マシン アクセス制限の長所と短所

目次

概要

この資料はマシン アクセス制限（3 月）と直面する問題を記述し問題にソリューションを提供したものです。

個人的所有のデバイスの増加で、システム アドミニストレータがネットワークのある特定の一部へのアクセスを制限する団体所有のアセットだけに方法を提供することは重要ことです。 このに説明がある問題資料問題安全にこれらの関心領域を識別しユーザ接続性に中断なしで認証する方法を。

前提条件

要件

Cisco は十分にこの資料を理解するために 802.1X のナレッジがあることを推奨します。 この資料はユーザ 802.1X 認証を用いる習熟度を仮定し、3 月の使用に、およびもっと一般に結ばれる問題および長所をマシン 認証強調表示します。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

問題

3 月は基本的に現在および普及した Extensible Authentication Protocol （EAP）方式のほとんどで固有よくある問題を解決するように試みます即ちそのマシン 認証およびユーザ認証は別々、無関係なプロセスです。

ユーザ認証はほとんどのシステム アドミニストレータに詳しの 802.1X 認証方式です。 概念は信任状のセットが物理的な人を（表すこと信任状（username/password）が各ユーザに与えられる、および何人か個人の間で）同様に共有することができますことです。 従って、ユーザはそれらの信任状が付いているどこでもネットワークからのログインできます。

マシン認証は技術的に同じですが、ユーザは一般的に信任状プロンプト表示されません（または証明書を）入力するために; コンピュータかマシンはそれを単独でします。 これはマシンが既に保存される信任状を備えるように要求します。 送信 される ユーザ名はマシンが <MyPCHostname を > ホスト名として設定されて備えていれば、**host/<MyPCHostname>** です。 すなわち、それはホスト名に先行している**ホストを**送信 します。

Microsoft Windows および Cisco アクティブ ディレクトリに直接関連していなくてが、このプロセスはマシンがアクティブ ディレクトリにのでコンピュータ ホスト名加入される場合より簡単にされます-ドメイン データベースに追加され、信任状は（30 日毎に）デフォルトで更新しましたネゴシエートされ、マシンで保存されます。 これはマシンがアクティブ ディレクトリに加入される、信任状はユーザからの非表示をとどまります場合マシン 認証がデバイスのあらゆる型から可能性のあるであるが、大いにより簡単におよび透過的にされことを意味します。

ソリューションとして 3 月

これが設定されている前にソリューションが 3 月を完了する Cisco アクセスコントロールシステム （ACS）か Cisco Identity Services Engine （ISE）のためであるが考慮するべき長所および欠点がありますと言うことは容易です。 方法これを設定する ACS または ISE ユーザガイドに説明がある推奨ですそれおよびいくつかの可能性のある障害物を考慮するために従ってこの資料はかどうか単に記述します。

賛成論

3 月はユーザおよびマシン 認証が全く別途であるので発明されました。 従って、RADIUSサーバはユーザが会社所有のデバイスからのログインなる確認を実施できません。 3 月によって、RADIUSサーバは、特定のユーザー認証のために、（Cisco 側の ACS か ISE、）X 時間（一般的に 8 時間、しかし必要があること同じエンド ポイントのためのユーザ認証に先行するこれに有効なマシン 認証があるです設定可能実施します）。

従って、マシン 認証はマシンがドメインに加入される、RADIUSサーバはドメインへの接続とこれを確認します場合マシン信任状が RADIUSサーバによって知られていれば、一般的に成功し。 それは正常なマシン 認証がネットワークにフルアクセスを提供した、または制限された アクセスだけ完全にありますかどうか確認するネットワーク管理者まで; 一般的に、これはクライアントとアクティブ ディレクトリの間で少なくともクライアントがユーザパスワードまたはダウンロードグループ ポリシー オブジェクト（GPOs）の更新のような操作を行うことができるように接続を開きます。

ユーザ認証がマシン 認証が時間の前のカップルで行われなかったデバイスから来れば、ユーザはユーザが普通有効でも、否定されます。

フルアクセスはユーザに認証がマシン 認証が時間の過去カップルで行われたエンド ポイントから有効、完了されて場合その時だけ許可されます。

反対論

このセクションは 3 月使用の反対論を記述します。

3 月および Microsoft Windows 要求元

3 月の後ろの概念は成功するユーザ認証のためユーザに有効な信任状がある、正常なマシン 認証はそのクライアントから同様に記録 する必要がありますことそれだけでなく、なりますです。 そのに問題がある場合、ユーザは認証を受けることができません。 起こる問題はこの機能がロックアウト ネットワークへのアクセスを取り戻すためにクライアントをリブートさせる正規のクライアント時々不注意にできることことです。

