

特権パスワードの安全な管理



あらゆるIT資産には、少なくとも1つのローカルの、特権ログインアカウントがあります。これにはワークステーション、サーバー、ネットワークデバイス、データベース、アプリケーション、およびその他が含まれます。また、資産の中には、サービスを実行するためのものや、1つのアプリケーションから他のアプリケーションを実行するために認証が必要な特権アカウントを持っているものもあります。

特権アカウントのパスワードは、ソフトをインストールしたり、デバイスを管理したり、技術的なサポートのために使用されます。システムの機能とデータに無制限にアクセスできる「全権」を持っていることもあります。その結果、事実上、特権パスワードの毀損は、デバイス全体への毀損となります。

特権パスワードの安全な管理はITセキュリティに不可欠です。このドキュメントは、事実上、多数の機密パスワードを効果的に管理するための技術的課題を特定し、ソリューションを示しています。

概要:ビジネス上の問題

多くの大企業では、何百にもわたるサーバーやワークステーションが常時作動しています。たいていの場合、一つの管理者共用パスワードが一定の設定情報を持つすべてのサーバー毎や一定のタイプのワークステーション毎に使われています。これはデータセンターや、クライアントサポートスタッフにとっては、とても都合がよく、メンテナンスやワークステーションの更新をしないといけない時は一つのパスワードさえ覚えておけばいいので、ログインも容易だからです。

このような、固定的なパスワードや、周知されてしまっている管理者用パスワードの利用は、オペレーション上や、セキュリティ上の問題を発生させることにもつながります。

- 管理者が複数のITスタッフと共用しているパスワードを使ってログインし、設定変更を行ったり、その他の情報にアクセスした際、トレースやログは残っていても、どのITスタッフが行ったのかまではわかりません。もし設定変更などによりシステムにエラーや機能不全が生じた場合、誰が起こした問題なのかがわかりません。
- 同じ管理者用IDやパスワードが多くのシステムに存在する場合、パスワード変更を実施するのは大変に手間がかかります。その結果、管理者用パスワードは変更されないまま同じのが使われ、既に退職した元社員でも知っているということになります。

これらの問題は、管理者パスワードが変更されないのでは、セキュリティの脆弱性の要因になり、そして、退職したIT担当者が在職期間を超えて持ち続けることとなります。これは内部統制上、明確な侵害となります。: 元従業員は、会社のシステムの管理アクセス権を持つべきではありません。

ほとんどの企業/組織では、堅固な内部管理は義務となっています。HIPAAやGLBなどのプライバシー保護法律、およびSOXなどのコーポレートガバナンスに関する法律では、極秘データを含むシステムが、不正アクセスに対して安全であることが必要とされています。したがって、特権パスワードの効果的な管理はオプションではなく、必要条件です。

簡単なソリューション:パスワードのランダムイズ

静的な共有特権パスワードを排除する当然の方法は、定期的にそれらを変えることです。あらゆる機密パスワードが毎日ランダムイズされるなら、制御の問題は軽減されるでしょう。

ITユーザが、頻繁に特権パスワードを使用する必要があるため、パスワードをランダムイズすることは、ソリューションの半分でしかありません。ITユーザがパスワードを変えることによってアクセス権を制御する追加機能が必要です。:

1. ITユーザが、頻繁に特権パスワードを使用する必要があるため、パスワードをランダムイズすることは、ソリューションの半分でしかありません。ITユーザがパスワードを変えることによってアクセス権を制御する追加機能が必要です:
2. ITユーザーがどのアカウントを、いつアクセスできるか、に関するアクセス制御
3. アカウントビリティを確立する当該アクセスを記録する監査ログ

基本的なアカウントに対し、多くのパスワードをランダムイズして、かつパスワード値のアクセスを制御するソリューションは、複雑になります。以下のセクションはそのようなソリューションを成功裡に展開するために解決しなければならない技術的課題について説明します。

技術的課題 / ソリューション要件

定期的に管理者証明書をランダム化して、記録しておく基本的なプロセスを説明するのは簡単ですが、そのようなプロセスを何千もの装置に対して、安全で、かつフェールセーフで行うのは大きな課題です。

以下の章では、そのようなシステムが扱わなければならない技術的課題について説明します。

プラットフォーム・サポート

どんなタイプのIT資産にも、ローカルの管理者パスワードがあります。まず、各デバイスをネットワークにつなげるのにローカルの管理者パスワードを使用しなければならないため、ネットワーク資格証明書がデバイスを管理するのにも使われるのは通常のやり方です。

