Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud Computing

Powerd by simplilearn

Caltech | Center for Technology & Management Education

PG CC - Microsoft Azure Architect Design: AZ:304

Powered by simplilearn

Design Governance

Learning Objectives

By the end of this lesson, you will be able to:

- Recommend a strategy for tagging
- Recommend a solution for using Azure policy
- Recommend a solution for using Azure blueprints
- Recommend a solution that leverages Azure resource graph

A Day in the Life of an Azure Architect

You are working as an Cloud Architect in a Fortune 500 organization.

You need to design a solution for developers which would grant them the ability to provision certain Azure Resources determined by the company. This will that help enforce corporate standards and analyze compliance at scale as an Azure Architect.

To achieve all of the above, along with some additional features, we would be learning a few concepts in this lesson that will help you find a solution for the above scenario.

Recommend a Strategy for Tagging

Tags

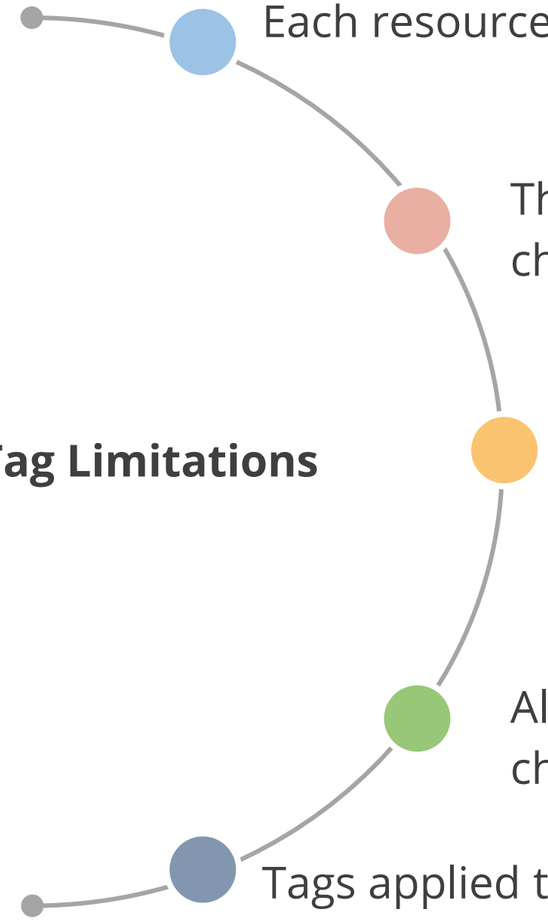
Tags logically organize your resources.

They consist of a name and value and help to retrieve related resources from different resource groups.

Daily Usage						
Usage Date	Meter Category	Unit	Consume	Resource Gr	Instance Id	Tags
5/14/2015	"Virtual Machines"	"Hours"	3.999984	"computeRG	"virtualMachines/catalogVM	"{"costCenter":"finance", "env":"prod"}"
5/14/2015	"Virtual Machines"	"Hours"	3.999984	"businessRG	"virtualMachines/dataVM"	"{"costCenter":"hr", "env":"test"}"

This approach is helpful when you need to organize resources for billing or management.

Limitations of Tags



- Each resource or resource group can have a maximum of 50 tag name/value pairs.
- The tag name is limited to 512 characters and the tag value is limited to 256 characters.
- For storage accounts, the tag name is limited to 128 characters and value to 256 characters.
- All tag names and values in virtual machines are limited to a total of 2048 characters.
- Tags applied to resource groups are not inherited by the resources in that resource group.

