排除SWA/WSA中的Kerberos身份验证故障

目录

简介

本文档介绍使用票证安全验证网站和单点登录系统中的Kerberos协议。

术语

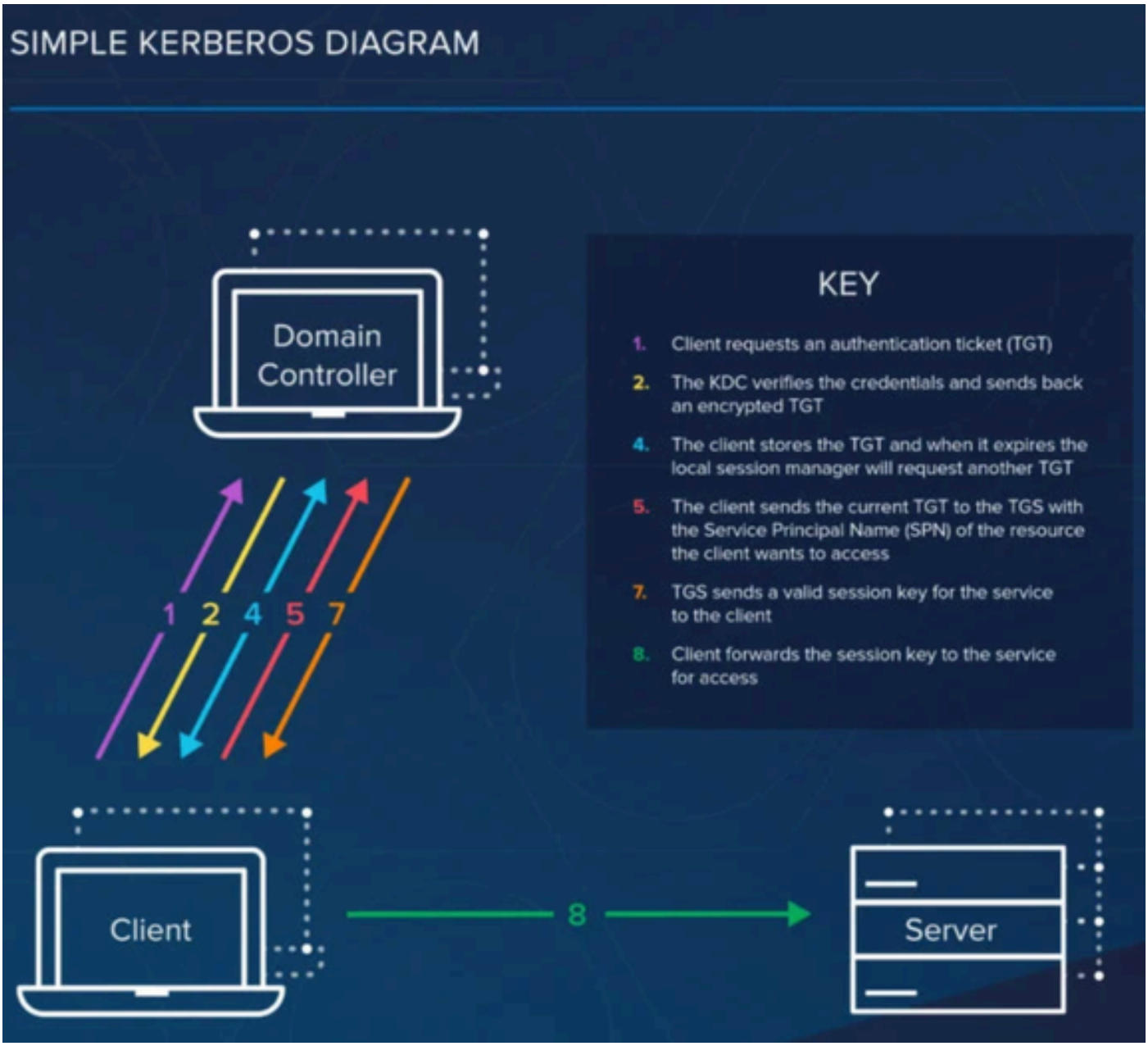
WSA	Web 安全设备
CLI	命令行界面
AD	Active Directory
SPN	服务主体名称
KDC	Kerberos密钥分发中心
TGT	身份验证票证
TGS	票证授予服务

