排除SWA上的Kerberos身份验证故障

目录

简介

术语

先决条件

- 要求
- 使用的组件

Kerberos网络流

- SWA中的Kerberos身份验证流程
- SPN有什么作用？
- Active Directory服务器配置

故障排除

- 使用SPN命令排除Kerberos故障
- SPN命令和输出的示例
  - 情形 1：找不到SPN。
  - 方案 2：已找到SPN。
- 排除SWA上的Kerberos故障
- 在Kerberos数据库中找不到服务器

相关内容

简介

本文档介绍Kerberos身份验证的基本信息以及排除安全Web设备(SWA)中Kerberos身份验证故障的步骤。

术语

- SWA:Secure Web Appliance
- CLI：命令行界面
- 广告:Active Directory
- DC:域控制器
- SPN:服务主体名称
- KDC:Kerberos密钥分发中心
- TGT:票证授予票证（身份验证票证）
- TGS:票证授予服务
- HA:高可用性
- VRRP:虚拟路由器冗余协议

- CARP:通用地址冗余协议
- SPN:服务主体名称
- LDAP:轻型目录访问协议

先决条件

要求

Cisco 建议您了解以下主题：

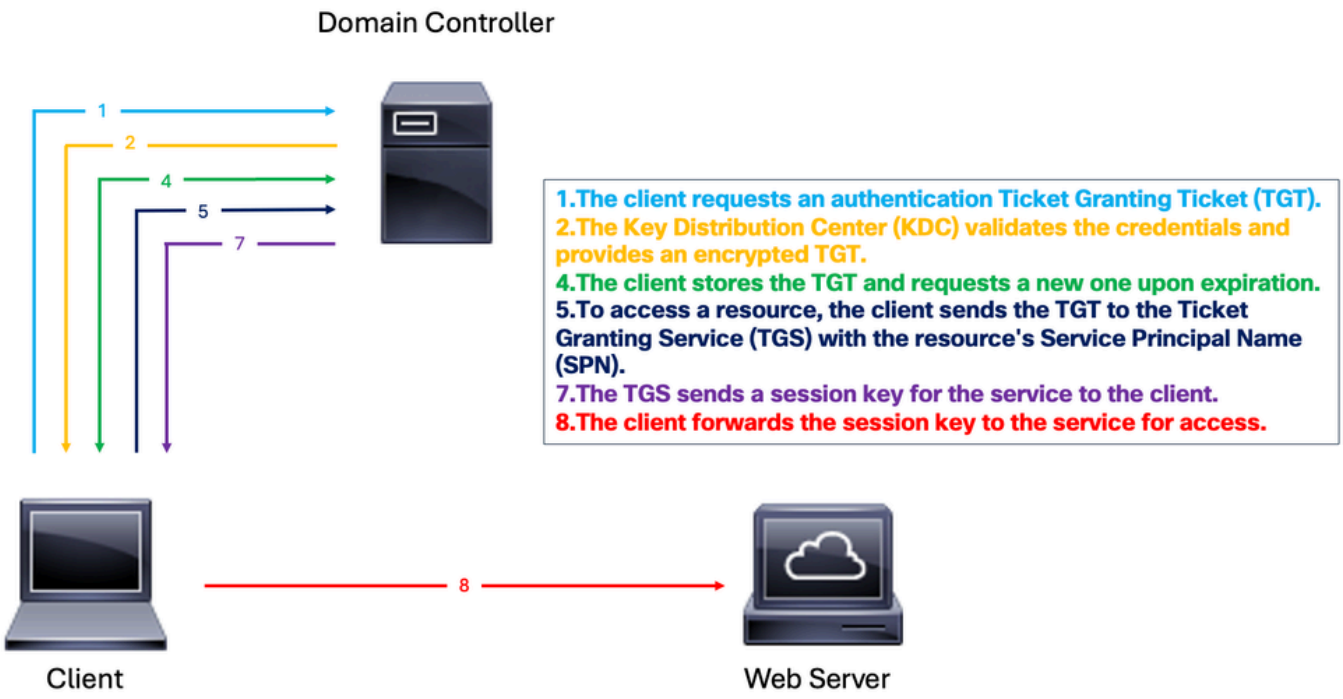
- SWA上的身份验证和领域
- Active Directory和Kerberos身份验证