Tagging Example

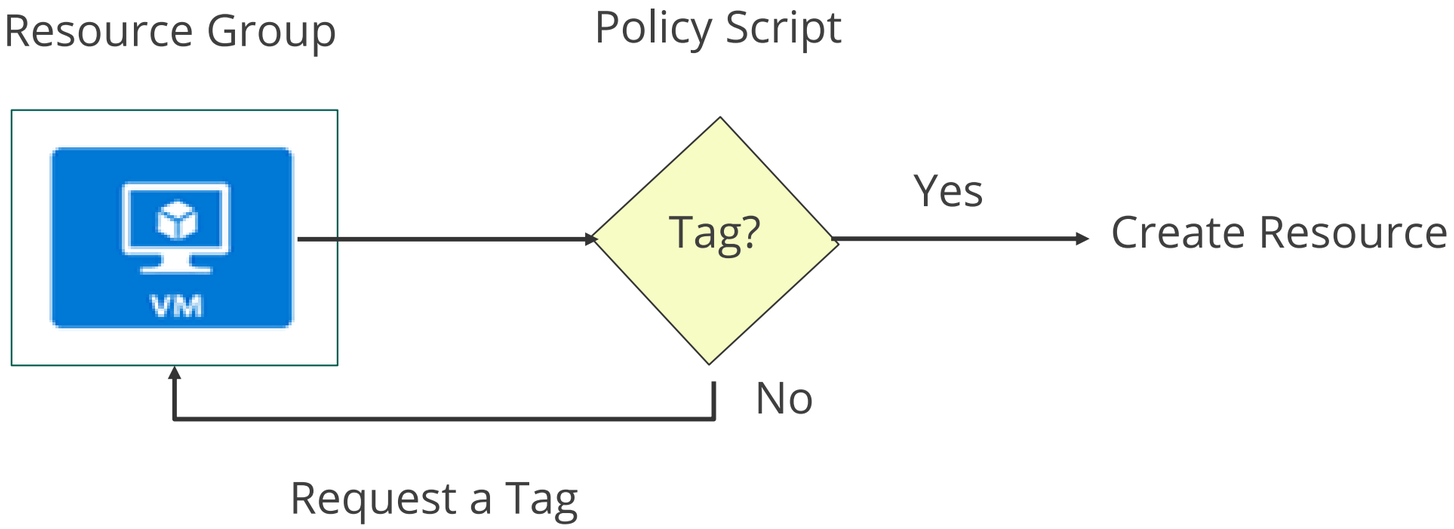
Tag type	Tag	Mandatory/ optional	Description	Data type
Technical	Region	Mandatory	Location	String
Technical	Environment	Mandatory	Dev, Stage, Prod	String
Technical	MaintenanceWindow	Mandatory	Patching window	String
Automation	Expiration Date	Optional	Terminate resource automatically	String
Automation	Time Window	Optional	Server online	JSON
Business	Department	Mandatory	Service belonging to department	String

Tagging Example

Tag type	Tag	Mandatory/ optional	Description	Data type
Business	Application name	Mandatory	Application name	String
Business	Cost center	Mandatory	Cost center ID	String
Business	Description	Optional	Text description of the entity	String
Business	TechnicalContact	Mandatory	Group responsible for application	String
Security	Data classification	Mandatory	Classification of data	String
Security	Regulatory compliance	Optional	Compliance requirement	JSON

Enforcing Tags with Policy

The workflow of enforcing tags using Azure policy is shown below:



Enforcing Tags with Policy

Policy	Description
Apply tag and its default value	Appends a specified tag name and value, if that tag is not provided. You specify the tag name and value to apply.
Billing Tags Policy Initiative	Requires specified tag values for cost center and product name. Uses built-in policies to apply and enforce required tags. You specify the required values for the tags.
Enforce tag and its value	Requires a specified tag name and value. You specify the tag name and value to enforce.
Enforce tag and its value on resource groups	Requires a tag and value on a resource group. You specify the required tag name and value.

Recommend a Solution for using Azure Policy

Azure Policy

Azure Policy is a service to create, assign and manage policies.

Policies enforce different rules and effects over resources, so those resources stay compliant with your corporate standards and service level agreements.

Example: You can have a policy to allow only a certain SKU size of virtual machines in your environment.

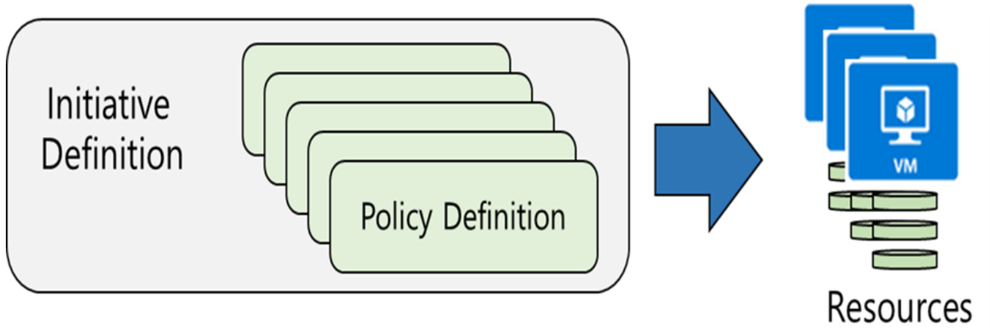
Azure Policy

There are azure policy advantages:

- **Enforcement and compliance** – Turn on policies for resources and get real time policy evaluation and enforcement
- **Apply policies at scale –** Apply multiple policies and aggregate policy states with policy initiative
- **Remediation –** Real time remediation

Implementing Azure Policies

These are the steps to implement Azure policies:

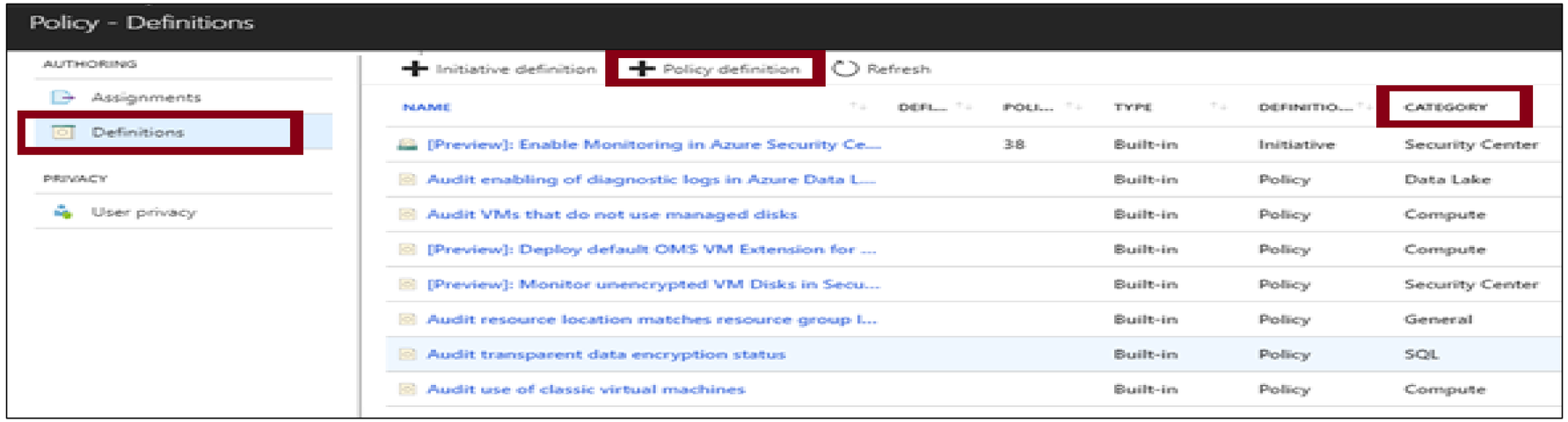


- Browse Policy Definitions
- Create Initiative Definitions
- Scope the Initiative Definition
- View Policy evaluation results

Browse Policy Definitions

A policy definition defines under what condition a policy is enforced and what effect to take.

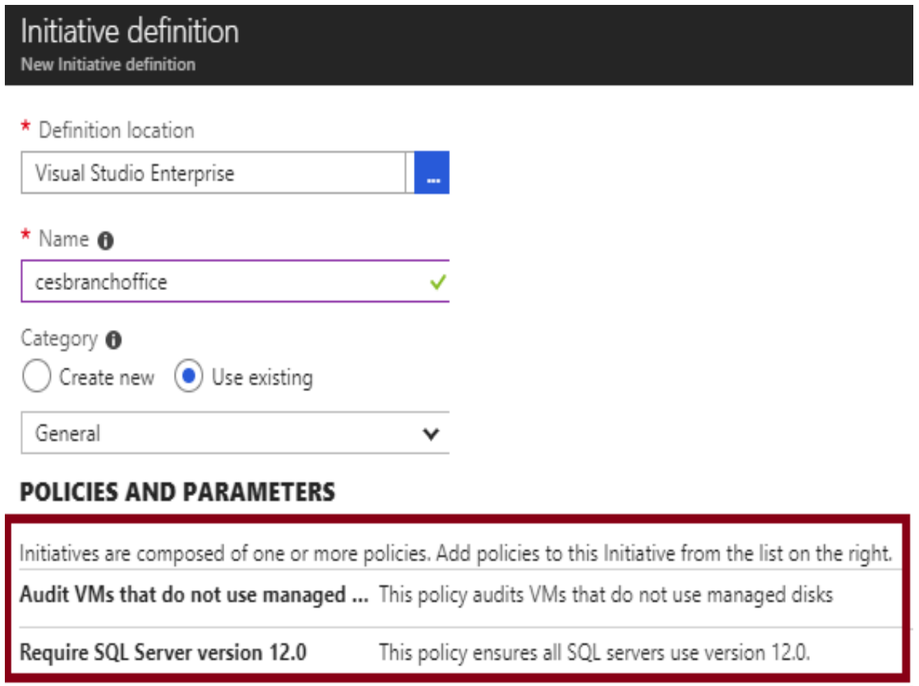
Example: User could prevent VMs from being deployed if they are exposed to a public IP address.