高可用性	高可用性
VRRP	虚拟路由器冗余协议
鲤鱼	通用地址冗余协议

知识和要求

- Active Directory和身份验证。
- WSA上的身份验证和领域

Kerberos网络流



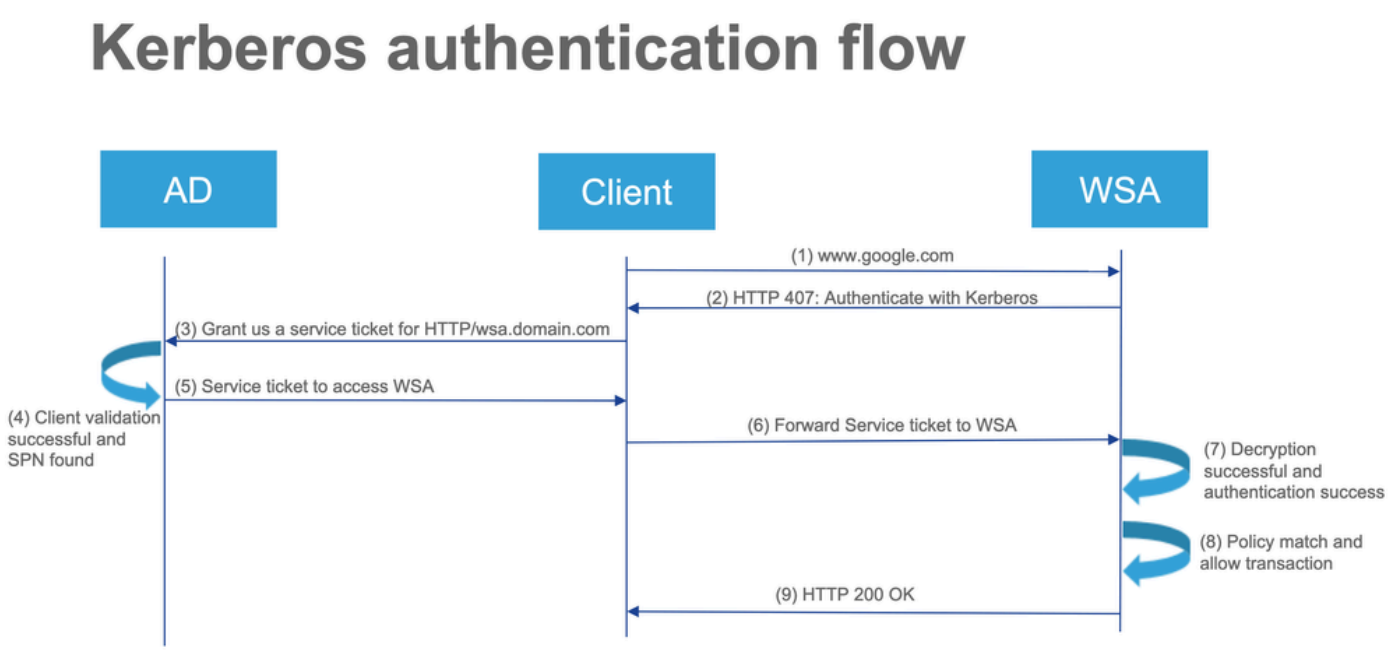
下面是在核化环境中进行身份验证的基本步骤：

1. 客户端向密钥分发中心(KDC)请求票证授予票证(TGT)。
2. KDC验证客户端计算机用户凭证并发送回加密的TGT和会话密钥。
3. TGT使用票证授权服务(TGS)密钥进行加密。
4. 客户端存储TGT，并在到期时自动请求新的TGT。

要访问服务或资源，请执行以下操作：
1.客户端将TGT与所需资源的服务主体名称(SPN)一起发送到TGS。
2. KDC验证TGT并检查用户客户端计算机访问权限。

