可用性が高く、セキュリティで保護されたクラウドソリューションの展開

可用性が高く、セキュリティで保護されたクラウド ソリューションの展開

著者および寄稿者

DAVID BILLS – Microsoft Trustworthy Computing

CHRIS HALLUM – Microsoft Windows

YALE LI – Microsoft IT

MARC LAURICELLA – MicrosoftTrustworthy Computing

ALAN MEEUS – Windows Phone

DARYL PECELJ – Microsoft IT

TIM RAINS – Microsoft Trustworthy Computing

FRANK SIMORJAY – Microsoft Trustworthy Computing

SIAN SUTHERS – Microsoft Trustworthy Computing

TONY URECHE – Microsoft Windows

目次

エグゼクティブ サマリ

今日、多くの組織がクラウド アプリケーションの柔軟性とパフォーマンスの向上を重視しています。柔軟性とパフォーマンスは確かに重要ですが、必要なときにいつでもクラウド アプリケーションに接続して使用できるということも重要です。この文書では、技術責任者が、パブリック クラウドかプライベート クラウドかに関係なく、使用しているクラウド サービスをユーザーが常に使用できるようにするための主要な方法論について説明します。

俯瞰的な見方をすると、クラウド セッションというものは、コンピューティング デバイスを使用して、内部または外部のエンティティが運用する、組織のクラウド ベースのサービスに接続する顧客で成り立っているといえます。可用性が高いクラ

ウド サービスを計画するときには、サービスに関わるすべての関係者の期待と責任を考慮することが重要です。計画の際には、現実のテクノロジの限界、および障害が発生する可能性を認識する必要があります。さらに、障害の発生時に、ユーザーに対するサービス可用性への影響を最小限に抑えながら、障害の切り離しと修復を行うために適切な設計がどれほど重要かを理解する必要があります。

この文書では、可用性が高くセキュリティで保護されたクライアント接続を維持できる強固なクラウド ソリューションを展開する例を紹介します。さらに、実際の例を使用してスケーラビリティの問題について説明します。この文書は、障害の影響の軽減、可用性の高いサービスの提供、そして全ユーザーにとっての最善のエクスペリエンス、以上 3 つを実現するテクニックの説明を目的とします。

はじめに

コンピューティング インフラストラクチャーに高い信頼性を期待している顧客は、クラウド サービスにも同じ期待を抱きます。たとえば、稼働時間は、一般的に信頼性の指標として使用されます。最近のユーザーは、99.9% (スリー ナインと呼ばれます) ～ 99.999% (ファイブ ナイン) の稼働時間を当然と考えます。これは、年間のダウンタイム時間を 9 時間 (99.9% の場合) から 5 分 (99.999%) にすることと同じです。サービス プロバイダーはしばしば予定されていた停止と予定外の停止を区別します。しかし、IT 管理者ならよく分かっていると思いますが、予定されていた変更でも予想外の問題が発生することがあります。予想外の問題が 1 つ発生しただけでも、99.9% のサービスの約束を守ることは危うくなるのです。

最終的に信頼性は顧客満足度に関するものであり、信頼性の管理は、単純に稼働時間では測定できないより微妙な問題です。たとえば、決してダウンしない、しかし処理速度が遅く使いづらいサービスを想像してください。高い顧客満足度の維持は多面的な課題ですが、信頼性は、顧客満足の他の側面を構築するための土台になります。クラウド ベースのサービスは、始めから信頼性を念頭において設計する必要があります。この文書ではクラウド サービスの信頼性に関する次の原則について説明します。

- サービス指向のアーキテクチャーの使用
- 機能の分離の導入
- 障害に備えた設計
- テストおよび測定の自動化
- サービス レベル契約の理解

信頼性およびユーザーの期待度の測定

前述した稼働時間のほかにも検討すべき信頼性の指標が存在します。コンピューターのハードウェアの信頼性の一般的な基準は平均故障間隔 (MTTF) です。ある部品に障害が発生した場合、修理されるまでユーザーはその部品が提供するサービスを使用できません。しかし、MTTF では半分の状況しかわかりません。障害から修復までの時間を追跡するために、平均修復時間 (MTTR) という測定基準が業界で作成されました。サービスの信頼性の重要な基準を計算するために、MTTF/MTTR という計算式を使用することができます。この計算式では、修理にかかる時間を半分に短縮すると、測定される信頼性が 2 倍になることが分かります。たとえば、MTTF が 1 年間で MTTR が 1 時間であることが歴史的に実証されているオンラインサービスの状況について考えてみます。可用性の測定に着目した場合、MTTR を 30 分に半減させることは MTTF を 2 年に倍増させることと同じです。