管理者パスワードを管理するシステムは、有益であるためには、多くの範囲のプラットフォームをサポートすることが必要です。これには、ワークステーション、Windowsサーバー、Unixサーバー、ネットワークルータ、データベースサーバー、ERP アプリケーション、見ドレンジャーサーバー(iSeries、VMSなど)、メインフレーム・コンピュータ、ディレクトリ、その他が含まれます。つまり、機密データを持っていたり、そのオペレーションがビジネスに重要であるすべての機器がサポートされなければなりません。

ワークステーション: 設置場所と接続性

パスワード管理システムは、固定ネットワークアドレスを持ち、常時ネットワークに接続されているサービスとは容易に接続することができます。ところが、中央パスワード管理システムからの、ワークステーションへの接続は次の理由によりより困難となります。:

- ▶ ワークステーションがモバイル機器として用いられます。特にノートブックPCは、利用場所が頻繁に変わります。
- ▶ 一か所で使われていたとしても、DHCPの利用により、ワークステーションIPアドレスは、動的に変更されているかもしれません。
- ▶ ワークステーションは、頻繁に電源を切られることがあり、その場合、ネットワーク側からの問いかけに 응답しません。
- ▶ ワークステーションは、未使用期間に、ネットワークから取りはずされたり、移動されたりすることがあります。
- ▶ ワークステーションは、ファイアウォールで保護され、ワークステーションに対するインバウンド接続をブロックされる場合があります。

まとめると、ワークステーションから中央サーバーへの接続は簡単ですが、その逆は不可能に近いことがあるということです。

ワークステーションの上のローカルの管理者パスワードを安全にするためには、パスワード管理システムは、設置場所、接続性、アドレス、およびファイアウォールなどの課題を解決しなければなりません。

何百万もの資格証明への拡張性

大きな組織には、何千台ものワークステーション、サーバー、およびアプリケーションがあるかもしれません。それら各IT資産が毎日新しい管理者パスワードを得るなら、安全に管理しなければならないパスワードの総数は、履歴を含めるとすぐに何百万ものパスワードになってしまいます。

管理対象装置がクラッシュして、バックアップメディアから回復する場合、古いパスワードが必要となるので、パスワード履歴を現在のものと一緒に格納する必要があるのに注意してください。

管理者パスワードを管理するスケーラブルなソリューションでは、毎日何万ものパスワードをランダム化して、何百万ものパスワード履歴を恒久的に保持できなければなりません。

高信頼オペレーションと競合条件


管理者パスワードを管理する堅固なシステムは、特定の管理者アカウントのためにデータベース上に保持されているパスワードが、対象のシステム上のパスワードに合致していることを確実にしなければなりません。パスワード変更の試みが更新の途中に失敗しても、これは守られなければなりません。

例えば、パスワード管理システムがIT資産上に新しいパスワードを設定したときに、接続失敗となったら、実際には、新しいパスワードか古いパスワードのどちらが有効なのか明確でなくなります--このときデータベース上の格納値を更新すべきでしょうか？

管理者パスワードを管理する堅固なシステムでは、データベースに保存するパスワードがいつも正しいものであることを確実にしなければなりません。--パスワード更新の途中で事故が起こったとしてもです。

フォールトトレランス:ハードウェア、ネットワーク、施設上の問題

パスワードマネジメントシステムはフォールト・トレラントでなければなりません。もし、使えない状況が発生すると、IT従事者は業務ができなくなります--これは、システムに壊滅的な事故を引き起こしかねません。

"アプライアンス" (note) を含むハードウェアサーバーは、時に、ディスククラッシュ、電源障害等で障害を起こす場合があります。ネットワーク接続、特に広域接続では、時々切れる場合があります。また、データセンター全体が、停電や、地震、台風、竜巻や、洪水のために停止することもあります。

特権パスワード管理システムの1つが故障しても、それが管理するパスワードは利用可能でなければなりません。これは少なくとも2つのサーバーを、理論上異なったサイトで動作させることにより達成されます。つまり、1つのサーバーか1つのデータセンターがオフラインになっても、IT担当者は、パスワードを扱うことができ、担当業務を継続することができます。

サーバーとサイト間の耐障害性はサーバー間のデータ複製を必要とします。そのようなデータ複製はリアルタイムで行われなければなりません。代替手段 -- 予定時間起動のバッチ複製 -- では、不十分です。例えば動くバックアップ・システムが夜に動作することを考えてください。パスワード管理サーバーがバックアップサイクルが始まる直前ダウンしてしまったら、その日の新しいパスワードは失われてしまいます。毎日パスワードを変えるなら、ほとんどあらゆるシステムの現時点の管理者パスワードを失うという大惨事になります。