3. TGS向客户端发送特定于服务的会话密钥。
4.客户端为服务提供会话密钥以证明访问，服务授予访问权限。

WSA中的Kerberos身份验证流程



1. 客户端请求通过WSA访问www.google.com。
2. WSA以HTTP 407状态响应，请求身份验证。
3. 客户端使用加入域时获得的TGT向AD服务器请求HTTP/wsa.domain.com服务的服务票证。
4. AD服务器验证客户端并发出服务票证，如果成功，并且找到WSA的SPN（服务主体名称），则继续下一步。
5. 客户端将此票证发送到WSA。
6. WSA解密票证并检查身份验证。
7. 如果身份验证成功，则WSA会验证策略。
8. 如果允许事务，WSA会向客户端发送HTTP 200 OK响应。

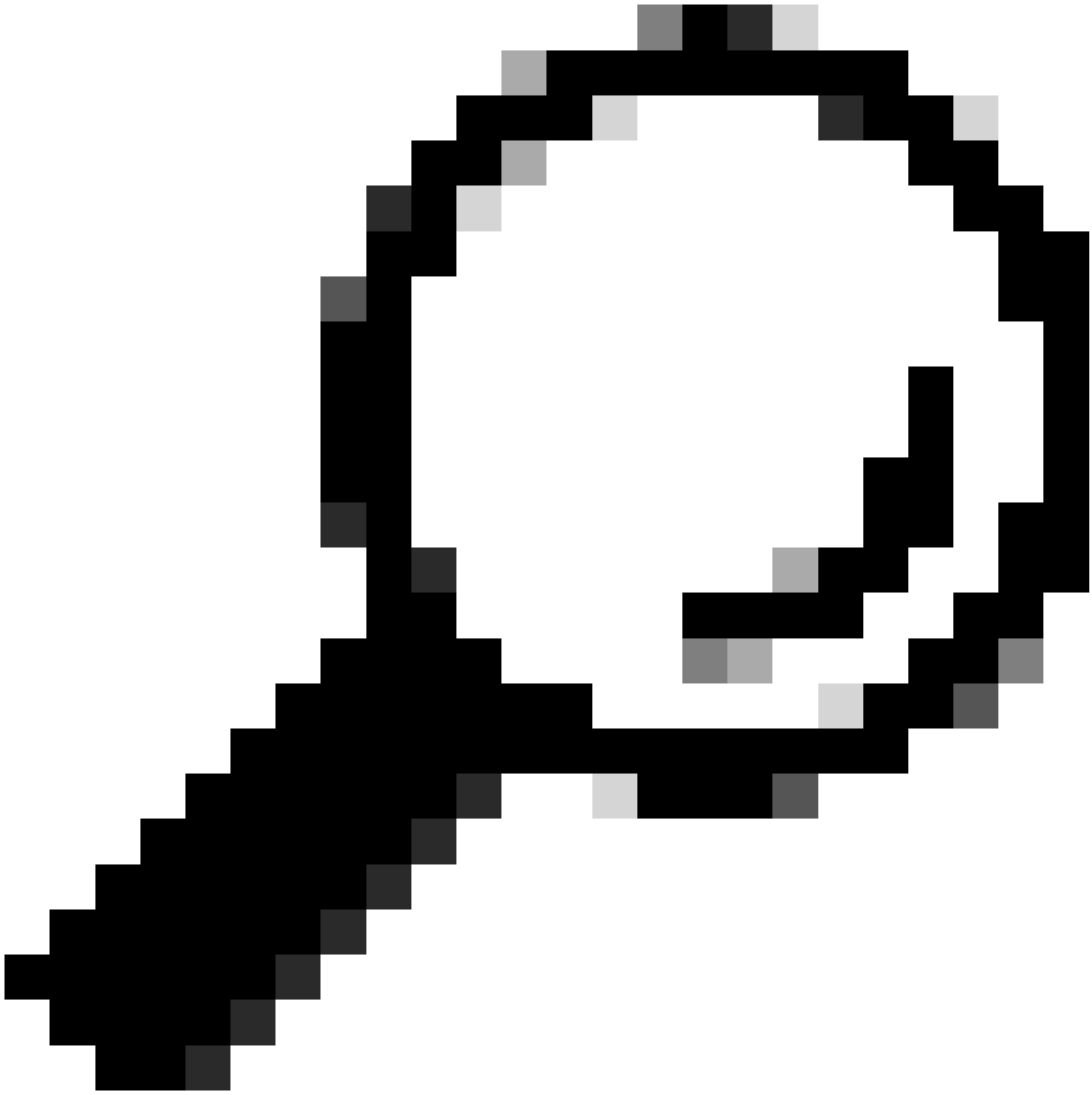
SPN有什么作用？

服务主体名称(SPN)唯一标识Kerberos身份验证中的服务实例。它将服务实例链接到服务帐户，使客户端无需帐户名称即可请求对服务进行身份验证。密钥分发中心(KDC)实施中的每个帐户（例如AD或开放式LDAP）都有一个SPN。虽然SPN严格标识服务，但在服务也充当客户端的场景中，有时会错误地使用它来指代客户端名称(UPN)。

在Kerberos中，服务主体名称(SPN)唯一标识网络中的服务实例。它允许客户端请求特定服务的身份验证。SPN将服务实例链接到其帐户，使Kerberos能够正确验证和授权对该服务的访问请求。

Active Directory服务器配置

- 创建新用户帐户或选择要使用的现有用户帐户
