Azure Policy: Overview and Key Concepts

Azure Policy is a governance tool in Microsoft Azure that enables you to define and enforce rules and regulations across your Azure resources. It helps you maintain compliance with organizational standards, regulatory requirements, and internal policies.

Key Features of Azure Policy

- **Policy Definition:** Define what is and isn't allowed within an Azure environment.
- **Policy Assignment:** Attach a policy to a scope, which could be a subscription, resource group, or management group.
- **Policy Evaluation:** Policies continuously monitor and evaluate resources for compliance.
- **Remediation:** Non-compliant resources can be remediated automatically or manually.
- **Compliance Reporting:** Provides insights and reports on the compliance state of resources.

Core Concepts

1. **Policy Definitions:**
    - A policy is a set of rules written in JSON format.
    - Policies can enforce specific actions like denying certain actions, auditing, or enforcing resource configuration.
2. **Policy Assignment:**
    - Policies are assigned to a specific scope, such as a subscription, resource group, or management group.
    - Each assignment can include parameters to customize the policy's behavior.
3. **Policy Parameters:**
    - Allow customization of policies by defining values that can be provided during policy assignment.
    - Example: Assigning a policy that restricts the use of specific VM sizes.
4. **Policy Effects:**
    - **Deny:** Prevents actions that don't comply with the policy.
    - **Audit:** Tracks non-compliance but doesn't block actions.
    - **AuditIfNotExists:** Checks if a certain resource exists and audits if it doesn't.
    - **DeployIfNotExists:** Deploys a resource if it doesn't exist.
    - **Modify:** Modifies resources to meet policy requirements.
5. **Compliance States:**
    - **Compliant:** The resource meets all policy rules.
    - **Non-compliant:** The resource doesn't meet policy rules.

- **NotApplicable:** The policy does not apply to the resource.
- **Unknown:** The compliance state cannot be determined.

Using Azure Policy

Step 1: Define a Policy

- You can use built-in policies or create custom ones.
- Define the policy by specifying the conditions in the policy rule and the desired effect.

Step 2: Assign a Policy

- Once a policy is defined, assign it to a scope like a subscription or resource group.
- You can apply it to a management group for broader control.

Step 3: Monitor Compliance

- Azure Policy continuously monitors compliance and provides insights via the Azure portal.
- The **Compliance Dashboard** provides an overview of policy compliance at the subscription or resource group level.

Step 4: Remediate Non-compliance

- Some policies can trigger automatic remediation actions, such as creating missing resources or modifying resources to bring them into compliance.
- You can manually remediate non-compliant resources through Azure portal or CLI.

Common Use Cases

- **Restrict Resource Creation:** Restricting the creation of certain types of resources, such as specific virtual machine sizes, regions, or resource types.
- **Enforcing Tags:** Ensuring that resources have the required tags for proper billing or organization.
- **Enforcing Security Configurations:** Enforcing the use of secure network configurations, such as requiring encryption or specific network rules.
- **Cost Management:** Preventing the creation of expensive resources like large virtual machines or storage accounts.

Best Practices for Using Azure Policy

- **Start with Built-in Policies:** Leverage Azure's built-in policies before creating custom ones.
- **Scope Wisely:** Apply policies at the appropriate scope, like resource groups or subscriptions, to avoid over-application.
- **Use Parameters:** Use parameters to make policies reusable and flexible.
- **Monitor Regularly:** Keep track of compliance using the Compliance Dashboard to quickly address non-compliant resources.

Conclusion

Azure Policy is a powerful tool for enforcing governance and compliance across Azure resources. It helps organizations meet regulatory requirements, optimize resource usage, and maintain a secure and compliant environment. By defining policies, assigning them, and monitoring their compliance, organizations can ensure they adhere to best practices and governance standards.