Microsoft moves IT infrastructure management to the cloud with Azure

At Microsoft Core Services Engineering and Operations, formerly Microsoft IT, we're embracing digital transformation and the culture changes that go with it. With over 90 percent of our IT infrastructure in the cloud, we're adopting Microsoft Azure monitoring, patching, backup, and security tools to create a customer-focused self-service management environment centered around DevOps and modern engineering principles. As we continue to benefit from the growing feature set of Azure management tools, we'll deliver a fully automated, self-service management solution that gives us visibility over our entire IT environment. The result? Business groups at Microsoft will be able to adapt IT services to best fit their needs.

Digital transformation at Microsoft

We're a global IT organization that strives to meet Microsoft business needs. Azure is the default platform for our IT infrastructure. We host 90 percent of our IT infrastructure in the cloud. Here are a few details:

- 124,000 employees
- 587 locations
- 1,200 Azure subscriptions
- 1,600 Azure-based applications
- 11,000 Azure infrastructure-as-a-service (IaaS) virtual machines
- 384,000 managed devices

Like most IT organizations, we have our roots in the datacenter. In the past, our traditional hosting services were mostly physical, on-premises environments that consisted of servers, storage, and network devices. Most of the devices were owned and maintained for specific business functions. Technologies were very diverse and needed people with specialized skills to design, deploy, and run them. Our achievements were limited by the time required to plan and implement the infrastructure to support the business.

As technology evolved, we began to move out of the datacenter and into the cloud. Cloud-based infrastructure created new opportunities for us and has transformed the IT infrastructure we manage. We continue to grow and adapt in a constantly changing IT landscape.

Traditional IT technologies, processes, and teams

Our traditional datacenters were managed by a legion of IT pros, who supported the diverse platforms and systems that made up our infrastructure. Physical servers, and later virtual servers, numbered in the tens of thousands, spanning multiple datacenters and comprising a mass of metal and silicon to be managed and maintained. Platform technologies ranged from Windows, SQL Server, BizTalk, and SharePoint farms to third-party solutions such as SAP and other information security–related tool sets. Server virtualization evolved from Hyper-V to System Center Virtual Machine Manager and System Center Orchestrator.

To provide a stable infrastructure, we used structured frameworks, such as IT Infrastructure Library/Managed Object Format (ITIL/MOF). Policies, processes, and procedures in the framework helped to enforce and control security and availability, and to prevent failures. Microsoft product engineering groups that used hosting services had a similar adoption process for their application and service needs, which were based on ITIL/MOF.

This model worked well for traditional IT infrastructure, but things began to change when cloud computing and Azure began to influence the IT landscape.

Evolution of the hybrid cloud

As IT infrastructure and services began to move to the cloud, the nature of the cloud and how we treat it changed. We've now been hosting IT services in Azure for a long time, and as Azure has evolved and grown, so has our engagement with Azure services and the volume of our IT services hosted in Azure.

Early Azure: IT-owned, IaaS, and lift-and-shift

In the early years, Azure was IT-only. We had full control of cloud development, implementation, and management. We could create and manage solutions in Azure, but it was a siloed service.

The infrastructure consisted primarily of IaaS virtual machines that hosted workloads in the cloud the same way that they hosted workloads in on-premises datacenters. Efficiency gains were small and infrastructure management still used the same tools—sometimes hosted in the cloud, and sometimes hosted on-premises and connected to the cloud. It was very much a lift-and-shift migration from the datacenter to the cloud, and our management processes imitated the on-premises model in much the same way. The datacenter remained the focus, but that was changing.

Azure evolves: PaaS, co-ownership, and cloud-first

As Azure matured and more of our infrastructure and services moved to the cloud, we began to move away from IT-owned applications and services. The strengths of the Azure self-service and management features meant that a business group could handle many of the duties that we offered as an IT service provider—which meant that they could build solutions that were more agile and responsive to their needs.

Azure platform-as-a-service (PaaS) functionality matured, and the focus moved from IaaS-based solutions to PaaS-based solutions. Azure became the default target for IT solutions; datacenter decommissioning began as more solutions moved to or were created in Azure. Monitoring and management was becoming cloud-focused as we pointed more of our System Center Operations Manager (SCOM) and System Center Configuration Manager (SCCM) instances at the cloud. Azure-native management started to mature.

