Cloud Computing

Caltech | Center for Technology & Management Education

Designing Infrastructure Solutions on Azure

Powerd by simplilearn

Design a Governance Solution

Learning Objectives

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

- Analyze different areas of Azure management
- Apply the governance strategies
- Create management groups and subscriptions
- Create and manage resource groups
- Recommend a strategy for tagging

Learning Objectives

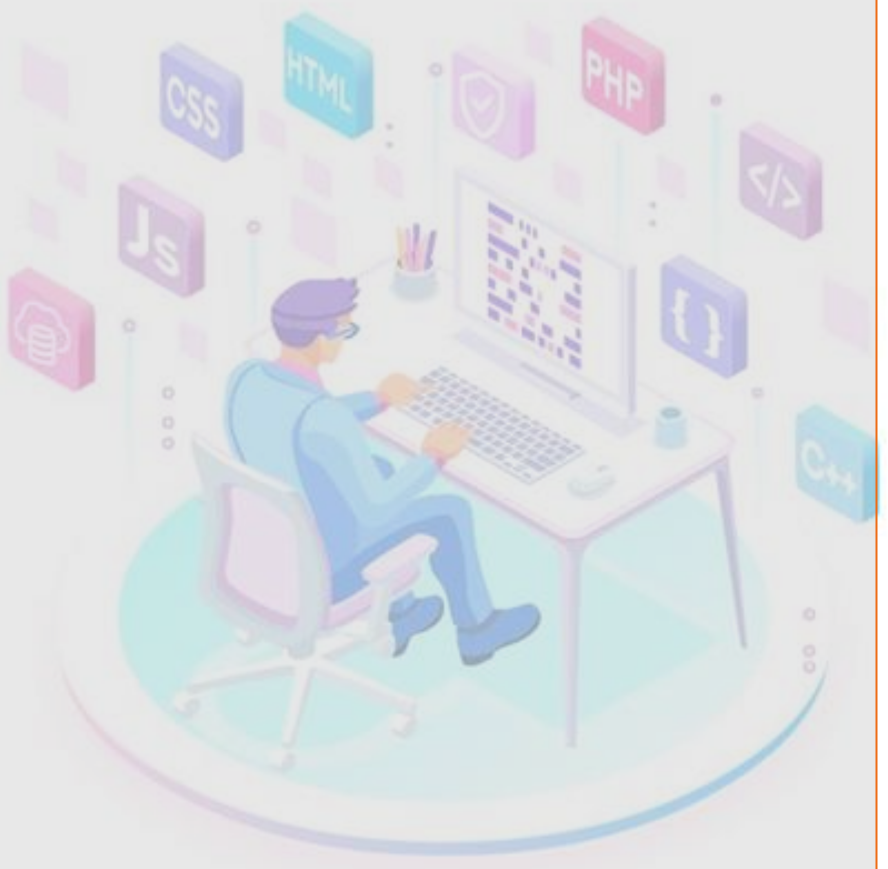
By the end of this lesson, you will be able to:

- Recommend a solution for using Azure blueprints
- Recommend a solution for using Azure policy

A Day in the Life of an Azure Architect

You are working as a cloud architect in a Fortune 500 organization. You need to design a solution for developers that would grant them the ability to provision certain Azure resources as determined by the company. This will help enforce corporate standards and analyze compliance at scale as an Azure Architect.

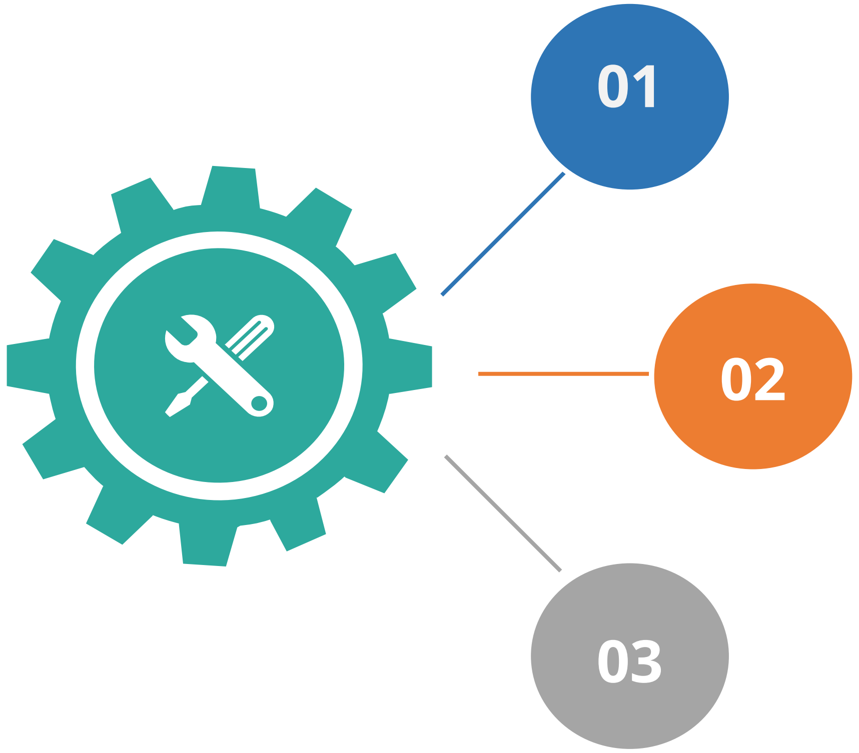
To achieve all of the above, along with some additional features, we would be learning a few concepts in this lesson that will help you find a solution for the above scenario.



Design Governance

Azure Management

Governance in Azure is basically an aspect of Azure Management.