- User can import policies from GitHub
- Policy Definitions have a specific JSON format

Create Initiative Definitions

There are steps to create initiative definitions:

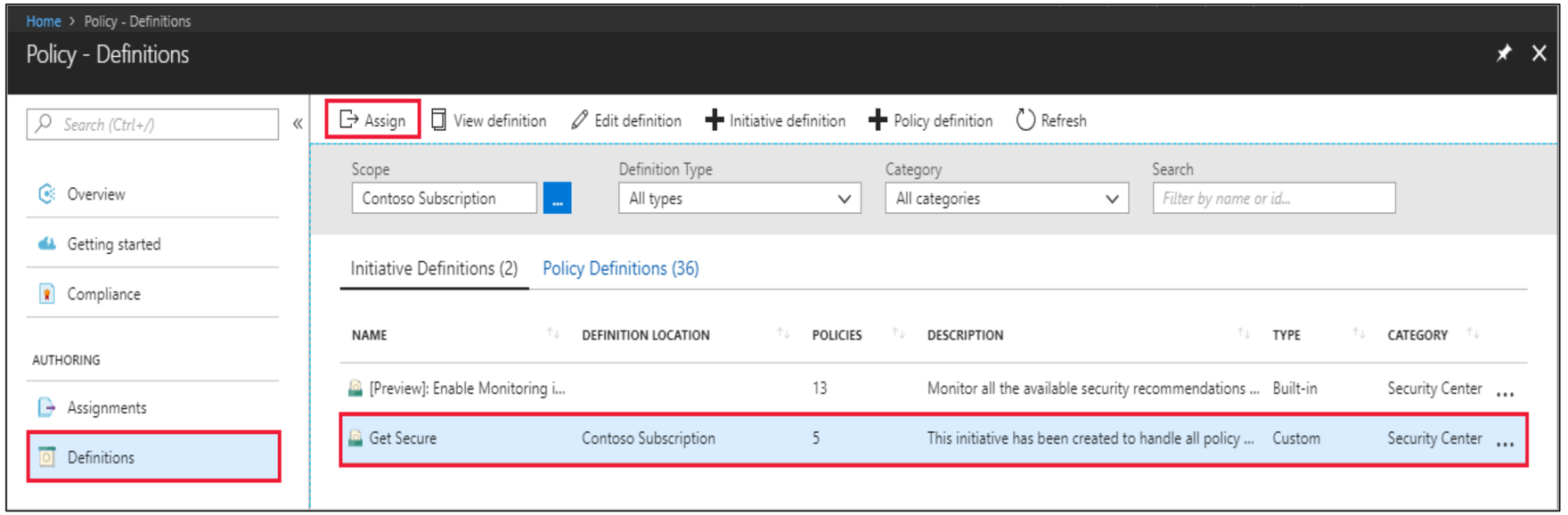


- Group policy definitions
- Include one or more policies
- Requires planning

Scope the Initiative Definition

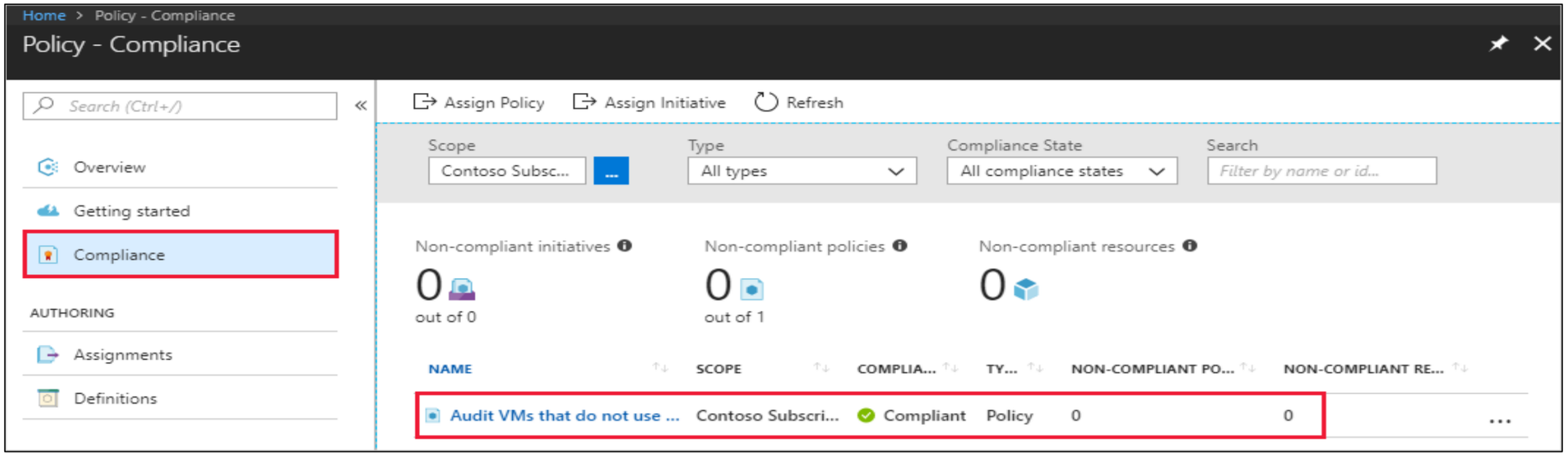
The scope determines on what resources or group of resources the policy gets enforced.