転送上、格納上の暗号化

特権パスワードの漏洩はビジネスリスクを意味します。多くの特権パスワードの漏洩は壊滅的なビジネスリスクを意味するかもしれません。そのため、特権パスワードを管理するシステムは暗号でこれらのパスワードを保護しなければなりません。記録のために格納されるときも、ユーザとそれ自身の間や、複製サーバーや、管理対象装置とそれ自身の間で転送されるときにもです。

接続性とファイアウォール

ネットワークは、侵入者に対して層状的な防御を実現するために、一層セグメント化されています。これは、パスワード管理システムが1つのネットワークセグメントに括り付けられ、対象となる特権パスワードを持つIT資産が別のセグメントに付けられてる状況を作り出してしまいます。

ファイアウォールを越えたシステムのパスワードを管理するためには、パスワード管理システムでは、ファイアウォール上にパスワード更新情報を送ることが必要となります。これは簡単でないかもしれません: 多くのネットワーク・プロトコルが、デザイン上安全でなく(例えば、WindowsのSMB、オラクルのSQL*ネット、平文LDAP、平文HTTPなど)、当然な理由でファイアウォール管理者にブロックされてしまいます。

この問題に対処するために、効果的なパスワード管理システムは、ターゲットシステムネイティブのネットワーク・プロトコルを、自身のプロトコルで置き換えることができればなりません。パスワード管理システムのネットワーク・プロトコルはファイアウォールを透過できるものでなくてはなりません。

サービスとアプリケーション

機密パスワードの利用は、人のIT担当者だけに限っているわけではありません。ウェブサーバーやアプリケーションパスワードなどのソフトウェアを起動するのに使用される、サービスアカウントもあります。また、あるコンピュータ上のサービスが、別のコンピュータにあるかも知れない別のサービスを認証するために用いるアプリケーションパスワードなどもあります。

多くのシステムの上では、サービスパスワードは固定であり、アプリケーションパスワードはスクリプト、プログラムまたはテキストファイルに埋め込まれています。これらのパスワードはちょうど管理者アカウントと同様に強力なログインIDを解錠します。

機密パスワードを管理する効果的なソリューション、はIT従事者に利用される管理者パスワードの管理に加え、サービスとアプリケーションパスワードと管理するメカニズムを持つべきです。これは2つの特定の機能を必要とします。:

1. あるプログラムを起動するアカウントのパスワードがランダム化された後に、そのプログラムを起動したい別のプロ

グラムに自動的にその新しいパスワードを通知する機能。

2. 一つのアプリケーションが、別のアプリケーションに対して認証に使うパスワードを安全に取ってくるができるAPI。

アクセスコントロール

すべてのIT従事者がすべての特権アカウントにアクセスできる必要はありません。同様に、パスワード入手用APIを呼び出すアプリケーションは、正当に接続する必要があるサービスだけのためにパスワードを得られるようにすべきです。

そうしたセキュリティポリシーを施行するために、パスワード管理システムは、特定のユーザ(人またはソフトウェアエージェント)が特定の特権アカウントへのアクセス権が与えられるべきかどうかを判断できるような、柔軟なアクセス管理基盤を持つ必要があります。

監査証跡と警告

資産とそれらのパスワードの検索、アクセス制御ポリシーの変更を含む、パスワード管理システムでのすべてのアクションが監査可能でなければなりません。これにより、ユーザとその動作の間にアカウントビリティの連鎖を確立することができます。

また、それは監査可能事象と警告をリンクすることも意味があります。例えば、正当なユーザが特定のサーバーの管理者パスワードを検索する場合、そのサーバー所有者は、そのイベントについてのメールを受け取りたいかもしれません。

アカウントビリティを確立し、監査要件を満たし、システム所有者が変則的な管理者アクティビティがあったときに適宜対応するためには、特権パスワード管理システムは、パスワードへの詳細なアクセスログを持ち、その監査データを永続的に保管し、それを単に記録するだけでなくセキュリティイベントに対するアクションを取れるようにする必要があります。

アーキテクチャ上の要素

前章で説明した各要件は、パスワード管理ソリューションの中で、適切な構成要素を用いて対応することができます。これらの構成要素を以下のセクションで説明します。:

プラットフォームサポート

広範囲なターゲットシステムタイプと統合するためには、豊富なコネクタを提供する必要があります。

ワークステーション: 設置場所と接続性

ユーザーワークステーションには、定期的にパスワード管理サーバーのセントラルクラスタに接続し、ローカルに管理されるアカウントの新規パスワードを要求するクライアントソフトウェアをインストールし、利用可能とすべきです。

