Solucionar problemas de autenticação Kerberos em SWA

Contents

- Introdução
- Terminologia
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Fluxo de rede Kerberos
  - Fluxo de autenticação Kerberos em SWA
  - Qual é a finalidade do SPN?
  - Configuração do Servidor do Ative Diretory
- Troubleshooting
  - Troubleshooting de Kerberos com Comandos SPN
  - Exemplos de comandos SPN e saída
    - Cenário 1: SPN Não Encontrado
    - Cenário 2: SPN Encontrado
  - Troubleshooting de Kerberos em SWA
  - Servidor não encontrado no banco de dados Kerberos
- Informações adicionais e referências

Introdução

Este documento descreve os conceitos básicos da Autenticação Kerberos e as etapas para solucionar problemas da Autenticação Kerberos no Secure Web Appliance (SWA).

Terminologia

SWA	Dispositivo da Web seguro
CLI	Interface da linha de comando
ANÚNCIO	Diretório ativo
DC	Controlador de domínio

SPN	Nome da Entidade de Serviço
KDC	Centro de Distribuição de Chaves Kerberos
TGT	Tíquete de autenticação (Tíquete de concessão de tíquete)
TGS	Serviço de concessão de tíquete
HA	Alta Disponibilidade
VRRP	Virtual Router Redundancy Protocol (Protocolo de redundância de roteador virtual)
CARPA	Common Address Redundancy Protocol (Protocolo de redundância de endereço comum)
SPN	Nome da Entidade de Serviço
LDAP	Lightweight Diretory Access Protocol

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Ative Diretory e autenticação Kerberos.
- Autenticação e territórios em SWA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Fluxo de rede Kerberos