MTTR を重視する場合、スタンバイ サーバーの一式を構築し、障害発生時に早急に復旧できるような十分な冗長性を持つ設計にすることで、障害時に予想される影響を軽減し、信頼性の向上を追求することができます。このような軽減方法は、クラウド プロバイダーから提供されるサービス レベル契約 (SLA) に常に文書化されている必要があります。文書化することによって、ある程度の障害発生が予想されること、そして障害の影響を最小限に抑えるための最善の方法は MTTF を増やし、MTTR を減らすことであると暗黙に通知します。

以下のセクションでは、可用性の高いクラウド ベースのサービスを設計するための主要アーキテクチャー要件について詳しく説明します。

サービス指向アーキテクチャー

有効なクラウド テクノロジを採用するには、適切な設計パターンが必要です。サービス指向のアーキテクチャーでは、コンポーネントの実装がそれぞれ独立し、後から導入された新しいコンポーネントからもすぐに利用できるようにインターフェイスを上手に設計する必要があります。この方法でアーキテクチャーを設計すると、障害時に問題があると見なされるコンポーネントを適切に処理できるので全体的なシステムのタウンタイムが減少します。

機能の分離

機能の分離は関心の分離 (SoC) とも呼ばれる設計パターンの 1 つで、各コンポーネントには単一の機能あるいは密接に関連する少数の機能だけを実装し、コンポーネントどうしは重複せず、疎結合で連携します。この文書の後半の図 1 に示す 3 階層のアーキテクチャーは、機能の分離の典型的な例です。このアプローチを使用すると、異なる地域やネットワークに機能を分散することができるため、特定のサーバーに障害が発生したときにそれぞれの機能が存続できる可能性が最も高くなります。図では、それぞれを地域的に分割できる冗長なフロントエンド Web サーバー、メッセージ キュー、およびストレージを示しています。

自動フェールオーバー

コンポーネントのインターフェイスが、Uniform Resource Identifier (URI) を使用して登録されている場合、DNS 参照と同じように簡単に代替のサービス プロバイダーにフェールオーバーすることができます。サービスの場所の代わりに URI を使用すると、稼働しているサービスを簡単に見つけることができるようになります。

フォールト トレランス

グレースフル デグラデーションとも呼ばれるフォールト トレランス、つまり耐障害性は、サービスの構成要素をいかに不必要な依存関係を発生させずに構築できるかにかかっています。ユーザーの Web インターフェイスができる限り簡素化され、ビジネス ロジックやバックエンドと切り離されていると、他のコンポーネントの障害時に通信チャネルが存続できるため、組織とユーザーとのつながりを維持することができます。さらに、Web インターフェイスを使用して、組織のクラウドベースのサービスの各部分の現在の状況をユーザーに知らせることができます。このアプローチにより、ユーザーがサービスの完全復旧の予想時間を理解できるだけでなく、ユーザーの満足度も向上します。

障害復旧計画

時にはサービス障害が発生するということを予想しておく必要があります。ハードウェア障害、ソフトウェアの欠陥、人為的な災害、または自然災害がサービス障害を引き起こす可能性があります。典型的な問題については、障害発生時にトラブルシューティング担当者が何を確認し、どのような対処をすべきかが分かるよう、サー

ビスの導入までにしっかりと計画を作成しておく必要があります。しかし、ブラック スワン イベントと呼ばれるような巨大な環境障害も周期的に発生するので、計画作成中にそのような事象を考慮する必要があります。ブラック スワン理論では、これらの予想できない事象が総合的に通常のサービス停止よりも大きな影響を与えると仮定します。

テストおよび測定

稼働中のサービスについては、2 種類のテストと測定が適切です。テスト サーバーによるサービスの自動ポーリングを行うと、障害を早期に発見して報告することで MTTR を短縮できます。

それから、展開の直前または直後にユーザー リサーチを実施し、ユーザーの反応を理解し、不満要因を特定する必要があります。ユーザーのフィードバックを得る方法としては単純にユーザーに尋ねる方法が簡単です。ただし、その都度ではなく間隔を置いて尋ねるようにします。回答率が低くても、有効なデータは得られるはずです。また、ユーザーから主要業績評価指標 (KPI) を取得して、月次のステータス レポートを作成することもできます。

クラウド プロバイダー

今日のクラウド サービスでは、新しいテクノロジにより、1970 年代から存在する 2 つの概念が実現されています。

- 仮想コンピューターのイメージとリモート管理が可能な仮想ハードディスク ドライブによる、コンピューター ハードウェアの仮想化の実現。
- 物理的および仮想ハードウェアの能力の制御が可能な管理ツールによる、高速な拡張性とアジリティ (俊敏性) の実現。

IT 担当者として、こうした概念および強力な機能を理解することは重要です。「エグゼクティブ サマリ」でも述べていますが、この文書の概念は、進歩的な IT 部門の中ではすでに当然の選択肢となっている、パブリック クラウドとプライベート クラウドの両方に適用されます。プロジェクトでは、最初の段階から、ユーザーへのサービス提供の中断を最小限に抑えることができるクラウド設計および管理サービス重点を置くようにしてください。

