MICROSOFT AZURE MONITOR

Define IT compliance with Azure Policy

Good IT governance involves planning your initiatives and setting priorities on a strategic level to help manage and prevent issues.
You need good governance when:
•You have multiple engineering teams working in Azure
•You have multiple subscriptions in your tenant
•You have regulatory requirements that must be enforced
•You want to ensure standards are followed for all IT allocated resources

You could enforce standards by not allowing teams to directly create Azure resources - and instead have the IT team define and deploy all cloud-based assets.

This approach is often the solution in on-premises situations, but this requirement reduces the team agility and ability to innovate

Instead, Azure provides several tools you can use to enforce and validate your standards, while still allowing your engineering teams to create and own their own resources in the cloud.

Azure Policy

Azure service you use to create, assign and, manage policies. These policies enforce different rules and effects over your resources so that those resources stay compliant with your corporate standards and service level agreements.

Azure Policy meets this need by evaluating your resources for noncompliance with assigned policies

With the right type of policy, existing resources can be brought into compliance.

Imagine we allow anyone in our organization to create virtual machines (VMs).

Once the policy is implemented, Azure Policy will stop anyone from creating a new VM outside the list of allowed stock keeping units (SKUs).

How are Azure Policy and RBAC different?

At first glance, it might seem like Azure Policy is a way to restrict access to specific resource types similar to role-based access control (RBAC). However, they solve different problems. RBAC focuses on *user actions at different scopes*. You might be added to the contributor role for a resource group, allowing you to make changes to anything in that resource group. Azure Policy focuses on *resource properties during deployment* and for already-existing resources. Azure Policy controls properties such as the types or locations of resources. Unlike RBAC, Azure Policy is a

Creating a policy

The process of creating and implementing an Azure Policy begins with creating a *policy definition*.

1.Create a policy definition
2.Assign a definition to a scope of resources
3.View policy evaluation results

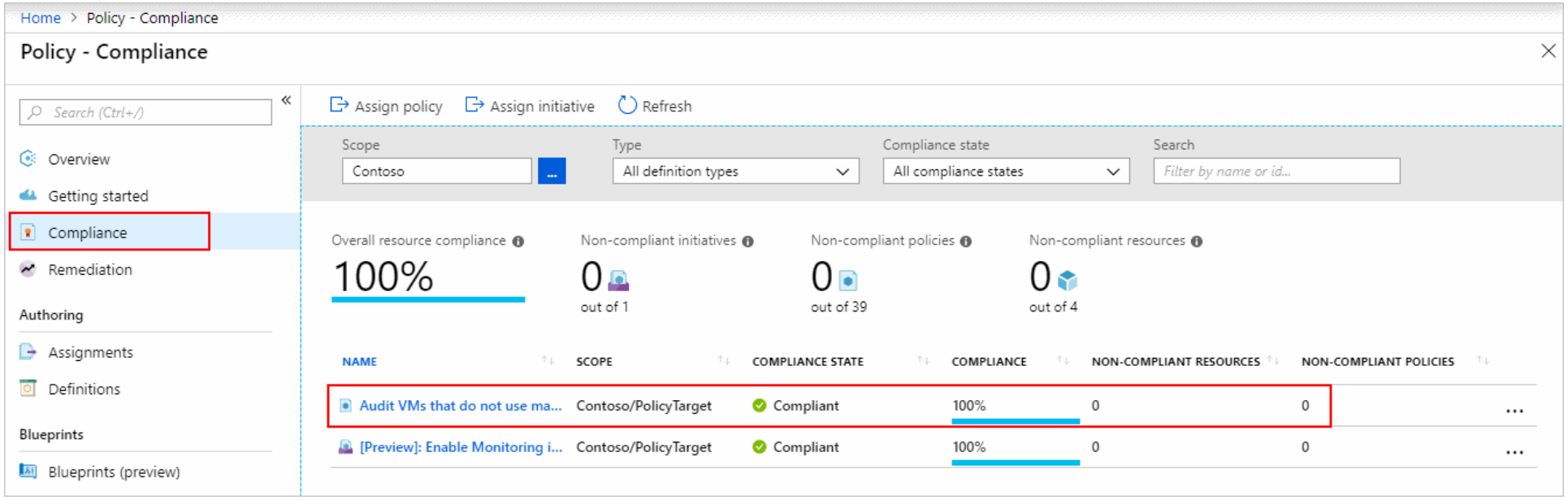
Here are some of the most common policy definitions you can apply.

