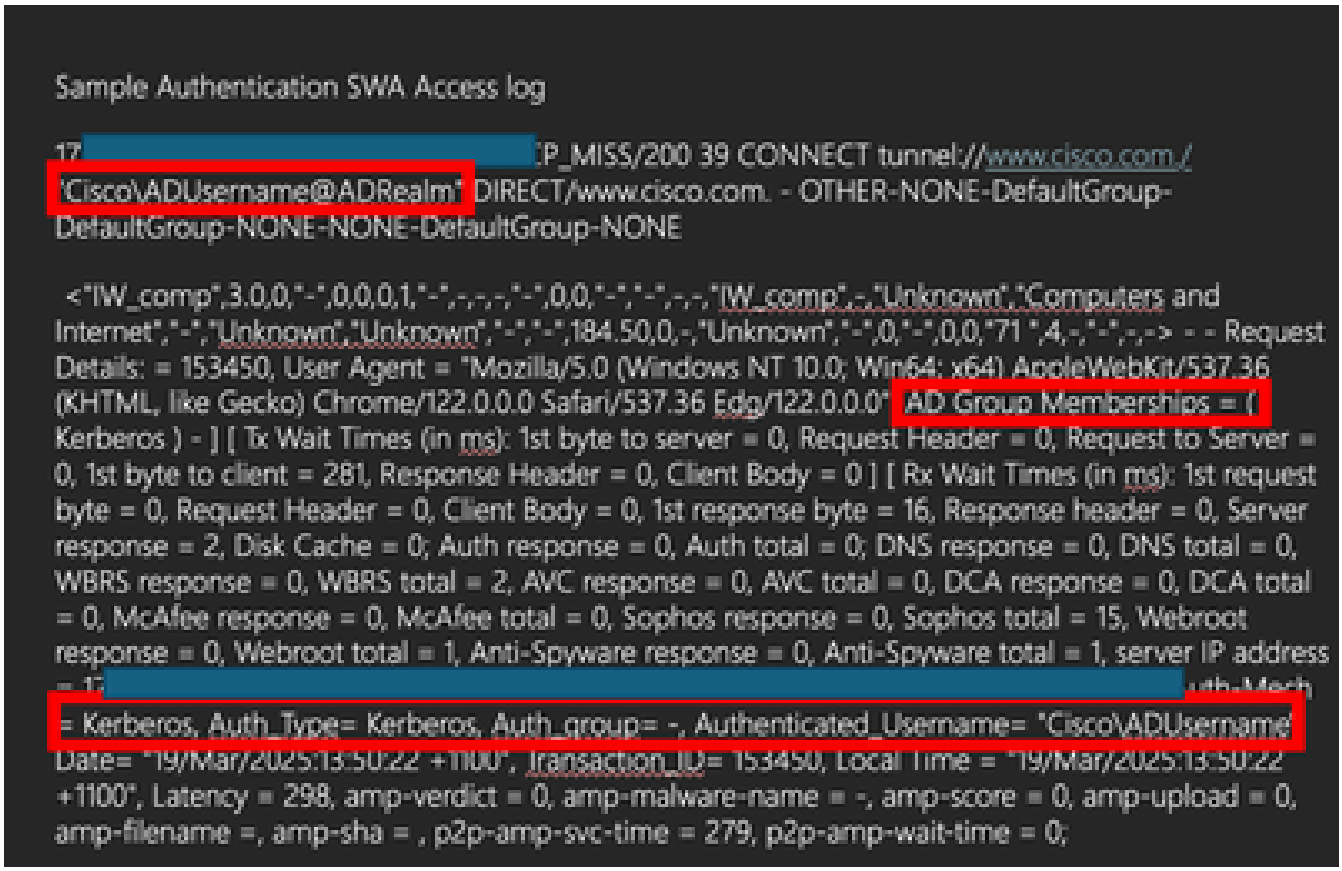
  (b) SWA

- Registros de acceso con el especificador de formato personalizado %m habilitado. Debe mostrar el mecanismo de autenticación que se utilizó para una transacción específica.
- Para obtener detalles de autenticación detallados, agregue estos campos personalizados a los registros de acceso de los proxies que funcionan/no funcionan para obtener más información o consulte el hipervínculo Agregar parámetro en los registros de acceso.
- En la GUI de SWA, navegue hasta Administración del sistema > Suscripción de registro > Registros de acceso > Campos personalizados > Agregar esta cadena para problemas de autenticación:

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

        a;
```

- Registro de acceso SWA para los detalles de autenticación de usuario.
- Cisco SWA registra los nombres de usuario autenticados con el formato Dominio\username@authentication_realm:



- Ejecute Test Authentication Realm Settings desde la GUI. Navegue hasta Network > Authentication, luego haga clic en el nombre de su rango en la sección Test Current Settings. Haga clic en Iniciar prueba.

No se encontró el servidor en la base de datos Kerberos

Un caso de error común es que las solicitudes web fallan con "Servidor no encontrado en la base de datos Kerberos":

```
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!
```

En este caso, el error indica que el nombre principal de servicio correspondiente al valor de la dirección proxy proxyha.local no está registrado en el servidor de Active Directory. Para resolver el problema, sería necesario confirmar que el SPN http/proxyha.local está registrado en AD DC y agregado a una cuenta de servicio adecuada.

Información adicional y referencias

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).