マシン アクセス制限の長所と短所ページ

目次

概要

このドキュメントでは、Machine Access Restriction（MAR）で発生する問題について説明し、この問題の解決策を提供します。

個人所有のデバイスが増加するなか、システム管理者にとって、ネットワークの特定の部部分へのアクセスを企業所有のアセットだけに制限することがますます重要になってきています。 このドキュメントで説明する問題は、このような問題領域を確実に特定し、ユーザ接続性に混乱を与えることなく認証を行う方法に関連してきます。

前提条件

要件

このドキュメントを完全に理解するためには、読者に 802.1x の知識があることが推奨されます。このドキュメントでは、読者にユーザ 802.1x 認証の知識があることを前提に、MAR の使用あるいはより広い意味でのマシン認証に使用に伴う関連と利点を明らかにします。

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

MAR は基本的に、現在広く使われている Extensible Authentication Protocol（EAP）方式の大部分に伴う共通の問題を解決することを目的としています。その問題とは、マシン認証とユーザ認証が分離されていて、関連性のないプロセスになっていることです。

ユーザ認証は、ほとんどのシステム管理者にとって馴染み深い 802.1x 認証方式で行われます。その概念としては、各ユーザにクレデンシャル（ユーザ名/パスワード）を与え、そのクレデンシャル一式によって個人を表すというものです（クレデンシャルが複数のユーザで共有されることもあります）。したがって、これらのクレデンシャルを使用すれば、ユーザはどこからでもネットワークにログインできます。

技術に関して言うと、マシン認証もユーザ認証と同じですが、マシン認証ではユーザにクレデンシャルの入力は求められません。 クレデンシャル（または証明書）は、コンピュータまたはマシン自体から送信するするためです。 したがって、マシンにあらかじめ証明書が保管されている必要があります。 たとえば、マシンにホスト名として <MyPCHostname> が設定されている場合、送信されるユーザ名は **host/<MyPCHostname>** となります。 つまり、**host/** の後に続けてユーザ名を送信するということです。

Microsoft Windows と Cisco Active Directory に直接関連するわけではありませんが、マシンが Active Directory に参加しているとすれば、コンピュータのホスト名はドメイン データベースに追加され、クレデンシャルはネゴシエートされてマシン上に保管されるため（デフォルトでは 30 日ごとに更新されます）、このプロセスのほうが認証が容易になります。 つまり、マシン認証はあらゆるタイプのデバイスから行うことができますが、マシンが Active Directory に参加していれば認証がより簡単かつトランスペアレントになり、クレデンシャルがユーザから隠された状態になることを意味します。

解決策としての MAR

Cisco Access Control System（ACS）または Cisco Identity Services Engine（ISE）で解決策となるのは MAR を実施することであると言うのは簡単ですが、MAR を実装する前に検討しなければならない利点と欠点があります。 MAR を実装する方法は ACS または ISE ユーザ ガイドで適切に説明されているため、このドキュメントでは MAR の実装を検討すべきかどうか、そして考えられる問題についてのみ説明します。

利点

MAR が考案された理由は、ユーザ認証とマシン認証が完全に分離されていることにあります。ユーザ認証とマシン認証が分離されていると、ユーザが企業所有のデバイスからログインしなければならない場合には、RADIUS サーバが検証を強制できません。 MAR では、RADIUS サーバ（シスコ側では ACS または ISE）が特定のユーザ認証について、過去 X 時間（通常は 8 時間ですが、この時間は設定可能です）以内にマシン認証が成功しているという要件を強制できます。この要件は、同じエンドポイントに対するユーザ認証よりも優先されます。

したがって、マシン証明書が RADIUS サーバで既知であればマシン認証は成功します（通常、マシンがドメインに参加している場合は、RADIUS サーバはドメインへの接続でマシン証明書を検証します）。 マシン認証が成功した場合にネットワークへのフル アクセスを許可するか、あるいは制限されたアクセスだけを許可するかは、完全にネットワーク管理者の判断に任されます。 通常は、マシン認証の成功によってクライアントと Active Directory との間の接続が開くため、クライアントがユーザ パスワードの更新やグループ ポリシー オブジェクト（GPO）のダウンロードなどといったアクションを実行できるようになります。

過去数時間以内にマシン認証が行われていないデバイスからユーザ認証が行われた場合、通常は有効であるユーザであっても、そのユーザにはアクセスが拒否されます。

フル アクションがユーザに与えられるのは、認証が有効であり、過去数時間以内にマシン認証が行われたエンドポイントから行われている場合のみです。

欠点

ここでは、MAR の使用に伴う欠点について説明します。

MAR と Microsoft Windows サプリカント

MAR の背後にある概念は、ユーザ認証を成功させるためには、ユーザが有効なクレデンシャルを持っていることだけが要件となるだけでなく、そのクライアントからのマシン認証の成功がログに記録されていることも要件となるというものです。 これらの要件のいずれかに問題があると、ユーザの認証は失敗します。 MAR で問題になるのは、この機能によって正当なクライアントが意図せずにロックアウトされる可能性があることです。その場合、クライアントはネットワークへのアクセスを取り戻すために、リブートしなければならなくなります。