クラウド プロバイダーの期待と責任

組織と組織自らが選択したクラウド プロバイダーの間には、おのずと共有できる責任感が存在します。カスタム アプリケーションの場合、クラウド プロバイダーは、フェールオーバーや監視機能など開発者が使用する特定の機能を元にして信頼性を実現するサービスを設計します。開発者は、信頼性を達成可能なゴールとして、これらの機能をよく理解した上で使用する必要があります。

クラウドベースのインフラの上にソリューションを実装する組織は、サービスの可用性を保証する必要があります。ユーザーは、このような種類のサービスに対して電話と同程度の信頼性を期待します。サービス停止が発生するとしても、それはまれであり地域的に限定されている必要があります。組織がこうしたことを保証するためには、サービスから期待できる点とサービスの利用者が提供しなければならない点について、プロバイダーとよく話をして明確にしておかなければいけません。あいまいな点を残したままにしておくと、障害によりユーザー向けサービスが停止したときに、自動的な回復ではなく責任の転嫁が発生する可能性があります。

プライベート クラウドでも同じことを考慮する必要があります。IT 組織は、インフラストラクチャーの責任範囲を社内の専門家に分配し、彼らにプライベート クラウドを構築してもらってもかまいません。クラウド サービスには、信頼性の高いプラットフォームを提供することが期待されます。残りの IT チームはその上に組織のビジネス ニーズを満たす革新的なソリューションを構築することができます。しかし、アウトソースされたクラウド サービスの場合と同じように、透明な運用と期待の明確な文書化は、責任範囲の曖昧かつ不完全な定義から生じる失敗を回避するために役立ちます。

クラウドの可用性

一般的に、パブリック クラウド サービスは、地理的に分散し、専門的に管理されたサーバー ファームとネットワーク デバイスの集まりを使用して高可用性を実現します。特定の高価値コンテンツのためにプライベート クラウドを構築しているような非常に大きな企業でも、パブリック クラウド サービスを利用してアプリケーション ソリューションをホストするメリットはあります。さらに、大規模なパブ

リック クラウドは、需要が予想を超えてもサーバーを増やすことで対応できるため、その容量は実際には無制限であるといえます。サーバーの過度な容量を軽減させることには複数の利点があります。中でも特にすばらしいのは、ほとんどのパブリック クラウド モデルでは実際に使用されるまで容量超過分が課金されないことです。

多くのクラウド プロバイダーは、次のような機能を標準で提供することで可用性と応答性の向上を実現しています。

- ラウンドロビン DNS
- コンテンツ分配ネットワーク
- 自動フェールオーバー
- 地理的な可用性ゾーン

可用性のための設計

前述のように、可用性の向上を実現する最も効果的な方法は MTTR を短縮することです。クラウドにより地理的およびネットワークのダイバーシティーを確保できる場合は、負荷分散により、障害が発生したコンポーネントから稼働しているコンポーネントにユーザーを自動的に振り分けます。ネットワーク負荷分散のような比較的単純な機能も、組織とクラウド プロバイダーまたは DNS の間の予想外の相互作用の影響を受ける可能性があります。こうした相互作用は、予期していなかったサービスの不安定状態を引き起こす可能性があります。

たとえば、分散サービス拒否 (DDoS) 攻撃は、すべてのクラウド サービスで緩和対策を講じなければならない、可用性に対する外部からの攻撃です。しかし、緩和対

策は慎重に行わないと、セキュリティ関連の経験が少ない組織の場合、意図しないときにアプリケーションが使用不能になり、結果として DDoS 攻撃と同じようなダウンタイムが発生する可能性があります。DDoS の緩和対策は、規模を利用すると (つまりクラウド プロバイダーまたは ISP によって) 最も効果的に実現できる機能の例です。

ほとんどの主要なクラウドベンダーは、信頼性およびセキュリティに関する認定を受けており、クラウド セキュリティ アライアンス (CSA) の STAR (Security, Trust, and Assurance Registry) プログラムなどにも報告を行っています。[1] STAR 自体は比較的新しく立ち上げられたものですが、IT 管理者は、社内システムの大半はこのような第三者による検査を受けていないということを考慮する必要があります。共同で負担されるコストでこのような保証を取得できることもパブリック クラウド サービスのメリットです。

可用性の高いクラウドベースのソリューションを作成することの利点と課題を評価するときには、前述したような既知の問題はもちろん、展開するソリューションに固有のビジネスを中断させるような障害の脅威分析を設計に含めることが重要です。一般的に、脅威分析ではセキュリティに対する攻撃のみが考慮されますが、効果的に設定されたクラウド ソリューションでは、他の種類の可用性の損失を考慮し、その緩和策も計画します。

