Guide to Modern Monitoring:

HOW TO GAIN VISIBILITY AND IMPROVE OPERATIONS IN AZURE

VIAcode

Microsoft Azure is a cloud services platform that helps organizations build, run, and manage applications. The benefits of Azure help make moving to the cloud an easy decision. By moving to Azure, organizations can:

- Accelerate development and deployment cycles
- Improve application and data management
- Reduce operating costs
- Enhance data and application security
- Improve application availability and reliability

Despite the many advantages offered with an Azure deployment, many companies aren't prepared to manage the monitoring requirements needed to ensure their new cloud-based infrastructure is working as effectively and efficiently as possible.

MONITORING IN AZURE IS VERY DIFFERENT FROM MONITORING AN ON-PREMISE INFRASTRUCTURE

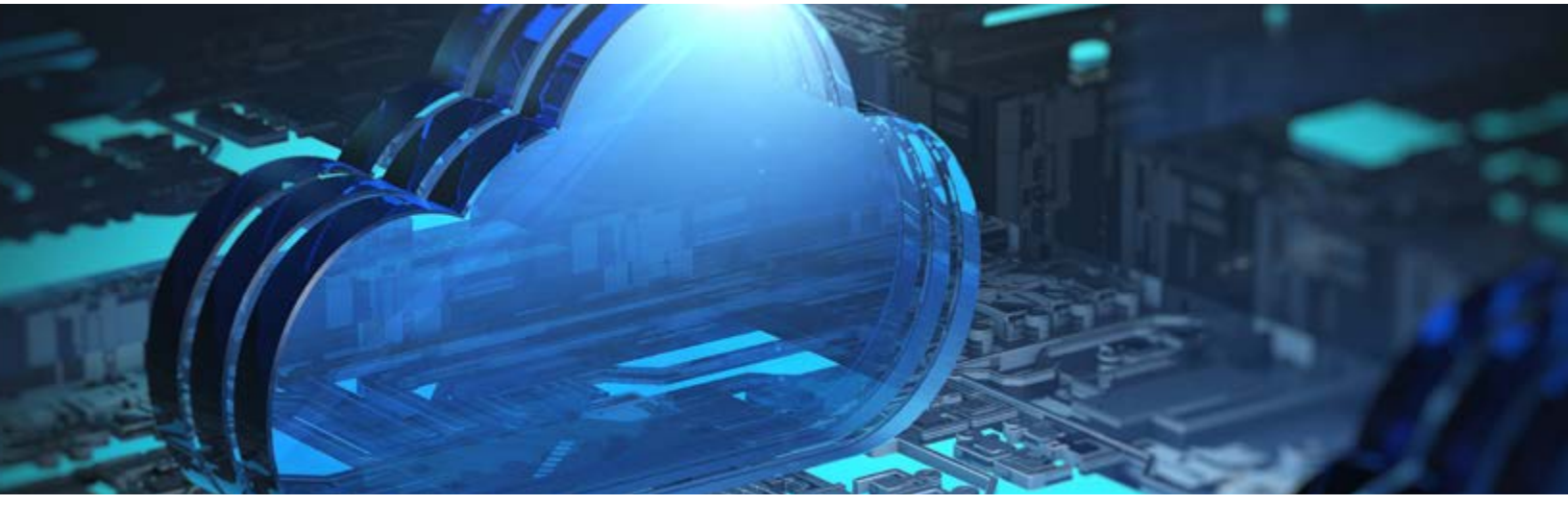
While similarities exist between on-premise and cloud monitoring, cloud monitoring offers superior scalability and manageability, along with a lower total cost of ownership. However, monitoring in the cloud requires different skills, tools and processes than on-premise monitoring, particularly when it comes to achieving observability across critical components, such as:

- Cost
- VM and Services Provisioning
- Security

Careful and thorough monitoring ***is essential to reduce risk and waste in Azure***. Not having an effective Azure monitoring plan in place can have a significant impact. Current cloud statistics reveal:

- 30% of cloud spend is a waste
- Overprovisioning cloud infrastructure costs businesses over $8.7 billion annually
- 53% of businesses claim that visibility is a barrier to adopting a cloud-based infrastructure
- The cost of noncompliance in a cloud-based infrastructure is 2.7 times the cost of noncompliance in an on-premise environment
- 60% of cloud-based backups are incomplete

A well-established monitoring process built on the foundation of the Azure Cloud Monitoring Framework can help businesses minimize and even proactively avoid these sorts of risks, liabilities, and unnecessary expenses.



