当客户端使用NEGOEXTS时， Auth通过WSA失效

Contents

[Introduction](#)
[背景信息](#)
[问题：当客户端使用NEGOEXTS时， Auth通过WSA失效](#)
[解决方案](#)

Introduction

本文如何描述对overocme问题，当Auth通过Cisco Web安全工具时(WSA)失效，当客户端使用NEGOEXTS时。

背景信息

Cisco Web安全工具(WSA)能验证用户运用根据用户或组的策略。是可用的其中一个方法是Kerberos。当使用Kerberos作为认证方法在身份时， WSA回复客户端的与401的HTTP请求(透明)或407 (包含报头的明确) HTTP回应WWW**验证：协商**。 这时，客户端发送与**授权的**一个新的HTTP请求：**协商**报头，包含通用的安全性服务应用程序结口(GSS-API)和简单的保护的协商(SPNEGO)协议。在SPNEGO下，用户提交支持的**mechTypes**。这些是WSA支持的mechTypes ：

- KRB5- Kerberos使用的auth方法，如果客户端正确支持Kerberos并且被配置，并且，如果是存在被获取的一张有效Kerberos票为服务
- NTLMSSP- Microsoft NTLM安全使用的支持提供程序方法，如果有效Kerberos票不是可用的，然而协商auth方法支持

问题：当客户端使用NEGOEXTS时， Auth通过WSA失效

在微软视窗中更多最新版本，支持一个新的auth方法呼叫NegoExts，是扩展名对协商认证协议。当唯一的支持的方法是NEGOEXTS和NTLMSSP时，此mechType比NTLMSSP被认为安全和由客户端更喜欢。更多信息可以在此链路找到：

引入对协商认证程序包的扩展

此方案典型地发生，当协商auth方法选择时，并且没有KRB5 mechType (很可能由于想念WSA服务的一张有效Kerberos票)。如果客户端选择NEGOEXTS (可以被看到作为在wireshark的NEGOEX)，则WSA unabled处理auth处理，并且auth为客户端失效。当这发生时，这些日志在auth日志被看到：

```
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 ........
```

当auth发生故障时，这发生：

如果客户权限是启用的-客户端分类为**未经鉴定**并且重定向到网站

如果客户权限是失效的-客户端看到另外401或407 (根据代理方法)与在响应标题出席的剩余的auth方法(再没有提交Negotiate)。如果配置， auth提示可能发生NTLMSSP和基本的auth。如果没有其他auth方法(身份为Kerberos仅被配置)，则auth发生故障。

解决方案

对此问题的解决方案对或者从身份取消Kerberos auth -或修理客户端，以便得到WSA服务的一张有效Kerberos票。