當客戶端使用NEGOEXTS時，身份驗證通過WSA失敗

目錄

簡介

本檔案介紹當使用者端使用NEGOEXTS時，如何透過思科網路安全裝置(WSA)驗證失敗時克服問題。

背景資訊

思科網路安全裝置(WSA)可以對使用者進行身份驗證，以根據使用者或組應用策略。可用的方法之一是Kerberos。在身份中使用Kerberos作為身份驗證方法時，WSA會使用401（透明）或407（顯式）HTTP響應來回覆客戶端的HTTP請求，該響應包含標頭**WWW-Authenticate:協商**。此時，客戶端傳送一個具有授權的新HTTP**請求：協商**報頭，其中包含通用安全服務應用程式介面(GSS-API)和簡單保護協商(SPNEGO)協定。在SPNEGO下，使用者顯示其支援的**mechTypes**。以下是WSA支援的mechTypes:

- KRB5 — 如果客戶端上支援Kerberos且配置正確，並且對於正在訪問的服務存在有效的Kerberos票證，則使用Kerberos身份驗證方法
- NTLMSSP — 在沒有有效的Kerberos票證但支援協商身份驗證方法的情況下使用的Microsoft NTLM安全支援提供程式方法

問題：當客戶端使用NEGOEXTS時，身份驗證通過WSA失敗

在較新版本的Microsoft Windows中，支援稱為NegoExts的新身份驗證方法，它是協商身份驗證協定的擴展。此mechType被認為比NTLMSSP更安全，並且當僅支援的方法是NEGOEXTS和NTLMSSP時，客戶端會首選此方法。欲知更多資訊，請訪問以下連結：

[Negotiate Authentication Package的擴展簡介](#)

此案例通常在選擇了Negotiate auth方法但沒有KRB5 mechType（最可能的原因是WSA服務缺少有效的Kerberos票證）的情況下發生。 如果客戶端選擇NEGOEXTS（在wireshark中可能顯示為NEGOEX），則WSA無法處理身份驗證事務，並且客戶端的身份驗證失敗。發生這種情況時，身份驗證日誌中會顯示以下日誌：

```
14 Nov 2016 16:06:20 (GMT -0500) Warning: PROX_AUTH : 123858 : [DOMAIN]Failed to parse NTLMSSP packet, could not extract NTLMSSP command14 Nov 2016 16:06:20 (GMT -0500) Info: PROX_AUTH : 123858 : [DOMAIN][000] 4E 45 47 4F 45 58 54 53 00 00 00 00 00 00 00 00 NEGOEXTS ........
```

身份驗證失敗時，會發生以下情況：

如果啟用了訪客許可權 — 客戶端被分類為**Unauthenticated**，並重定向到網站

如果禁用訪客許可權 — 客戶端將呈現另一個401或407（取決於代理方法），其餘身份驗證方法將顯示在響應報頭中（協商不會再次顯示）。 如果配置了NTLMSSP和/或基本身份驗證，則可能會出現身份驗證提示。如果沒有其他身份驗證方法（僅針對Kerberos配置身份），則身份驗證會失敗。

解決方案

此問題的解決方法是從身份中刪除Kerberos身份驗證，或者修復客戶端，使其獲得適用於WSA服務的有效Kerberos票證。