- 注册要用于所选用户帐户的SPN
- 确保未注册重复的SPN



提示：带WSA的负载均衡器或流量管理器/流量整形器的Kerberos有何不同？不是将HA虚拟主机名的SPN与用户帐户关联，而是将HTTP流量重定向设备（例如：LoadBalancer或Traffic Manager）的SPN与AD上的用户帐户关联。

使用SPN命令排除Kerberos故障

以下是用于管理Kerberos环境中的服务主体名称(SPN)的有用“setspn”命令的列表。这些命令通常从Windows环境中具有管理权限的命令行界面运行。

列出特定帐户的SPN:	setspn -L <用户/计算机帐户名> 列出为指定帐户注册的所有SPN。

将SPN添加到帐户：	setspn -A <SPN> <User/ComputerAccountName> 将指定的SPN添加到给定帐户。
从帐户中删除SPN:	setspn -D <SPN> <User/ComputerAccountName> 从给定帐户中删除指定的SPN。
验证SPN是否已注册：	setspn -Q <SPN> 检查指定的SPN是否已在域中注册。
列出域中的所有SPN	setspn -L <用户/计算机帐户> 列出域中的所有SPN。
设置计算机帐户的SPN:	setspn -S <SPN> <用户/计算机帐户名> 将SPN添加到计算机帐户，确保没有重复的条目。
重置特定帐户的SPN:	setspn -R <User/ComputerAccountName> 重置指定帐户的SPN，帮助解决重复的SPN问题。

