Azure resource inventory helps manage operational efficiency and compliance

One of the benefits of Microsoft Azure is the ease and speed in which cloud resources and infrastructure can be created or changed. Teams across Microsoft can scale up or scale down their cloud resources to meet their workload demands by adding or removing compute, storage, and network resources.

Microsoft IT has developed tools and processes that help us effectively manage physical IT assets and resources. But with the increase in cloud resources comes some unique challenges. Conventional processes weren't adequately giving us visibility into self-provisioned usage and related risks. Teams and business units at Microsoft could acquire cloud resources on behalf of the organization without passing through the traditional controls that give us some level of oversight and governance.

The adoption of self-service cloud technologies was making it difficult for us to keep up with rapid changes. We needed better visibility into Azure resource utilization for individual employees, groups, and roles. To improve our ability to manage Azure resources and to help ensure compliance, we developed processes to help us:

- Create and maintain an inventory of the Azure subscriptions and resources used within the enterprise.
- Define a methodology to help us correlate detailed resource-level records with operational visibility. This provides a cross-checked resource management mechanism that can be audited.
- Develop a system for Azure usage management that uses the inventory to help us drive the most efficiency and value from our Azure resources.

Improving the efficiency of Azure resources

In a cloud environment, performance and availability of business workloads are often addressed by initially overestimating the compute and storage resources required. We didn't have visibility to collect usage data or to determine whether the resources required to run an application were in alignment with the demand or needs of the business. To be more efficient with resources, we needed a way to identify underutilized capacity, dormant or orphaned resources, and other undesirable artifacts that can lead to increased costs and unnecessary risk or complexity. Our starting point in addressing the challenge was to gather and maintain an accurate inventory of the resources within Azure to help ensure that the proper controls are practiced, optimize resources, and mitigate unsanctioned cloud use.

Reducing risks through increased visibility

As an IT organization, we can’t manage risks that we can’t see. We require visibility into our environment to help us effectively measure, manage, and protect our infrastructure and systems. For our behavior-based Security Incident and Event Management (SEIM) systems to perform their functions, they rely on an accurate view into IT infrastructures. When assessing compliance, security, cost-effectiveness, efficiency, troubleshooting, or other important functions, we need the capability to view and delve into every resource to determine its purpose, who can access it, and its value to the business.

Understanding the risk and usage profiles of both sanctioned and unsanctioned Azure cloud resources requires the collection of accurate Azure resource and usage information—they’re necessary for correlating risks and behaviors. Implementing appropriate controls and a method to monitor for unsanctioned usage helps us reduce the risks associated with unsanctioned and unknown cloud resources. Those risks include:

- **Inefficient use of resources.** Trying to manage and support unsanctioned cloud resources consumes unnecessary time, effort, and expense. Audits and investigations can provide inaccurate or less effective results, and it can be difficult, or impossible, for us to enforce security policies on unsanctioned cloud resources.
• **Process maturity and execution inefficiencies.** Although we’re working to advance operational levels of process maturity, unsanctioned and unknown cloud resources can lead to inefficiencies in:
  - Compliance and policy audits, and overall audit effectiveness.
  - Inventory and configuration management processes and practices.
  - Patch and vulnerability management.
  - Quality and operational processes.

• **Data loss or leakage.** Unsanctioned and unknown cloud resources expand our threat surface. If cloud services are used to store business data, it occurs outside of our organizational policies and controls—and that data could be exposed, or exploited.

Creating an Azure resource inventory with usage and reporting capabilities

Just about everything in Azure that’s associated with an account or a subscription is considered a resource. There can be thousands of resources used for a single Azure deployment, including virtual machines, Azure Blob storage, address endpoints, virtual networks, websites, databases, and third-party services.

To be able to produce a comprehensive inventory, we needed to be able to answer the following questions about all of the Azure resources in use across the organization:

• What is it?
• Where is it?
• What is it worth?
• Who can access it?

We’re responsible for managing the on-premises and cloud resources in our environment at Microsoft. Because cloud services are self-service and constantly changing, we needed to ensure that any methodology that we created to inventory Azure resources was agile enough to keep pace.
We designed an Azure inventory solution that would collect subscription information from our internal billing system, resource and usage data from Azure Resource Manager, and store it in an Azure SQL database. The collected data could then be audited and reported on.

Figure 1. High-level architecture of the Microsoft IT Azure resource inventory solution

Step 1: Locating and identifying the subscriptions within the enterprise

Subscriptions help us organize access to cloud service resources. They also help control how resource usage is reported, billed, and paid for. Each subscription can have a different billing and payment setup, so you can have different subscriptions and different plans by department, project, regional office, and so on. Every cloud service belongs to a subscription, and the subscription ID may be required for programmatic operations.

To identify which subscriptions we had in the environment, we generated a list from our internal billing system. The list we pulled from the internal billing system represented our “universe” view of all of the Azure subscriptions we would be collecting resource information for in Azure Resource Manager.