- Assign the definition to a scope
- Select the subscription, and optionally the resource group



Note: Currently, an Initiative Definition can have up to 100 policies.

Determine Compliance



Non-compliant initiatives

- **Non-compliant policies** – Number of Policy assignments with at least one non-compliant resource.
- **Non-compliant resources** – Once a condition is evaluated against your existing resources and found true, then the resources are marked as non-compliant with the policy.

Policy Effects

Policy creates a list of all assignments that apply to the resource and then evaluates the resource

Policy Effect	What happens?
Deny	The resource creation/update fails due to policy.
Disabled	The policy rule is ignored (disabled). Often used for testing.
Append	Adds additional parameters/fields to the requested resource during creation or update. A common example is adding tags on resources such as Cost Center or specifying allowed IPs for a storage resource.
Audit, AuditIfNotExists	Creates a warning event in the activity log when evaluating a non-compliant resource, but it doesn't stop the request.
DeployIfNotExists	Executes a template deployment when a specific condition is met. For example, if SQL encryption is enabled on a database, then it can run a template after the DB is created to set it up a specific way.

- Requests to create or update a resource through Azure Resource Manager are evaluated by Azure Policy first
- Policy processes several of the effects before handing the request to the appropriate Resource Provider to avoid violates policy

Assisted Practice

Azure Policy Creation

Duration: 10 Min.

Problem Statement:

You've been asked to assist your organization in developing an Azure governance solution that helps enforce corporate standards and analyze compliance at scale as an Azure Architect.

Assisted Practice: Guidelines

Steps to create an Azure policy and assign it to a resource:

1. Log in to the Azure Portal
2. Select Azure Policy
3. Create new Policy definition page
4. Add information in the new policy page
5. View the policy created
6. Assign a resource

Assisted Practice

Azure Policy Assignment

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you have been asked to aid your company with an Azure governance solution that can be utilized by Azure Policy to determine which resources are assigned to which policies or initiatives.

Assisted Practice: Guidelines

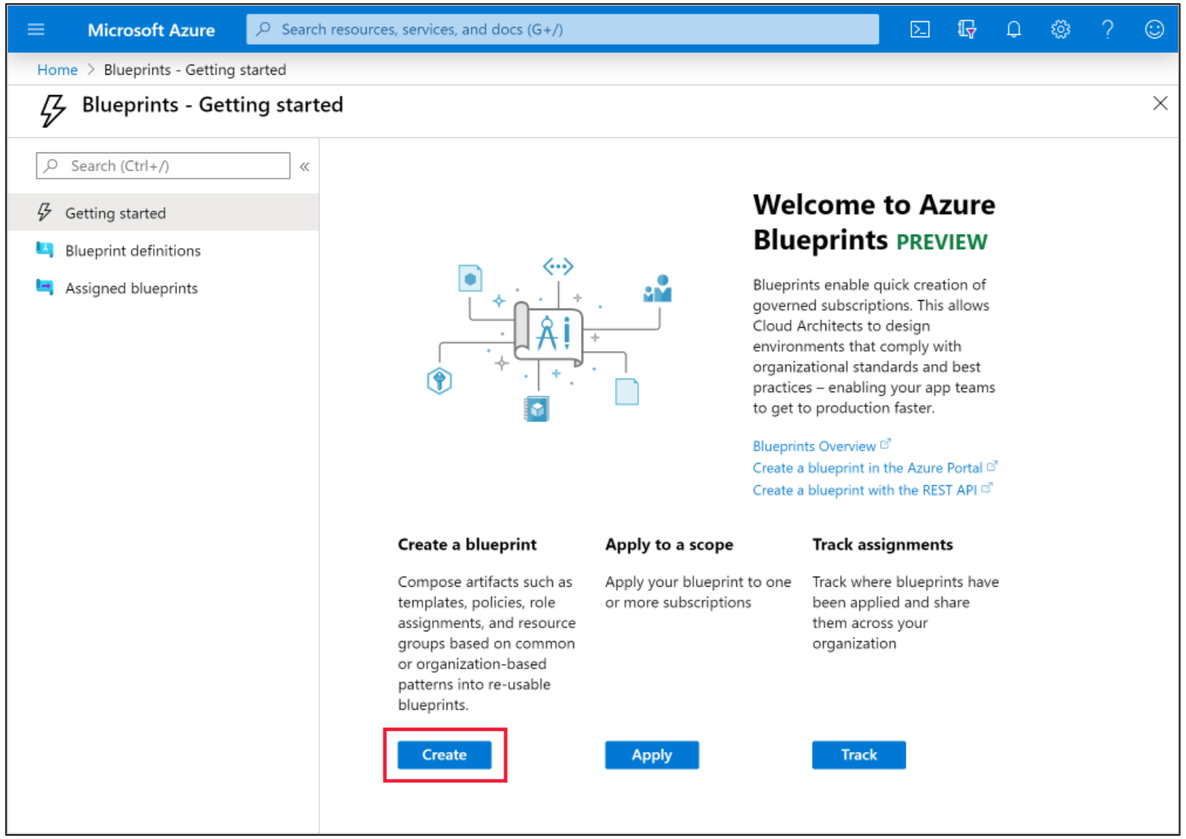
Steps to assign a policy assignment:

1. Login to your azure portal and click on More services
2. Search for Azure Policy and then select Policy
3. In the Policy pane, select Assignments and then click on Assign policy

Recommend a Solution for Using Azure Blueprints

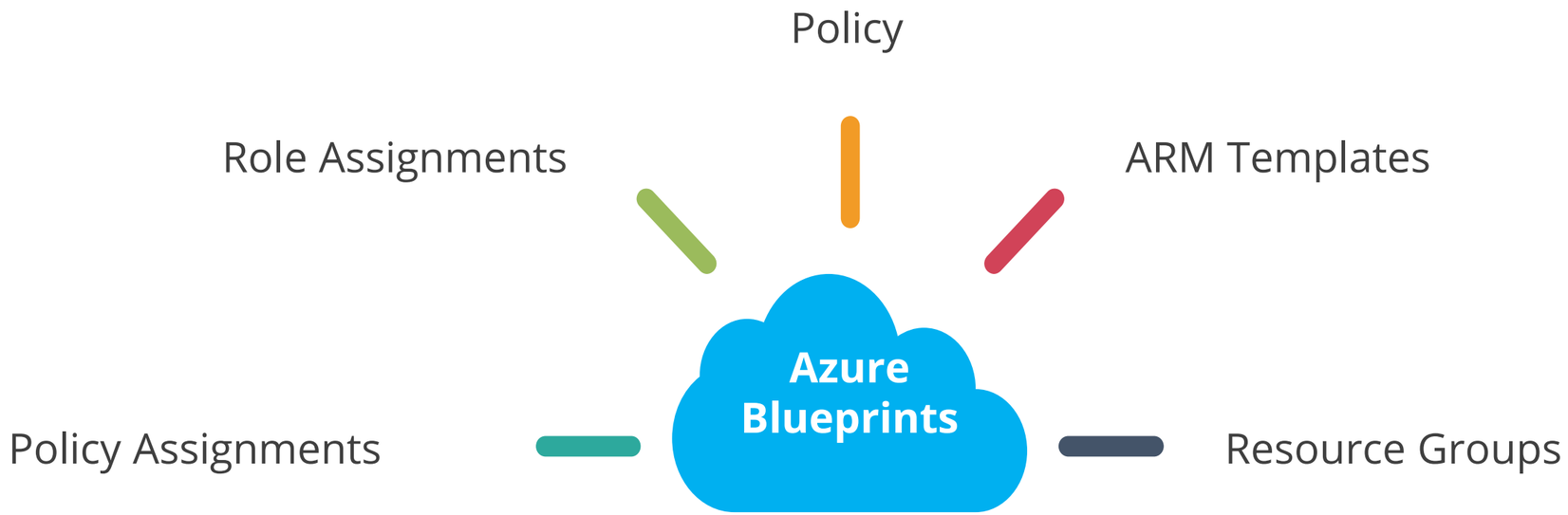
Azure Blueprints

Azure Blueprints enables defining a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.



