排除SWA中的Kerberos身份驗證故障

目錄

簡介

本檔案介紹Kerberos驗證的基本知識以及解決安全Web裝置(SWA)中Kerberos驗證問題的步驟。

技術

SWA	安全網路設備
CLI	命令列介面
AD	Active Directory
資料中心	域控制器
SPN	服務主體名稱
KDC	Kerberos金鑰發佈中心

TGT	身份驗證票證（票證授予票證）
TGS	票證授予服務
HA	高可用性
VRRP	虛擬路由器備援協定
鯉魚	通用位址備援通訊協定
SPN	服務主體名稱
LDAP	輕量型目錄存取通訊協定

必要條件

需求

思科建議您瞭解以下主題：

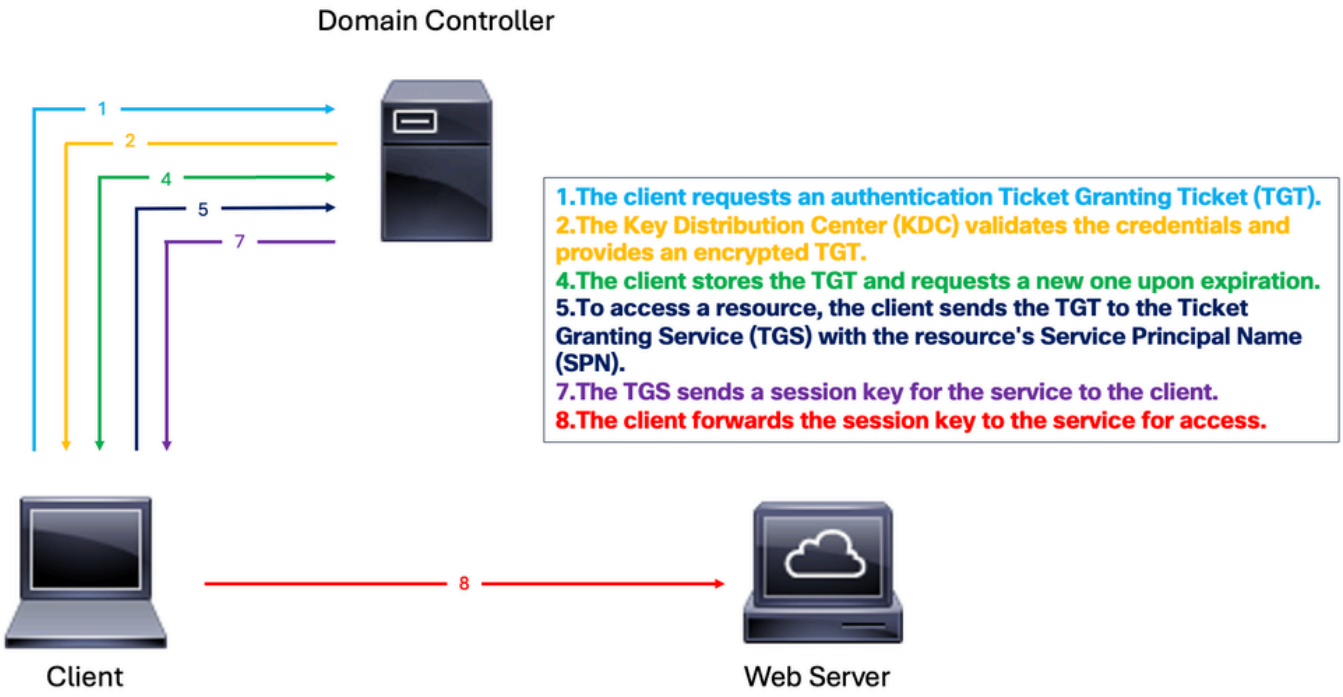
- Active Directory和Kerberos身份驗證。
- SWA上的身份驗證和領域。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

