Apply and monitor infrastructure standards with Azure Policy

1 IT Compliance

Definition: Azure Policy

An Azure service to create, assign and manage policies

RBAC focuses on user actions at different scopes whereas Azure Policy focuses on resouce properties during deployment. Azure Policy is a default allow and explicit deny system, in contrast with RBAC

1.1 Creating a policy

To apply a policy you will:

- Create a policy definition
- Assign a definition to a scope of resources
- View policy evaluation results

1.1.1 Policy definition

A policy definition expresses what to evaluate and what action to take

The policy definition itself is represented as a JSON file

1.1.2 Applying Azure Policy

This can be done using the Azure portal or one of the command line tools, it takes the following parameters

Parameter	Description
Name	The actual name of the assignment
DisplayName	Display name for the policy assignment
Definition	The policy definition, based on which you're using to create the assignment
Scope	A scope determines what resources or grouping of resources the policy assignment gets enforced on

1.2 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. Similarly, this can be done through the command line

1.3 Assigning a definition to a scope of resources

Definition: Policy assignment

A policy definition that has been assigned to take place within a specific scope

Policy assignments are inherited by all child resources. This inheritance means that if a policy is applied to a resource group, it is applied to that resource group.

1.4 Policy effects

Policy effect	What happens
Name	The actual name of the assignment
Deny	The resource creation/update fails due to policy
Disabled	The policy rule is ignored
Append	Adds additional parameters/field to the requested resource during creation or update
Audit, AuditifNotExists	Creates a warning event in the activity log, but doesn't stop the request
DeployIfNotExists	Executes a template deployment when a specific condition is met

2 Organise policy with initiatives

Definition: Initiative definition

A set or group of policy definitions to help track your compliance state for a larger goal

Definition: Initiative assignment

An initiative definition assigned to a specific scope

3 Enterprise governance management

Definition: Azure Management Groups

Containers for managing access, policies and compliance across multiple Azure subscriptions

Management groups allow you to order your Azure resources hierarchically into collections, which provide a further level of classification that is above the level of subscriptions.

4 Azure Blueprints

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

- Role assignments
- Policy assignments
- Azure resource manager templates
- Resource groups

The process of implementing Azure Blueprints consists of the following high-level steps:

1. Create an Azure Blueprint
2. Assign the blueprint
3. Track the blueprint assignments

The Azure Blueprints service is backed by the Azure Cosmos database to provide low latency and high availability.

4.1 Comparison with Resource Manager Templates

Blueprints sit above Resource Manager Templates, also including resource groups, policies and role assignments.

Blueprints can be managed directly in Azure, whereas Resource Manager Templates have to be managed separately.

4.2 Comparison with Azure Policy

Including a policy in a blueprint enables the creation of the right pattern or design during assignment of the blueprint.

5 Compliance Manager

Microsoft provides resource transparency using the following tools

5.1 Microsoft Privacy Statement

This explains what personal data Microsoft processes, how it is processed and for what purpose

5.2 Microsoft trust center

This contains all the details about how Microsoft implements and supports security, privacy, compliance and transparency in all Microsoft cloud products.

5.3 Service Trust Portal

This hosts the compliance manager service and is the Microsoft public site for publishing audit reports.

5.4 Compliance Manager

This provides the following features:

- Combines
    1. Audit results
    2. Information Microsoft compiles internally for its compliance with regulations
    3. An organisation's self assessment of their own compliance with these standards and regulations
- Enables you to assign, track, and record compliance and assessment-related activities
- Provides a compliance score to track progress
- Provides a repository for managing evidence relating to compliance
- Produces reports

6 Monitoring service health

6.1 Azure Monitor

This maximizes the availability and performance of applications using telemetry.

6.1.1 Data sources

Data Tier	Description
Application monitoring data	Data about the performance and functionality of written code
Guest OS monitoring data	Data about the OS your application is running
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 and azure itself
Azure tenant monitoring data	Data about the operation of tenant-level Azure services

6.1.2 Diagnostic Settings

Activity logs record when resources are created or modified
Metrics tell you how the resource is performing and the resources it's consuming

You can enable diagnostics

- Enable guest-level monitoring
- Performance counters - collect performance data
- Event logs - Enable various event logs
- Crash dumps - enable or disable
- Sinks - send your diagnostic data to other services for more analysis
- Agent - configure agent settings

6.1.3 Getting more data from your apps

Application insights - Monitors the availability, performance and usage of your web applications

Azure Monitor for containers - Monitors the performance of container workloads

Azure Monitor for VMs - Monitors the performance and health of your Windows and Linux VMs

6.1.4 Responding to alert notifications

Alerts - Azure notifies you of critical conditions using alerts and can attempt to take corrective actions
Autoscale - Ensures you have the right amount of resources running to manage the load on your application effectively

6.2 Azure Service Health

This provides guidance when issues with Azure notify you, it is composed of the following views:

- Azure Status - Global view of the health state of Azure Services
- Service health - Tracks the state of your services in the regions you use them
- Resource health - Diagnose and support when an Azure service issue affects your resources