Azure リソース インベントリが運用効率とコンプライアンスの管理を支援

Microsoft IT にとって、Microsoft Azure リソースを管理する従来のプロセスは、セルフ プロビジョニングされたクラウドの利用状況について十分に把握できる可視性を備えたものではありませんでした。この課題を克服するため、マイクロソフトは、全社の Azure サブスクリプションおよびリソースのインベントリを作成し、これを管理しています。これには、リソースの管理と監査を行うためのリソースや利用状況に関する詳細なレコードが含まれています。インベントリとともに、マイクロソフトは、Azure リソースの効率性と価値の実現を支援する Azure の利用状況管理用システムを開発しました。

Microsoft Azure のメリットの 1 つとして、クラウド リソースとインフラストラクチャの作成や変更を素早く簡単に行えることが挙げられます。マイクロソフトのチームは、コンピューティング リソース、ストレージ リソース、およびネットワーク リソースを追加/削除することで、クラウド リソースを拡大/縮小し、ワークロードの需要を満たすことができます。

Microsoft IT は、物理的な IT 資産およびリソースの効果的な管理を支援するさまざまなツールやプロセスを開発してきました。しかし、クラウド リソースの増加に伴い、いくつかの特有の課題が生じています。従来のプロセスは、セルフ プロビジョニングされた使用や関連するリスクについて十分に把握できる可視性を備えていませんでした。マイクロソフトのチームや部署は、一定レベルの監視とガバナンスを実現する従来の制御プロセスを経ずに、組織に代わってクラウド リソースを取得できていました。

セルフサービスのクラウド テクノロジの採用によって、マイクロソフトでは、急速な変化に対応することが難しくなっていました。マイクロソフトは、個々の従業員、グループ、および役割の Azure リソースの使用における可視性を向上させる必要がありました。Azure リソースを管理し、コンプライアンスの確保を支援する能力を向上させるため、マイクロソフトは、以下を支援するプロセスを開発しました。

企業内で使用されている Azure サブスクリプションおよびリソースのインベントリの作成と管理。

リソース レベルの詳細なレコードと運用の可視性との関連付けを支援する方法の定義。これにより、監査可能なクロスチェック済みのリソースの管理メカニズムが実現されます。

インベントリを使用して、Azure リソースの効率性と価値の最大化の促進を支援する Azure の利用状況管理用システムの開発。

Azure リソースの効率性向上

クラウド環境では、必要なコンピューティング リソースやストレージ リソースを最初に多めに見積って、ビジネス ワークロードのパフォーマンスや可用性に対応することが多々あります。マイクロソフトでは、利用状況のデータを収集したり、アプリケーションの実行に必要なリソースがビジネスの需要やニーズと整合しているのか判断したりするための可視性が存在してい

ませんでした。リソースの効率性を向上させるため、マイクロソフトは、コストを増大させ、不要なリスクや複雑さを生じさせるおそれがある、使用効率の低いキャパシティ、使用されていないリソース、孤立したリソース、およびその他の望ましくない成果物を特定する方法を必要としていました。マイクロソフトは、この課題に対処するため、Azure 内のリソースの正確なインベントリの収集と管理を行うことで、適切な制御が行われるよう徹底し、リソースを最適化して、承認されていないクラウドの使用を抑制するところから始めました。

可視性向上によるリスクの低減

IT 組織であるマイクロソフトは、目に見えないリスクを管理することはできません。マイクロソフトが必要としているのは、インフラストラクチャやシステムの効果的な評価、管理、および保護に役立つ環境の可視性です。マイクロソフトの行動ベースのセキュリティ インシデントおよびイベント管理 (SIEM) システムは、その機能を果たすために IT インフラストラクチャの正確なビューに頼っています。また、コンプライアンス、セキュリティ、コスト効率、効率性、トラブルシューティング、またはその他の機能を評価する際、各リソースを表示し、掘り下げて、そのリソースの目的や、そのリソースにアクセスできるユーザー、そのリソースがビジネスにもたらす価値を確認できる機能が必要になります。

承認された Azure クラウド リソースと承認されていない Azure クラウド リソースの両方のリスクおよび利用状況に関する特性を理解するには、Azure リソースや利用状況に関する正確な情報を収集する必要があります。これらは、さまざまなリスクや行動を関連付けるために必要となります。適切な制御プロセス、および承認されていない使用を監視する手法を採り入れることで、承認されていないクラウド リソースや未知のクラウド リソースに伴うリスクを低減させることができます。このリスクには以下のようなものがあります。