Kerberos網路流程



影象：Kerberos流示例

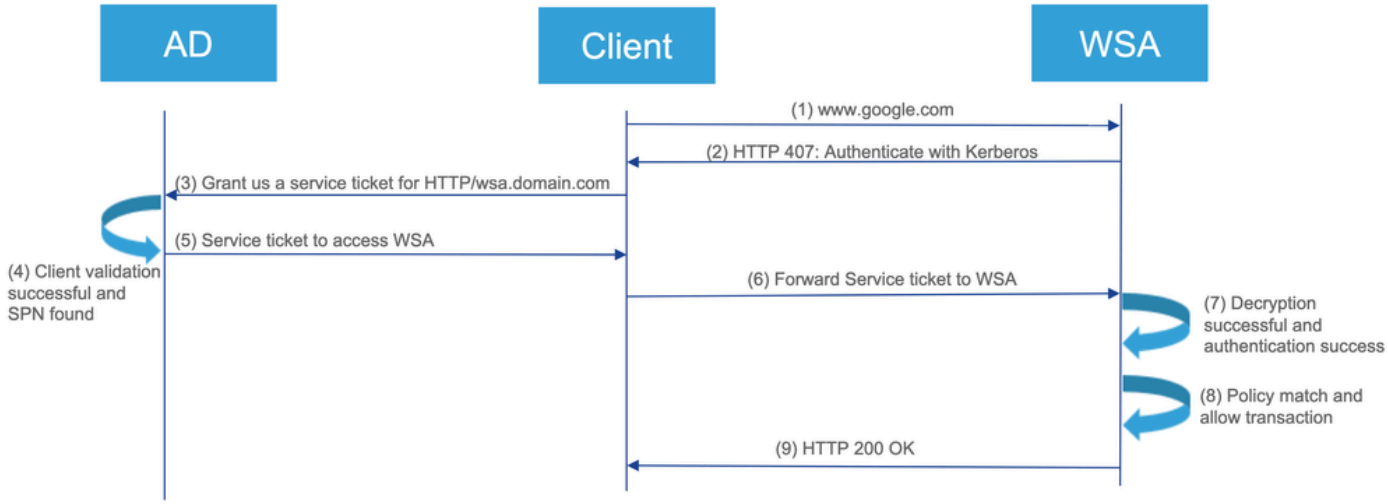
下面是在Kerberized環境中進行身份驗證的基本步驟：

1. 客戶端向金鑰分發中心(KDC)請求票證授予票證(TGT)。
2. KDC驗證客戶端電腦使用者憑證，並傳送回加密的TGT和會話金鑰。
3. TGT使用票證授權服務(TGS)金鑰加密。
4. 客戶端儲存TGT並在到期時自動請求新一個TGT。

要訪問服務或資源，請執行以下操作：
1.客戶端將TGT與所需資源的服務主體名稱(SPN)一起傳送到TGS。
2. KDC驗證TGT並檢查使用者客戶端電腦訪問許可權。

3. TGS向客戶端傳送服務特定的會話金鑰。
4.客戶端為服務提供會話金鑰以證明訪問，並且服務授予訪問許可權。

SWA中的Kerberos驗證流



1. 客戶端請求通過SWA訪問www.google.com。
2. SWA以「HTTP 407」狀態響應，要求進行身份驗證。
3. 客戶端使用加入域時獲得的TGT從AD伺服器為HTTP/SWA.domain.com服務請求服務票證。
4. AD伺服器驗證客戶端並發出服務票證，如果成功，並且找到SWA的SPN（服務主體名稱），則繼續執行下一步。
5. 客戶端將此票證傳送到SWA。
6. SWA解密票證並檢查身份驗證。
7. 如果身份驗證成功，SWA將驗證策略。
8. 如果允許事務，SWA會向客戶端傳送「HTTP 200/OK」響應。