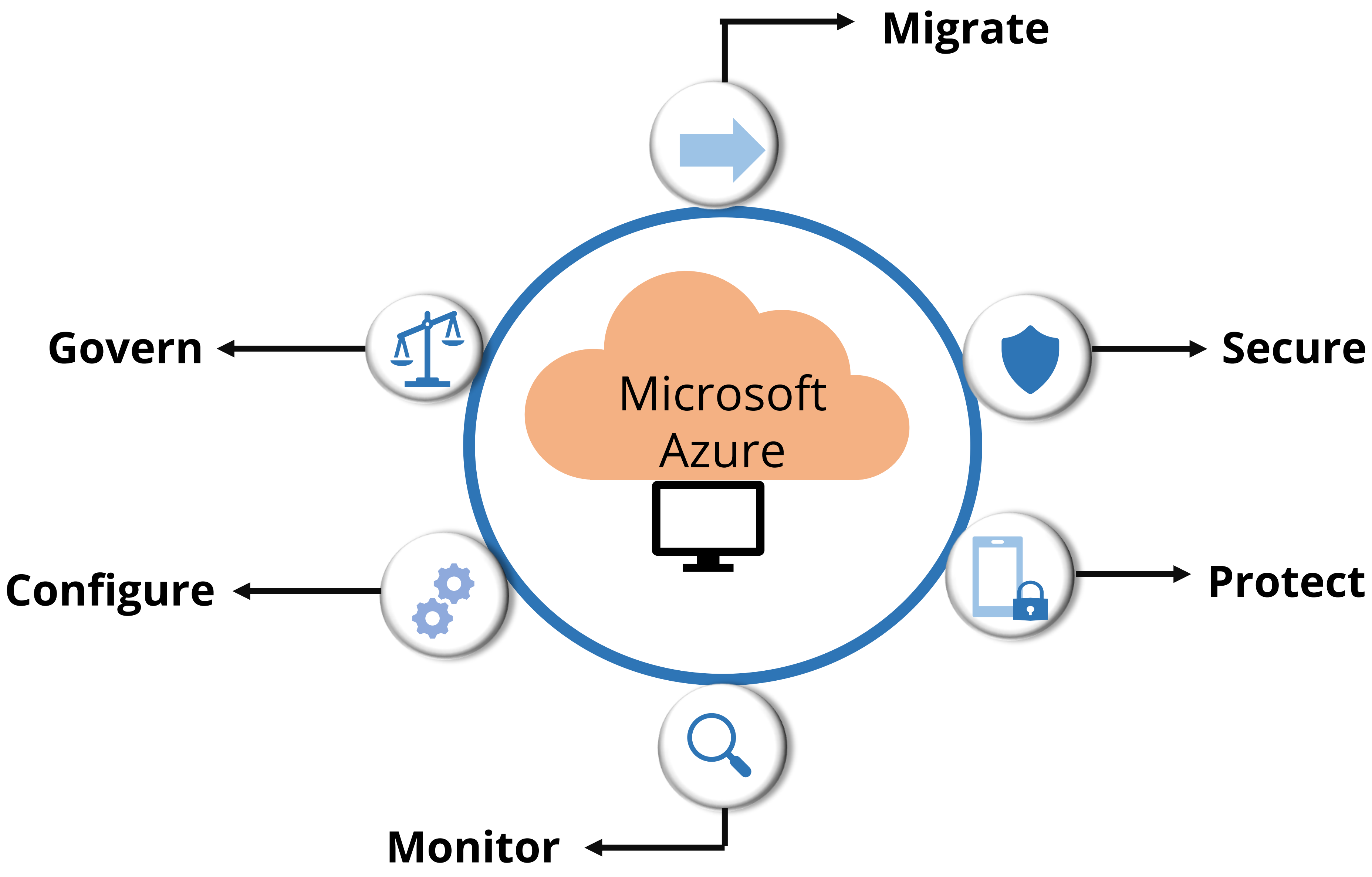
01 Management in Azure refers to the tasks and processes required to maintain your business applications and the resources that support them.

02 Azure has many services and tools that work together to provide complete management.

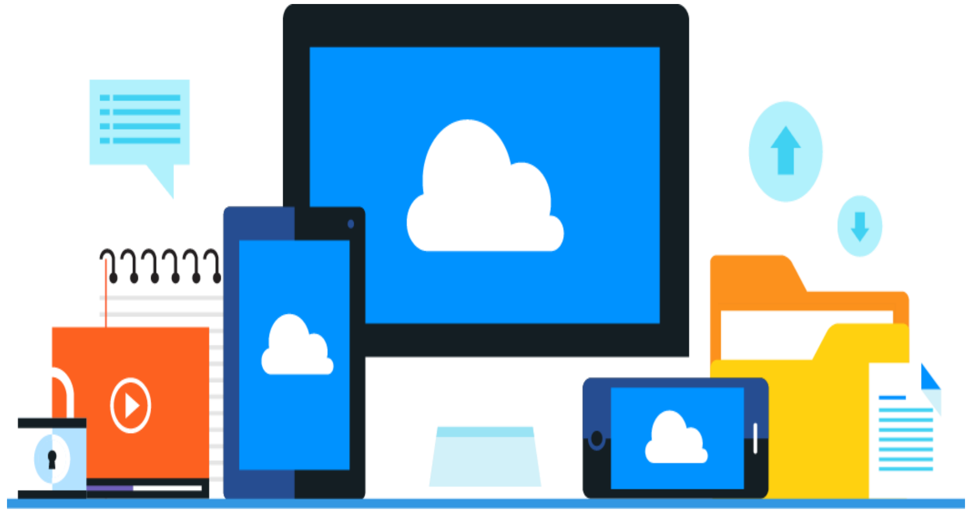
03 The first step in designing a complete management environment is to acknowledge the different tools and how they work together.