ESTABLISH AN AZURE CLOUD MONITORING FRAMEWORK

The Azure Cloud Monitoring Framework is a core set of best practices and strategies that any organization needs to maximize observability (and, as a result, manageability) across their Azure environment. It is also foundational to the development of a Cloud Center of Excellence (CCoE). Each of the core pillars of a CCoE – financial management, security and operations – has specific requirements for monitoring and alerting. The Azure Cloud Monitoring Framework ensures each pillar of a CCoE is able to achieve its core function:

FINANCIAL MANAGEMENT

Aligning cost investments with business expectations

OPERATIONS

Maintaining proper availability and performance of cloud environment

SECURITY

Proactively increasing security depth and eliminating vulnerabilities

DESIGN TIME VS. RUN TIME MONITORING

The Azure Cloud Monitoring Framework looks at monitoring through two lenses:

DESIGN TIME
How things should be configured based on best practices

RUN TIME
What's going on now

Developing a monitoring framework that focuses on Design Time and Run Time enables businesses to choose and implement the right tools to quickly escalate notifications to the proper channels as well as eliminate potential communication gaps for optimized operational efficiency and cost savings. In other words, a strong and comprehensive monitoring foundation ensures better availability and, if appropriate, improved service level agreement (SLA) achievement. Also, understanding monitoring from these perspectives allows organizations to anticipate and adjust a process ***before an issue impacts the Azure environment.*** Let's take a closer look at Design Time vs. Run Time Monitoring as it affects Financial Management, Operations and Security.

DESIGN TIME MONITORING

There are many tools available to help drive Design Time visibility and monitoring, including these Microsoft Azure services:

- Azure Advisor
- Azure Policy
- Azure Automation

These tools offer some essential out-of-the-box capabilities and functionality. While they may boost visibility and help improve operations, it's also important to note any tool will have gaps that clients need to be aware of and need to have a plan to address upon implementation:

Azure Advisor

Functionality

Azure Advisor offers insight across all three Cloud Center of Excellence Pillars: Financial Management, Operations, and Security.

Considerations

Cost and reliability monitoring for Azure Advisor can be limited. Out-of-the-box logging may be focused on data that is not important to your operations, and as a result, organizations can incur unnecessary costs collecting data that is never used. Because you must think critically before implementing any recommendations, fine-tuning (customizing) the logging process is an important step towards driving the best possible outcomes.

Azure Policy

Functionality

Azure Policy helps to codify governance of the Azure environment and infrastructure. It allows for the development of customized, company-specific operational policies, along with providing out-of-the-box capabilities that can be immediately implemented. For example, Azure Policy can enforce tagging rules that help annotate specific Azure costs and cost centers. Azure Policy includes built-in compliance benchmarks for a wide range of industry-specific policies.

Considerations

Out of the box, Azure Policy offers no native alerting. As a result, businesses need to establish a process that ensures someone goes into the system to identify potential policy violations or the company must implement customized coding that integrates with an existing IT service management solution (ITSM) and triggers automated alerts and notifications.

Azure Automation

Functionality

Azure Automation improves management across the Azure environment by providing process automation, configuration management, update management and other capabilities critical to your infrastructure. Important from a design time monitoring perspective, Azure Automation includes two services for managing Windows infrastructure: State Configuration to update services and applications, and Update Management to manage operating system updates/patches.

Considerations

Azure Automation offers no out-of-the-box alerts. It's a great tool to build on top of, but customization is essential to maximizing its value.

RUN TIME MONITORING

Much like Design Time monitoring, there are also many services available to help drive Run Time visibility and monitoring.

Azure Cost Management

Functionality

Azure Cost Management allows users to define and manage budgets and economic forecasts.

Considerations

Effective use of Azure Cost Management requires budget and alerts to be properly defined. However, Azure Cost Management alerts do not natively integrate into a single ticketing system and most alert connectors only pick up Azure Monitor alerts; incorporating cost alerts, therefore, means custom development is needed.