この「プルモード」アプローチは、断続的に接続し、ダイナミックIPアドレスを用いるデバイスに対して、セントラルサーバーのパスワードを「プッシュ」アウトの問題を解決します。

何百万もの資格証明への拡張性

複数の、同時にアクティブなパスワード管理サーバーをサポートし、各々がサーバー新規パスワードをプッシュし、かつ各々がワークステーションにオンデマンドで新規パスワードを提供できるようにします。

スケールの拡大ニーズに従って、サーバーの数を増加できるようにします。サーバーは、ロードバランサーの後ろに配置し、ユーザーとワークステーションからみた複雑さ排除すべきです。

リソースの自動ディスカバリと自動構成

周期的なパスワード変更を行う何千台ものデバイスを手動で構成するのは、現実的ではありません。代わりに、特権パスワード管理システムには、自動ディスカバリインフラストラクチャが必要です。

1. 自動的にサーバーとワークステーションを見つける。
2. 自動的に管理者とサービスアカウントを見つける。
3. 周期的なパスワード更新のためにシステムとアカウントを構成する。
4. ソフトウェアコンポーネントに新規サービスアカウントパスワードを通知します。

高信頼オペレーションと競合条件/h4>

格納されているパスワードを実際に更新する前にパスワード更新を確認する、信頼できるプロトコルが、特に

ワークステーションには必要です。

パスワード履歴は無期限に保有するべきです。IT資産が破損して、バックアップメディアから回復しなければならないときに、バックアップが取られた日時以降のパスワードを提供することができます。

フォールトトレランス: ハードウェア、ネットワーク、及びデータセンタの問題

([_label_req-ha](#))で言及したように、複数のサーバーが必要です。サーバーはマルチマスター構成でそれぞれパスワードをランダム化するだけでなく、各サーバーが、完全なデータセットを収容し、そのデータのすべてのローカルのアップデートを他のすべてのサーバーに複製するべきです。

複数のサーバーは、異なるデータセンターにインストールするべきです。ローカルサーバーにローカルの資産に関するパスワードを管理させることによって、性能チューニングの機会を与えます。また、それは1つのデータセンターでの災害の場合、フォールトトレランス性を実現します。1つのデータセンターがオフラインになっても、他のデータセンターのパスワード管理サーバーは、動作し続けることができ、かつ完全なデータセットを持ちます。

転送上、格納上の暗号化

パスワード管理システムの暗号化システムは、鍵管理を中心にデザインされています。: キーはどのように生成されるか? 鍵は、データや、サーバー、エンドユーザー、管理対象デバイスとどのように関係しているか? 鍵管理は、本資料がカバーする範囲を超え、非常に高度な話題であり、別途議論することになります。それでは、いくつかの基本的な点を説明します。:

1. HTTPSを使ったユーザーインターフェイスで、ユーザはシステムにサインインすることができます。 -- つまり HTTP over SSL.
2. 一般に、パスワード管理システムとターゲットサーバー間の通信は、通常ネイティブプロトコルが使われますが、そのセキュリティは、強いもの (例, HTTPS, SSH or LDAPS) から弱いもの (例, SQL *Net, LDAP) まであります。IPSecなどの外的な手段は、いくつかのターゲットとの通信を保護するのに適しています。
3. ワークステーションとパスワード管理システム間の通信は、HTTPSを使用するか、または別の主要なハンドシェイクプロトコルを使用することで暗号化できるかもしれません。
4. 複数のパスワード管理サーバー間の通信は、SSL (1通の暗号証明書をサーバー毎にこう購入要)を使用するか、サーバー毎に生成されるシメトリックサーバーキーを使用することで暗号化することができます。

接続性とファイアウォール

セキュアでないプロトコルを使わずにファイアウォールを越えた通信を行うために、パスワード管理システムはファイアウォールの両側にコンポーネントを持たせる必要があります。ネットワークセグメント毎に1つのデータベースにパスワードストレージを断片化しなければならない状況を避けるために、プロキシサーバーを提供するのが現実的です。--すなわち、一方のネットワークセグメントでコネクタを動かして、他方のネットワークセグメントのサーバーでパスワードをアップデートすることになります。

プライマリパスワード管理サーバーとパスワード管理プロキシサーバーとの通信は簡単で、任意に付与されたTCPポートの上の暗号化されたプロトコルで行われます。これは、堅固で、安全で、ファイアウォール管理者にとって、容易に理解し、展開できるものです。

サービスとアプリケーション

サービスアカウントのためのパスワード管理

サービスを開始するために使用するパスワードを管理するためには、パスワード管理システムは、パスワードのランダム化に成功した後に、プラグインコードを実行できなければなりません。このインストールに固有のコードの機能は、新しいパスワード値をネットワークコンポーネントに通知することです。.