Azure Blueprints

Azure Blueprints are a declarative way to orchestrate the deployment of artifacts such as:



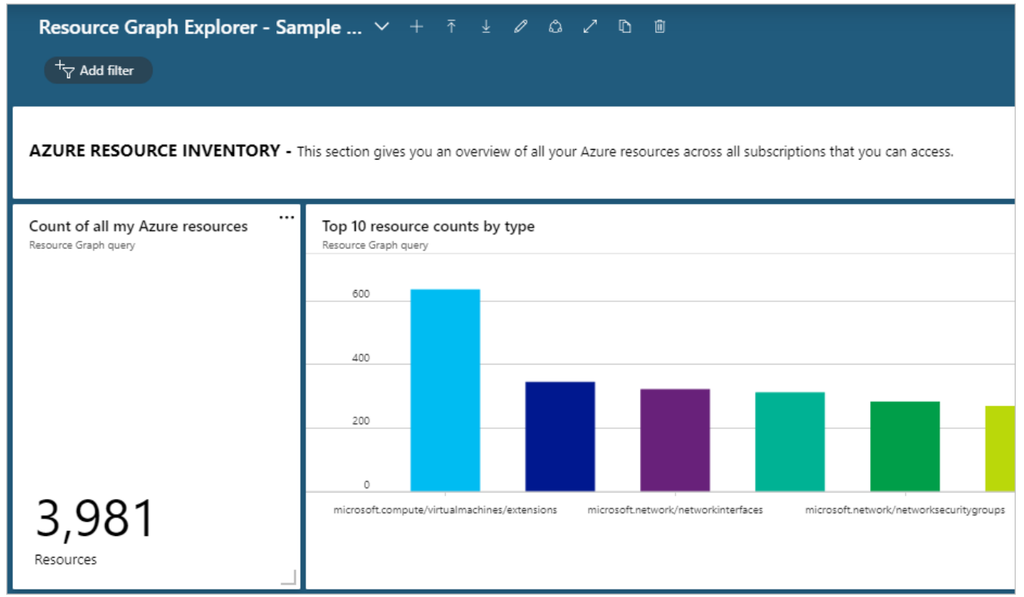
Azure Policy Versus Azure Blueprints

Azure Policy	Azure Blueprints
Helps to enforce organizational standards and to assess compliance at-scale	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
Provides an aggregated view to evaluate the overall state of the environment	Makes it possible for development teams to rapidly build and stand up new environments with the trust they're building within organizational compliance
Helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources	Objects in Blueprint are duplicated across various Azure regions. Regardless of which Azure Blueprints region the resources are deployed to, replication ensures low latency, high availability, and consistent access to user’s blueprint objects.

Recommend a Solution that Leverages Azure Resource Graph

Azure Resource Graph

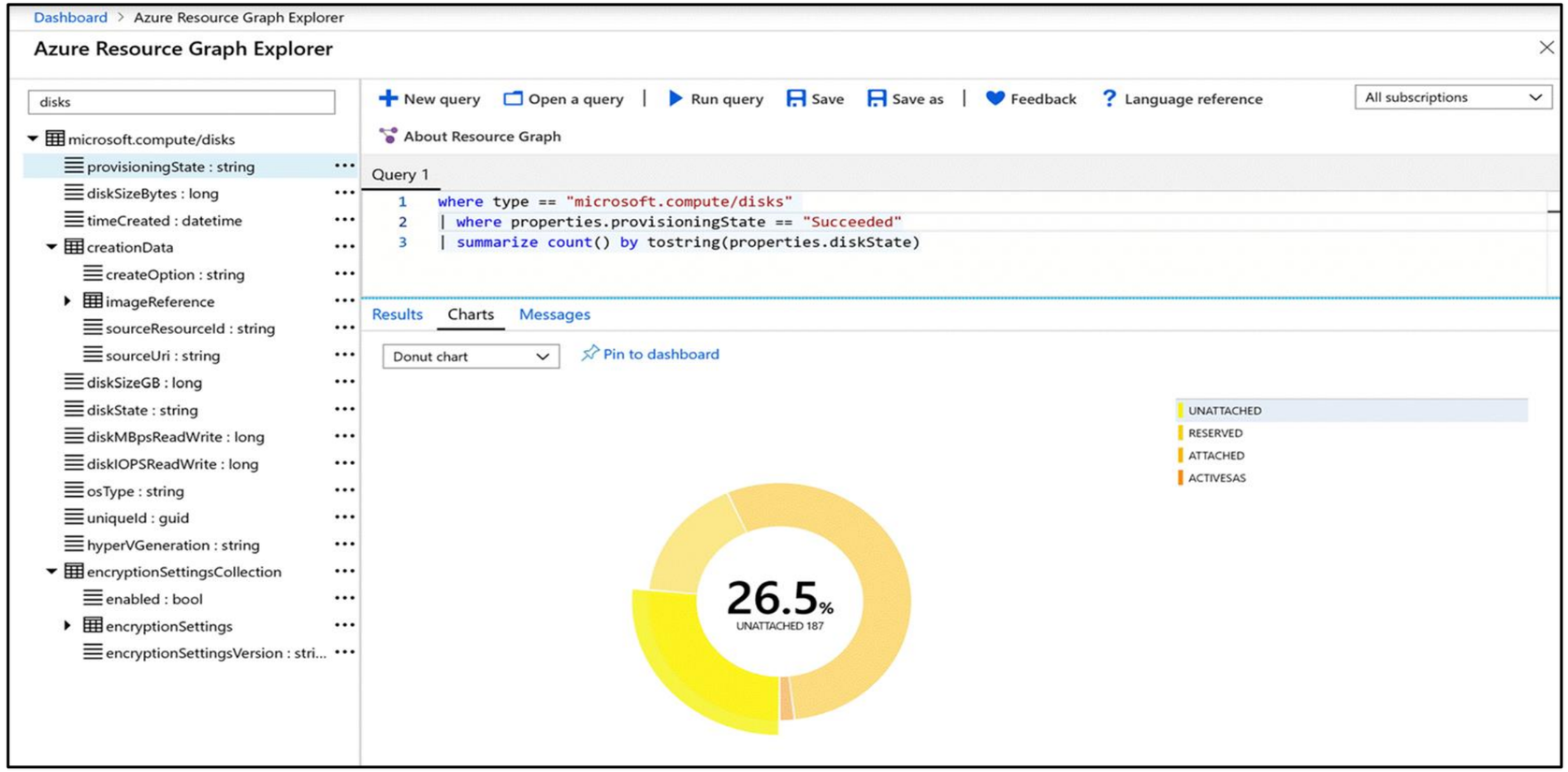
It is a service in Azure that extends Azure Resource Management by allowing users to explore resources in a more efficient manner.