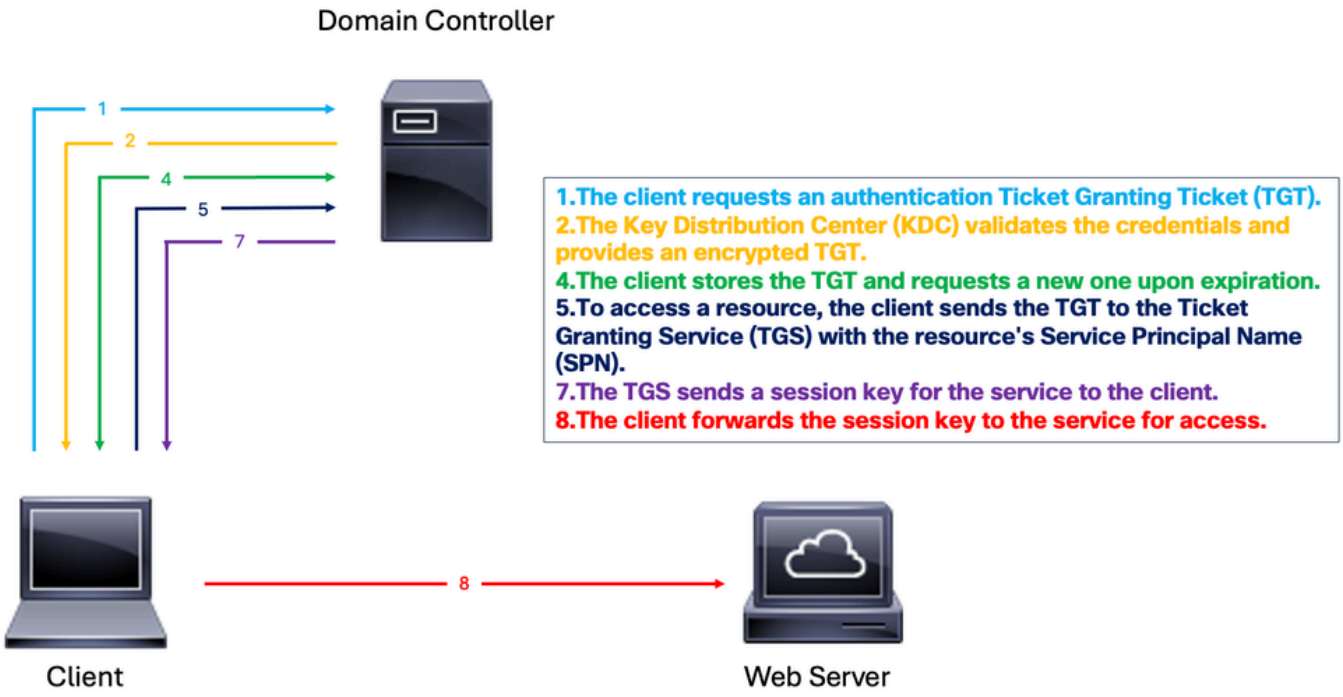


Imagem: Exemplo de fluxo Kerberos

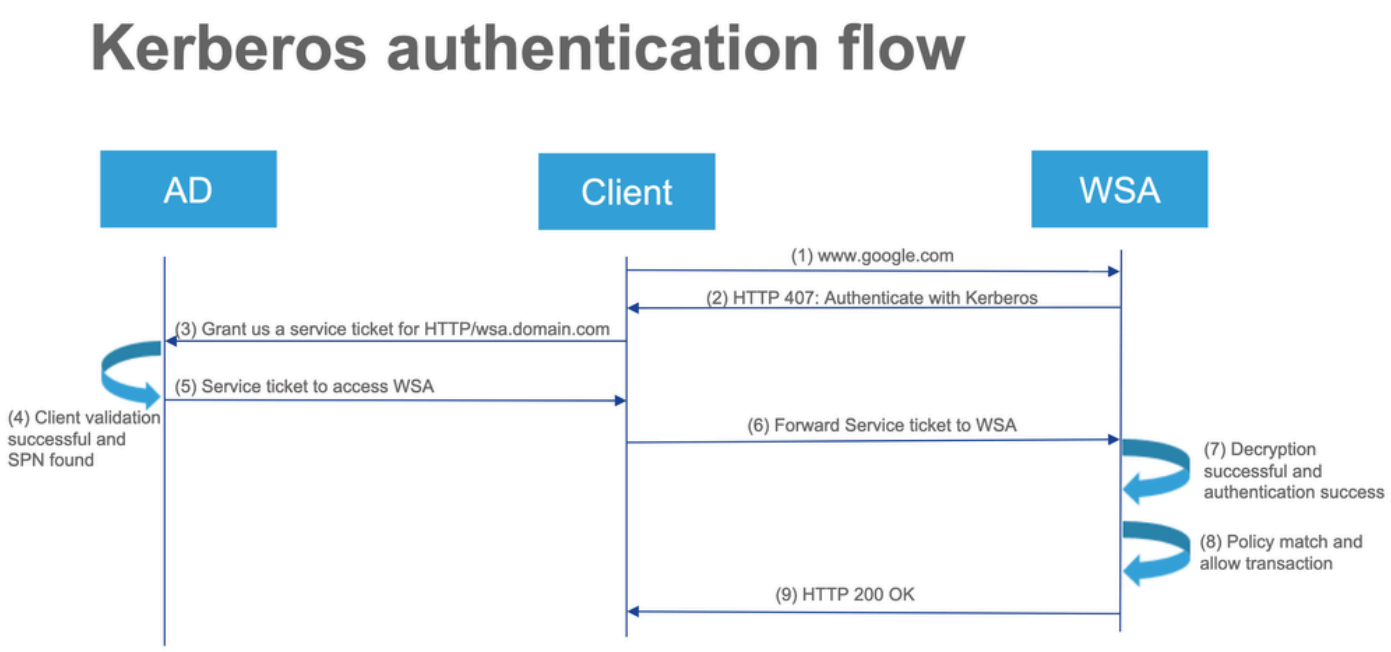
Estas são as etapas básicas da autenticação em um ambiente Kerberizado:

1. O cliente solicita um TGT (Tíquete de Concessão de Tíquete) do KDC (Centro de Distribuição de Chaves).
2. O KDC verifica as credenciais do usuário da máquina cliente e envia de volta um TGT criptografado e uma chave de sessão.
3. O TGT é criptografado com a chave secreta do TGS (Serviço de Concessão de Tíquete).
4. O cliente armazena o TGT e solicita automaticamente um novo quando ele expira.

Para acessar um serviço ou recurso:
1. O cliente envia o TGT ao TGS junto com o Nome da Entidade de Serviço (SPN) do recurso desejado.
2. O KDC verifica o TGT e os direitos de acesso à máquina cliente do usuário.

3. O TGS envia uma chave de sessão específica de serviço ao cliente.
4. O cliente fornece a chave de sessão ao serviço para comprovar o acesso e o serviço concede o acesso.