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

Kerberos网络流



图像：Kerberos网络流量示例

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KDC请求TGT。

2. KDC验证客户端计算机用户凭证，然后发回加密的TGT和会话密钥。

3. TGT使用TGS密钥加密。

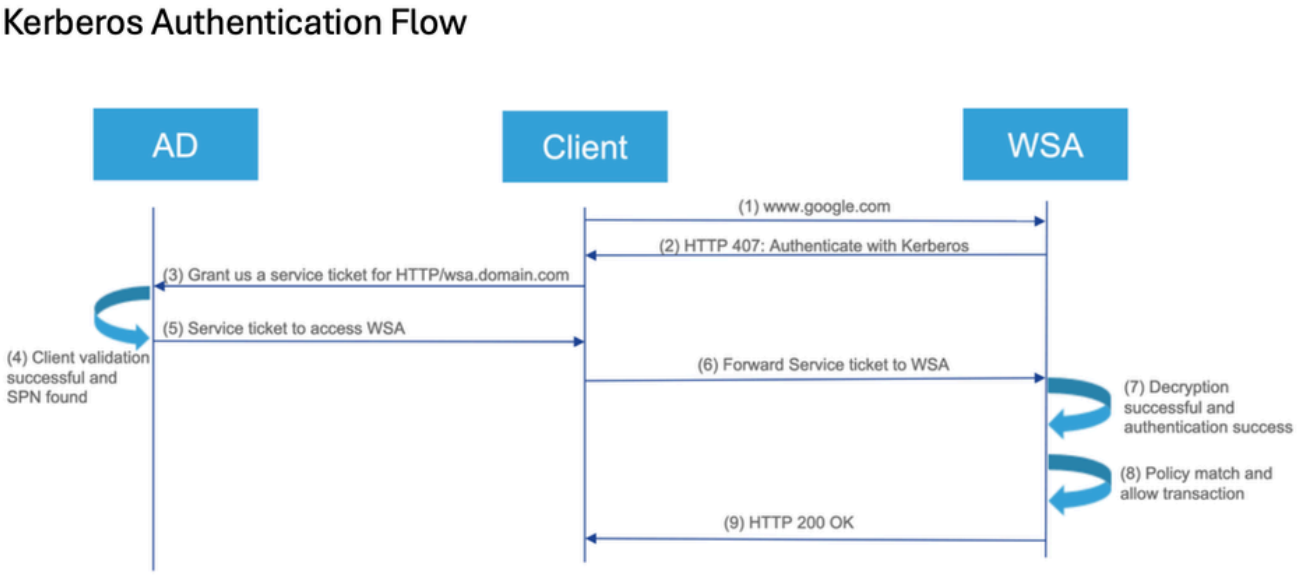
4.客户端存储TGT并在到期时自动请求新的TGT。

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。

SWA中的Kerberos身份验证流程



1.客户端请求通过SWA访问www.google.com。

2. SWA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/SWA.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，发现SWA的SPN，则继续下一步。

5.客户端将此票证发送到SWA。

6. SWA解密票证并检查身份验证。

7.如果身份验证成功，SWA将验证策略。

8.如果允许事务，SWA将向客户端发送HTTP 200 OK响应。

SPN有什么作用？

SPN唯一标识Kerberos身份验证中的服务实例。它可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。KDC实施中的每个帐户（例如AD或OpenLDAP）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，SPN唯一地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

1.创建新用户帐户或选择要使用的现有用户帐户。

2.注册要用于所选用户帐户的SPN。

3.确保未注册重复的SPN。



提示：带SWA的Kerberos在负载均衡器或流量管理器/流量整形器之后有何不同？

- 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，负载均衡器或流量管理器）的SPN与AD上的用户帐户关联。

可以找到实施Kerberos的最佳实践：

- 安全Web设备最佳实践
- 为SWA连接配置防火墙端口

故障排除

使用SPN命令排除Kerberos故障

这是用于在Kerberos环境中管理SPN的有用setspn命令的列表。这些命令通常在Windows环境中从具有管理权限的命令行界面运行。

列出特定帐户的SPN:	`setspn -L` 列出为指定帐户注册的所有SPN。

将SPN添加到帐户：	`setspn -A` 将指定的SPN添加到给定帐户。
从帐户中删除SPN:	`setspn -D` 从给定帐户中删除指定的SPN。
验证SPN是否已注册：	`setspn -Q` 检查指定的SPN是否已在域中注册。
列出域中的所有SPN	`setspn -L` 列出域中的所有SPN。
设置计算机帐户的SPN:	`setspn -S`

	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` 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：