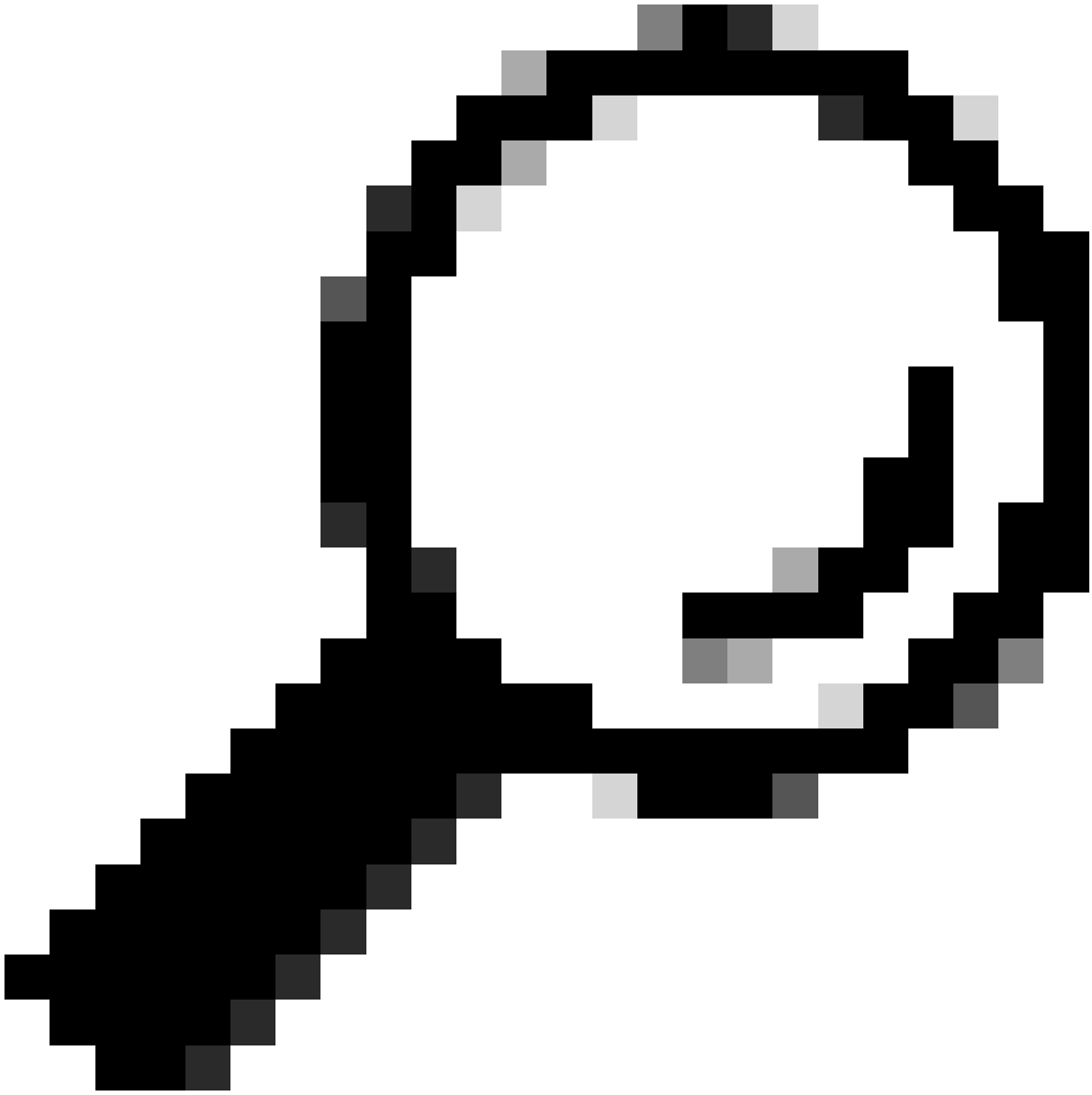
SPN的作用是什麼？

服務主體名稱(SPN)唯一標識Kerberos身份驗證中的服務例項。它將服務例項連結到服務帳戶，使客戶端無需帳戶名稱即可請求對服務的身份驗證。金鑰分發中心(KDC)實施中的每個帳戶（如AD或Open LDAP）都有一個SPN。雖然SPN嚴格標識服務，但在服務也充當客戶端的場景中，有時會錯誤地使用它來引用客戶端名稱(UPN)。