Policy definition	Description
Allowed Storage Account SKUs	This policy definition has a set of conditions/rules that determine whether a storage account that is being deployed is within a set of SKU sizes. Its effect is to deny all storage accounts that do not adhere to the set of defined SKU sizes.
Allowed Resource Type	This policy definition has a set of conditions/rules to specify the resource types that your organization can deploy. Its effect is to deny all resources that are not part of this defined list.
Allowed Locations	This policy enables you to restrict the locations that your organization can specify when deploying resources. Its effect is used to enforce your geographic compliance requirements.
Allowed Virtual Machine SKUs	This policy enables you to specify a set of VM SKUs that your organization can deploy.
Not allowed resource types	Prevents a list of resource types from being deployed.

Identifying non-compliant resources

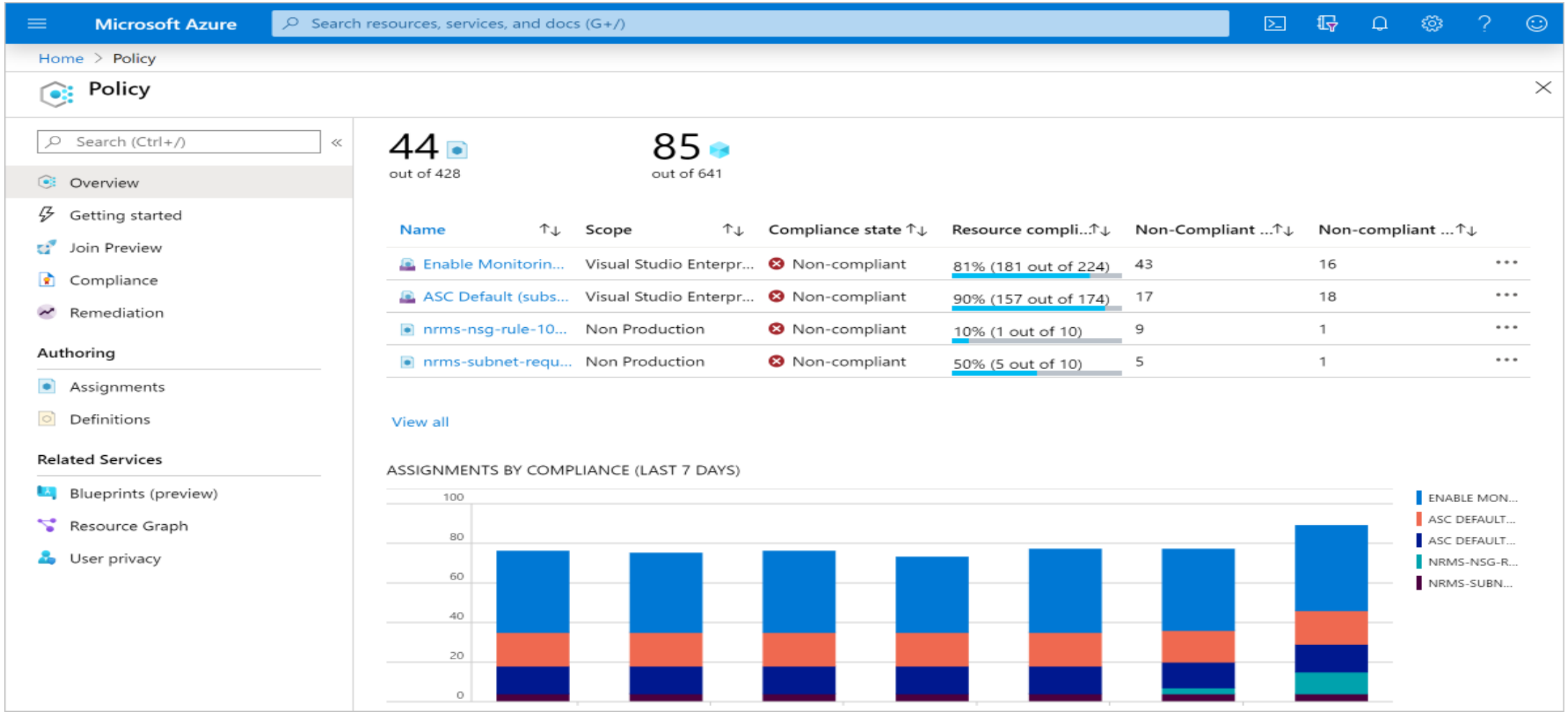
We can use the applied policy definition to identify resources that aren't compliant with the policy assignment through the Azure portal