いくつかのプラグインが共通に使えます。例えば、Windows Service Controlマネージャ、Scheduler、およびIISウェブサーバーは、すべて、指名されたユーザーとしてプロセスを実行するために補助記憶装置にパスワードを保存します (セキュリティデータベースの外)。他のプログラムも同じ要件であるかもしれないので、新しいパスワードを通史するプログラムのインフラストラクチャは、拡大して使えると思われます。(そのため、プラグインとしています)。

アプリケーションパスワードの管理

1つのアプリケーションで別のアプリケーションに認証するために使用されるパスワードを管理するには、アプリケーションが現在の証明書を得るためにAPIを利用する必要があります。例えば、ウェブアプリケーションは、そのAPIを使ってデータベースパスワードを得て、そのパスワードを使ってデータベースに接続し、ウェブページに表示するためのデータを読み込みます。

このタイプのAPIは循環問題を生じさせます：パスワードを必要とするアプリケーションは、どのようにパスワード管理システムにそれ自身を認証するか？ 当たり前の答えは、自身のパスワード(固定)を持つことですが、これは、好ましいものではありません、なぜなら、アプリケーションパスワード(ランダム化される)のセキュリティレベルを静的なパスワードに下げてしまいますし、特権パスワード管理システムの目的は、まさに静的なパスワードを排除することであるからです。

アプリケーションをAPIで認証するには、次のいくつかのオプションがあります。:

1. ワンタイム・パスワードを用いる。APIは、そこで求めるパスワードだけではなく、呼び出すアプリケーションが次の認証に使うために必要な新しいパスワードも扱うことができます
2. 呼び出すアプリケーションの環境特性を用いる。例えば、あるアプリケーションは、特定のIPアドレスからか、または特定のオペレーティングシステムを実行するデバイスからか、または、特定のチェックサムで実行可能なものから接続されたときだけに、APIへのサインインができると言ったものです。

アクセスコントロール

簡単なアクセスコントロールモデルは個々のパスワードと個人ユーザーの間の特権をマッピングします。例えば、ユーザーXはシステムZの上でログインID Yの現在のパスワードを検索できます。

システム、管理されたユーザアカウント、およびITユーザの数が成長するのに従って、このモデルは破たんしてしまいます。--単に、あまりに多くの関係があるからです。

より強力なモデルはユーザとリソースの間にセキュリティグループの概念を挿入します。基本的にはユーザはグループに括られます(各ユーザは複数のグループに属することができます)、そして各グループには、特権が割り当てられます。例えば、ユーザA、B、およびCはグループGに属するとします。グループGのメンバーは、システムYの上のログインID XとシステムWの上のログインID Zの現在のパスワード検索を許されています。

このモデルもまた、大規模な環境で管理するのも難しいかもしれません--明らかにユーザーは明確にグループに割り当てなければなりません(多数のユーザがいるための管理負担があり、また彼らの責任は頻繁に変化します)、そして、手動で多くのリソースを複数のグループに割り当てなければなりません。


最適なモデルは、ユーザ・グループとリソースグループの両方を定義して、2つのタイプのグループの間のアクセスコントロール(特権)を定義することです。例えば、ユーザA、B、およびCはユーザグループUG1に属します。リソースR、S、およびTはリソースグループRG1に属します。ユーザグループUG1のメンバーはリソースグループRG1のアカウントのためのパスワードを検索できます。

このモデルは最大の柔軟性と最小の管理負担を提供します。ユーザーとユーザーグループ、リソースとリソースグループとの関係付けを自動化することによって、さらに最適化を図ることができます。

1. リソースグループのユーザーメンバーシップは、コーポレートディレクトリにある、それぞれのアイデンティティ属性やグループメンバーシップに基づいて決定できます。(LDAP や Active Directory).
2. リソースグループにおけるリソースメンバーシップは、リソースの特性に基づいて決定できます。--例えば、IPアドレス、ハードウェアのクラス、オペレーティングシステム、システムの代表コンピュータオブジェクトのMACアドレスディレクトリOU、など

監査証跡と警告

ロギングはわかりやすいものです--イベント発生時にすべてのイベントを記録し、そして、ユーザー指向、リソース指向などでイベント履歴をシエスレポートを提供します。

 **Hitachi ID Systems, Inc.**

500, 1401 - 1 Street SE, Calgary AB Canada T2G 2J3 Tel: 1.403.233.0740 Fax: 1.403.233.0735 E-Mail: sales@Hitachi-ID.com

www.Hitachi-ID.com