在Kerberos中，服務主體名稱(SPN)唯一地標識網路中的服務例項。它允許客戶端請求特定服務的身份驗證。SPN將服務例項連結到其帳戶，使Kerberos能夠正確驗證和授權對該服務的訪問請求。

Active Directory伺服器配置

1. 建立新使用者帳戶或選擇要使用的現有使用者帳戶。
2. 註冊要用於所選使用者帳戶的SPN。
3. 確保未註冊重複的SPN。



提示：Kerberos與SWA在負載平衡器或流量管理器/流量整形器之後有何不同？不是將HA虛擬主機名的SPN與使用者帳戶相關聯，而是將HTTP流量重定向裝置的SPN相關聯(例如：LoadBalancer或Traffic Manager)。

可以找到實施Kerberos的最佳實踐：

- 安全網路裝置最佳實踐
- 為SWA連線配置防火牆埠

疑難排解

使用SPN命令排除Kerberos故障

以下是在Kerberos環境中管理服務主體名稱(SPN)的有用命令setspn的清單。這些命令通常在Windows環境中使用管理許可權從命令列介面運行。

列出特定帳戶的SPN:	setspn -L <使用者/電腦帳戶名> 列出為指定帳戶註冊的所有SPN。
向帳戶新增SPN:	setspn -A <SPN> <使用者/電腦帳戶名> 將指定的SPN新增到給定帳戶。
從帳戶中刪除SPN:	setspn -D <SPN> <使用者/電腦帳戶名> 從給定帳戶中刪除指定的SPN。
驗證SPN是否已註冊：	setspn -Q <SPN> 檢查指定的SPN是否已在域中註冊。
列出域中的所有SPN	setspn -L <使用者/電腦帳戶> 列出域中的所有SPN。
為電腦帳戶設定SPN:	setspn -S <SPN> <使用者/電腦帳戶名> 向電腦帳戶新增SPN，確保沒有重複的條目。
重置特定帳戶的SPN:	setspn -R <使用者/電腦帳戶名> 重置指定帳戶的SPN，有助於解決重複的SPN問題。

