

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

[はじめに](#)

[背景説明](#)

[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](#)

[解決策](#)

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) はユーザが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せん。利用可能のメソッドの 1 つは Kerberos です。Kerberos を識別で認証方式として使用するとき、WSA はヘッダ WWW 認証するが含まれている 401 (透過的な) または 407 (明示的な) HTTP 応答のクライアントの HTTP 要求に答えます: 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:

- Kerberos 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、設定されれば使用する KRB5- Kerberos auth 方式があれば
- 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機能の概要](#)

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 Kerberos 有効な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