Large-scale Azure: Service line–owned, IT-managed, PaaS-first

PaaS quickly became a focus for developers in our business groups, as they realized the agility and scalability they could achieve with PaaS-based solutions. Those developers shifted to PaaS for applications as we transitioned away from IaaS and virtual machine-based solutions.

With the advent of Azure Resource Manager, which permitted a broader level of user control over Azure services, we saw service lines begin to take ownership of their solutions, and business groups started to manage their own Azure resources. The datacenter became an inconvenient necessity for apps that couldn't move to Azure. We still used SCOM and SCCM as the primary monitoring and management tools, but we had moved almost all our instances into IaaS implementations in Azure. Azure-native management became a mature product, and we started to consider and plan what a completely cloud-based management environment would look like.

Azure in a DevOps culture: Service line–managed, Internet-first, business-first

We're nurturing a DevOps culture in IT—DevOps has transformed the way that Azure solutions are developed and operated. Our Azure solutions offer an end-to-end view for our business groups. They're agile, dynamic, and data-intensive. Continuous integration and continuous development create a continual state of improvements and feature releases.

The Azure solutions that our business groups use are designed to respond to their business needs. We actively seek and use Azure-native tools for control over and insight into IT environments, in Azure first—but also back to the datacenter where required. We're a long, long way past managing a stack of metal. The modern workplace is here at Microsoft, and it changes every day.

Realizing digital transformation

In the modern workplace, the developers and IT decision makers in our business groups have an increasingly critical business role. Our business groups need the autonomy to make IT decisions that serve their business needs in the best way possible. With 90 percent of our IT infrastructure in Azure, we're increasingly looking to the agility, scale, and manageability that Azure provides. Using this scale, we solve business needs and provide the framework for a complete IT organization, from infrastructure to development to management.

Managing the modern hybrid cloud

Our modern hybrid cloud is 90 percent Azure—and Azure is the primary platform for infrastructure and management tools. Azure is not only the default platform for IT solutions—it *is* our IT solution. Just as PC sprawl occurred in the late 1990s and server sprawl did the same thing in the 2000s, cloud sprawl is a growing reality. Implementing new cloud solutions to manage the cloud environment and the remaining on-premises infrastructure is critical for our organization.

Embracing decentralized IT

Decentralized IT services are a big part of digital transformation. We need a management solution that offers us—and our business groups—what we need to manage our IT environments. We always want to maintain governance over security and compliance of Microsoft as a whole, but we also realize that decentralized IT services are the most suitable model for a cloud-first organization. By decentralizing services and ownership in Azure, we offer our business groups several benefits:

- Greater DevOps flexibility.
- A native cloud experience: subscription owners can use features as soon as they're available.
- Freedom to choose from marketplace solutions.
- Minimal subscription limit issues.
- Greater control over groups and permissions.
- Greater control over Azure provisioning and subscriptions.
- Business group ownership of billing and capacity management.

Our goal in the management of modern hybrid cloud continues to be a solution that transforms IT tasks into self-service native cloud solutions for monitoring, management, backup, and security across our entire environment. With this solution, our business groups and service lines have reliable, standardized management tools, and we can maintain control over and visibility into security and compliance for our entire organization.

The areas where we retain oversight include:

- General IT and operational policy implementation, as approved by the subscription owner. Areas include compliance, operations, and incident management.
- Shared network connectivity over ExpressRoute, as needed.
- Visibility into infrastructure inefficiencies and self-service tool development.

Our management solution has to be as agile as the solutions we manage, and we provide best practices, standards, and consulting for Azure management solutions to ensure that our business groups are getting the most out of the platform.

Supporting digital transformation with Azure management tools

Managing the hybrid cloud in Azure encompasses a wide range of services and activities. For our business groups to improve, they need to monitor their apps and solutions to recognize issues and opportunities. They need a patching and management solution that keeps systems up to date, manages configuration, and automates common maintenance tasks.