SPN命令和輸出的示例

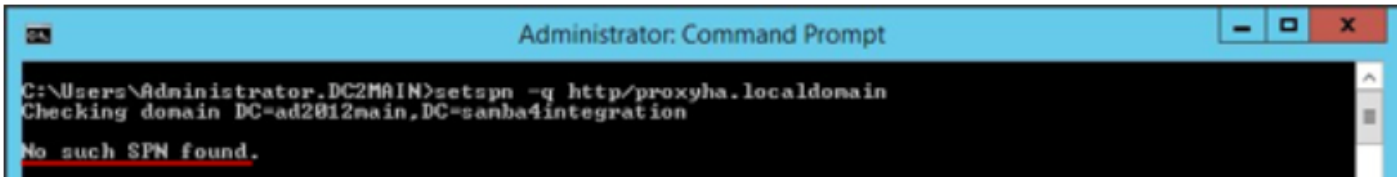
提供的示例演示了以下用途：

- 使用者/電腦帳戶：vrpserviceuser
- SPN:http/WsaHostname.com或http/proxyha.localdomain

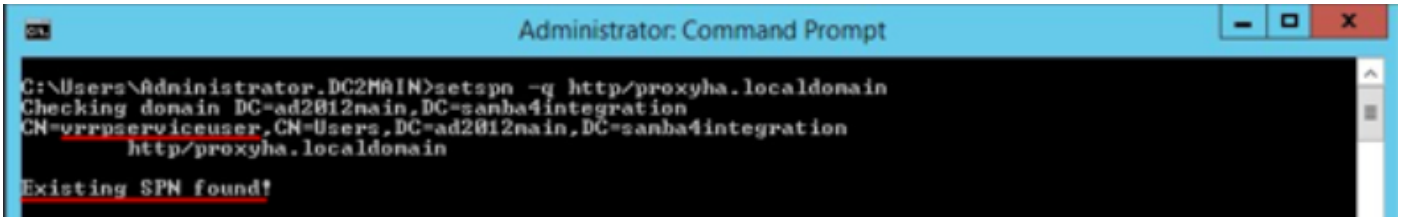
檢查SPN是否已與使用者帳戶關聯：
setspn -q <SPN>

setspn -q http/proxyha.localdomain

案例 1:未找到SPN



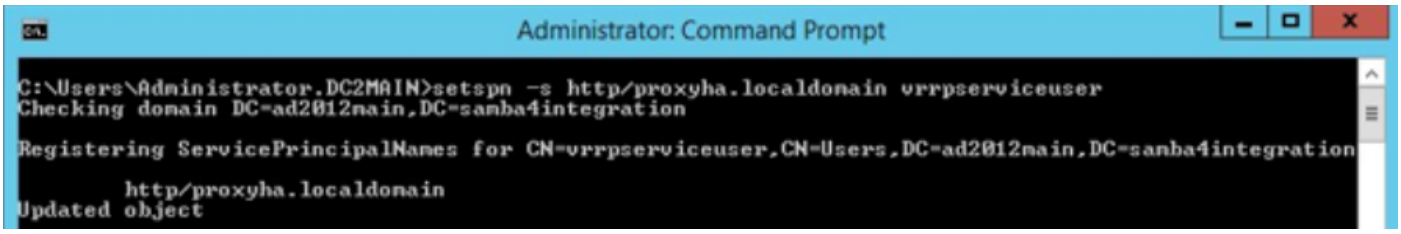
案例 2:已找到SPN



- 將SPN與有效的使用者/電腦帳戶關聯：

語法:setspn -s <SPN> <使用者/電腦帳戶>

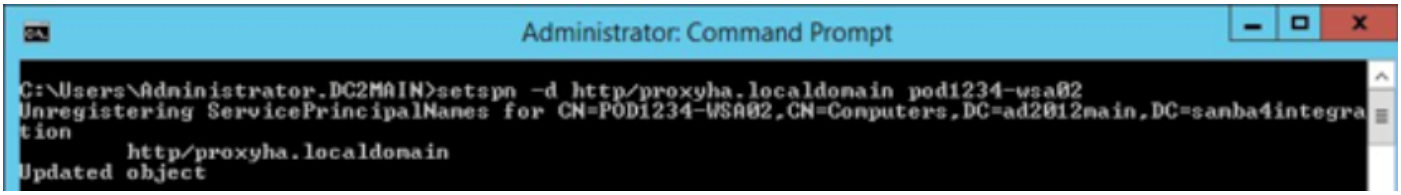
舉例來說：setspn -s http/proxyha.localdomain vrpserviceuser



- 刪除/刪除已與使用者或電腦帳戶關聯的SPN:

語法:setspn -d <SPN> <使用者/電腦帳戶>

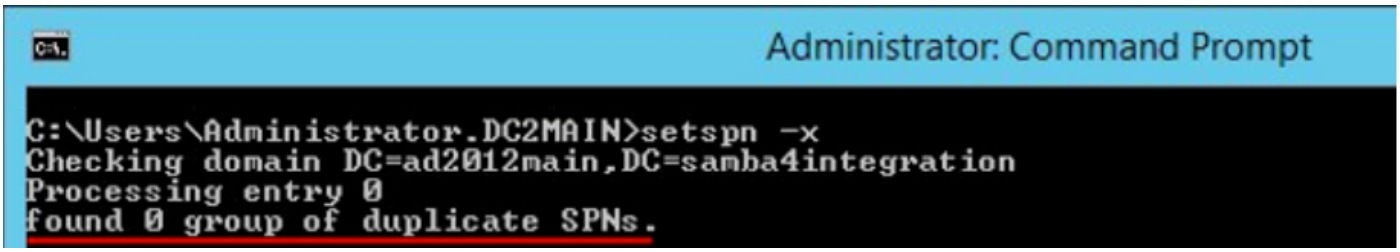
舉例來說：setspn -d http/proxyha.localdomain pod1234-wsa0