SPN命令和输出的示例

提供的示例演示了以下用途：

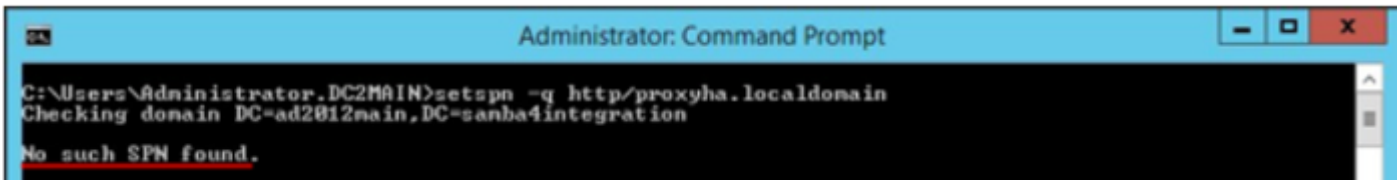
用户/计算机帐户：vrpserviceuser

SPN:http/WsaHostname.com或http/proxyha.localdomain

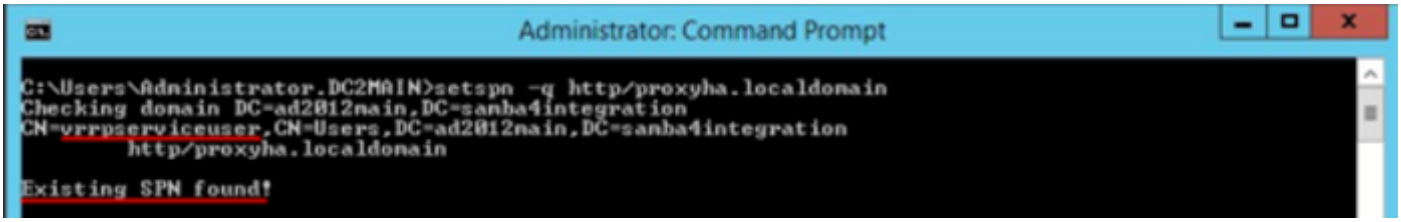
- 检查SPN是否已与用户帐户关联：
  setspn -q <SPN>

setspn -q http/proxyha.localdomain

情形 1：找不到SPN



