

# 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[ソリューションとして 3 月](#)

[賛成論](#)

[反対論](#)

[3 月および Microsoft Windows サプリカント](#)

[3 月およびさまざまな RADIUS サーバ](#)

[3 月および配線ワイヤレス 切り替え](#)

[解決策](#)

## 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団体所有のアセットだけにネットワークのある特定の一部にアクセスを制限する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。

このドキュメントの情報は、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、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 問題

3月には基本的に電流および普及した Extensible Authentication Protocol (EAP) メソッド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。概念は資格情報のセットが物理的な人を (表すこと資格情報 (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、ユーザはそれらの資格情報との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 資格情報プロンプト表示されません (または認証を) 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資格情報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も、このプロセスはマシンがアクティブ ディレクトリにのてコンピュータ 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、資格情報は (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、資格情報はユーザからの非表示をとどめます場合マシン 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 資格情報が 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 サブリカント

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資格情報がある、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。それに問題がある場合、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 ネットワークに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当な クライアント時々不注意にできることことです。

Microsoft Windows はブート時にだけ ( 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、だれかのロ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ロード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。ACS バージョン 5.4 および それ 以降 サポートだけ傷つきます。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 ACS 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。それはラップトップの MAC アドレスおよび最後の正常なマシン認証のタイムスタンプの表単にです。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引き起こす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 サブリカント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、またはリポートするとき、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 チェーニングと EAP-FAST 行うことも可能性のあるです。これは基本的に資格情報、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すばらし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 credentials 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 チェーニングなしで 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。