Azure Monitor

Functionality

Azure Monitoring is used for activity-based alerting, metric-based alerting, synthetic transaction alerts, and log-based alerts. It provides tons of insights on operations within Azure.

Considerations

The challenge with Azure Monitor is the absence of out-of-the-box alerting. If you're used to an ecosystem of alerts, you will need to integrate Azure Monitor alerts into your own alerting system, again with custom development or a third-party connector.

Azure Defender

Functionality

Azure Defender delivers cloud security and cloud workload protection to find potential security gaps and risks within the cloud environment. The system provides built-in alerting and is an important tool for monitoring your security posture.

Considerations

As with other tools mentioned, Azure Defender alerts are not integrated with other service alerts or with an ITSM out of the box. And since most connectors will not pick up these alerts, custom development is required in order to transform your ticketing system into a single source of truth for capturing, reviewing and triaging all Azure alerts.

Azure Sentinel

VIAcode recommends starting with Azure Defender for Cloud and eventually moving to Azure Sentinel if appropriate. Azure Sentinel has built-in algorithms that provide out-of-the-box alerting, however, only if you connect all the appropriate data streams (a potential gap). Additionally, Azure Sentinel can be cost prohibitive.

IMPLEMENTING YOUR MONITORING STRATEGY: *Our Three Step Process*

As noted above, consideration for how alerts are aggregated and reviewed is critical. You have to identify the ideal services for your cloud-based environment and configure them for your monitoring needs. The Azure Cloud Monitoring Framework provides guidance on how to develop a strategy that is right for your organization and that:

- Assesses needs
- Identifies services
- Configures services
- Aggregates alerting
- Defines triage process

IT IS CRUCIAL TO NOTE THAT NO OUT-OF-THE-BOX TOOL OFFERS IT ALL.

Many businesses find it challenging to find the expertise and time needed to properly implement the monitoring framework. Luckily, they do not need to go at it alone. VIAcode's Cloud Center of Excellence (CCOE) services deliver the people, processes, and tools needed to ensure Azure environments are monitored and managed effectively.

STEP 1.

BASE-LEVEL MONITORING AND OBSERVABILITY

The first step is to define your base-level monitoring – how you will monitor the most important factors and components in your cloud infrastructure. We recommend the following tools across each main pillar within a Cloud Center of Excellence.

Financial Management

- Azure Policy
- Azure Cost Management

Operations

- Azure Advisor
- Azure Monitor
- Azure Policy

Security

- Azure Defender for the Cloud
- Azure Policy

In order to define base-level monitoring, at a minimum, an organization should consider:

1. Implementing tagging on every resource. There should be three tags on each resource in order to ensure visibility and accountability for financial management: resource owner, cost center and service name.
2. Establish your budget and budget alerts.
3. Consider each of the Azure Advisor recommendations. These are based on best practices that Microsoft compiled from their customers' experience. Not each of the recommendations needs to be implemented, but the decision to implement or suppress should be deliberate.
4. At a minimum, implement availability monitoring to determine if services are up or down (synthetic transaction monitoring) and capacity monitoring to make sure applications are able to perform as expected.
5. Implement out-of-the-box policies from Azure Policy like the built-in backup policy that facilitates consistency and enforces backups for your database, SQL Server, etc.
6. VIAcode recommends implementing the paid version of Defender for the Cloud which includes built-in alerting and built in compliance policies for industry standards and benchmarks.

Remember, it's usually not enough to just identify and deploy these services. You will also need to define alerting thresholds, ensure the appropriate components of your environment are being monitored, and perform other customization as appropriate for your environment and business needs.

STEP 2.

ITSM SYSTEM INTEGRATION

Once you've determined what you will monitor, it's vital to connect all individual tools and systems into a single internal ticketing system and into your ticketing process to ensure alerts and recommendations don't get overlooked.

Usually accomplished via custom coding and APIs or a 3rd-party connector, this integration allows you to automate the ticketing process. Every event that one of the monitoring services detects will be documented. The incident record will include all the necessary information to troubleshoot the event, and the incident can be routed to the appropriate team for resolution.

ITSM integration provides your organization with greater visibility into your Azure environment, greater accountability among technical teams, and a faster mean time to resolution for any issues that arise.