Azure Management

The following diagram illustrates the different areas of management that are required to maintain any application or resource:



Azure Management

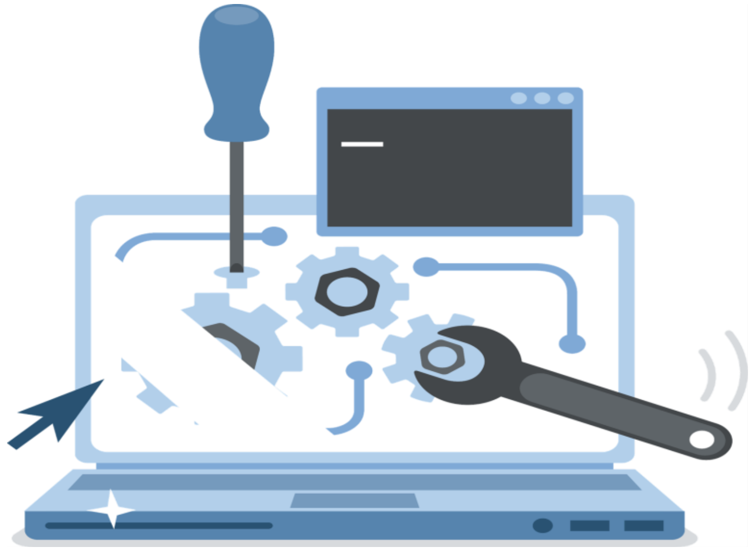


Monitor

Monitoring is the act of collecting and analyzing data to audit the performance, health, and availability of resources.

Configure

Configure refers to the initial deployment and configuration of resources and ongoing maintenance.



Azure Management

Govern

Governance provides mechanisms and processes to maintain control over applications and resources in Azure.

Secure

It means managing the security and resources of users' data, which involves assessing threats, collecting and analyzing data, and compliance with the applications and resources.

Azure Management

Protect

Protection refers to keeping the applications and data available with outages that are beyond control.

Migrate

Migration refers to transitioning workloads currently running on-premises to the Azure cloud.

Governance Strategies

Governance Strategies

Governance provides mechanisms and processes to maintain control over the applications and resources in Azure.

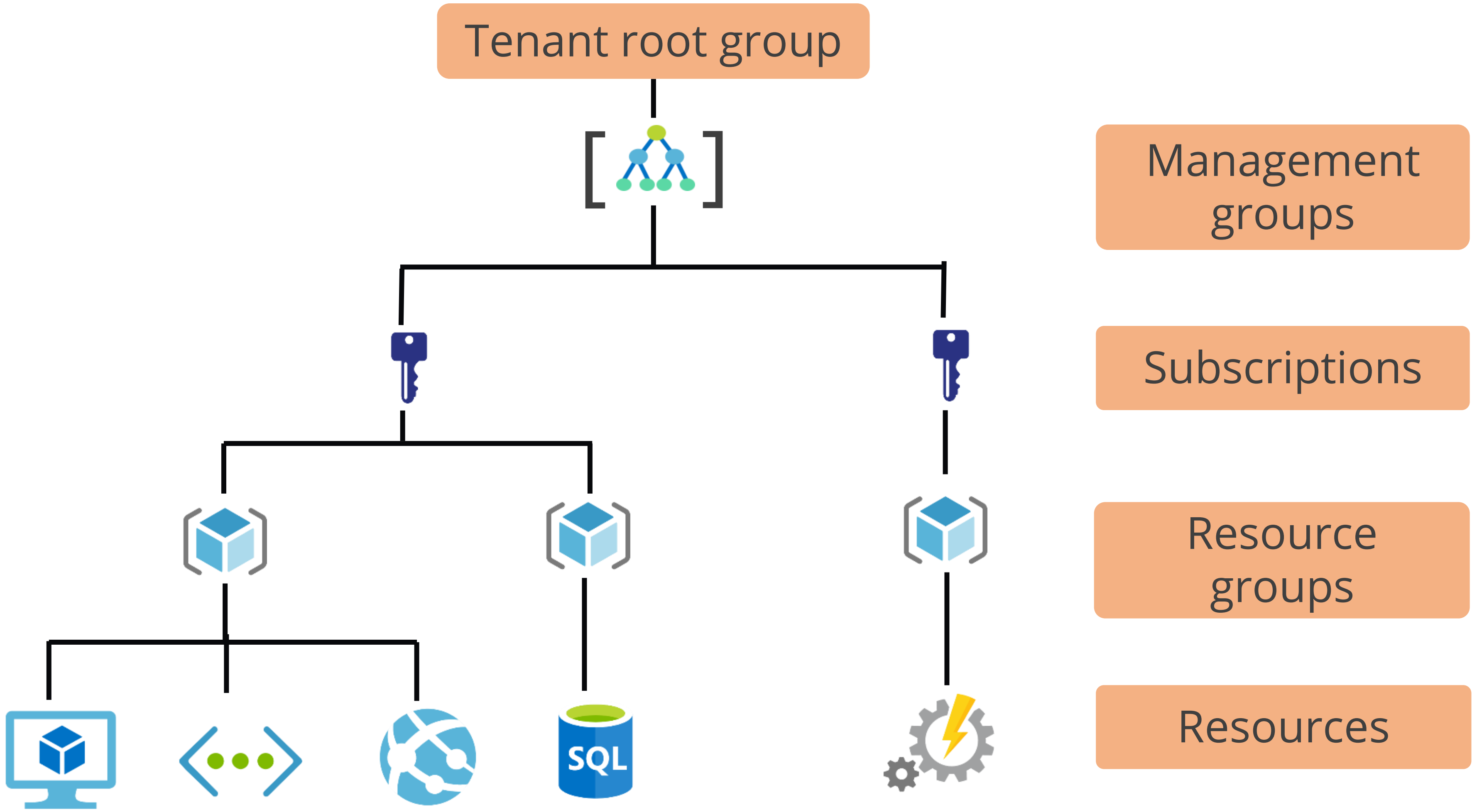
Governance Strategies involve determining the requirements, planning initiatives, and setting strategic priorities.

Two important Governance Strategies are:

- Azure Policies
- Resources Tags

Governance Strategies

Users must create a hierarchical structure to apply governance strategies as mentioned in the below diagram:



Note

The Tenant root group contains all the management groups and subscriptions.