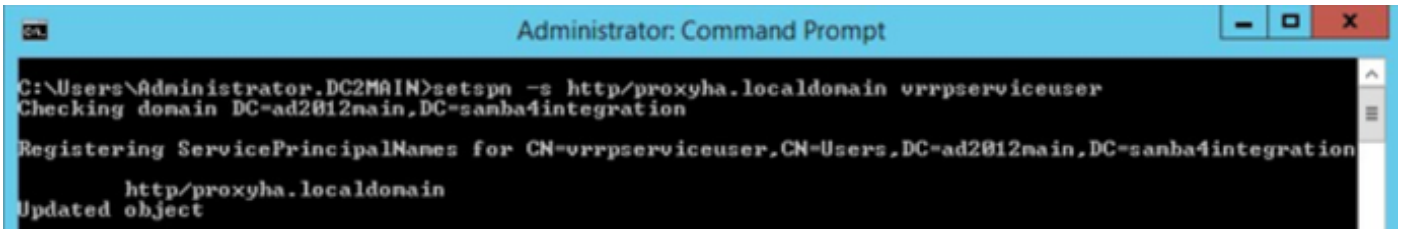
方案 2：已找到SPN



- 将SPN与有效的用户/计算机帐户关联：

语法:setspn -s <SPN> <用户/计算机帐户>

例如：setspn -s http/proxyha.localdomain vrrpserviceuser



- 删除/删除已与关联的SPN

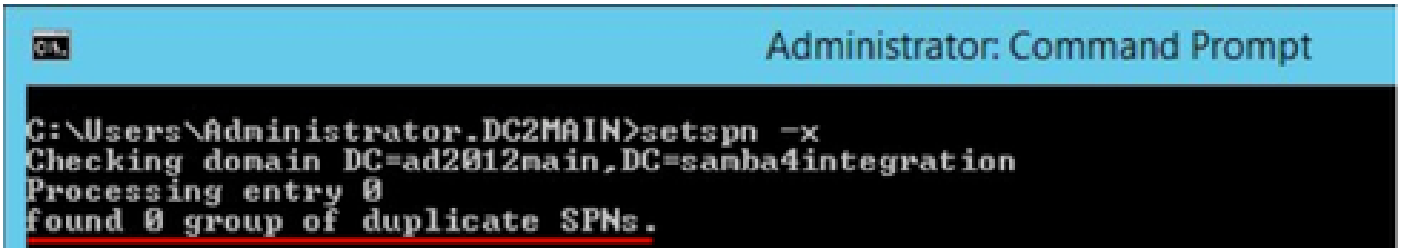
用户/计算机帐户：

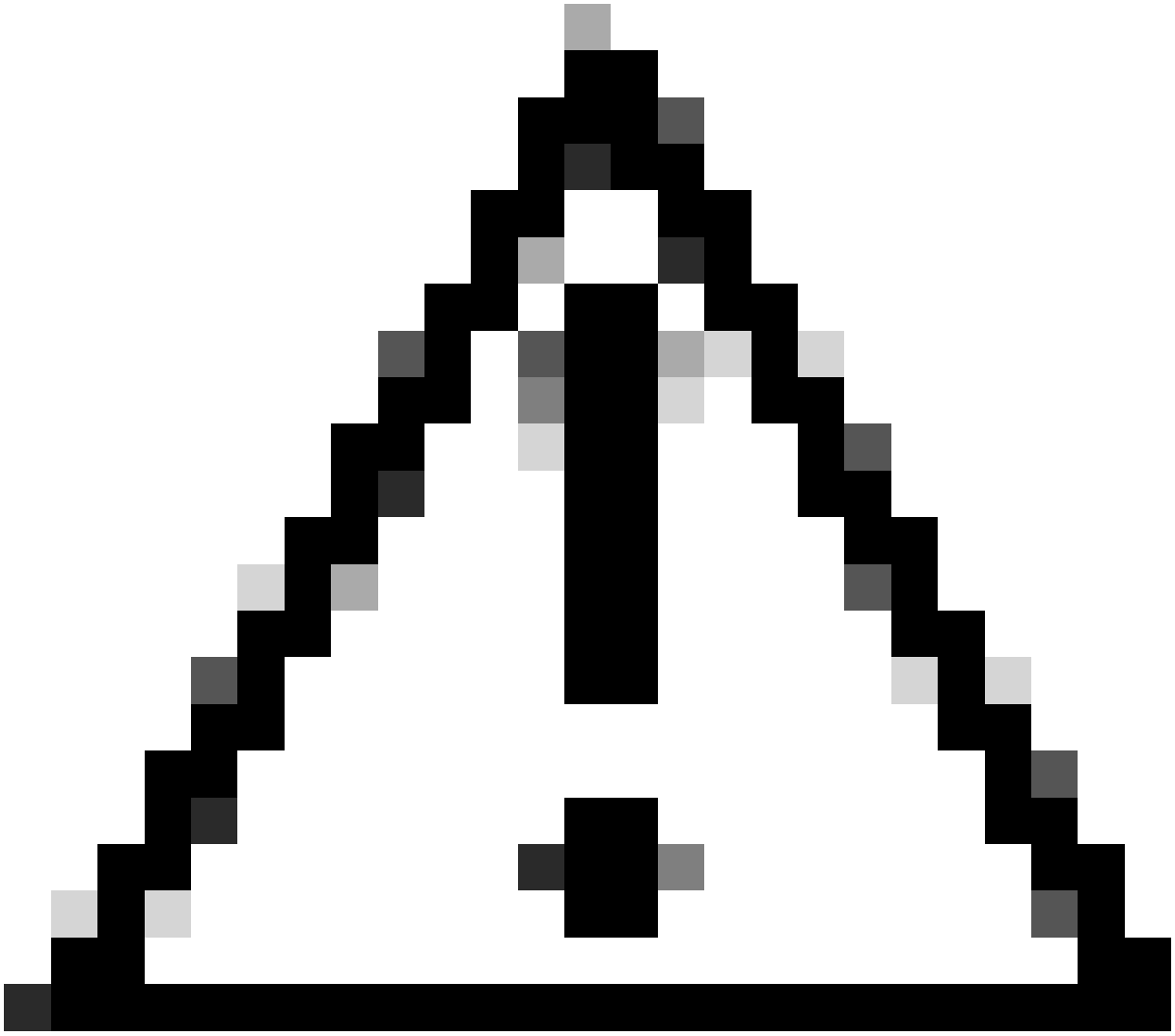