Fluxo de autenticação Kerberos em SWA



1. O cliente solicita acesso a www.google.com através do SWA.
2. O SWA responde com um status "HTTP 407", solicitando autenticação.
3. O cliente solicita um tíquete de serviço do servidor AD para o serviço HTTP/SWA.domain.com usando o TGT que obtém durante o ingresso no domínio.
4. O servidor AD valida o cliente e emite um tíquete de serviço. Se for bem-sucedido e o SPN (Service Principal Name) do SWA for encontrado, ele prossegue para a próxima etapa.
5. O cliente envia esse tíquete ao SWA.
6. O SWA descriptografa o tíquete e verifica a autenticação.
7. Se a autenticação for bem-sucedida, o SWA verificará as políticas.
8. O SWA envia uma resposta "HTTP 200/OK" ao cliente se a transação for permitida.

Qual é a finalidade do SPN?

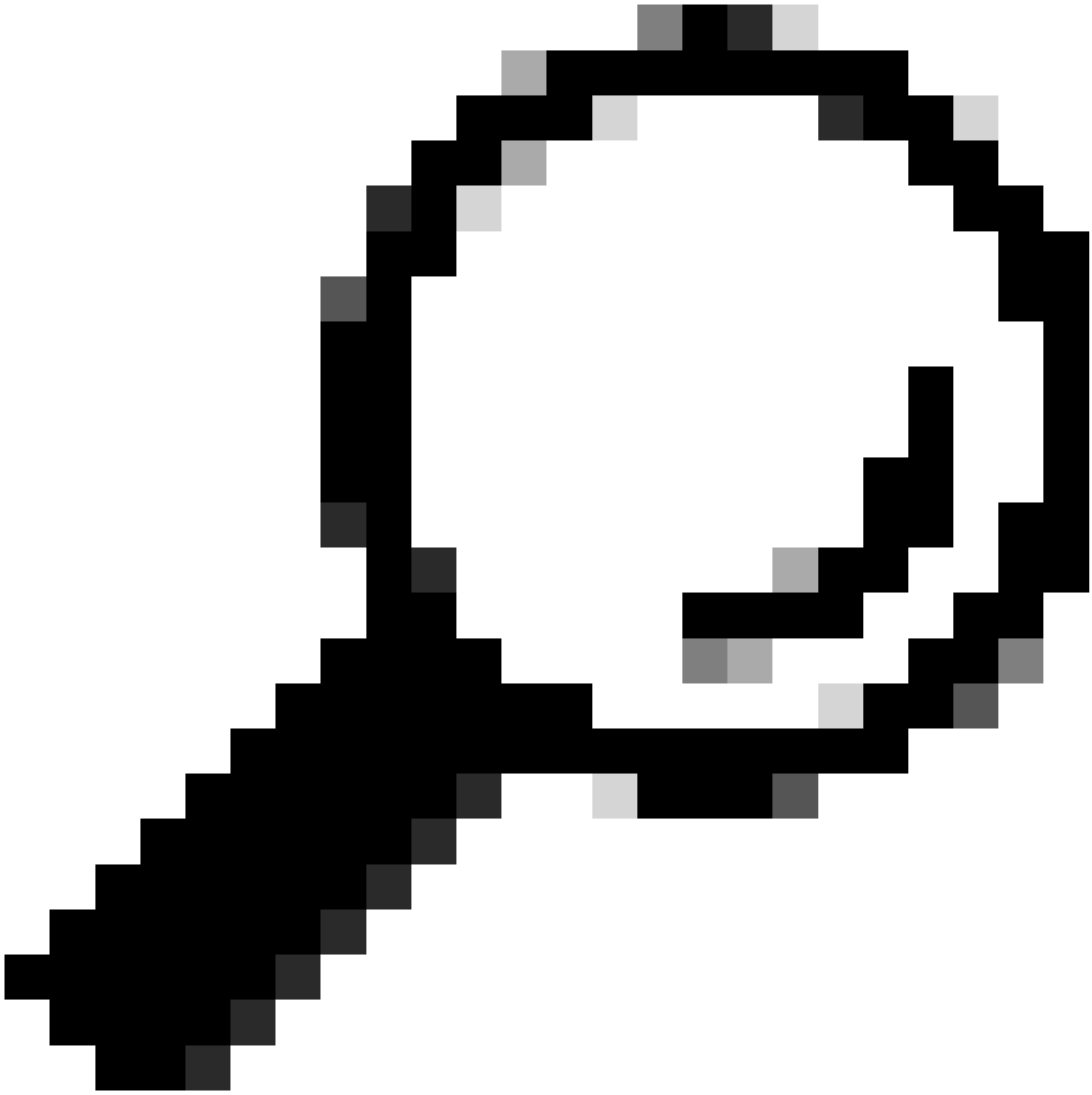
Um SPN (Nome da Entidade de Serviço) identifica exclusivamente uma instância de serviço na autenticação Kerberos. Ela vincula uma instância de serviço a uma conta de serviço, permitindo que os clientes solicitem autenticação para o serviço sem precisar do nome da conta. Cada conta em uma implementação do Centro de Distribuição de Chaves (KDC), como AD ou Open LDAP, e tem um SPN. Embora o SPN identifique estritamente um serviço, às vezes ele é usado por engano para se referir ao nome do cliente (UPN) em cenários onde o serviço também atua como um cliente.