Governance Strategies

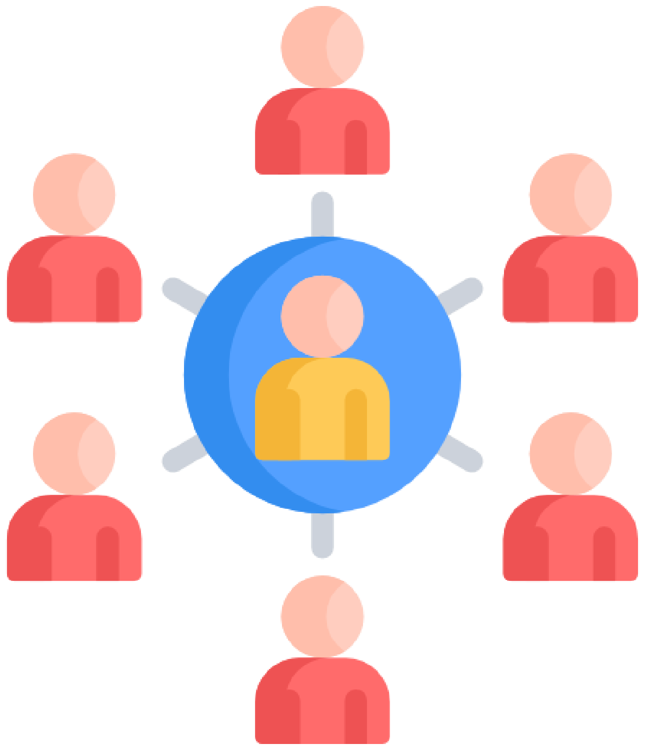
A typical Azure hierarchy has four levels:

- **Management Groups:** They help users manage access, policy, and compliance for multiple subscriptions.
- **Subscriptions:** They are logical containers that serve as units of management and scale.
- **Resource Groups:** These are logical containers into which Azure resources are deployed and managed.
- **Resources:** They are instances of services that users create.

Design for Management Groups and Subscriptions

Management Groups

Azure Management Groups provide an efficient way to manage access, policies, and compliance across an enterprise.



It manages access through a hierarchy made up of management groups and subscriptions.

Management Groups

01 Management groups provide a level of scope above subscriptions.

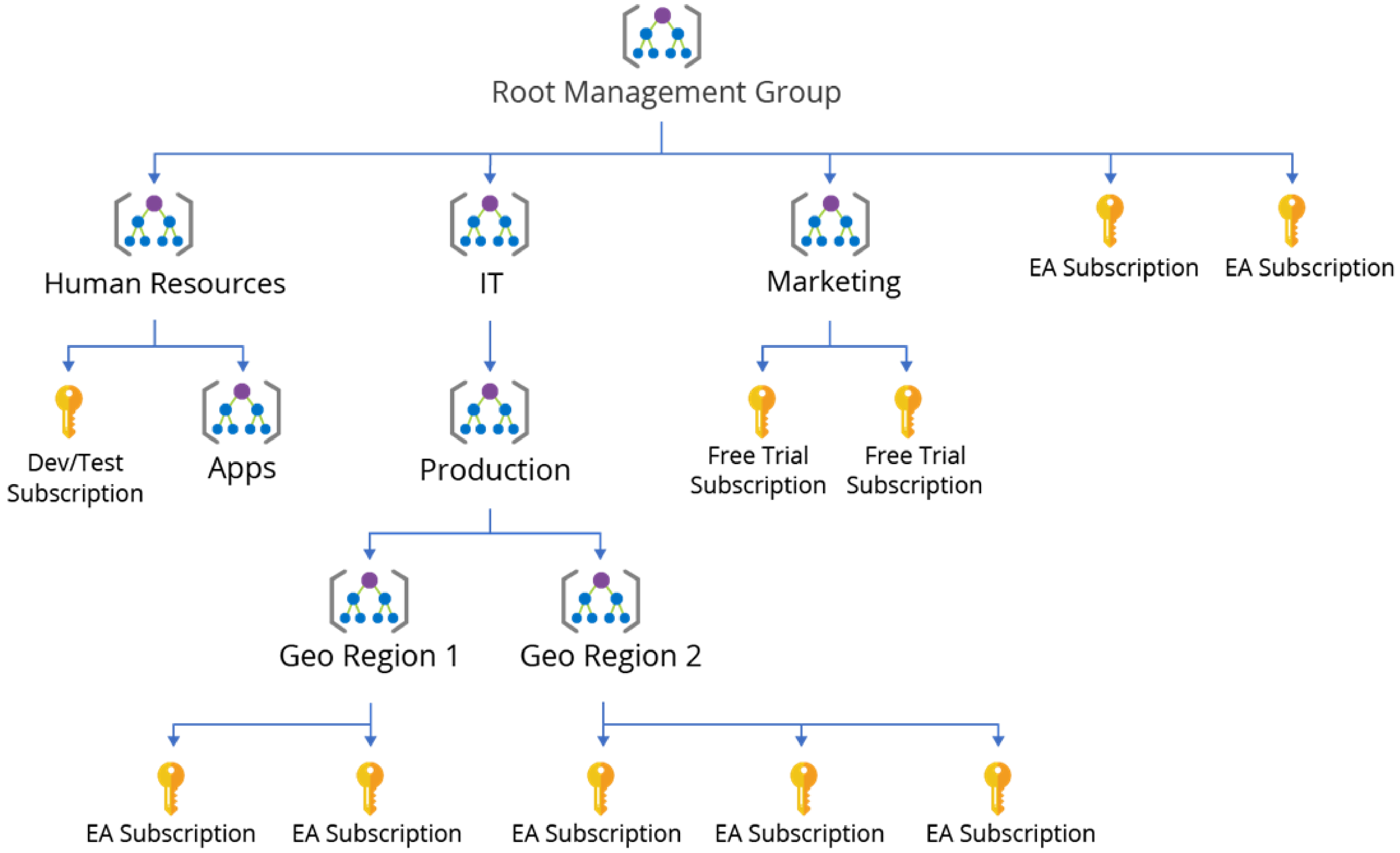
02 Subscriptions can be organized into containers called Management Groups.

03 Management groups are organizationally aligned through custom hierarchies and grouping.

04 Management groups provide enterprise-level management on a wide scale, regardless of the sort of subscriptions a user has.