The results match what you see in the Resource compliance tab of a policy assignment in the Azure portal:



View policy evaluation results

Azure Policy can allow a resource to be created even if it doesn't pass validation. In these cases, you can have it trigger an audit event that can be viewed in the Azure Policy portal, or through command-line tools.

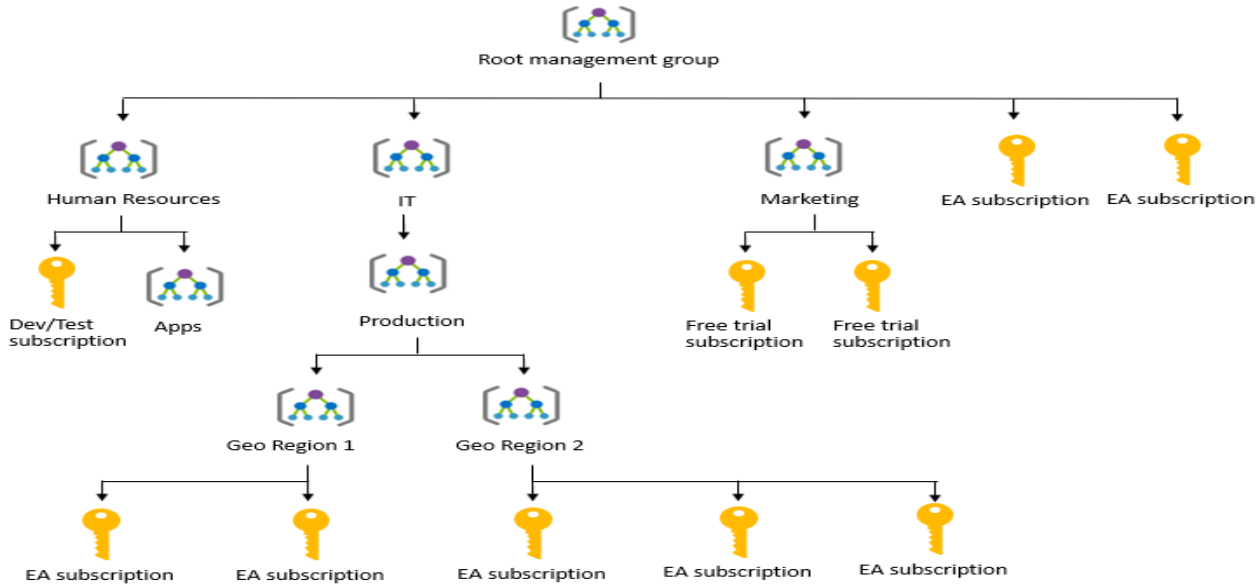


Enterprise governance management

Access management occurs at the Azure subscription level. This control allows an organization to configure each division of the company in a specific fashion based on their responsibilities and requirements.