No Kerberos, um Service Principal Name (SPN) identifica exclusivamente uma instância de serviço em uma rede. Permite que os clientes solicitem autenticação para um serviço específico. O SPN vincula a instância do serviço à sua conta, permitindo que o Kerberos autentique e autorize corretamente as solicitações de acesso a esse serviço.

Configuração do Servidor do Ative Diretory

1. Crie uma nova conta de usuário ou escolha uma conta de usuário existente para usar.
2. Registre o SPN a ser usado na conta de usuário escolhida.

3. Certifique-se de que nenhum SPN duplicado esteja registrado.



Tip: Qual é a diferença entre o Kerberos com SWA por trás do balanceador de carga ou um Traffic Manager/Traffic Shaper? Em vez de associar o SPN para o nome de host virtual HA a uma conta de usuário, associe o SPN para o dispositivo de redirecionamento de tráfego HTTP (por exemplo: LoadBalancer ou Traffic Manager) com uma conta de usuário no AD.

As Melhores formas de aprendizado para a implementação do Kerberos podem ser encontradas:

- Práticas recomendadas de dispositivos da Web seguros
- Configurar portas de firewall para conexões SWA

Troubleshooting

Troubleshooting de Kerberos com Comandos SPN

Esta é uma lista de comandos setspn úteis para gerenciar SPNs (Service Principal Names) em um ambiente Kerberos. Esses comandos são normalmente executados em uma interface de linha de comando com privilégios administrativos em um ambiente Windows.

Listar SPNs para uma conta específica:	setspn -L <User/ComputerAccountName> Lista todos os SPNs registrados para a conta especificada.
Adicionar um SPN a uma conta:	setspn -A <SPN> <User/ComputerAccountName> Adiciona o SPN especificado à conta fornecida.
Excluir um SPN de uma conta:	setspn -D <SPN> <User/ComputerAccountName> Remove o SPN especificado da conta fornecida.
Verifique se um SPN já está registrado:	setspn -Q <SPN> Verifica se o SPN especificado já está registrado no domínio.
Listar todos os SPNs no domínio	setspn -L <Conta do usuário/computador> Lista todos os SPNs no domínio.
Defina um SPN para uma conta de computador:	setspn -S <SPN> <User/ComputerAccountName> Adiciona um SPN a uma conta de computador, garantindo que não haja entradas duplicadas.
Redefinir SPNs para uma conta específica:	setspn -R <User/ComputerAccountName> Redefine os SPNs da conta especificada, ajudando a resolver problemas de SPN duplicados.

Exemplos de comandos SPN e saída

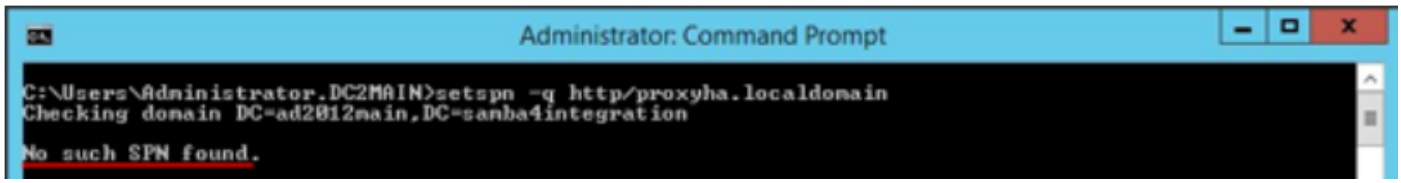
Os exemplos fornecidos demonstram o uso:

- Conta de Usuário/Computador: vrrpserviceuser
- SPN: http/WsaHostname.com ou http/proxyha.localdomain

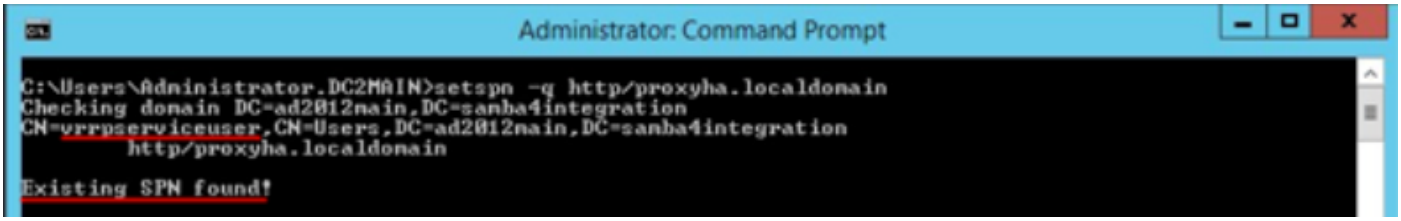
Verifique se o SPN já está associado a uma conta de usuário:
setspn -q <SPN>

setspn -q http/proxyha.localdomain

Cenário 1: SPN Não Encontrado



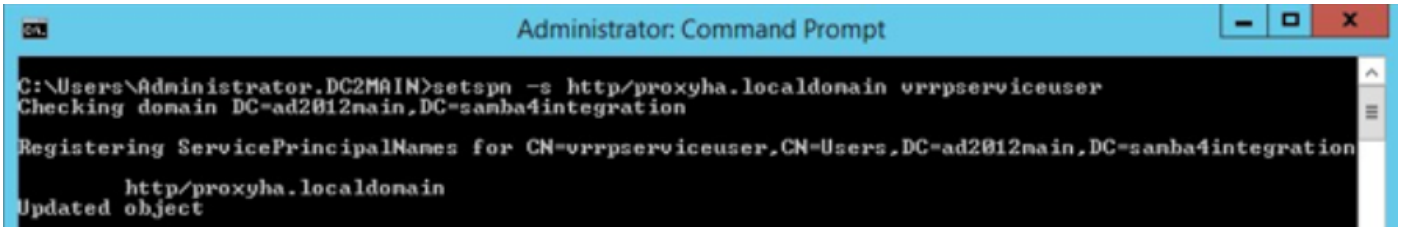
Cenário 2: SPN Encontrado



- Associe um SPN a uma conta de usuário/computador válida:

Sintaxe: setspn -s <SPN> <Conta do usuário/computador>

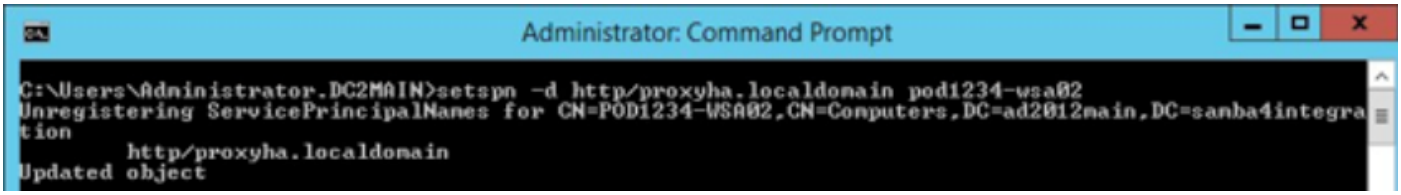
Por exemplo: setspn -s http/proxyha.localdomain vrrpserviceuser



- Excluir/Remover um SPN que já está associado a uma conta de usuário ou computador:

Sintaxe: setspn -d <SPN> <Conta do usuário/computador>

Por exemplo: setspn -d http/proxyha.localdomain pod1234-wsa0

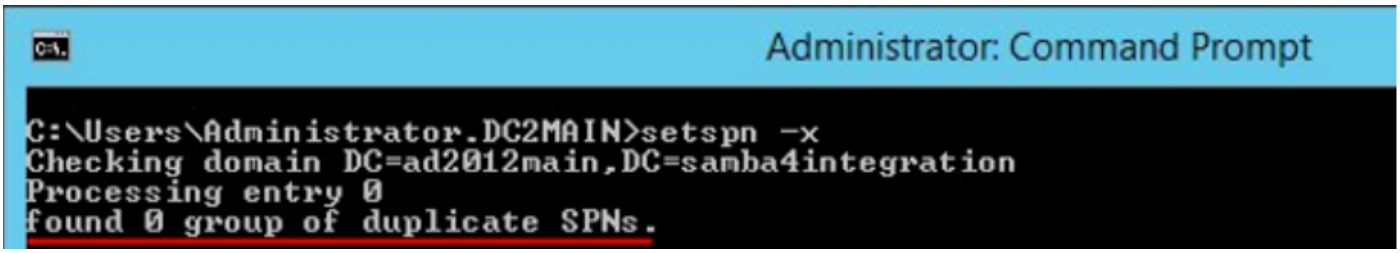


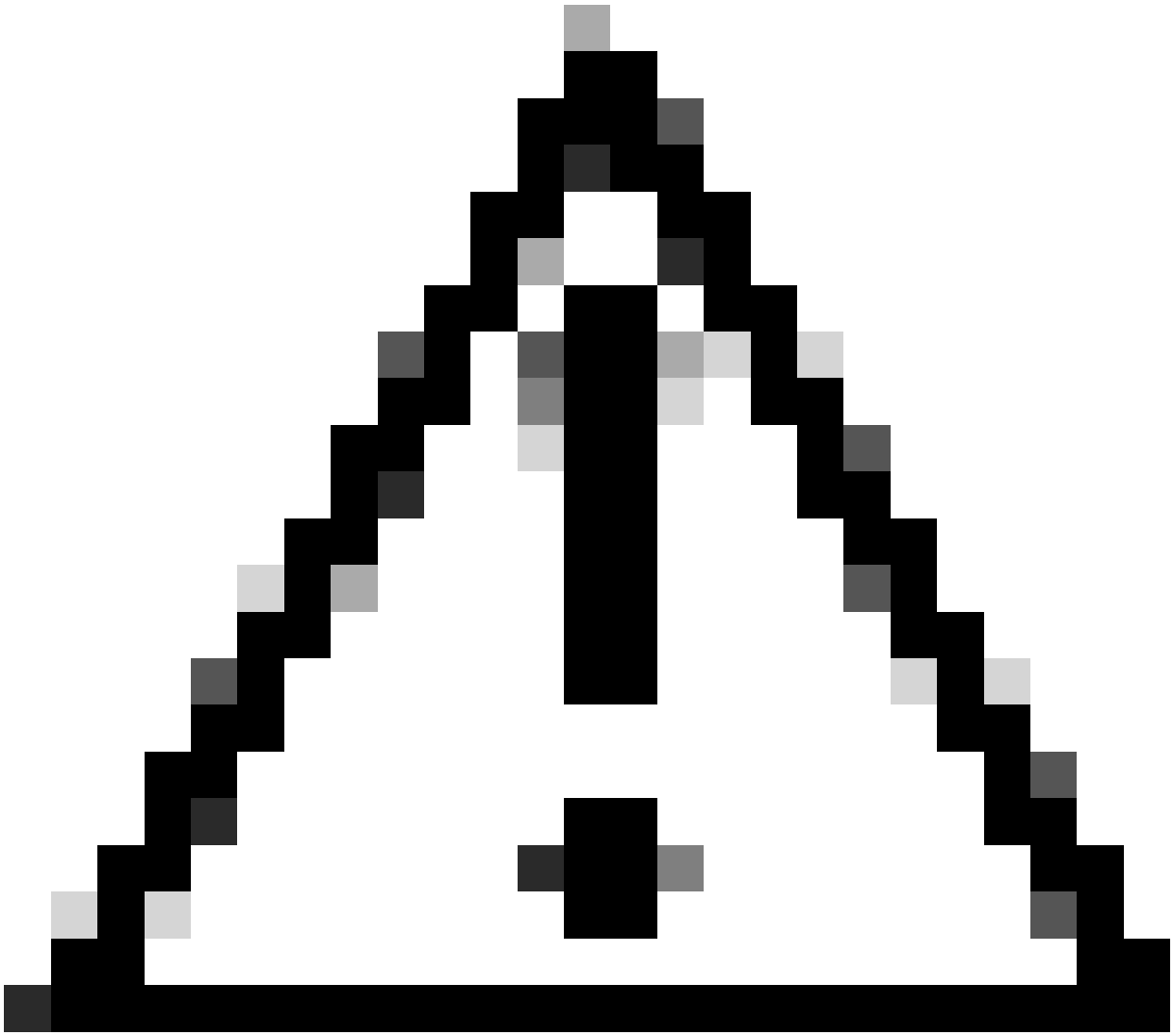
Certifique-se de que não haja SPNs duplicados para o nome de host virtual HA, pois as falhas