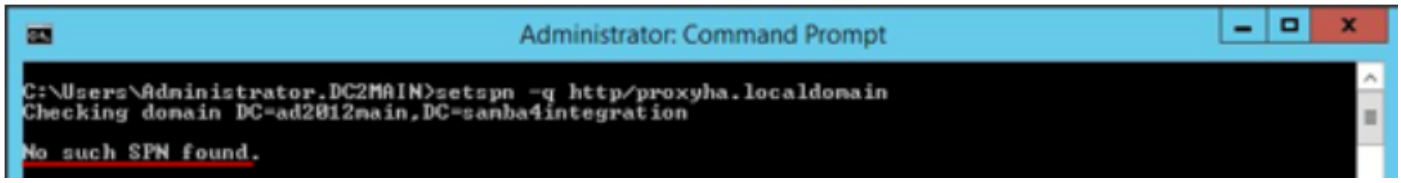
- 用户/计算机帐户:vrpserviceuser
- SPN:http/WsaHostname.com或http/proxyha.localdomain

检查SPN是否已与用户帐户关联：

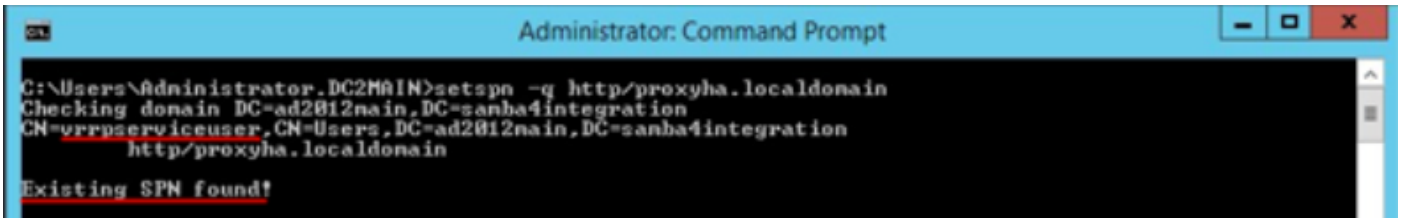
```
setspn -q
```

```
setspn -q http/proxyha.localdomain
```