Management Groups

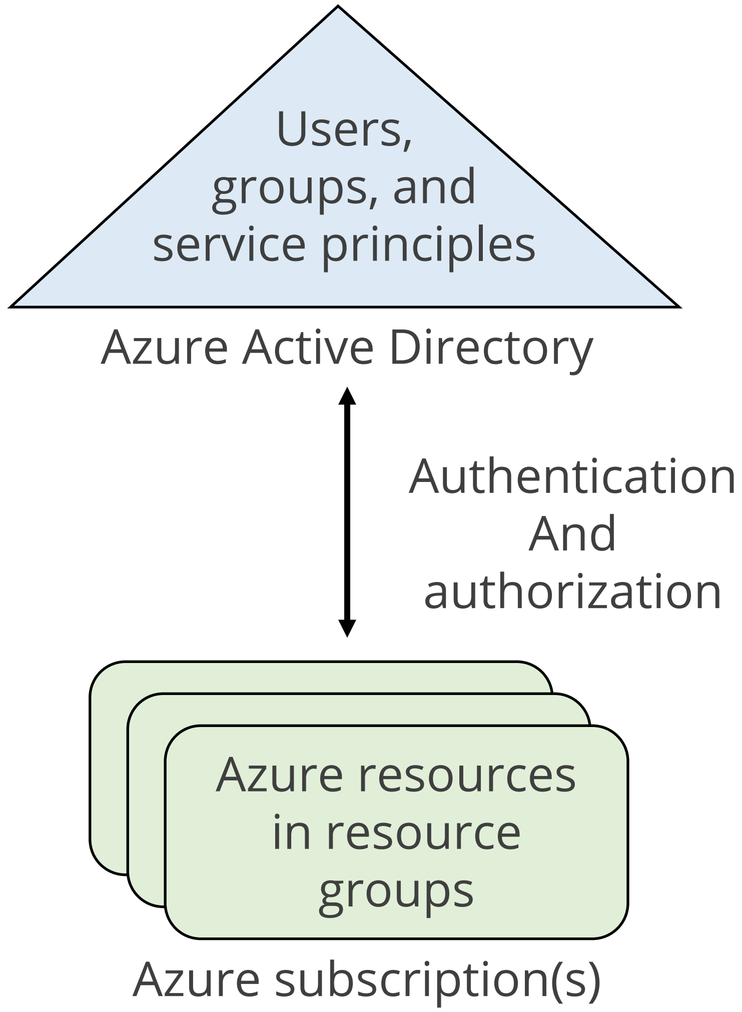
Building a governance hierarchy is shown below:



Source: https://docs.microsoft.com/

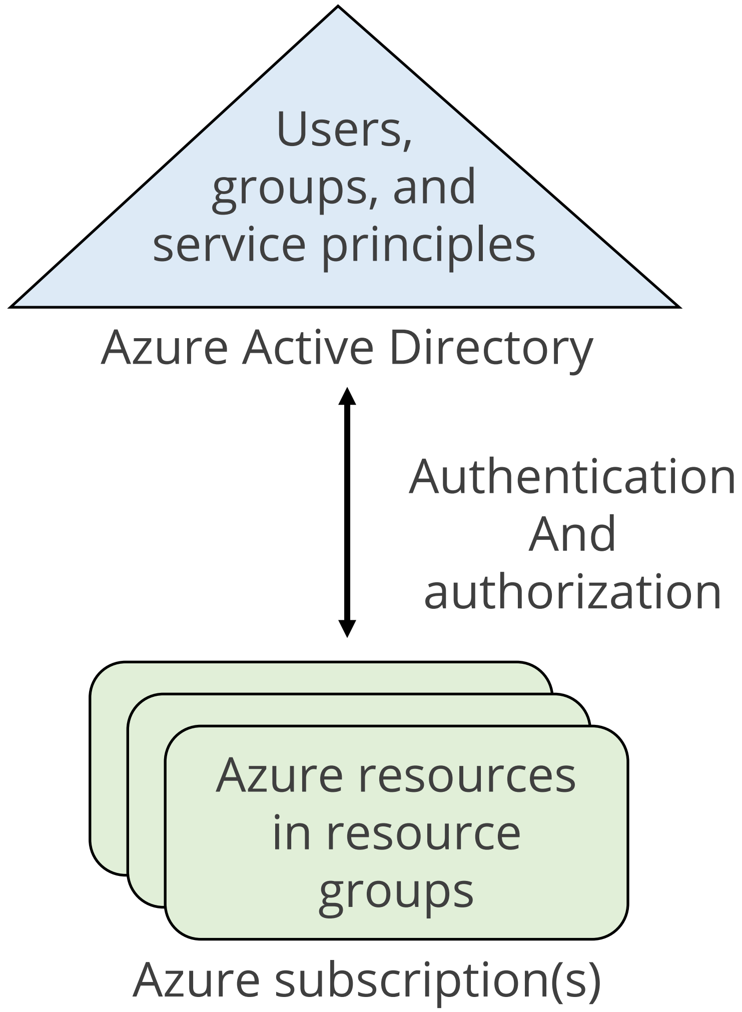
Azure Subscriptions and Accounts

An Azure account is connected to a subscription, which is a logical unit of Azure services.


Users, groups, and service principles
Azure Active Directory
Authentication And authorization
Azure resources in resource groups
Azure subscription(s)

- Azure services are billed on a per subscription basis.
- Subscriptions have accounts and are associated with Azure AD.

Azure Subscriptions and Accounts



Users, groups, and service principles
Azure Active Directory
Authentication And authorization
Azure resources in resource groups
Azure subscription(s)

- An account is an identity in Azure AD or in a directory that is trusted by Azure AD.
- The most common way to allow a user access to Azure services is to add them to the Azure AD directory linked to the subscription.