次の図は、冗長機能を備えた一般的な 3 階層の設計を示しています。各要求にはコンポーネントへの応答が可能な複数のパスがあります。一番左側は、要求の送信元になるラップトップ コンピューターなどのユーザー デバイスです (ここでも、使用可能な場合はラウンドロビン DNS とネットワーク負荷分散機能の使用を検討し

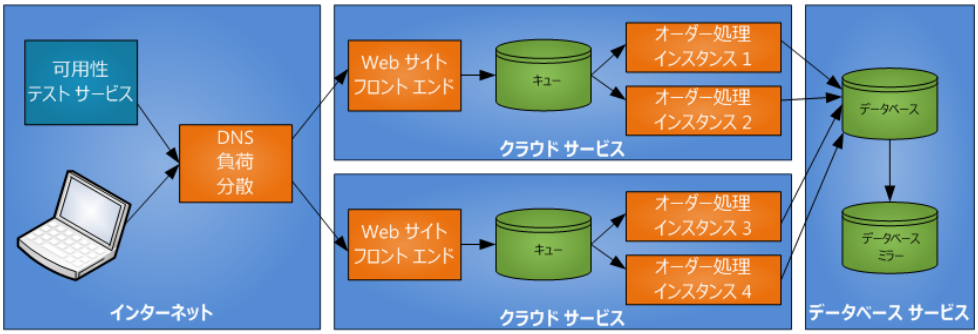
[1] Security, Trust and Assurance Registry (STAR) (https://cloudsecurityalliance.org/star/)

ます)。縦に並んでいる自動可用性テスト サービスが、できる限り多くのシステムを調べて、障害をすばやく報告して必要な修復をすぐに開始できるようにしています。

図のクラウド サービスは機能の分離を示しています。この分離により、ユーザーへのネットワーク パスに両方のパスで障害になるような共通のコンポーネントがなくなります。各クラウド サービス サイト内にはコンポーネントの冗長性を追加することができます。このシナリオでは、クラウド サービス プロバイダーによってキューが提供される場合があります。両方のサイトで共通データベースを共有する必要がある場合は、組織のアプリケーションのアーキテクチャー側で、ミラー化されたデータベース コピーを実行する他のサイトにフェールオーバーさせるようなデータ トラフィックの転送を実装する必要がありますが、多くのパブリック クラウド サービスではデータ冗長性機能を標準で提供しているため、それを検討してもいいでしょう。

この例のソリューションでは、フロント エンドのインターネット、中間層のクラウド サービス、バックエンドの組織のアプリケーションの間のそれぞれで負荷分散を行っています。実際の負荷を使用してこれらの各コンポーネントの無効化テストを実行し、フェールオーバー オプションが計画どおり機能することを確認する必要があります。

図 1 可用性のための設計



Web サイトのフロントエンド コンポーネントが十分に簡素化されている場合、ユーザーは常に企業のブランド イメージとステータス情報を見ることができるため、企業自体の信頼性を確信することができます。コンポーネントと接続の簡素化は、システム全体の信頼性と可用性にとって重要です。密接に相互接続された複雑なシステムでは、問題が発生したときの保守とデバッグが困難です。

クラウドの組織ユーザー

プライベート クラウド プロバイダーまたはパブリック クラウド プロバイダーからクラウド サービスを購入する組織は、クラウド プロバイダーの責任およびそれらの責任の制限を十分に理解する必要があります。同様に、クラウド プロバイダーは、ユーザーに提供するソリューションの可用性とセキュリティの要件を理解する必要があります。完全なクラウド ソリューションには、完全に信頼できる実装方法が必要であり、さらにソリューション独自の機能と組織の要件を統合したサービスを作成するクラウド サービス プロバイダーの能力が必要です。幸いなことに、この統合は、組織にとっての最も大きな革新と付加価値が生まれる部分です。

組織の責任

クラウド プロバイダーの責任範囲が規定されて十分に理解され、サービス レベル契約に文書化された時点で、まだ緩和されていないすべての脅威は顧客である組織の責任になります。潜在的な未対応の脅威を特定するためのベスト プラクティスは、すべての潜在的な脅威を特定するためのブレーンストーミング セッションを実施し、その後でクラウド プロバイダーの責任範囲とされている脅威を除外することです。残った脅威を緩和する責任は組織にあります。次のリスクと責任の一覧は、検討すべき脅威の種類の指針として使用できます。