- **リソースの非効率な使用:** 承認されていないクラウド リソースの管理やサポートを行おうとした場合、不要な時間、労力、およびコストが費やされます。また、監査や調査を実施した際、不正確な結果または有効性に乏しい結果となる場合があります。さらに、承認されていないクラウド リソースに対してセキュリティ ポリシーを適用することが難しい場合や不可能な場合もあります。
- **プロセス成熟度および実行の非効率性:** マイクロソフトはプロセス成熟度の運用レベル向上に取り組んでいますが、承認されていないクラウド リソースや未知のクラウド リソースは以下を非効率にするおそれがあります。
    - コンプライアンスやポリシーの監査、および監査全体の効率性
    - インベントリや構成の管理プロセスおよび手法
    - パッチや脆弱性の管理
    - 品質および運用プロセス
- **データの損失と漏洩:** 承認されていないクラウド リソースや未知のクラウド リソースは、脅威を受ける対象範囲を拡大させます。クラウド サービスを使用してビジネス データを保管している場合、組織のポリシーや制御の枠外でこれが行われ、そのデータが漏洩したり、悪用されたりするおそれがあります。

利用状況データおよびレポート機能を備えた Azure リソース インベントリの作成

アカウントやサブスクリプションに関連付けられている Azure のほぼすべての要素がリソースと見なされます。1 つの Azure 展開で数千ものリソースが使用されることもあります。これには、仮想マシン、Azure Blob ストレージ、アドレス エンドポイント、仮想ネットワーク、Web サイト、データベース、サードパーティ サービスが含まれます。

包括的なインベントリを作成するため、マイクロソフトは、組織で使用されているすべての Azure リソースについて、以下の質問に答えられる必要がありました。

- それはどのようなリソースですか。
- そのリソースはどこにありますか。
- そのリソースにはどのような価値がありますか。
- そのリソースには誰がアクセスできますか。

マイクロソフトは、自社の環境でオンプレミス リソースとクラウド リソースを管理する責任を負っています。クラウド サービスはセルフサービスで常に変化しているため、Azure リソースのインベントリを作成するために考案した手法のすべてが、その変化に対応するのに十分な俊敏性を備えるよう徹底する必要がありました。

マイクロソフトは、内部の請求システムからサブスクリプション情報を収集し、Azure リソース マネージャーからリソースや利用状況に関するデータを収集して、それらのデータを Azure SQL データベースに保管する Azure インベントリ ソリューションを設計しました。その結果、収集されたデータを監査し、それらのデータに関するレポートを作成できるようになりました。