Getting an Azure Subscription

There are the following types of Azure subscriptions:

- **Enterprise Agreement:** Customer makes an upfront monetary commitment to Azure
- **Reseller:** Open licensing program
- **Microsoft partner:** Find a partner that can design and implement a cloud solution
- **Free trial account:** Customer can use a free Azure credit to try out different tiers and types of Azure services

Azure Subscriptions and Service Limits

Microsoft Azure limits are also called quotas.

Managing limits

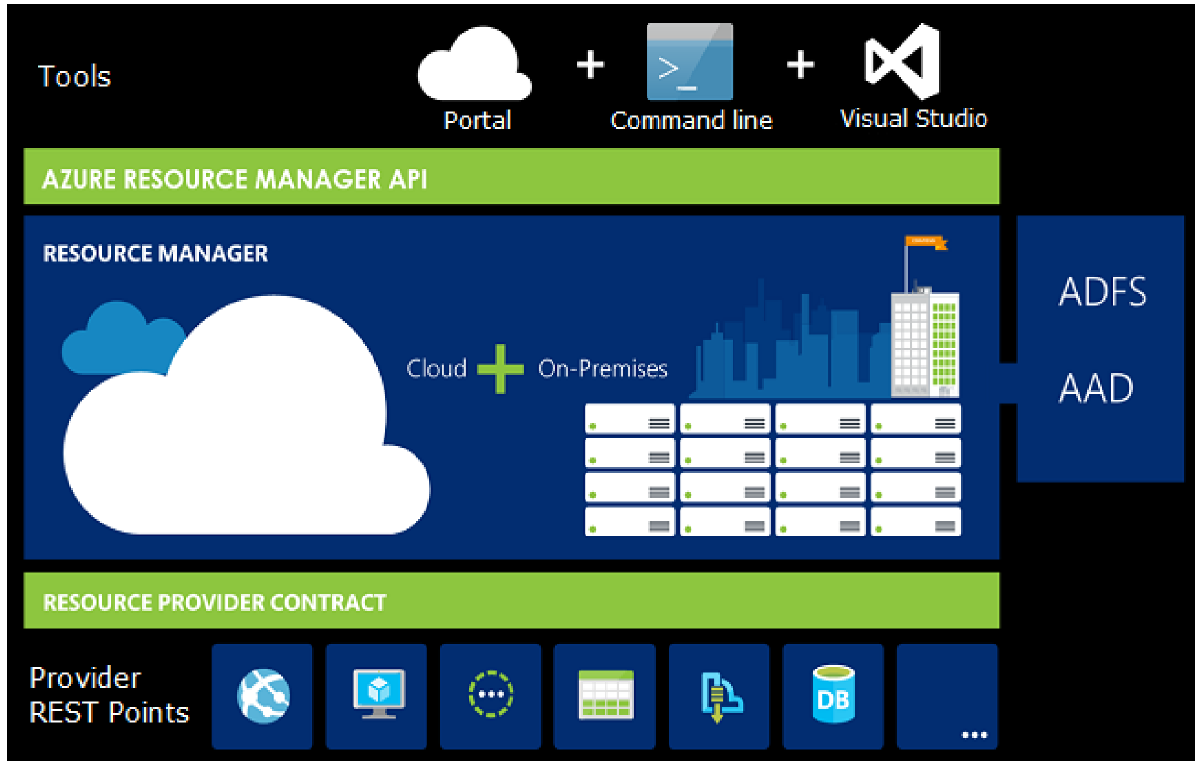
- Some limits apply to the regional level.
- The user can raise soft limits by raising an online customer support request at no charge.
- These limits keep on changing.
- To check the latest limits, navigate to:

  https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits

Design for Resource Groups

Resource Manager

Azure Resource Manager is the service that manages and deploys Azure resources.



- Renders a consistent management layer
- Facilitates collaboration with the resources in solution as a group
- Enables deployment, updating, or deletion using a single, coordinated operation
- Provides security, auditing, and tagging features

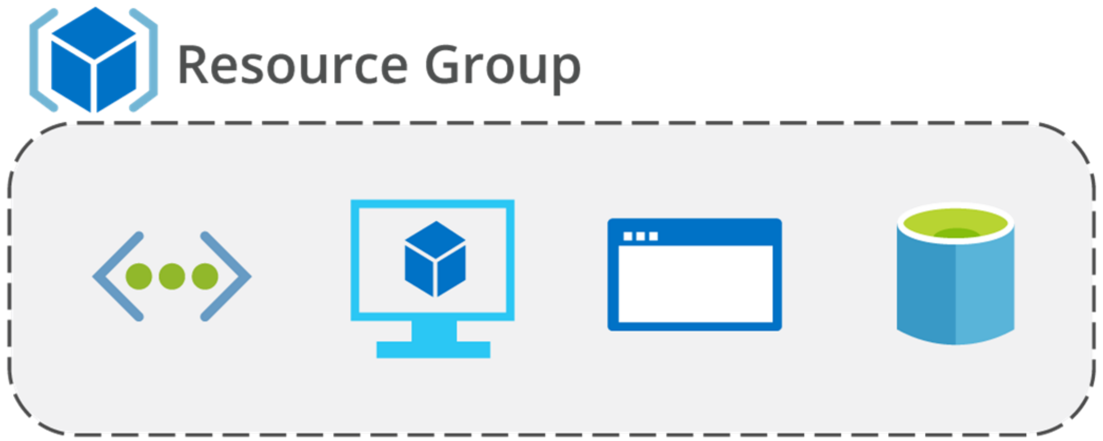
Note

Select the tools and APIs that are best suited.

image source: https://docs.microsoft.com/en-in/

Resource Groups

A Resource Group is a logical grouping of resources.