语法:setspn -d <SPN> <用户/计算机帐户>

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

确保HA虚拟主机名没有重复的SPN，因为稍后可能会发生故障：
应使用的命令:setspn -x

因此，客户端不提供Kerberos服务票证，并且Kerberos身份验证失败。



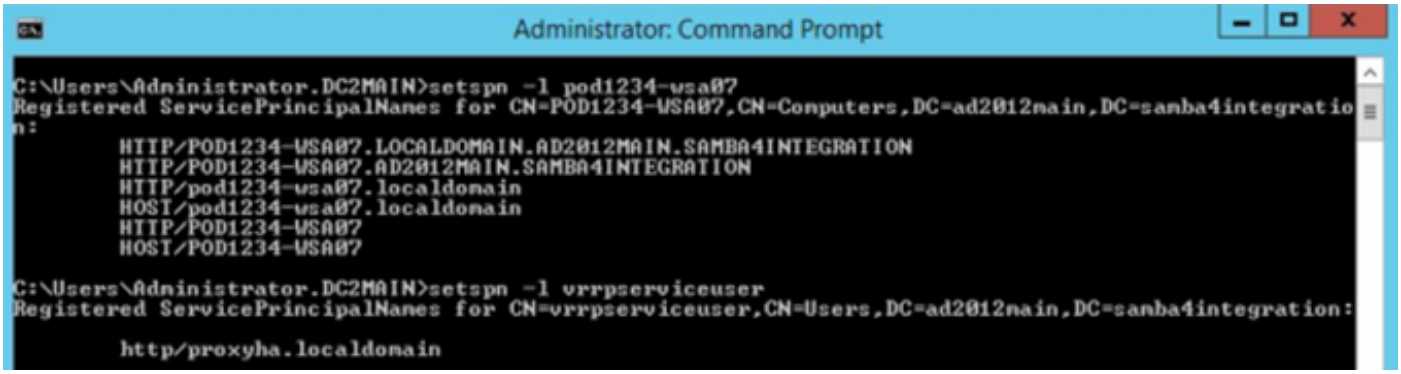


警告：如果发现重复项，请使用setspn -d命令删除重复项

- 列出与帐户关联的所有SPN:

语法:setspn -l <用户/计算机帐户>

例如：setspn -l vrrpserviceuser



排除WSA上的Kerberos故障

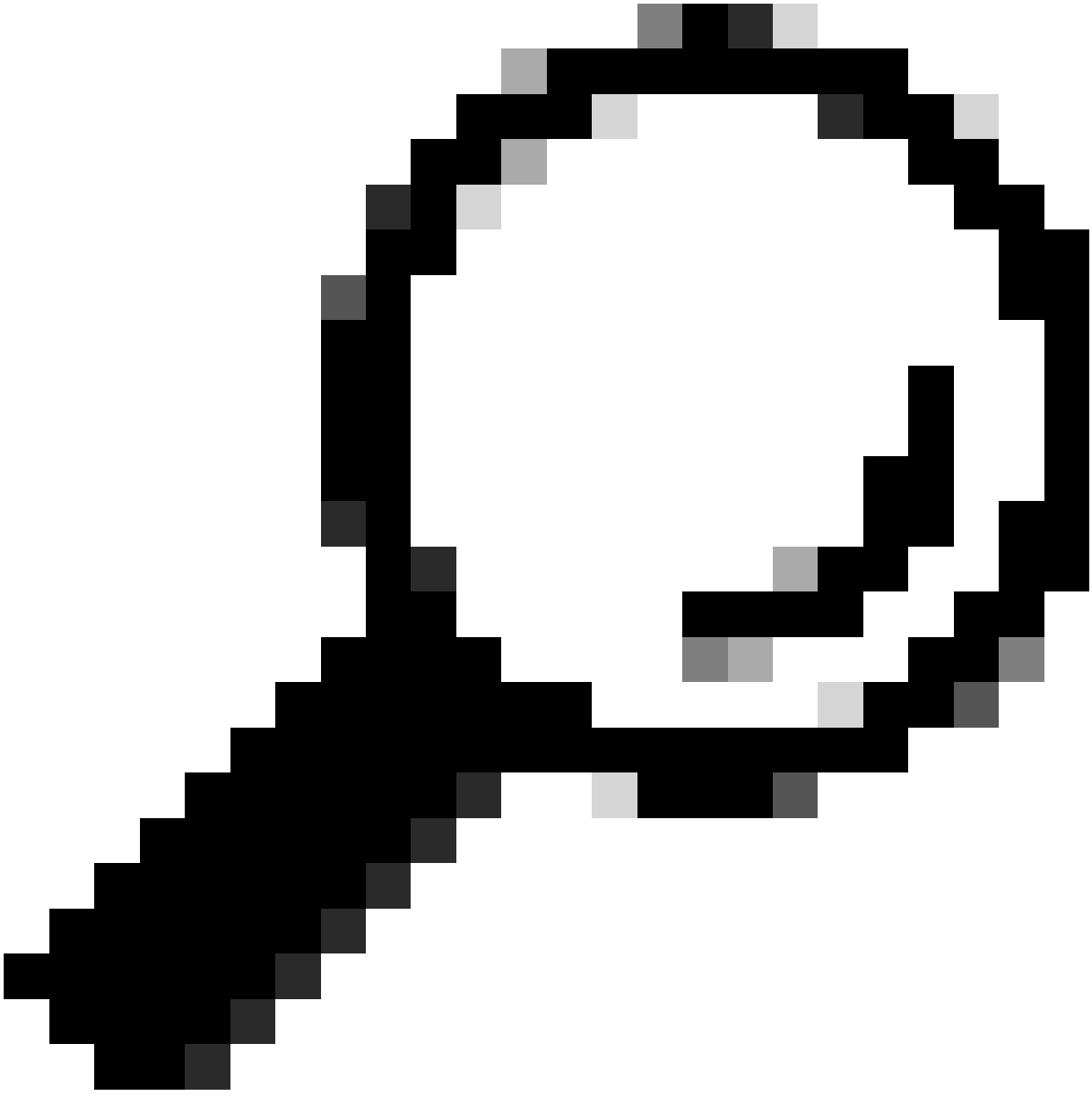
排除kerberos身份验证问题时TAC需要获取的信息

- 当前配置详细信息
- 身份验证日志（最好在调试或跟踪模式下）
- 捕获的数据包（使用适当的过滤器）：

  (a)客户设备

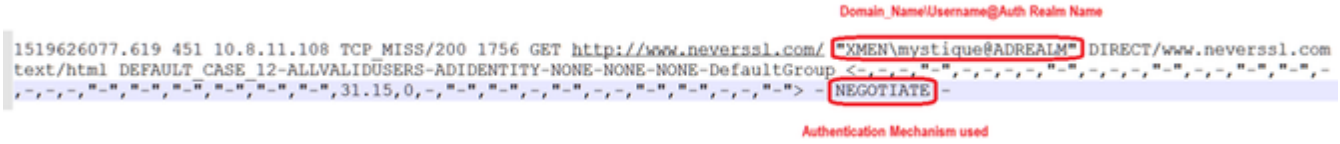
  (b)WSA

- 启用了%m自定义格式说明符的访问日志。这必须显示用于特定事务的身份验证机制。



提示：有关详细的身份验证详细信息，请将这些自定义字段添加到正在工作/未工作的代理上的访问日志中，以获取详细信息
在WSA GUI上，导航至>系统管理>日志订阅>访问日志>自定义字段>添加此字符串以解决身份验证问题
服务器IP地址= %k，客户端IP地址= %a，Auth-Mech = %m，Auth_Type= %m，Auth_group= %g，Authenticated_Username= %A，Date= %L，Transaction_ID= %I身份验证响应= %:<a，身份验证总计= %:>a;

用户身份验证详细信息的WSA访问日志快照



- 一个常见的错误案例是Web请求失败，显示“Server not found in Kerberos database”：

curl -vx proxyha.localdomain:3128 —proxy-negotiate -u:http://www.google.com/

*即将连接到代理proxyha.localdomain端口3128(#0)

*已连接到proxyha.localdomain(10.8.96.30)端口3128(#0)

<需要HTTP/1.1 407代理身份验证

<通过：1.1 pod1234-wsa02.localdomain:80(Cisco-WSA/10.1.2-003)

<内容类型：文本/html

gss_init_sec_context()失败：:在Kerberos数据库中找不到服务器

<Proxy-Authenticate:协商

<连接：关闭

* HTTP/1.1代理连接设置关闭！

在这种情况下，该错误表示与代理地址值proxyha.localdomain对应的服务主体名称未在Active Directory服务器上注册。要解决此问题，需要确认SPN http/proxyha.localdomain已在AD DC上注册并添加到正确的服务帐户。

- 此超链接中介绍了实施kerberos的最佳实践：

安全Web设备最佳实践

其他信息和参考

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。