Microsoft Windows は、マシンの起動時（ログイン画面が表示された時点）にのみマシン認証を行います。 ユーザがユーザ クレデンシャルを入力すると同時に、ユーザ認証が行われます。 また、ユーザがログオフすると（ログイン画面に戻ると）、新しいマシン認証が行われます。

以下に、MAR によって問題が生じる場合がある理由を説明するシナリオ例を紹介します。

ユーザ X は終日、ワイヤレスで接続された自分のラップトップで作業しています。 仕事が終わった後、ユーザ X はラップトップを閉じて職場を後にしました。 これにより、ラップトップはハイバネーション モードになります。 翌日、ユーザ X が出社してラップトップを開くと、 ワイヤレス接続を確立できなくなっています。

Microsoft Windows はハイバーネーション モードに移る際に、現状のシステムのスナップショットを取ります。これには、誰がログインしていたかというコンテキストも含まれます。 MAR にキャッシュされたユーザ ラップトップのエントリは、夜間に有効期限が切れてパージされます。けれどもラップトップに電源が入っていると、マシン認証は行われません。 ハイバーネーションで記録された内容に従って、マシン認証の代わりにユーザ認証が行われます。 この問題を解決するには、ユーザをログオフするか、コンピュータをリブートするしか方法はありません。

MAR は優れた機能ですが、ネットワーク中断の原因となる可能性もあります。 MAR の仕組みを理解するまでは、MAR を原因とするネットワーク中断をトラブルシューティングするのは困難です。 MAR を実装する場合は、エンドユーザに勤務時間が終わったらコンピュータを適切にシャットダウンして、すべてのマシンからログオフするよう教育することが重要となります。

MAR と各種 RADIUS サーバ

ロード バランシングと冗長性のためにネットワーク内で複数 RADIUS サーバを使用するのはよくあることです。 けれども、すべての RADIUS サーバが共有 MAR セッション キャッシュをサポートしているわけではありません。 ACS バージョン 5.4 および それ 以降および ISE バージョン 2.3 および それ 以降 サポートだけノード間のキャッシュ 同期を傷つけます。 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/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。

MAR と有線/ワイヤレス間の切り替え

多くの RADIUS サーバの MAR キャッシュは、MAC アドレスに依存します。 MAR キャッシュは

、ラップトップの MAC アドレスとマシン認証に最後に成功した時点のタイムスタンプからなる単純なテーブルです。 このテーブルにより、サーバは過去 X 時間以内に特定のクライアントがマシン認証に成功したかどうかを把握できます。

けれども、ラップトップを有線接続で起動した後 (したがって、有線で接続された MAC からマシン認証が行われた後) 、その当日にワイヤレスに切り替えたとしたらどうなるでしょうか。 その場合、RADIUS サーバには、ワイヤレス MAC アドレスを有線 MAC アドレスに相関させて、過去 X 時間内にマシン認証が成功したかどうかを把握する手段はありません。 この問題の唯一の解決方法は、いったんログオフしてから、Microsoft Windows がワイヤレスで別のマシン認証を行うことです。

解決策

Cisco AnyConnect には多くの機能がありますが、とりわけ大きな利点として挙げられるのは、マシン認証とユーザ認証をトリガーするようプロファイルが事前に設定されていることです。 その一方、マシン認証が行われるのがログオフまたは再起動した場合のみであるという点で、Microsoft Windows サプリカントの場合と同じ制約事項があります。

また、AnyConnect バージョン 3.1 以降では、EAP チェーニングによる EAP-FAST を行えるようになっています。 これは基本的に、クレデンシャルの 2 つのペア (マシンのユーザ名/パスワードとユーザのユーザ名/パスワード) を同時に送信するというシングル認証です。 この場合、ISE では両方が認証に成功したことをチェックしやすくなります。 キャッシュは使用されず、前のセッションを取得する必要もないことから、この方法では信頼性が高くなります。

PC の起動時は、ユーザ情報がまだ使用できないため、AnyConnect はマシン認証のみを送信します。 ただし、ユーザがログインした時点で、AnyConnect はマシンとユーザ両方のクレデンシャルを同時に送信します。 さらに、接続が切断された場合や、ケーブルを抜いて再接続した場合、単一の EAP-FAST 認証でマシンとユーザのクレデンシャルが再度送信されます。これが、EAP チェーニングを使用しない前のバージョンの AnyConnect との違いです。

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 サプリカントで 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