Microsoft Windows はブート時でだけ (Login 画面が現われるとき) マシン認証を行います; ユーザがユーザーの資格情報を入力するとすぐ、ユーザ認証は実行された。 またユーザが (Login 画面へのリターン) ログオフすれば、新しいマシン認証は実行された。

3 月が時々問題をなぜ引き起こすか示すシナリオ例はここにあります:

ユーザは無線接続によって接続された彼のラップトップで X 1 日中機能していました。 結局は、彼はラップトップを単に閉じ、リーフははたらきます。 これは冬眠にラップトップを置きます。 翌日、彼はオフィスにもどって来、彼のラップトップを開きます。 この場合、彼は無線接続を確立することができません。

Microsoft Windows が冬眠するとき、だれがの口グオンされたかコンテキストを含む現在のステートのシステムのスナップショットを奪取 します。 夜通し、ユーザ ラップトップのための 3 月キャッシュされたエントリは切れ、削除されます。 ただし、ラップトップは動力を与えられるとき、マシン 認証を行いません。 それはユーザ認証に代りにそれが冬眠が記録したものだったので、まっすぐに入ります。 これを解決する唯一の方法はユーザを記録するか、または彼のコンピュータをリブートすることです。

3 月はよい機能であるが、ネットワーク不通を引き起こす可能性があります。 これらの中断は方法 3 月ははたらくことを理解するまで解決しにくいです; 3 月を設定するとききちんと毎日の終わりに各マシンからのコンピュータおよびログオフをシャットダウンする、方法についてのエンドユーザを教育することは重要です。

3 月およびさまざまな RADIUSサーバ

それはよくあります負荷バランシングおよび冗長性の目的でネットワークの複数の RADIUSサーバがあるために。 ただし、すべての RADIUSサーバが共用 3 月セッション キャッシュをサポートしません。 ノード間の ACS バージョン 5.4 および それ 以降および ISE バージョン 2.2 およびそれ 以降サポート 3 月キャッシュ同期だけ。 これらのバージョンの前に、それらが互いに対応しないのでマシン 認証を 1 つの ACS/ISE サーバに対して行い、別のものに対してユーザ認証を行うことはできません。

3 月および配線ワイヤレス切り替え

多くの RADIUSサーバの 3 月キャッシュは MAC アドレスに頼ります。 それは最後の正常なマシン 認証のラップトップおよびタイムスタンプの MAC アドレスの表単にです。 こうすればは、サーバ クライアントが最後の X 時間に認証されたマシンだったかどうか確認する場合があります。

ただし有線接続のラップトップを (従って配線された MAC からのマシン 認証は) 起動し、次に

ワイヤレスに日中切り替えれば、何が起こりますか。 RADIUSサーバにワイヤレス MAC アドレスを配線された MAC アドレスに関連させ、過去 X 時間に認証されたマシンだったことを確認する手段 (方法) がありません。 唯一の方法はワイヤレスでの Microsoft Windows 行ないを別のマシン認証ログオフし、持つことです。

解決策

多くのその他の機能の間で、Cisco AnyConnect にマシンおよびユーザ認証を誘発する前もって構成されたプロファイルの長所があります。 ただし、Microsoft Windows 要求元と見られると同じ制限は発生するただマシン認証に関してログオフするか、またはリブートするとき、見つけられます。

また、AnyConnect バージョン 3.1 および それ 以降と、EAP チェイニングと EAP-FAST 行うことも可能性のあるです。 これは基本的に信任状、マシン username/password およびユーザ username/password の 2 つのペアを送信 する同時に単一認証です。 ISE は、従って、より簡単に両方とも正常であることを確認します。 使用されるキャッシュおよび前のセッションを取得する必要無しでこれはより大きい信頼性を示しません。

PC が起動するとき、AnyConnect はユーザ情報が利用できないので、マシン 認証だけを送信 します。 ただし、ユーザ ログインに、AnyConnect はマシンおよびユーザ credentails を両方同時に送信 します。 また切断されるようになるか、またはプラグを抜いたり/、ケーブルを、マシンおよびユーザーの資格情報両方再度送信 されます EAP チェイニングなしで AnyConnect の以前のバージョンと異なる単一 EAP-FAST な 認証で再接続して下さい。

EAP-TEAP はこれらの認証の型をサポートすることを特になすが EAP-TEAP はまだこの日現在に多くののネイティブ要求元で OS サポートされませんので長期最もよいソリューションです