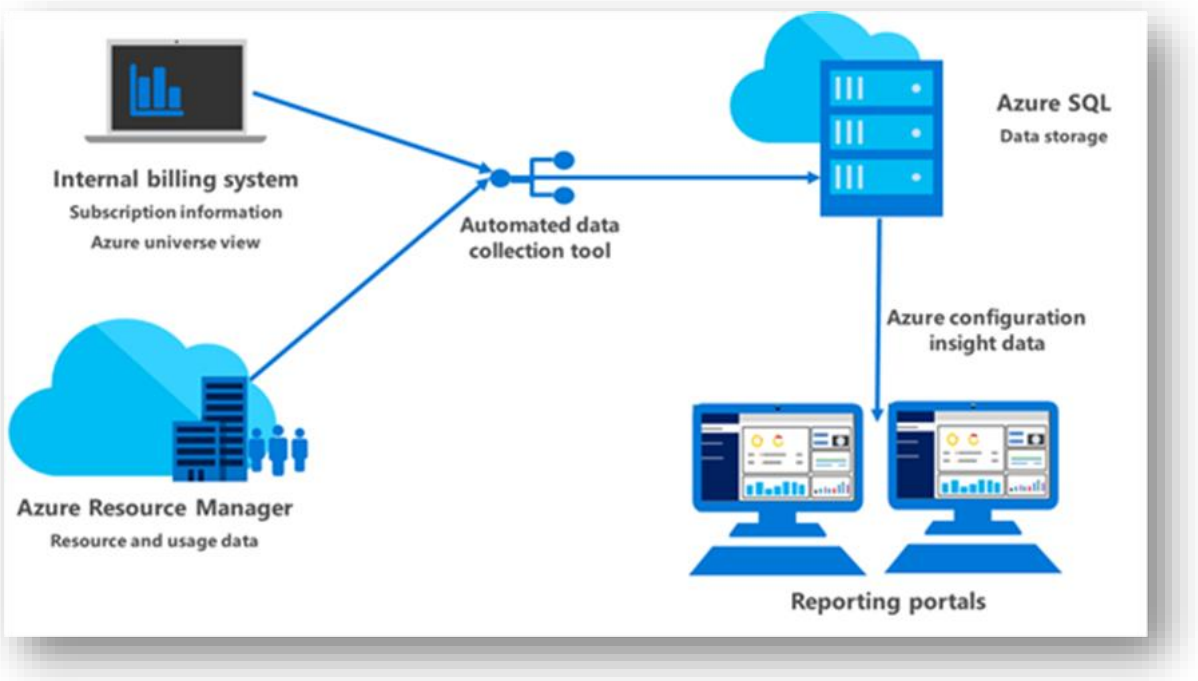

図 1: Microsoft IT の Azure リソース インベントリ ソリューションのアーキテクチャの概要

手順 1: 企業内のサブスクリプションの検出と特定

サブスクリプションは、クラウド サービス リソースへのアクセスを編成するうえで役立ちます。また、リソースの利用状況に関するレポート作成、請求、および支払をどのように行うかを制御するうえでも役立ちます。サブスクリプションは各々で請求や支払の設定が異なる場合があります。お客様も、部門、プロジェクト、地域オフィス等ごとに異なるサブスクリプションやプランが存在するかもしれません。クラウド サービスはそれぞれが 1 つのサブスクリプションに属しています。また、サブスクリプション ID がプログラムの運用で必要になる場合があります。

環境内にあるサブスクリプションを特定するため、マイクロソフトは、内部の請求システムを基にリストを作成しました。内部の請求システムから抽出したこのリストには、Azure リソース マネージャーでリソース情報を収集する対象となる Azure サブスクリプションがすべて網羅されていました。

注: Azure のエンタープライズ プログラム契約が有効なお客様は、Representational State Transfer (REST) API を通じて、利用状況や請求に関する情報にアクセスできます。最初に、エンタープライズ管理者が Microsoft Azure エンタープライズ ポータルでキーを生成し、API へのアクセスを有効にする必要があります。加入契約番号とキーにアクセスできるすべてのユーザーが、API やデータに読み取り専用でアクセスできます。

手順 2: サブスクリプションへのアクセスの確保

Azure リソース マネージャーは、クラウド リソースを管理するための一貫性のあるレイヤーを提供する、Azure 内で中央のコンピューティングの役割を担うコンポーネントです。また、リソースの利用状況に関する詳細なレポートやデータへのアクセスを提供する責任を担うコンポーネントでもあります。マイクロソフトは、Azure リソース マネージャーの REST API を使用し、Azure リソース マネージャーからリソースや利用状況に関する情報を抽出して、マイクロソフトが構築したデータ収集ソリューションに取り込んでいます。

Azure クラウドの利用状況やアクセス特権を効果的に監視する目的で、マイクロソフトの管理者は、サブスクリプションやリソースのリスト作成、監視、および管理を行うために、サブスクリプションやリソースについて把握できる可視性と管理アクセスの両方を必要としていました。マイクロソフトは、自動データ収集ツールへの読み取り専用アクセスを提供する Azure Active Directory のサービス プリンシパル オブジェクトを作成しました。

手順 3: サブスクリプションおよびリソースのメタデータ用のデータ ストレージ ソリューションの構築

マイクロソフトは、Azure SQL を使用し、請求システムや Azure リソース マネージャーから収集されるサブスクリプションおよびリソースのメタデータ用のストレージ ソリューションを構築しました。バックアップには Blob ストレージが使用されています。API から収集されるデータセットは標準ではないため、Azure SQL データベースにそのデータセットを格納する前に、そのデータセットの解析と構造化を行います。プライマリ データ ストレージ ソリューションは構造化されたデータのみをサポートしますが、バックアップ Blob ストレージは構造化されていないデータもサポートします。

手順 4: 自動データ収集ツールの構築

Azure リソース インベントリのデータは 60 個の API から供給されるため、手動プロセスを用いてそれらのデータを一定頻度で収集することはできませんでした。手動プロセスはスケーリングを行うことができず、コスト効率も良くありません。マイクロソフトは、多数の REST API を呼び出し、メタデータの収集と保管を毎日行う自動データ収集ツールを構築しました。この自動ツールは、60 個の Azure の REST API を呼び出す C# ネイティブ アプリケーションを実行している Windows 仮想マシンです。このアプリケーションは、Azure SQL データベースにデータセットを保管する前に、各データセットの戻り値を収集して解析します。その後、ツールによって Azure ストレージでバックアップ コピーが作成されます。