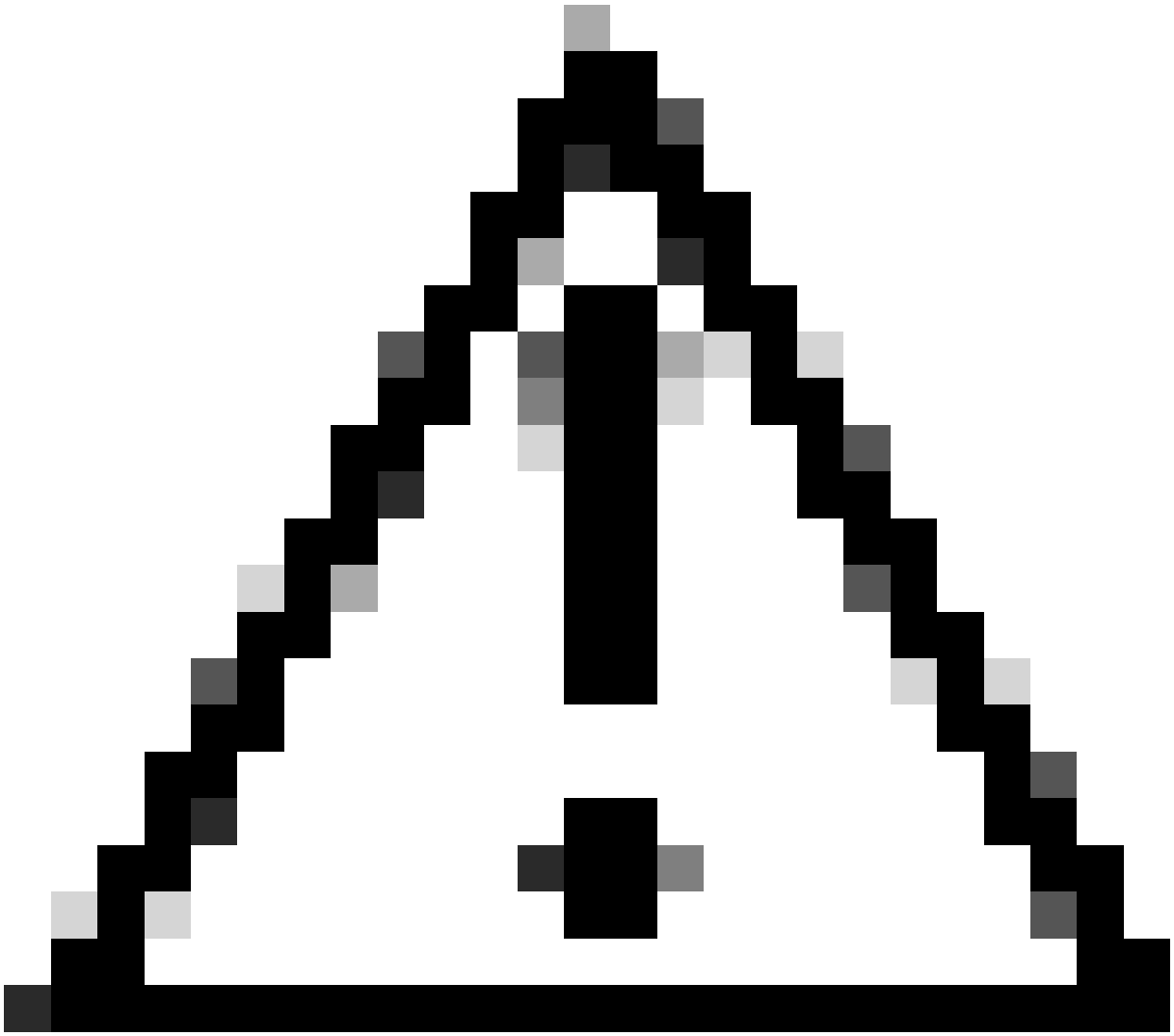


確保HA虛擬主機名沒有重複的SPN，因為以後可能會發生故障。

- 要使用的命令：setspn -x

因此，未向客戶端提供Kerberos服務票