情形 1：找不到SPN。



方案 2：已找到SPN。

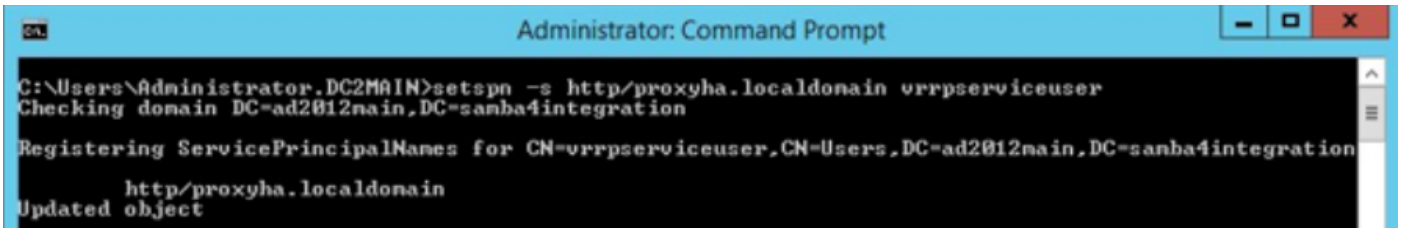


- 将SPN与有效的用户/计算机帐户关联：

```
setspn -s
```

例如：

```
setspn -s http/proxyha.localdomain vrrpserviceuser
```

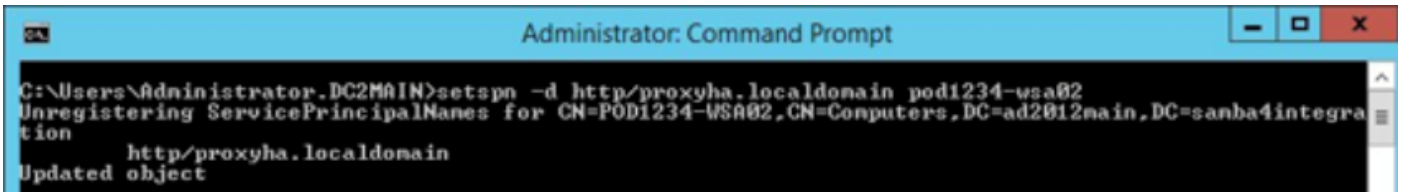


- 删除/删除已与用户或计算机帐户关联的SPN:

```
setspn -d
```

例如：

```
setspn -d http/proxyha.localdomain pod1234-wsa0
```

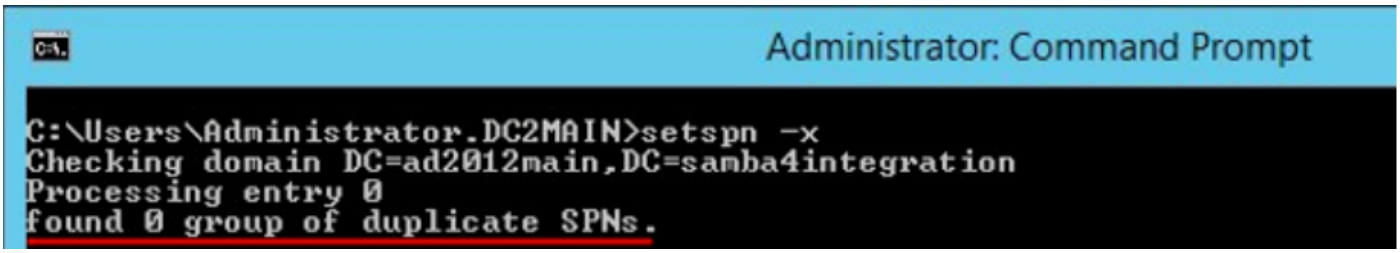


确保HA虚拟主机名没有重复的SPN，因为以后可能会发生故障。

- 要运行的命令：

```
setspn -x
```

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



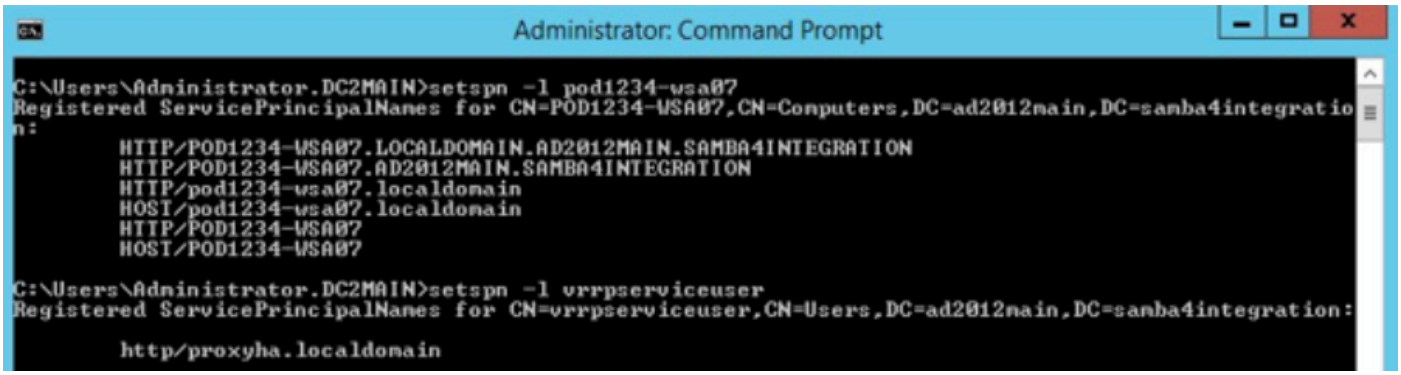
⚠ 警告：如果发现重复项，请删除运行setspn -d命令的重复项。

- 列出与帐户关联的所有SPN:

```
setspn -l
```

例如：

```
setspn -l vrrpserviceuser
```



排除SWA上的Kerberos故障

排除Kerberos身份验证问题时，思科支持部门需要的信息：

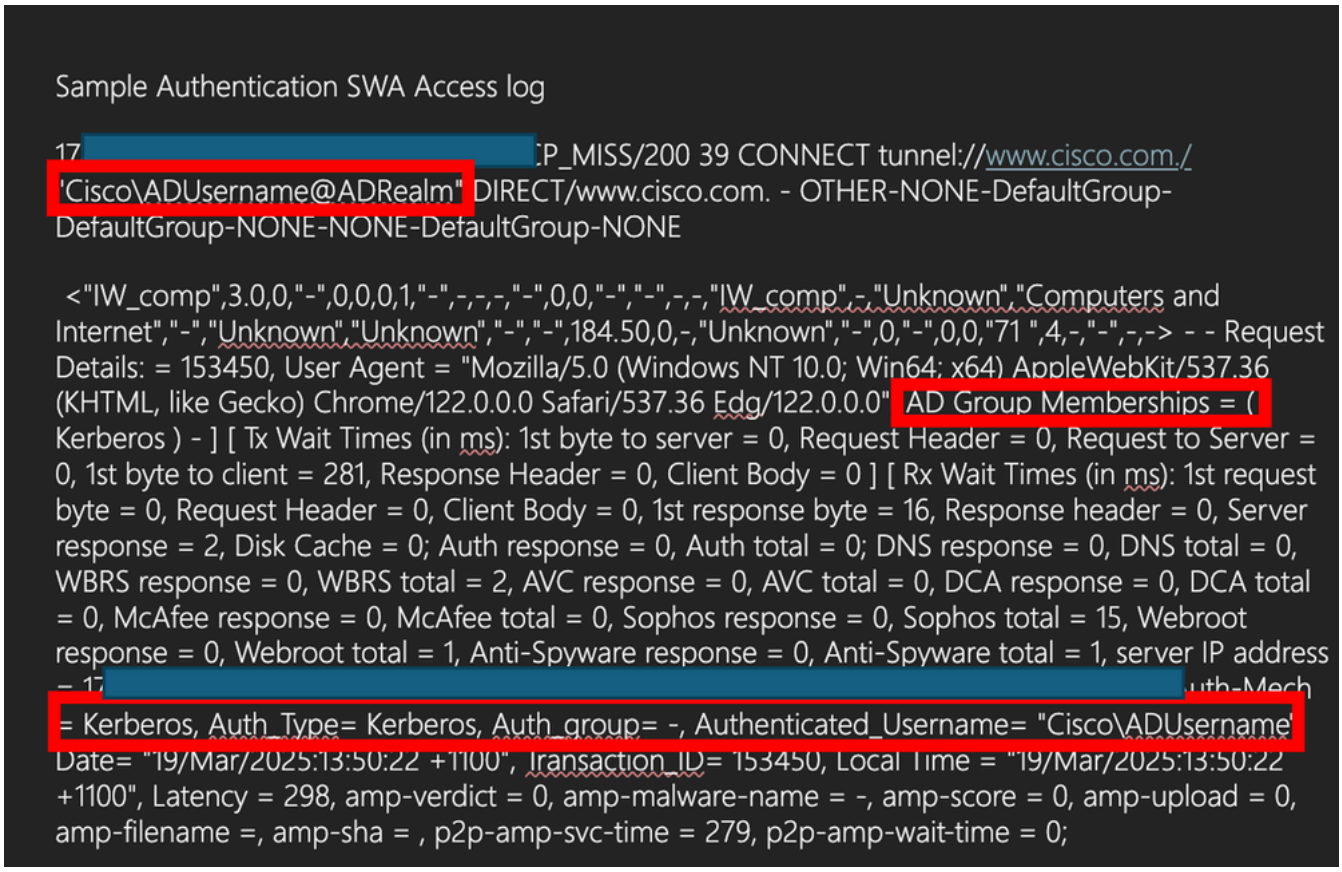
- 当前配置详细信息
- 身份验证日志（最好在调试或跟踪模式下）
- 捕获的数据包（使用适当的过滤器）：
  - 客户端设备
  - SWA
- 已启用%m自定义格式说明符的访问日志。这必须显示用于特定事务的身份验证机制。
- 有关详细的身份验证详细信息，请将这些自定义字段添加到正在工作/未工作的代理上的访问日志中，以检索其他信息或参阅在访问日志中添加参数。
- 在SWA GUI中，导航到系统管理>日志订阅>访问日志>自定义字段>添加此字符串以解决身份验证问题：

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

```
    a;
```

- 用户身份验证详细信息的SWA访问日志。

- Cisco SWA以Domain\username@authentication_realm格式记录经过身份验证的用户名：



- 从GUI运行测试身份验证领域设置。导航到网络>身份验证，然后在测试当前设置部分中单击领域的名称。
- 单击Start Test。

在Kerberos数据库中找不到服务器

一个常见错误案例是Web请求失败，显示“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!
```

在这种情况下，错误表示与代理地址值proxyha.local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.local已在AD DC上注册并添加到正确的服务帐户。

相关内容

- 配置安全Web设备以允许访客访问
- 在SWA中配置Active Directory身份验证
- 在SWA中配置Kerberos单点登录身份验证
- 绕过安全网络设备中的流量

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）。