It can query at scale over a series of subscribers, allowing the user to efficiently manage the environment.

Azure Resource Graph Query

The Azure Resource Graph query language includes a variety of operators and functions.



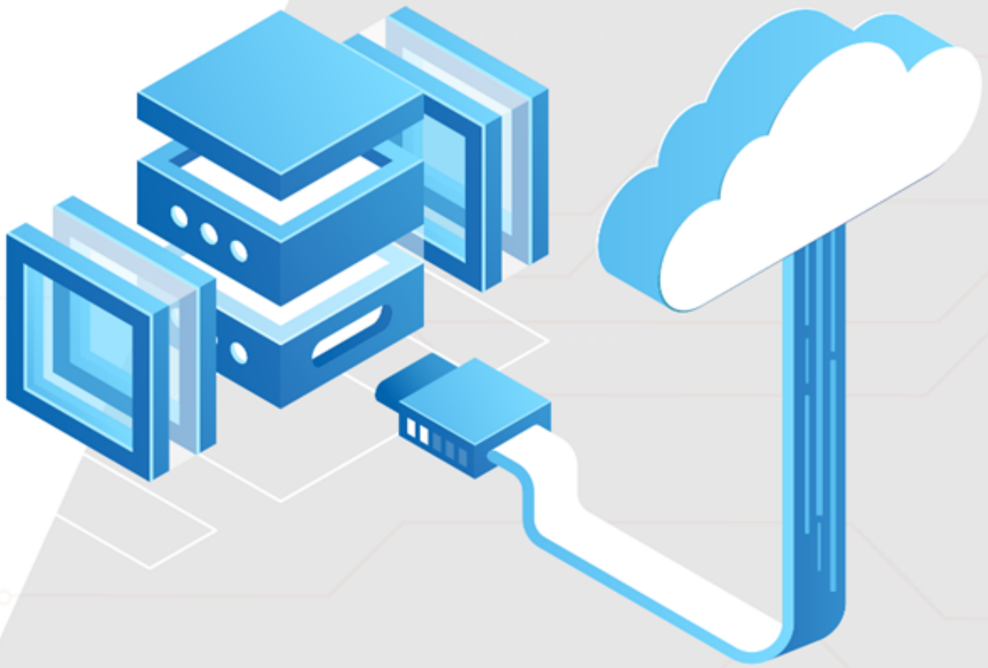
Azure Resource Graph Query

These are the features of Azure Resource Graph Query:

- Ability to query resources using resource properties to do advanced filtering, grouping, and sorting.
- Ability to explore resources iteratively based on governance requirements.
- Ability to evaluate the effects of policies on a large cloud system.
- Ability to track changes to resource attributes in great detail

Key Takeaways

- Policies enforce different rules and effects over resources.
- Azure Blueprints enable a user to create a repeatable set of Azure resources that adheres to an organization's standards.
- Azure Blueprints is a declarative way to orchestrate the deployment of artifacts such as Policy, ARM templates, and resource groups.
- Azure Resource Graph is a service in Azure that extends Azure Resource Management by allowing users to explore resources in a more efficient manner.



Thank you