Azure Management Groups are containers for managing access, policies, and compliance across *multiple* Azure subscriptions. Management groups allow you to order your Azure resources hierarchically into collections,

The following diagram shows an example of creating a hierarchy for governance using management groups.



Azure Blueprints

Adhering to security or compliance requirements, whether government or industry requirements, can be difficult and time-consuming. To help you with auditing, traceability, and compliance of your deployments, use **Azure Blueprint** artifacts and tools.

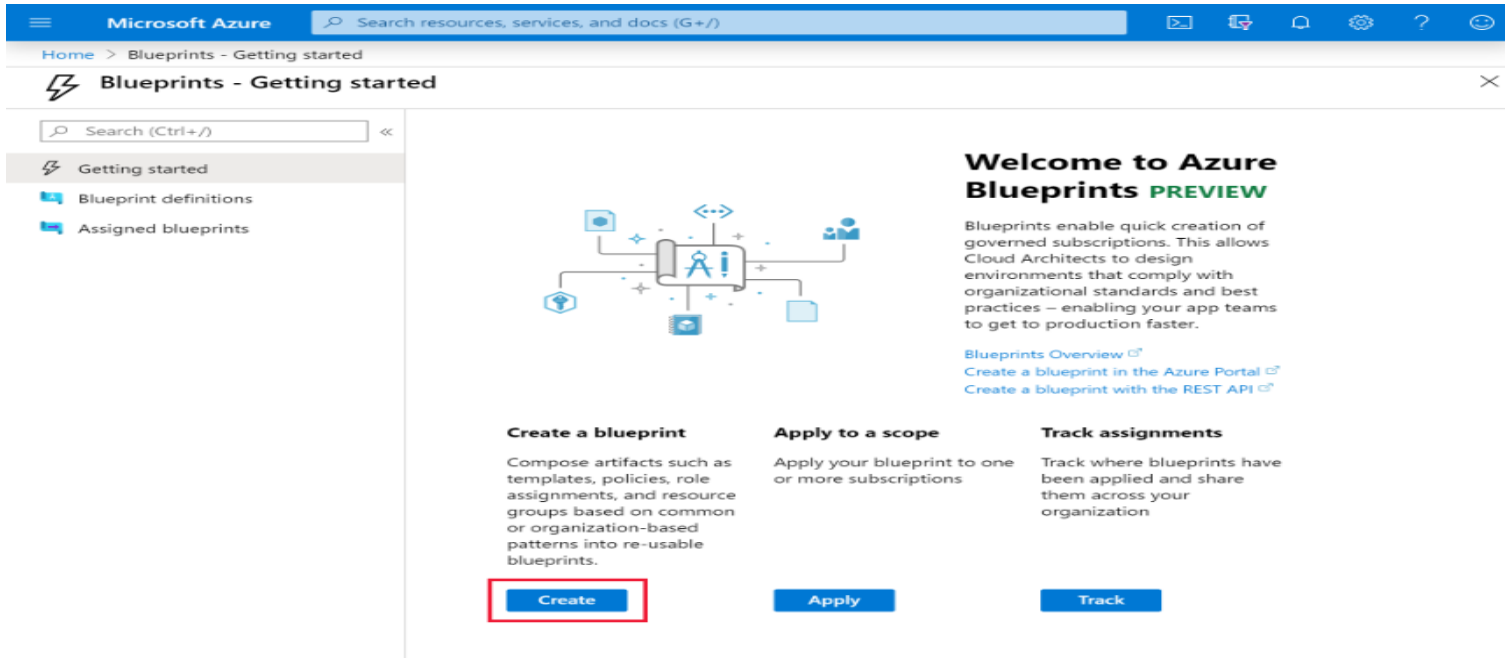
Just as a blueprint allows an engineer or an architect to sketch a project's design parameters,

Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.