**NOTE:** Customers with an Azure Enterprise Program Agreement can access usage and billing information through a representational state transfer (REST) API. An enterprise administrator must first enable access to the API by generating a key from the Microsoft Azure Enterprise Portal. Anyone with access to the enrollment number and the key has read-only access to the API and data.

Step 2: Ensuring access to the subscriptions

Azure Resource Manager is a central computing role within Azure that provides a consistent layer for administrating and managing cloud resources. It’s also the component responsible for providing access to detailed resource usage reports and data. We use Azure Resource Manager [REST APIs](https://docs.microsoft.com/en-us/azure/resource-manager/) to pull resource and usage information from Azure Resource Manager into the data collection solution we built.

To effectively monitor Azure cloud usage and access privileges, our administrators required both visibility and administrative access into subscriptions and resources to list, monitor, and manage them. We created an Azure Active Directory [service principle](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/) object that provides read-only access to our automated data collection tool.
Step 3: Building a data storage solution for subscription and resource metadata

We built a storage solution for subscription and resource metadata that we collect from the billing system and Azure Resource Manager using Azure SQL. We use Blob storage for backup. The datasets that we collect from the APIs aren’t standard, so we parse and structure them before we place them into the Azure SQL database. Our primary data storage solution supports only structured data, but our backup Blob storage supports unstructured data.

Step 4: Constructing an automated data collection tool

The data for the Azure resource inventory comes from 60+ APIs, so we couldn’t rely on manual processes to collect that data with any regular frequency. Manual processes don’t scale and aren’t cost effective. We constructed an automated data collection tool that calls the numerous REST APIs to capture and store the metadata on a daily basis. The automated tool is a Windows virtual machine that has a C# native application running on it that calls the 60+ Azure REST APIs. The application captures and parses the returns of each dataset before storing it in the Azure SQL database. The tool then creates a backup copy in Azure Storage.

Using an automated tool for data collection provides reliable results on a predictable schedule and saves us a great deal of time and money.

Step 5: Consolidate and link together datasets to create a subscription-level view

Each dataset represents a single object or view of the information. We use the unique subscription IDs and resource names to create subscription-level views that we can compare to our Azure baselines. After the data is consolidated and linked to its subscription ID and resource name, we can begin working with it to analyze and audit for specific activities, using familiar productivity tools like Power BI, Excel Power Query, or Excel PowerPivot. We regularly send Azure configuration insight reporting data to two internal portals—one that’s related to security and compliance, and another that reports organizational efforts to keep devices safe by keeping them current. We also use the resource information in our reporting to identify areas in which we have an opportunity to improve compliance through user education. Some of the reports we use include:

- **Azure Security Center alerts and compliance report.** With this report, we pull a list of alerts that are found in Azure Security Center and provide detailed statistics, such as the number of High, Medium, and Low alerts found in the environment and the top subscriptions that are seeing alerts. The target audience is application teams and their organizations to help focus their efforts.

- **Compliance reporting by group.** For our compliance reporting, we apply our baselines and aggregations to the Azure inventory. The compliance rates can be viewed at either an organization or team level to provide overall or drill-down information about compliance. The target audience is management and compliance leadership, to help them drive Azure security and compliance.

- **Compliance reporting for user role authorization.** This report helps us identify user role authorization, assess them against the baselines as defined by the security use case, or narrative, and determine corresponding compliance rates against it per resource. This report includes the:
  - Total number of administrators in the environment.
  - Average administrator counts across groups and teams.
  - Number and names of non-employees that have privileged roles in subscriptions (contributor, administrator, and so on).
  - Number of potential unauthorized assignments.
  - Names of the people who created the potential unauthorized assignments.
  - Role type assignment details.
• **Resource type count report.** This report includes a breakdown of resource type counts across the organization, including Azure SQL, Azure Virtual Network, virtual machines, Azure storage, and so on. It also contains a breakdown of resource type counts in the three fundamental cloud service models, infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

**Conclusion/Next steps**

We’ve improved our visibility of Azure resources, and that has numerous benefits. Azure makes it easier to provision virtual machines and scope and scale Azure resources for testing. The inventory makes us better able to identify qualified resources for testing products and services.

We can make better decisions about cloud utilization, and reduce costs. And we’re reducing risk through our ability to easily identify and mitigate unsanctioned cloud applications. We’re better able to manage and audit Azure resources, to meet compliance standards by providing oversight and governance.

We didn’t stop there—after creating the inventory, came the task of managing our resource and subscription configurations. To learn more, read [Analyzing Azure inventory data to optimize resources and reduce risk](microsoft.com/itshowcase).

**For more information**

**Microsoft IT**

[microsoft.com/itshowcase](microsoft.com/itshowcase)

Manage Azure resources with PowerShell and Resource Manager

Azure Resource Manager overview

[Analyzing Azure inventory data to optimize resources and reduce risk](microsoft.com/itshowcase)