- ローカルおよびクラウドでアクセス制御を適用する。データの損失はさまざまな理由で発生する可能性がありますが、攻撃者が有効なユーザーの ID を盗ん

だり自分の権限を昇格させて許可されていないアクセス権を取得したりしたときに発生するのが最も一般的です。ほとんどの組織は、フェデレーションが可能な従業員とパートナーのディレクトリを作成するか、自社のアカウントをクラウド環境内にミラー化します。しかし、異なる方法で認証する必要があるユーザーもいます。今後の柔軟性を意識するのであれば、フェデレーションをサポートし、社内ディレクトリと外部 ID プロバイダーの両方からの ID を受け付けるクラウド サービスを採用します。最近は、サービスの一部としてプロバイダー側がアクセス制御サービスを提供することがトレンドになっています。ベストプラクティスとしてアカウント データベースの重複を回避します。重複があると、パスワード データなどの含まれる情報に対する攻撃可能な場所が増えるためです。

- 転送中のデータを保護する。ストレージ内または転送中のデータが保護されていない場合、データ損失が発生する可能性があります。転送中のデータは、トランスポート層セキュリティ (TLS) を使用してエンドポイント間の暗号化を行うことで保護できます。ストレージ内のデータの保護はもう少し複雑です。暗号化は、クラウド内で提供できますが、同様にクラウド内で実行されるアプリケーションでデータを復号化する場合は、暗号化キーの特別な保護が必要です。暗号化キーと暗号化されたデータへのアクセスをクラウドに提供することは暗号化せずにデータを保存するのと変わらないということに注意する必要があります。
- 信頼された役割を保護する。管理機能を実行する権限や高価値のデータにアクセスする権限は通常、組織内のユーザーの役割を基にして付与されます。各ユーザーの役割は変化しても ID は変わらないため、各ユーザーの ID とその ID の承認済み役割の一覧との間に何らかのマッピングが存在している必要がありま

す。クラウド プロバイダーがアクセス制御を任されている場合、この一覧をクラウドに提供し、規定に従って管理してもらう必要があります。ベスト プラクティスは、SAML (Security Assertion Markup Language) などのクレームベース認証テクノロジの使用です。

- モバイル デバイス内のデータを保護する。モバイル デバイス内のユーザーの資格情報および他の機密データの保護は、セキュリティ ポリシーを適用できれば可能です。ベスト プラクティスは、Microsoft Exchange ActiveSync メールボックス ポリシーの設定です。すべてのデバイスがすべての ActiveSync ポリシーを実装するわけではありません。市場にはこうしたニーズに対応するさまざまな製品が出回っているので、組織はエンドポイント セキュリティ ソリューションを探してすべてのモバイル デバイスに展開および適用する必要があります。
- すべてのコードを SDL に従って開発する。アプリケーション コードは、クラウド プロバイダー (たとえばサンプル コードの形式で)、クラウド テナント組織、およびサードパーティから提供されます。Security Development Lifecycle (SDL) の一部として使用されるプロセスや、マイクロソフトによって作成されるソフトウェア開発セキュリティ保障プロセスなどの、脅威モデル作成プロセスではこの点を考慮する必要があります。複数のコンポーネントが認証などの関連機能を制御する場合、特に分析を必要とする領域として競合の可能性があります。
- MTTR が短縮されるように最適化する。脅威モデル作成プロセスではさらに、MTTR を短縮するためにさまざまな種類の予想される障害を考慮および指定する必要があります。想定される各障害について、機能を短時間で回復するために使用できるツールとテクノロジを指定します。

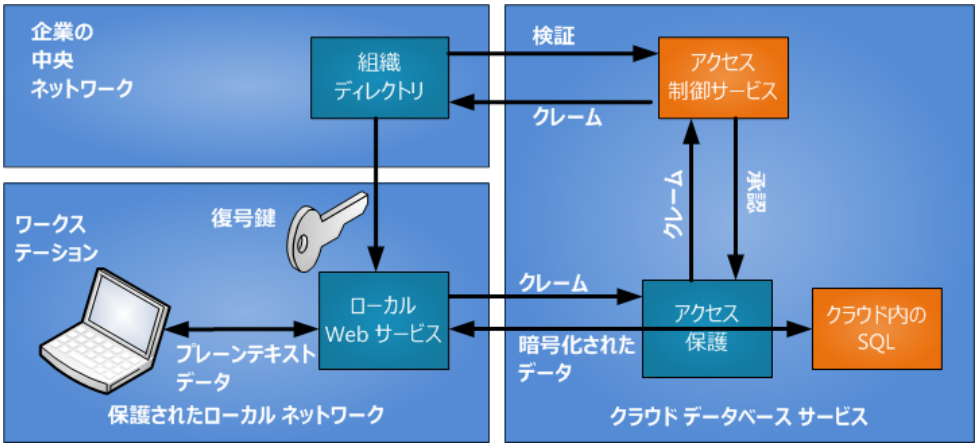
クラウドに保存される機密情報の可用性

クラウドは、可用性の高いアーキテクチャー内でデータのセキュリティ保護のためのいくつかの興味深いオプションを提供します。次のクラウド ソリューションの例をみてください。ここでは、セキュリティと可用性の両方の機能が組織とクラウドの間で分離されています。組織の機密情報はクラウドに保存されていますが、暗号化キーは組織内に保持されているので、クラウドに対する攻撃で機密情報が盗まれることはありません。クラウドに保存されているすべてのデータを暗号化してデータの漏えいを防止するという 1 つの選択肢があります。しかし、データの種類によって差別化することも可能です。その場合、価値が高いデータを暗号化によって保護し、価値が低いデータをアクセス制御のみで保護することができます。ここで、前に推奨した機能の分離および地理的な分散という設計原則を使用して耐性を向上させます。