We must protect data with a disaster recovery platform and ensure security and compliance for business groups and the entire company. We use the following tools in Azure to enable hybrid cloud management:

- Azure Monitor
- Application Insights
- Azure Automation
- Log Analytics
- Update Management
- Azure Backup
- Azure Policy
- Azure Security Center
- Azure Advisor

Monitoring the hybrid cloud

Monitoring is an essential task for our business groups and their service lines. They need to understand how their apps are performing (or not) and have insight into their environment. We've used SCOM for monitoring at Microsoft for more than 10 years—and a certain rhythm develops when you use a product for that long.

To ease the transition from SCOM to Azure monitoring, we've developed transition solutions that use native Azure functionality to recreate certain SCOM functions and views in Azure Monitor. The transition solutions consist primarily of PowerShell scripts and documentation. They give our business groups a familiar environment to work in while they become familiar with Azure monitoring. Our business groups can also start in a standardized environment with our built-in tested security and compliance components. This helps us maintain a centralized standard while allowing for decentralized monitoring. We maintain metrics for critical organizational services, but we leave operational monitoring to each business group.

Our Azure monitoring is designed to:

- **Create visibility.** We're providing instant access to a foundation set of metrics, alerts, and notifications across core Azure services for all business units.
- **Provide insight.** Business groups and service lines can view rich analytics and diagnostics across applications, as well as compute, storage, and network resources, including anomaly detection and proactive alerting.
- **Enable optimization.** Monitoring results help our business groups and service lines understand how users are engaging with their applications, identify sticking points, develop cohorts, and optimize the business impact of their solutions.

We're retiring our SCOM instances within the next three months, leaving Azure monitoring as the default for both cloud and on-premises monitoring. In the coming months, our transition will focus on:

- Automated installation and repair of the Microsoft Monitoring Agent using Azure Runbooks.
- Centralized visibility into comprehensive health and performance.
- Fully featured transition solution development to enable complete self-service monitoring in Azure.
- Complete transition from SCOM to Azure.

Patching, updating, and inventory management

We're piloting update and patch management in Azure for both cloud-based and on-premises infrastructure, and plan to roll out update management to the wider hybrid environment soon. As we've done for monitoring, we're using transition solutions to make it easier for business groups to transition from previously used on-premises tools to Azure.

Our patching processes depend on our preexisting solutions as we work through the transition to Azure. SCCM and associated agents provide the bulk of our patching, software distribution, and management process, but we're moving to Azure in a phased approach as our Azure subscriptions become ready to transition to Azure monitoring and management.

We've built transition solutions for our business groups to help them transition from the SCCM platform and other legacy tools to the Azure update management patching service. We're maintaining and modifying these transition solutions as we're ready for Azure features to replace the on-premises functionality.

From a patching and management perspective, we're focusing on:

- The transition of inventory management from Configuration Manager to Azure, including discovery, tracking, and management of IT assets.
- A software distribution feature comparison between Configuration Manager and Azure. This area is still maintained in Configuration Manager as we monitor the Azure feature set, to ensure that we create an Azure-based solution that fulfills the self-service requirements of our business groups.
- Continuing to transition our update processes to Azure Update Management for business groups.
- Enabling self-service patch management. We're developing an orchestrated deployment of operating system and application updates with Azure, including centralized compliance reporting.
- Creating and updating solutions to support the transition of the above areas, including Resource Manager templates, PowerShell scripts, documentation, and Azure Desired State Configuration.

The design for patching and management, as with monitoring, is to provide an Azure-based self-service solution for our business groups that gives them control over their patching and management environment while giving us the ability to centrally monitor for compliance and security purposes.

Ensuring recoverable data

With Azure as the primary repository for business data, it's extremely important to have an Azure backup solution with which our business groups and service lines can safeguard, retain, and recover their data. Our data recovery solutions address the following major areas of concern:

- Recover business data from attacks by malicious software or malicious activity.
- Recover from accidental deletion or data corruption.
- Secure critical business data.
- Maintain compliance standards.
- Provide historical data recovery requirements for legal purposes.

Our Azure data footprint is immense. We currently host 1.5 petabytes of raw data in Azure and use almost 9 petabytes of storage to back up that data.