證，並且Kerberos身份驗證失敗。



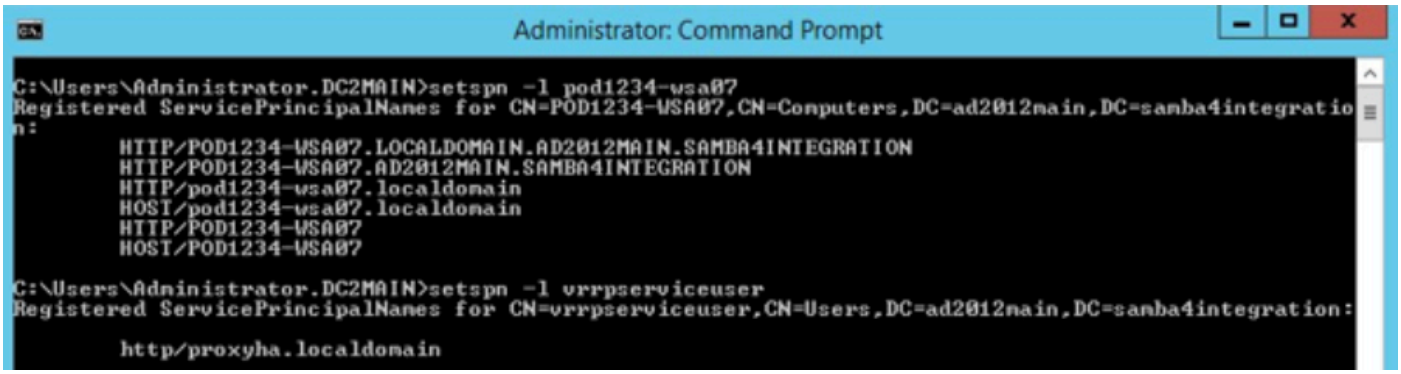


注意：如果找到重複項，請使用setspn -d命令刪除重複項。

- 列出與帳戶關聯的所有SPN:

語法:setspn -l <使用者/電腦帳戶>

舉例來說：setspn -l vrpserviceuser



疑難排解SWA上的Kerberos

疑難排解Kerberos驗證問題時，思科支援需要獲取資訊：

- 當前配置詳細資訊。
- 身份驗證日誌（最好在調試或跟蹤模式下）。
- 已進行的資料包捕獲（使用適當的過濾器）：

  (a)客戶裝置

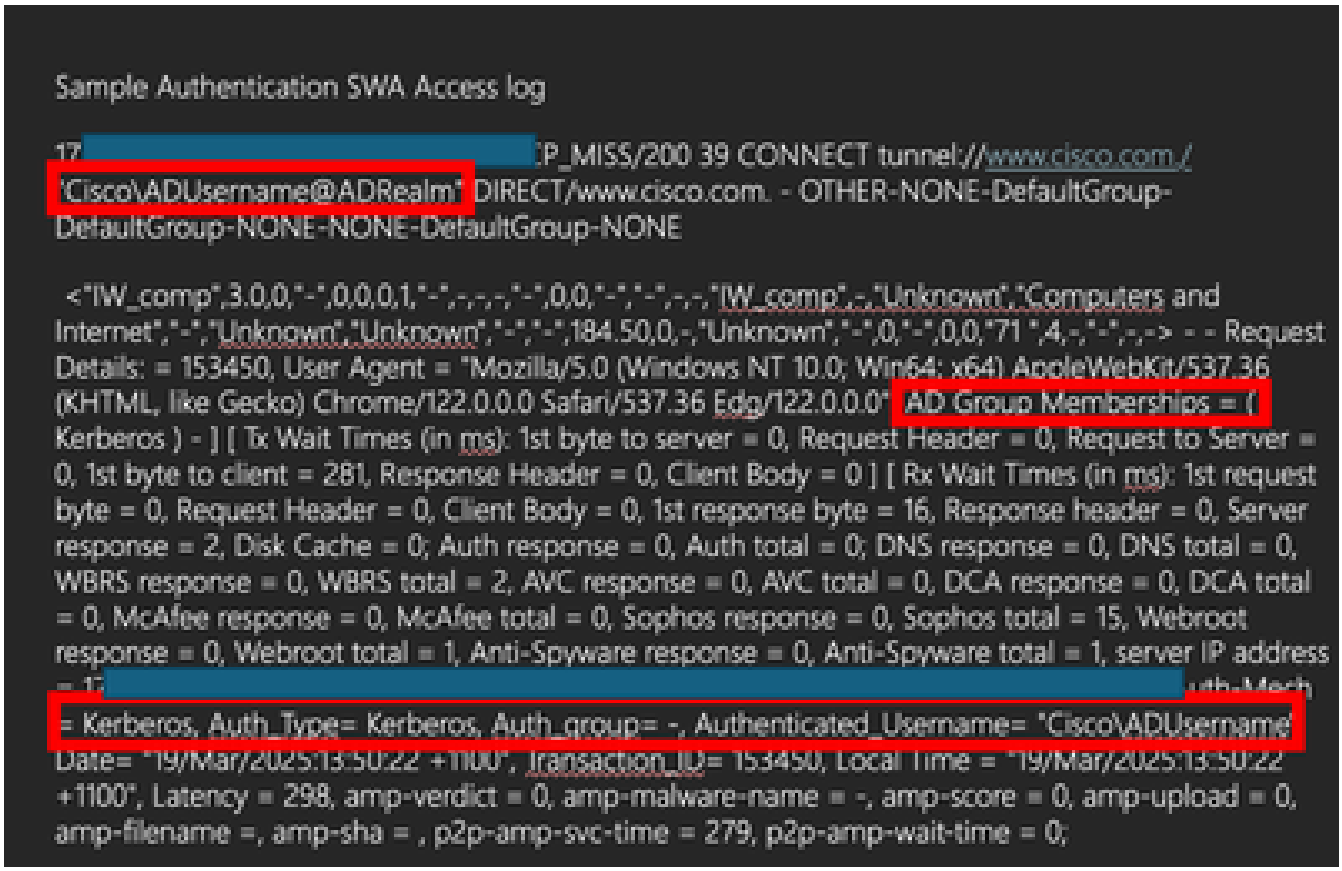
  (b)全部門性做法

- 已啟用%m自定義格式說明符的訪問日誌。這必須顯示用於特定事務的身份驗證機制。
- 有關詳細的身份驗證詳細資訊，請將這些自定義欄位新增到正在工作/正在工作的代理上的訪問日誌中，以獲取詳細資訊，或參閱超連結在訪問日誌中新增引數。
- 在SWA GUI中，導航到系統管理>日誌訂閱>訪問日誌>自定義欄位>新增此字串以解決身份驗證問題：

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

    a;
```

- 使用者身份驗證詳細資訊的SWA訪問日誌。
- Cisco SWA以Domain\username@authentication_realm格式記錄經過身份驗證的使用者名稱：



- 從GUI運行測試身份驗證領域設定。導航到Network > Authentication，然後在Test Current Settings部分中按一下領域的名稱。按一下Start Test。

在Kerberos資料庫中找不到伺服器

一個常見的錯誤情況是Web請求失敗，出現「Server not found in Kerberos database」（在Kerberos資料庫中找不到伺服器）：

```
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!
```

在這種情況下，錯誤表示與代理地址值proxyha.local對應的服務主體名稱未在Active Directory伺服器上註冊。要解決此問題，需要確認SPN http/proxyha.local已在AD DC上註冊並新增到正確的服務帳戶。

其他資訊和參考

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。