次の図は、データ保護シナリオの仕組みを示しています。データは、組織のネットワークに接続されているワークステーションで入力および取得されます。ネットワークはファイアウォールを使用して侵入からデータを保護します。ワークステーションはネットワーク内のサービスに接続し、このサービスはキーを使用してデータを暗号化および暗号化解除します。このキーは組織の中央ディレクトリから取得されるので、保護されたローカルのネットワークであればどのネットワークからもクラウドに保存されているデータにアクセスできます。

ユーザーは組織のディレクトリを使用して認証されます。また、認証と承認については、分散環境内にある使用可能な既存のアカウント リポジトリ (Active Directory など) を利用し、フェデレーションと SAML により集中制御を実現します。

図 2 クラウド内のデータの暗号化



上記の、クラウドにおけるデータ暗号化の例は 1 つのパターンとしてさまざまな実装で使用できます。データの復号化キーの保護により、クラウド環境におけるデータ漏えいの脅威を排除し、さらにプレーンテキスト データの組織のフル コントロール下での管理を実現します。また、分散アーキテクチャーを採用することでサービスの可用性も保証されます。

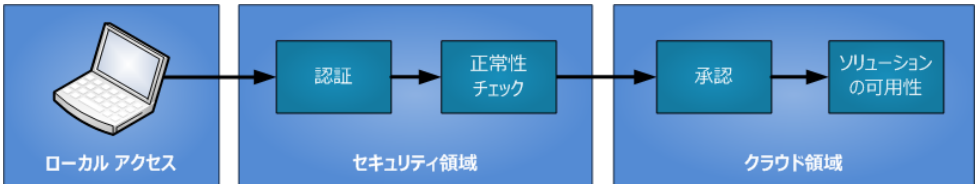
ユーザーおよびクラウドへのアクセスで使用されるデバイス

ユーザーは、単純に今やっている仕事を最後までできるかどうかという視点でクラウド サービスの可用性を評価します。つまり、クラウド サービスはもちろん、彼らがクラウドのアクセスに使用するデバイスが機能することも保証する必要があります。

ユーザーの期待とフィードバック

ユーザーは目的を達成できたかどうかを基にしてサービスの可用性を測定します。次の図は、ユーザーがクラウド リソースにアクセスするまでのプロセスの一般的な手順を示しています。最初に、ユーザーのデバイスがローカル ネットワークに接続し、認証される必要があります。次に、デバイスのセキュリティ状態または正常性をチェックし、役割ベースの認証プロセスなどの使用により、そのユーザーに対する適切なアクセス権を付与します。最後に、クラウド リソース自体が使用可能になっている必要があります。プロセスの構成要素のうちどれか 1 つでも失敗すると、ユーザーがタスクを完了するための機能がブロックされます。セキュリティ上の目的ではこのブロックが望ましいことがありますが、ユーザーは常にわずらわしさを感じます。

図 3 可用性の阻害要因



図中の一連の処理の中でどこか一か所でも問題が発生した場合は、問題の性質とソリューションの可用性を回復するために実行しなければならない手順をユーザーに知らせることが重要です。ユーザーの操作が必要な場合、指示は常に明確かつ簡潔である必要があります。

テストのための設計

自動化されたテスト プログラムは、ソリューションの障害を検出するために役に立ちます。ベスト プラクティスはオンライン テスト用のソリューションの設計です。顧客対応のサービスや Web ページは、重大な障害が発生したときにリアルタイム通知機能を使って自動エスカレーションを行ってくれる、自動クエリ プログラムに対応している必要があります。オンライン テストは、ソリューション サービスの可用性に関する重要な達成指標を提供できます。

可用性に対するユーザーの認識を伝達するための何らかの方法も実装するようにしてください。次に例を示します。

- ユーザーのクラウドへのアクセスにアプリケーションを使用している場合は、そのアプリケーションを利用してログインからクラウド データ取得までの時間などの統計情報を生成する。
- 定期的にセッション終了時に簡単なアンケートをユーザーに依頼する。
- ユーザー エクスペリエンス リサーチャーを現場に派遣してユーザーの意見を収集する。