Azure Blueprints makes it possible for development teams to rapidly build and deploy new environments with the trust they're building within organizational compliance using a set of built-in components, such as networking, to speed up development and delivery.

Azure Blueprints is a declarative way to orchestrate the deployment of various resource templates and other artifacts, such as:

- Role assignments
- Policy assignments
- Azure Resource Manager templates
- Resource groups



- The Azure Blueprints service is designed to help with environment setup.
- This setup often consists of a set of resource groups, policies, role assignments, and Resource Manager template deployments.
- A blueprint is a package to bring each of these artifact types together and allow you to compose and version that package—including through a CI/CD pipeline.

How it's different from Azure Policy

A blueprint is a package or container for composing focus-specific sets of standards, patterns, and requirements related to the implementation of Azure cloud services, security, and design that can be reused to maintain consistency and compliance.

A policy is a default-allow and explicit-deny system focused on resource properties during deployment and for already existing resources. It supports cloud governance by validating that resources within a subscription adhere to requirements and standards.

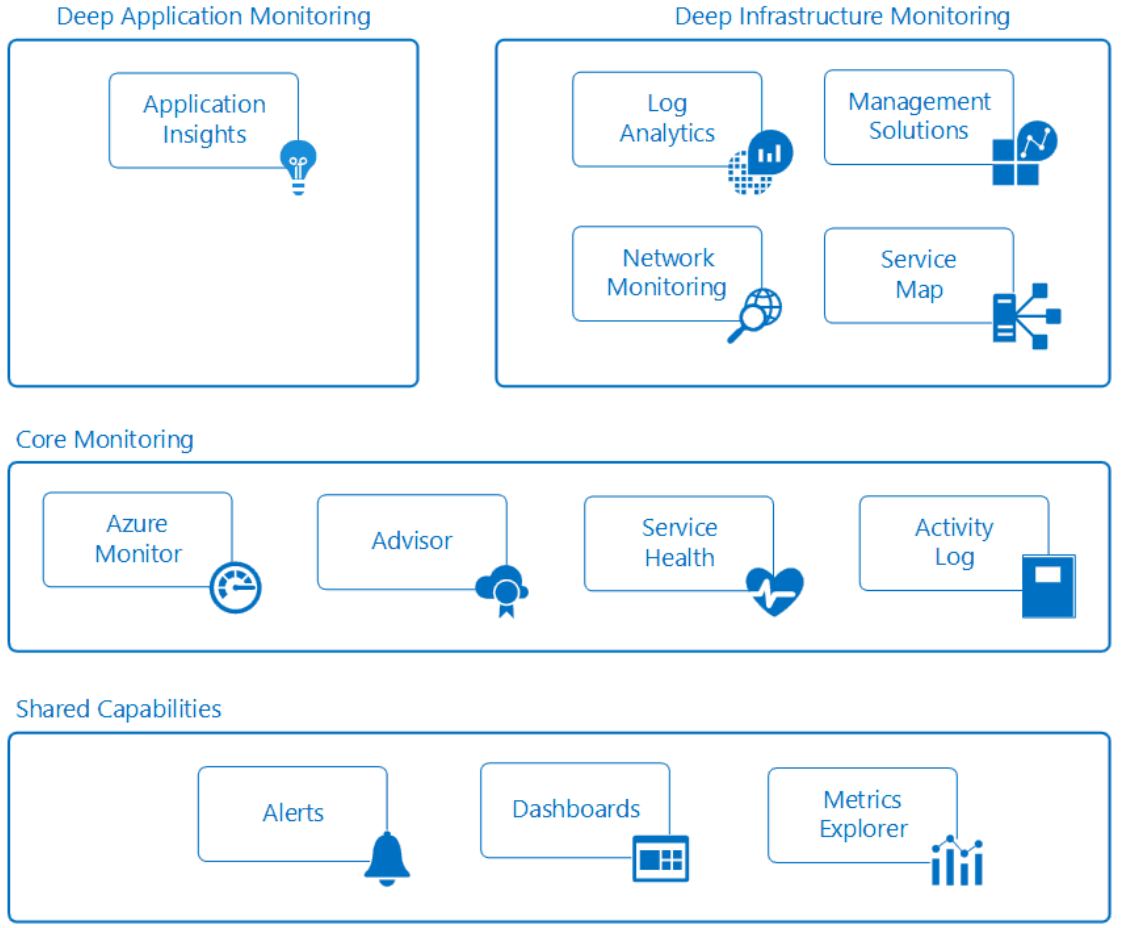
Azure Monitor

•Monitoring is the act of collecting data and analyzing to determine performance health and availability of the business application.

•An effective monitoring strategy helps to understand the detailed operations of the components and also increase uptime of the application.

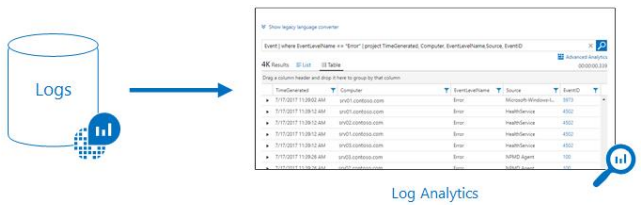
Following Broadly define tools of Monitoring

- Metrics Chart
- Log Analytics
- Dashboards
- Alerts
- Azure Advisor
- Activity Log



Monitoring data platform

- Data collected by Azure monitor fits in 2 broad categories metrics and logs.



- Many Azure resources metrics data is collected and visible on the Overview page.
- Log data collected by Azure can be analysed using queries.
- Kusto Query Language can be used to perform Simple as well as advanced queries.

What data does Azure Monitor collect

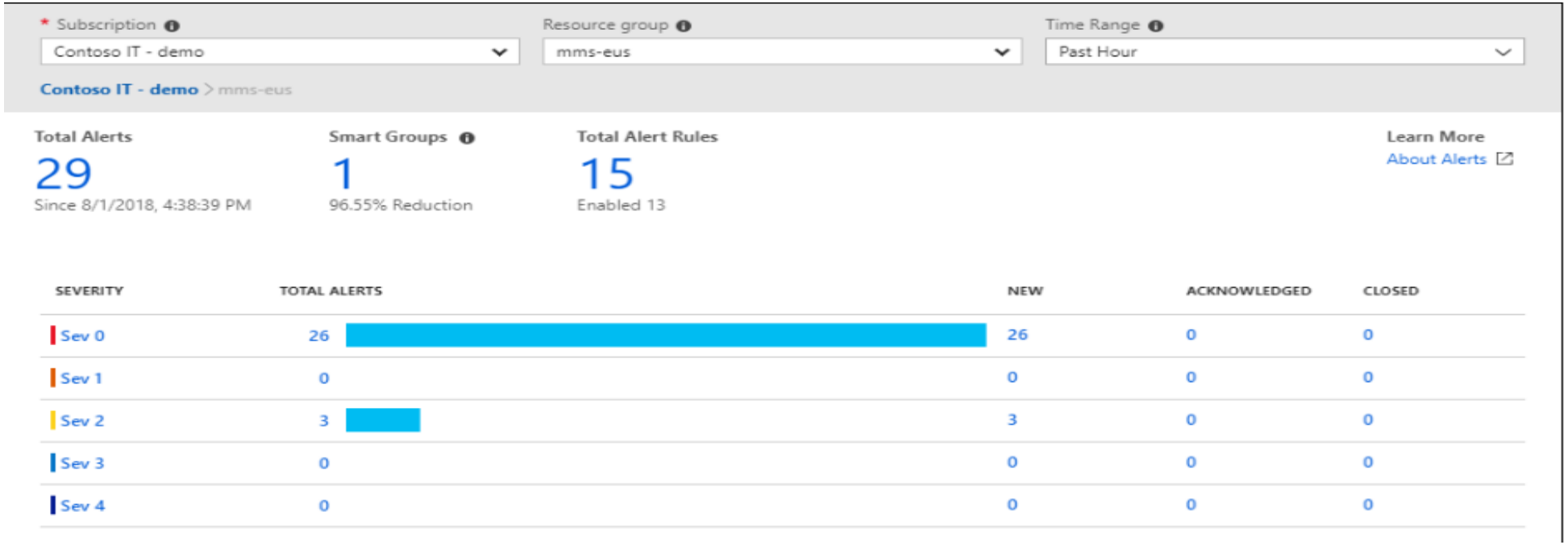
- Application Monitoring Data
- Guest OS monitoring Data
- Azure Resource Monitoring Data
- Azure Subscription Monitoring Data
- Azure Tenant Monitoring Data