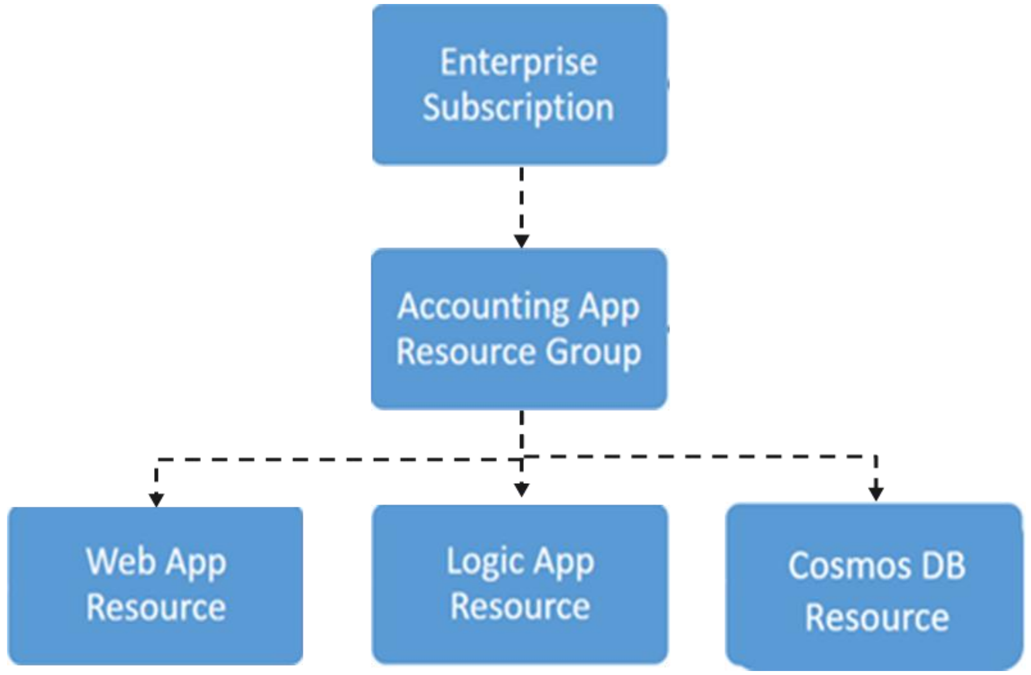


- Have fundamental concept of the Azure platform
- Ties to the resource life cycle
- Cannot be nested
- Must be allocated to each resource

Note

Most resources can be moved between resource groups.

Resource Groups and Deployments



- There can only be one resource group per resource.
- It is not possible to rename the resource groups.
- Groups can have a wide range of resources (services).
- They can also have resources from various regions.
- Deployments are made in stages.

Users can easily add, remove, and modify resources by scoping permissions to a resource group.

Resource Group Organization

Organizing for authorization

Since resource groups fall under the scope of RBAC, users can organize resources by who wants to manage them.

Organizing for life cycle

When a user deletes a resource group, all the resources inside the resource group are also deleted. It is suitable when resources are more disposable, such as in production environments.

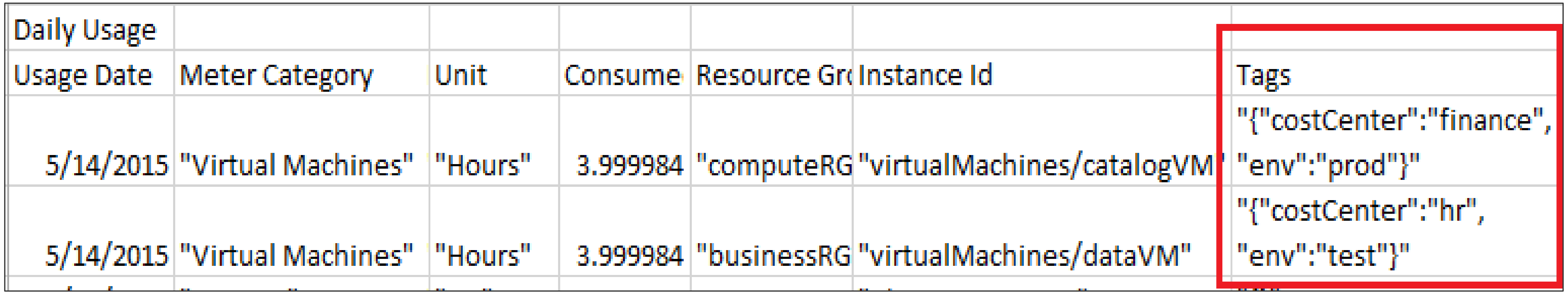
Organizing for billing

When a user place resources in the same resource group, it allows them to be grouped for billing reports.

Recommend a Strategy for Tagging

Tags

Tags logically organize the resources, and 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 users need to organize resources for billing or management.

Limitations of Tags

Tag Limitations

- Each resource or resource group can have a maximum of 50 tag names or 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