ユーザー デバイスの可用性

クラウド ソリューションのアクセスに使用するデバイスは、高価値情報を漏えいしないことが保証されていなければいけません。最近は、そうした情報へのアクセスにモバイル デバイスを使用するケースが増えてきています。そのため、デバイスのセキュリティまたは正常性を評価するための方法が必要になっています。クラウドを上手に設計すると、デバイスの正常性を評価したうえでユーザーの ID も検証することができます。このセクションでは、ユーザーがどこからでもクラウド ソリューションを利用できるような、デバイスの正常性評価を実装する方法を説明します。

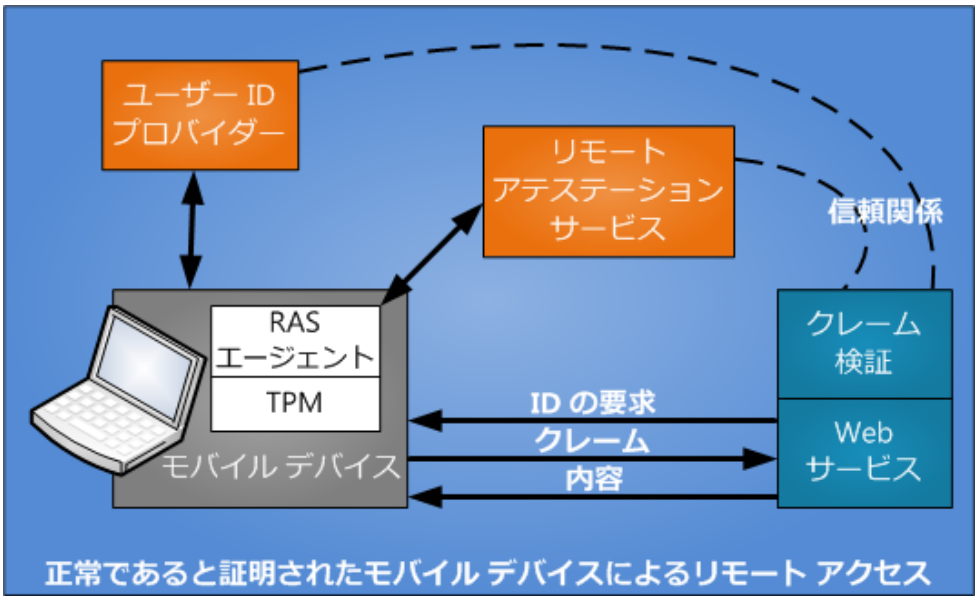
このソリューション例は、ユーザーが所有するデバイスから組織のネットワークにセキュリティで保護されたアクセスを確立するというニーズを想定しています。このようなシナリオは、BYOD (Bring Your Own Device、私的デバイス活用) と呼ばれることもあります。何年もの間、保護をめぐらせた境界によりすべてのリソース (そうしたリソースにアクセスするクライアント コンピューターも含む) を隔離することで、IT 部門は企業資産を保護することができました。BYOD シナリオの場合、ユーザーはどこからでも個人データにアクセスできる市販のデバイスを所有し、同じデバイスを使用して組織のリソースにもアクセスしたいと考えます。このような現象は IT のコンシューマライゼーションとして知られています。

このようなシナリオでは、ユーザー ID の確認、個人データの使用方法に関するユーザーの基本設定の学習はクラウド サービス側で対応する必要があります。また、サービス (または組織) 側で将来の利用または他のユーザーとの共有目的でユーザーの個人データを保存させたい場合はユーザー権限の付与なども行う必要があります。また、クラウド サービスが所有するコンテンツの中には、セキュリティで保護さ

れていると判断されたユーザー デバイスにしか公開しない内容があるかもしれません。多くのユーザーは、自分のプライバシー、ID、および資産がマルウェアから保護されていることを確認したい一方で、ほとんどのユーザーはセキュリティ メカニズムによる不便さを歓迎していない現状があります。

次の図は、モバイル デバイスの正常性をクラウドから評価するために構築されたソリューションです。モバイル デバイスは、クラウド内の ID プロバイダーに接続してユーザー認証を行います。Web サービス側に機密性の高い情報が保存されている場合、あるいは Web サービスがユーザーの意図であることを証明できる情報を取得しようとしている場合、続行する前にモバイル デバイスのセキュリティの検証を実行することがあります。ユーザーのデバイスは、ユーザー ID と共に送信可能な正常性の証明を受け取ります。

図 4 セキュリティで保護されたモバイル クライアント



Windows 8 デバイスは、セキュア ブートやトラスト ブートなどの低レベルのハードウェア テクノロジを使用して、低レベルのルートキットやブートキットから保護することができます。