自動データ収集ツールを使用することで、予測可能なスケジュールに基づいて信頼性の高い結果を実現し、多くの時間とコストを節約しています。

手順 5: サブスクリプション レベルのビューを作成するためのデータセットの統合と関連付け

各データセットは、1 つの情報のオブジェクトまたはビューに相当します。マイクロソフトは、独自のサブスクリプション ID とリソース名を使用して、Azure のベースラインと比較できるサブスクリプション レベルのビューを作成しています。データが統合され、そのサブスクリプション ID とリソース名に関連付けられると、Power BI、Excel Power Query、Excel PowerPivot などの使い慣れた生産性ツールでそのデータを使用して、特定のアクティビティに関する分析や監査を行えるようになります。マイクロソフトは、Azure の構成に関する洞察レポートのデータを 2 つの内部ポータル (セキュリティとコンプライアンスに関するポータル、およびデバイスを最新の状態に保つことでデバイスの安全を維持する組織の取り組みについて知らせるポータル) に定期的に送信しています。また、レポート内のリソースに関する情報を用いて、ユーザーの教育を通じてコンプライアンスを強化できる機会が存在する領域を特定しています。マイクロソフトは、以下のようなレポートを使用しています。

- **Azure Security Center のアラートおよびコンプライアンス レポート:** マイクロソフトは、このレポートを使用して、Azure Security Center で検出されたアラートのリストを抽出し、詳細な統計データ (環境内で検出された「高」、「中」、「低」のアラートの数、アラートが存在する重要なサブスクリプションなど) を提供しています。このレポートの対象者はアプリケーション チームおよびそれらの組織であり、これらのチームや組織が取り組みに集中できるよう支援します。
- **グループごとのコンプライアンス レポート:** コンプライアンス レポートのために、マイクロソフトは、Azure インベントリにベースラインや集計を適用しています。コンプライアンス率は組織レベルまたはチーム レベルで表示でき、コンプライアンスに関する全体的な情報を確認したり、詳細情報を確認したりすることができます。このレポートの対象者は管理およびコンプライアンス担当リーダーであり、これらのリーダーが Azure のセキュリティやコンプライアンスを推進できるよう支援します。
- **ユーザーの役割の権限に関するコンプライアンス レポート:** このレポートは、ユーザーの役割の権限を明らかにし、セキュリティのユース ケースや事例によって定義されているベースラインに照らしてそれらを評価し、リソースごとにこれに照らして対応するコンプライアンス率を判別するうえで役立ちます。このレポートには以下の情報が含まれています。
    - 環境内の管理者の総人数
    - グループやチームの管理者の平均人数
    - サブスクリプションにおいて特権付きの役割を有する非従業員の数と名前 (協力者、管理者など)
    - 承認されていない可能性がある割り当ての数
    - 承認されていない可能性がある割り当てを作成した人々の名前
    - 役割の種類の割り当てに関する詳細情報

- **リソースの種類数に関するレポート:** このレポートには、組織全体のリソースの種類数の内訳が含まれています。これには、Azure SQL、Azure 仮想ネットワーク、仮想マシン、Azure ストレージなどが含まれます。また、3 つの基本クラウド サービス モデル (サービスとしてのインフラストラクチャ (IaaS)、サービスとしてのプラットフォーム (PaaS)、およびサービスとしてのソフトウェア (SaaS)) におけるリソースの種類数の内訳も含まれています。

まとめ/次のステップ

マイクロソフトは、Azure リソースの可視性を向上させました。そして、これにはさまざまなメリットが存在します。Azure は、仮想マシンのプロビジョニング、およびテスト用の Azure リソースの調査やスケーリングを簡素化します。インベントリにより、マイクロソフトは、製品やサービスのテストに適したリソースをより効果的に特定できるようになっています。

マイクロソフトは、クラウドの使用に関する意思決定を改善し、コストを削減することができます。また、承認されていないクラウド アプリケーションを簡単に特定して抑制する機能によってリスクを低減させています。さらに、監視やガバナンスを実現することで、Azure リソースの管理と監査をより効果的に行い、コンプライアンス基準を満たすことができます。

マイクロソフトはそれで終わらせずに、インベントリを作成した後、リソースやサブスクリプションの構成を管理するタスクを開始しました。詳細については「Analyzing Azure inventory data to optimize resources and reduce risk」を参照してください。