podem ocorrer mais tarde.

- Comando a ser usado: setspn -x

Como resultado, o tíquete do Serviço Kerberos não é fornecido ao cliente e a autenticação Kerberos falha.



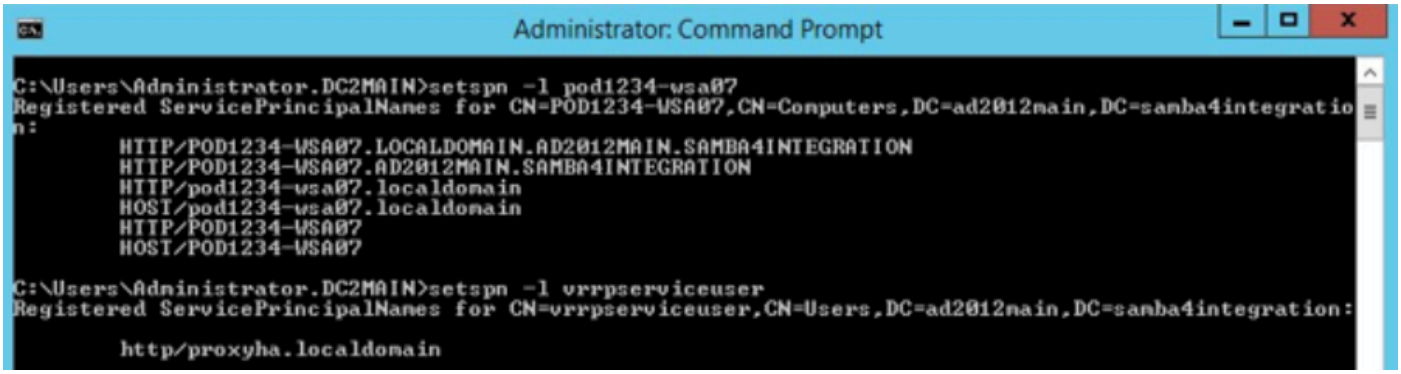


Caution: Se forem encontradas duplicatas, remova-as usando o comando setspn -d.

- Liste todos os SPNs associados a uma conta:

Sintaxe: setspn -l <Conta do usuário/computador>

Por exemplo: setspn -l vrrpserviceuser



Troubleshooting de Kerberos em SWA

Informações que o Suporte da Cisco precisa obter ao solucionar problemas de autenticação Kerberos:

- Detalhes da configuração atual.
- Logs de autenticação (preferencialmente no modo de depuração ou rastreamento).
- Capturas de pacotes usadas (com filtros apropriados):