セキュア ブートは、ルートキットによる攻撃を防ぐためのファームウェア検証プロセスのことで、Unified Extensible Firmware Interface (UEFI) 仕様の一部です。UEFI の意図は、ソフトウェア割り込み駆動型の古い BIOS システムに比べて、高速で効率的な 入出力 (I/O) を実現する最近のハードウェアとオペレーティング システムが通信するための標準的な方法を定義することです。

トラスト ブートは、(可能性は高くありませんがブート プロセスを改ざんできる場合でも) マルウェアを検出できる状況を作ります。このために正常性証明は付与されません。セキュア ブートはマルウェア対策ソフトウェア自体を保護します。

リモート アテステーション サービス (RAS) エージェントは、トラステッド プラットフォーム モジュール (TPM) によって保護されるメジャー ブート データを送信できます。デバイスが正常に起動した後で、ブート プロセスの測定 (たとえば Windows 8 のメジャー ブート) データが RAS エージェントに送信されて測定が比較され、正常性クレームをデバイスに送信することによってデバイスの正常性の状態 (良好、不良、不明) が伝達されます。

デバイスが健全である場合、その情報を Web サービスに渡し、組織のアクセス制御ポリシーを起動してアクセス権が付与されます。

コンテンツ プロバイダーの要件によっては、デバイスの正常性データとユーザーの ID 情報を SAML (Security Assertion Markup Language) または OAuth クレームの形式で組み合わせることができます。Active Directory などの ID プロバイダーは、

ユーザーの雇用主、コンテンツ プロバイダー、または Facebook などのソーシャル ネットワークに属している場合があります。データは、ほとんどの商用 Web サイトで既に使用されている不正検出サービスによって評価されます。続いて、コンテンツへのアクセスが、正常性のアサーション、またはクレーム、メリットに対する適切な信頼度レベルで承認されます。ユーザーがプロバイダーにトランザクションを要求するときに、必要に応じてコンテンツ プロバイダーからユーザーのデバイスへの追加要求ができるよう、これらのクレーム プロトコルは構造化されます。たとえば、高価値データまたは資金転送が要求された場合、トランザクションを完了する前にユーザーのデバイスを照会して追加のセキュリティ状態の確立が必要になる場合があります。

結論

前の例は、機能の分離を備え、セキュリティで保護されたサービス指向のアーキテクチャーを中心とするソリューションを説明しています。実証されたアーキテクチャー パターンでは、ソリューションを疎結合されたコンポーネントに分割します。このアプローチを使用すると、他のコンポーネントに致命的な障害が発生した場合でも、各コンポーネントを正常にフェールオーバーすることができます。どの個別のコンポーネントに障害が発生した場合でも、サービス全体は一部またはすべての機能を使用して稼働し続けることができます。この設計では、社外のパブリック クラウドによりソリューション スケーリングなどの別の機能を提供しながら、社内設置の機能を部分的に採用するハイブリッド ソリューションを使用することができます。

ベスト プラクティスとして、可用性はユーザーと同じ領域で運用されるサービスで監視する必要があります。さらに、地理的に分散された複数の場所からアクセスおよび運用可能な方法でサービスを設計および導入し、事故や自然災害の発生時に可用性を確保できるようにする必要があります。

クラウド サービスの開発者とサービス利用者は、障害を想定した予想、設計、テストのそれぞれの段階で、その都度コミュニケーションを図り、互いに協力しあう必要があります。こうしたコミュニケーションと協力は、ソリューションの成功とユーザーの満足度に直接的な影響を及ぼします。

参考資料

この文書で説明したシナリオおよびソリューションの詳細については、次のリソースを参照してください。以下で紹介するドキュメントは、クラウドベースのソリューションの可用性の設計において正しい意思決定を行うための追加情報を提供します。

- Microsoft System Center http://microsoft.com/systemcenter (現在、この Web サイトでは Release Candidate 2012 の情報を提供しています)
- クラウド コンピューティング: ハイブリッド クラウド環境におけるコントロールの実現 (英語)
  http://technet.microsoft.com/ja-jp/magazine/hh389788(en-us).aspx
- クラウド セキュリティ アライアンス - STAR (Security, Trust & Assurance Registry) (英語)
  https://cloudsecurityalliance.org/star/
- SQL Azure のセキュリティ ガイドライン (英語)
  http://social.technet.microsoft.com/wiki/contents/articles/1069.security-guidelines-for-sql-azure.aspx
- サービス指向アーキテクチャー - 設計パターン (英語)
  www.soapatterns.org/masterlist_c.php
- クラウドの不完全なセキュリティ: ツール、経験、透過性の不足 (英語)
  www.technewsworld.com/story/74890.html
- クラウドの概要: クラウド コンピューティング世代での競争上の優位性の実現 (PDF) (英語)
  http://download.microsoft.com/download/1/4/4/1442E796-00D2-4740-AC2D-782D47EA3808/16700%20HBR%20Microsoft%20Report%20LONG%20webview.pdf

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/reliability