Responding to critical situations

Setting up Alerts

Why ?

- Proactive Response to a situation which is critical or will be critical
- Informing right stakeholders on the issue.
- Right action at right time



Data sources

Azure Monitor can collect data from a variety of sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system and services it relies on, and down to the platform itself.

Data tier	Description
Application monitoring data	Data about the performance and functionality of the code you have written, regardless of its platform.
Guest OS monitoring data	Data about the operating system on which your application is running. This could be running in Azure, another cloud, or on-premises.
Azure resource monitoring data	Data about the operation of an Azure resource.
Azure subscription monitoring data	Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
Azure tenant monitoring data	Data about the operation of tenant-level Azure services, such as Azure Active Directory.

Diagnostic settings

As soon as you create an Azure subscription and start adding resources such as virtual machines and web apps, Azure Monitor starts collecting data. *Activity Logs* record when resources are created or modified and *Metrics* tell you how the resource is performing and the resources that it's consuming.

Application Insights is a service that monitors the availability, performance, and usage of your web applications, whether they're hosted in the cloud or on-premises. It leverages the powerful data analysis platform in Log Analytics to provide you with deeper insights into your application's operations. Application Insights can diagnose errors without waiting for a user to report them. Application Insights includes connection points to a variety of development tools, and integrates with Microsoft Visual Studio to support your DevOps processes.

Azure Monitor for VMs is a service that monitors your Azure VMs at scale, by analyzing the performance and health of your Windows and Linux VMs (including their different processes and interconnected dependencies on other resources, and external processes). Azure Monitor for VMs includes support for monitoring performance and application dependencies for VMs hosted on-premises, and for VMs hosted with other cloud providers.

Azure Service Health

Azure Service Health is a suite of experiences that provide personalized guidance and support when issues with Azure services affect you. It can notify you, help you understand the impact of issues, and keep you updated as the issue is resolved. Azure Service Health can also help you prepare for planned maintenance and changes that could affect the availability of your resources.

Azure Status provides a global view of the health state of Azure services. With Azure Status, you can get up-to-the-minute information on service availability. Everyone has access to Azure Status and can view all services that report their health state.

Service Health provides you with a customizable dashboard that tracks the state of your Azure services in the regions where you use them. In this dashboard, you can track active events such as ongoing service issues, upcoming planned maintenance, or relevant *Health advisories*. When events become inactive, they are placed in your *Health history* for up to 90 days. Finally, you can use the **Service Health** dashboard to create and manage service *Health alerts*, which notify you whenever there are service issues that affect you.

Resource Health helps you diagnose and obtain support when an Azure service issue affects your resources. It provides you with details about the current and past state of your resources. It also provides technical support to help you mitigate problems. In contrast to Azure Status, which informs you about service problems that affect a broad set of Azure customers, *Resource Health* gives you a personalized dashboard of your resources' health. *Resource Health* shows you times, in the past, when your resources were unavailable because of Azure service problems. It's then easier for you to understand if an SLA was violated.