  a) Dispositivo cliente

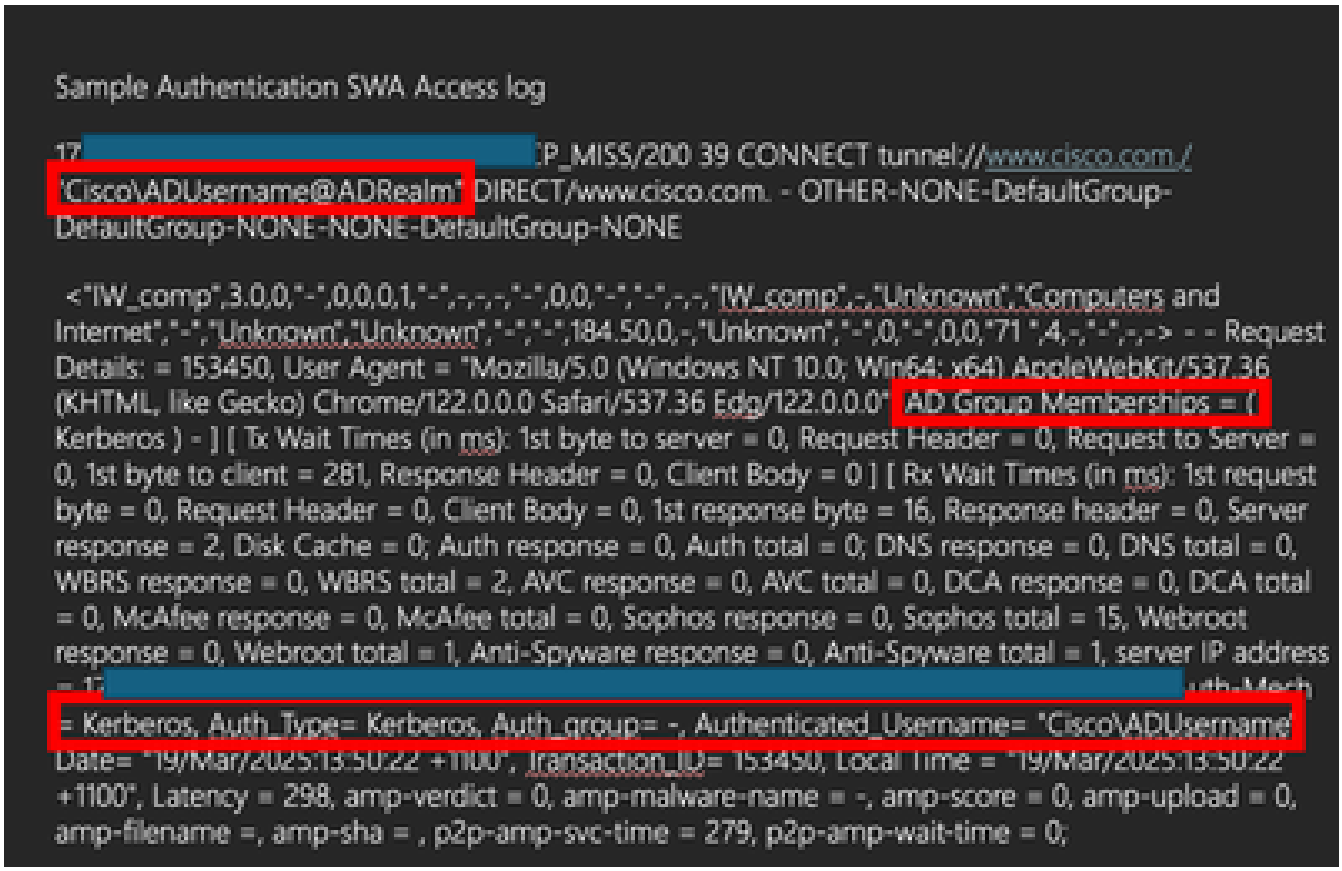
  b) SWA

- Logs de acesso com o especificador de formato personalizado %m habilitado. Isso deve mostrar o mecanismo de autenticação que foi usado para uma transação específica.
- Para obter detalhes detalhados sobre autenticação, adicione esses campos personalizados aos logs de acesso em proxies funcionais/não funcionais para obter mais informações ou consulte o hiperlink Adicionando parâmetro nos logs de acesso.
- Na GUI do SWA, navegue para Administração do sistema > Inscrição de log > Logs de acesso > Campos personalizados > Adicionar esta string para problemas de autenticação:

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

        a;
```

- Log de acesso SWA para detalhes de autenticação de usuário.
- O Cisco SWA registra nomes de usuário autenticados no formato Domínio\username@authentication_realm:



- Execute Test Authentication Realm Settings na GUI. Navegue até Network > Authentication e clique no nome do seu território na seção Test Current Settings. Clique em Start Test.

Servidor não encontrado no banco de dados Kerberos

Um caso de erro comum são solicitações da Web que falham com "Servidor não encontrado no banco de dados 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!
```

Nesse caso, o erro indica que o nome da entidade de serviço correspondente ao valor de endereço de proxy proxyha.local não está registrado no servidor do Ative Diretory. Para resolver o problema, seria necessário confirmar se o SPN http/proxyha.local está registrado no AD DC e adicionado a uma conta de serviço apropriada.

Informações adicionais e referências

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.