Third-party solutions like the VIAcode ITSM Connector provide a simple, streamlined integration between ticketing systems and the Microsoft Azure services. This connector consolidates different Azure signals into a single workflow and ticketing system, making it easier to track and manage issues.

STEP 3.

ONGOING MANAGEMENT AND OPTIMIZATION

Gathering the data into one system and escalating alerts is critical, but you cannot stop there. It is equally important to develop a cadence (daily, weekly, monthly, etc.) of activities to look at and analyze the data, provide regular cost analysis and cost reports, and take action on all alerts and recommendations in order to continually improve and optimize your cloud environment.

Steps you should take to ensure an efficient Azure infrastructure and a return on your Azure environment include:

1. Create a custom dashboard that aggregates data from all sources used and provides a customized visualization of all metrics involved
2. Routine analysis of your security score
3. Identify areas of improvement for your security posture
4. Implement financial management governance
5. Periodically review and adjust monitoring/alerting thresholds

Establishing ongoing management and optimization activities is core to the Azure Cloud Monitoring Framework, as this is the way to ensure operational visibility into your Azure environment. The following elements can help ensure visibility across the Cloud Center of Excellence's three main pillars:

Financial Management

- Azure Cost Reporting
- PBI Cost Reporting

Operations

- Built-in Azure Monitor Insights
- Custom Azure Dashboards
- Custom Azure Monitoring Workbooks

Security

- Secure Score
- Built-in Compliance Assessments
- Custom Azure Dashboards
- Custom Azure Monitoring Workbooks

DEVELOPING INTERNAL BEST PRACTICES TO SUPPORT YOUR AZURE CLOUD MONITORING FRAMEWORK

You've implemented and integrated the necessary steps to support a successful Azure Cloud Monitoring Framework. It's vital to continuously reevaluate your existing system as new systems, tools, and protocols are introduced to the cloud. VIAcode recommends the following best practices to maintain a cost-effective, streamlined, and secure cloud environment:

1. Periodically reassess base-level monitoring to determine the most important things in the cloud, including Azure Cost Reporting and PBI Cost Reporting.
2. Revisit your budget and alerting thresholds. Again, be intentional when deciding what alerts you should receive or suppress.
3. Connect all newly integrated components into your ticketing system and existing process to eliminate potential gaps.
4. Recalibrate the ticket management process as needed to reinforce cloud optimizations and improvements.

MOST COMPANIES DON'T HAVE THE RIGHT INTERNAL RESOURCES TO MONITOR AND MANAGE THEIR CLOUD ENVIRONMENT

When it comes to effectively monitoring your Azure environment, there is a lot to do. Many companies assume they can launch their cloud-based infrastructure and handle issues as they arise. However, having the people, processes, and tools needed to effectively manage and monitor the environment is challenging for most organizations. Additionally, not having a monitoring plan in place before implementation increases risks such as:

- Inability to detect a critical problem
- Security lapses that leave the system vulnerable
- Unnecessary expenses that go undetected

Some organizations have people or teams dedicated to monitoring. However, most do not, which can create significant liability for a business.

At VIAcode, our team of Azure professionals can work with your existing internal resources or serve as an entire outsourced team based on your specific needs. We create and implement customized strategies and solutions using both Azure services and our own built-for-Azure tools to drive efficiencies across all three critical pillars (Financial, Operational, Security) of a Cloud Center of Excellence.

We understand the complexities and challenges of developing an Azure Monitoring strategy and plan. Our team is ready to implement a plan that's right for your specific goals and concerns.

Learn more about

GAINING VISIBILITY AND IMPROVING OPERATIONS IN AZURE

Book a call with a VIAcode representative to discuss ways our Azure monitoring experts can help you identify issues before they become a problem, reduce costs, and eliminate security vulnerabilities.

SCHEDULE A CALL TO LEARN MORE

VIAcode
Microsoft Gold Partner

Follow VIAcode for more webinars, resources, and insights on Microsoft Azure optimization and management.

860-882-1150 | info@viacode.com | www.viacode.com |

REDMOND, WA OFFICE
8201 164th Ave NE, Suite 240
Redmond, WA 98052

WEST HARTFORD, CT OFFICE
7 South Main St, Suite 206
West Hartford, CT 06107