We're using Azure Backup as a self-service solution. It gives business groups more control over how they perform their backups and gives them responsibility for backing up their business data—because each business group knows its data better than anyone else.

We're using Azure Backup for virtual machine-level backup, and we're backing up some on-premises data to Azure using Azure Recovery Services vaults. We've created a packaged solution for backup management in Azure that consists of scripts and documentation—our business groups can use it to quickly and efficiently migrate to Azure Backup.

As with other areas of enterprise management, we're evaluating new features for Azure Backup that will offer more backup capabilities to our business groups.

Embedding security and compliance

Decentralization gets the greatest scrutiny when it comes to security and compliance. We're responsible for security and legal compliance for the organization, so our security controls are the most centralized of all the cloud management solutions we implement. However, centralization does not directly affect day-to-day solution management for our business groups and their service lines.

We leveraged a broad set of security and compliance practices and tools that are generally applied across all Azure subscriptions. The following imperatives govern the general application of security and compliance measures:

- **Azure Policy.** Using Azure Policy, we establish guardrails in subscriptions that keep our service engineers within governance boundaries automatically. Policy can help control a myriad of settings by default, including limiting the network configurations to safe patterns, controlling the regions and types of Azure resources available for use, and ensuring data is stored with encryption enabled.
- **Automation** gives us a chance to keep pace with the constantly changing cloud environment. DevOps is heavily centered on end-to-end automation, and we need to complement DevOps automation with automated security. Automated security saves significant time and cost for apps that are frequently updated, and we can quickly and consistently configure and deploy security.
- **Empower engineering teams.** In an environment where change is constant, we want to empower our engineering teams to make meaningful, consistent changes without waiting for a central security team to approve an app. Our engineers need the ability to integrate security into the DevOps workflow. They don't have to take extra measures to be secure, nor do they need to wait for a central security team to approve an app.
- **Maintain continuous assurance.** When development and deployment are continuous, everything that goes with them needs to follow suit—including security assurance. The old requirements for sign-offs or compliance checks create tension in the modern engineering environment. We want to define a security state and track drift from that state to maintain a consistent level of security assurance across the entire environment. This helps ensure that builds and deployments that are secure when they're delivered stay secure from one release iteration to the next and beyond.
- **Set up operational hygiene.** We need a clear view of our DevOps environment to ensure operational hygiene. In addition to understanding operational risks in the cloud, DevOps operational hygiene in the cloud requires a different perspective. We need to create the ability to see the security state across DevOps stages and establish capabilities to receive security alerts and reminders for important periodic activities.

Using the Secure DevOps Toolkit for Azure

The Secure DevOps Kit for Azure is a set of tools that offer a security-focused development workflow for our DevOps engineering teams working in the cloud. The kit empowers our teams to build and use Azure-based solutions in a consistent, repeatable, and efficient manner with security integrated at every stage.

We use the Secure DevOps Kit for Azure to approach cloud development security in the following areas:

- **Subscription security.** Ensures that a subscription is configured and provisioned with necessary security controls, including Azure Policy and appropriate logging.
- **Secure development.** Provides the ability to write secure code and spot-check secure configuration of cloud resources.
- **Continuous integration and continuous deployment (CI/CD) extensions.** Integrates security testing into CI/CD workflows.
- **Continuous assurance.** Helps ensure that the security state stays compliant and doesn't drift over time.
- **Alerting and monitoring capabilities.** Checks for security events and provides an effective remediation path for subscription and application security issues.
- **Telemetry dashboards.** Gets aggregate views of security patterns and trends to make concerted improvements.

Looking forward

At Core Services Engineering and Operations, our goal is a completely cloud-based, self-service management solution that gives our business groups concise control over their environments using Azure tools and features. We'll continue to offer updated Azure-based solutions, transitioning away from on-premises, System Center–based management. As we continue to transition business groups to cloud-based monitoring, we're growing our feature set and making our Azure-based management even better. We envision a near future where our management systems will be completely cloud based, decentralized, and automated—and our organization continuing to build our business in Azure.

For more information

Microsoft IT Showcase

microsoft.com/itshowcase