Auth は WSA によってクライアントが NEGOEXTS を使用するとき失敗します

目次

概要

この資料は overocme にクライアントが NEGOEXTS を使用するとき Auth が Cisco Web セキュリティ アプライアンス（WSA）を通って失敗するときどのように問題を記述したものです。

背景説明

Cisco Web セキュリティ アプライアンス（WSA）はユーザかグループに基づいてポリシーを適用するためにユーザを認証できます。 利用可能の方式の 1 つはケルベロスです。 ケルベロスを識別で認証方式として使用するとき、WSA はヘッダが含まれている 401 のクライアントの HTTP 要求に答えます（透過的な）または 407 （明示的な） HTTP応答は Www **認証します: ネゴシエートして下さい**。 この時点で、クライアントは**許可**の新しい HTTP 要求を送信 します: 一般的 な セキュリティ サービス適用業務プログラム インターフェース（GSS-API）および簡単な保護されたネゴシエーション（SPNEGO）プロトコルが含まれているヘッダを**ネゴシエートして下さい**。 SPNEGO の下で、ユーザはサポートする **mechTypes を**示します。 これらは WSA がサポートする mechTypes です:

- KRB5- 使用するケルベロス auth 方式はケルベロスがクライアントで、そしてアクセスされる有効な Kerberosチケット サービスのために正しくサポートされ、設定されればあれば
- NTLMSSP-方式が auth 方式を使用する Microsoft NTLM セキュリティ サポート プロバイダは有効な Kerberosチケットが利用できないが、ネゴシエートするサポートされます

問題： Auth は WSA によってクライアントが NEGOEXTS を使用するとき失敗します

Microsoft Windows のより多くの最近のバージョンでは、新しい auth 方式は呼出しましたネゴシエート認証プロトコルへ拡張である NegoExts をサポートされます。 この mechType は唯一のサポートされた方法が NEGOEXTS および NTLMSSP 時 NTLMSSP よりセキュアと考慮され、クライアントによって好まれます。 詳細はこのリンクで見つけることができます:

[ネゴシエート認証パッケージへの拡張の概要](#)

このシナリオは一般的にネゴシエート auth 方式が選択され、KRB5 mechType がないとき実行されます（多分 WSA サービスのための有効な Kerberosチケットが抜けていることによる）。 クライアントが NEGOEXTS を（wireshark の NEGOEX として見られるかもしれないです）選択すれば、auth トランザクションを処理するために WSA は unabled、auth はクライアントのために失

敗します。 これが発生するとき、これらの口グは auth 口グで表示されます:

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

auth が失敗するとき、これは発生します:

ゲスト特権がイネーブルになっていれば-クライアントは**非認証**として分類され、Webサイトにリダイレクトされます

ゲスト特権が無効なら-クライアントは応答 ヘッダーで示される残りの auth 方式とのもう 401 か 407 と（プロキシ方式によって）示されます（Negotiate 再度示されません）。 auth プロンプトは NTLMSSP や基本的な auth が設定される場合可能性が高いです発生する。 他の auth 方式が（識別はケルベロスのためにだけ設定されます）なければ、auth は単に失敗します。

解決策

この問題へのソリューションは識別から WSA サービスのための有効な Kerberosチケットを入手するようにに取除きましたりケルベロス auth を-または修復しますクライアントをあります。