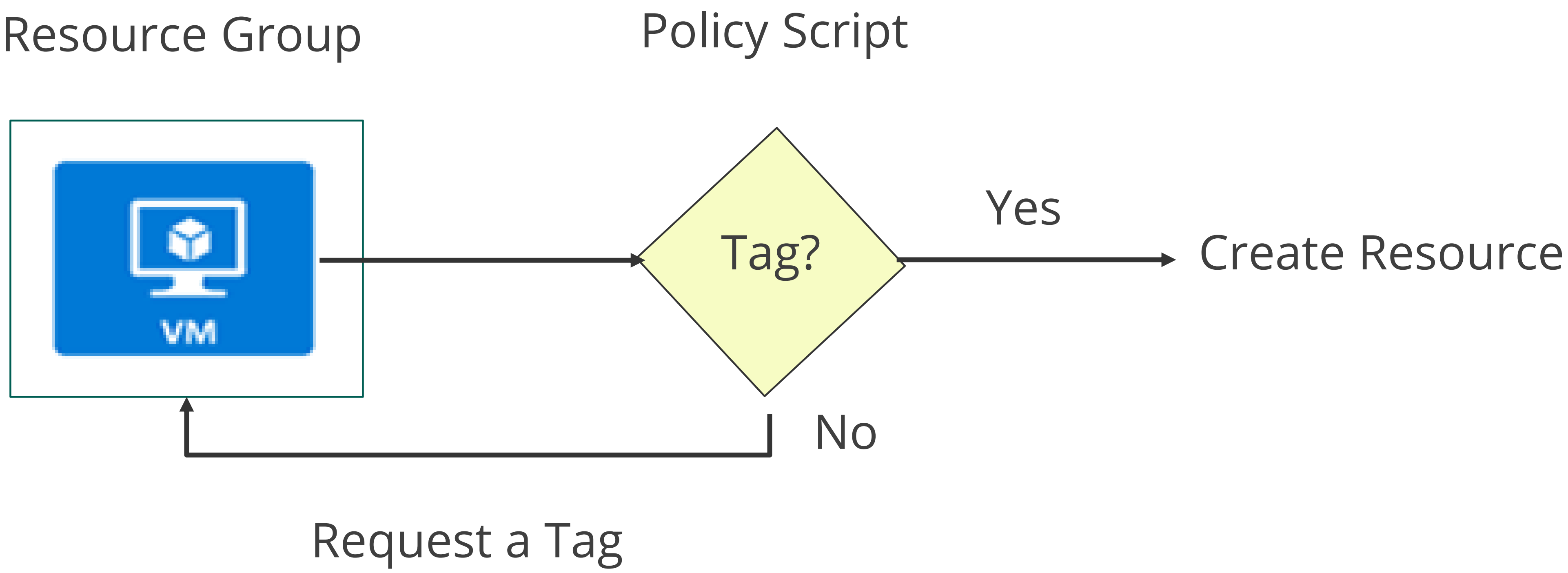
Tag type	Tag	Mandatory/ optional	Description	Data type
Technical	Region	Mandatory	Location	String
Technical	Environment	Mandatory	Dev, Stage, Prod	String
Technical	Maintenance window	Mandatory	Patching Window	String
Automation	Expiration date	Optional	Terminate resource automatically	String
Automation	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	Technical contact	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 • 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 • Specify the required values for the tags
Enforce tag and its value	• Requires a specified tag name and value • 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 • 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.

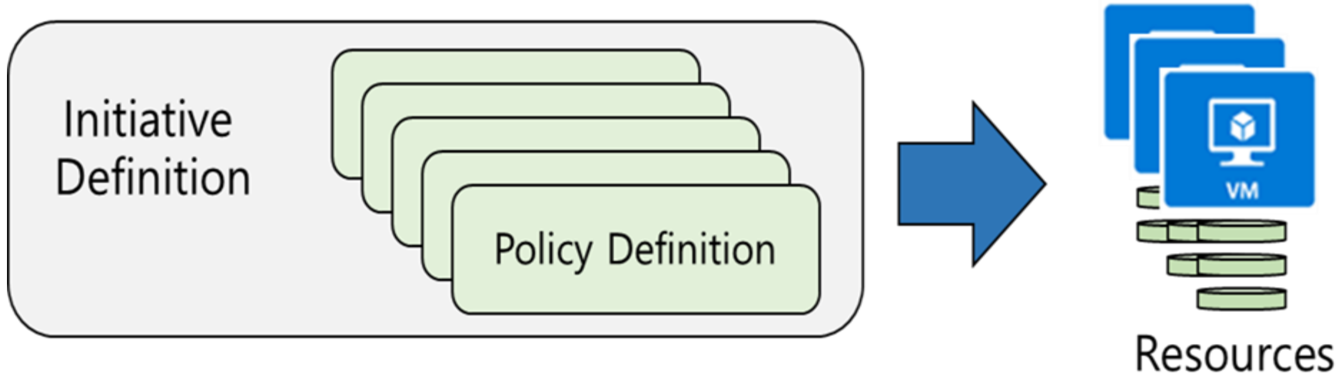
Example: Users can have the policy to allow only a certain SKU size of virtual machines in your environment.

Azure Policy Benefits

- **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:** Provides real-time remediation

Implementing Azure Policies

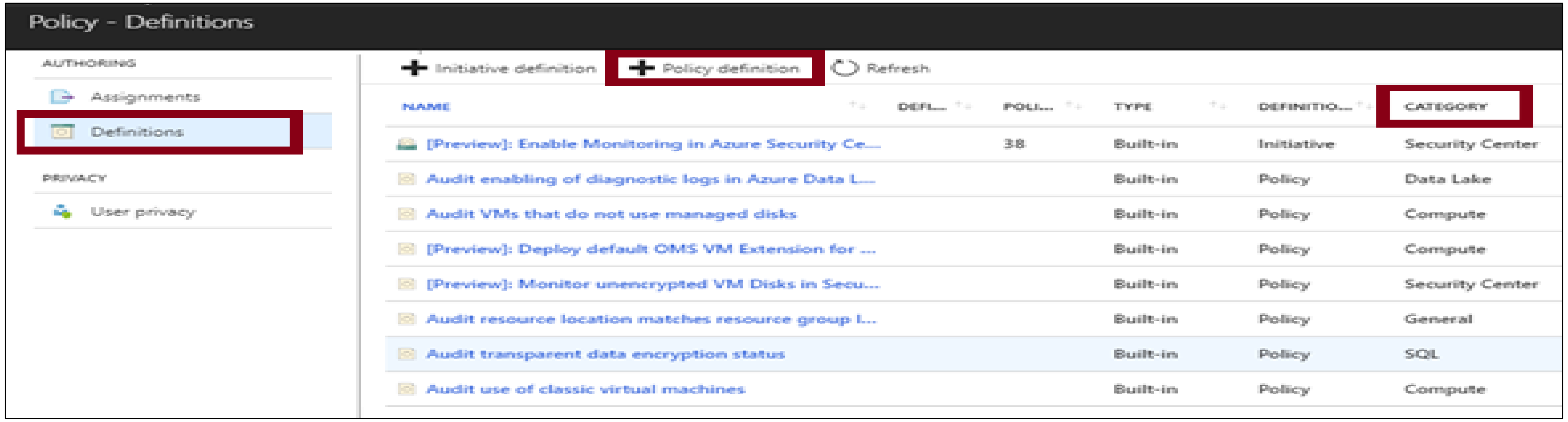
These are the steps to implement Azure policies:



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

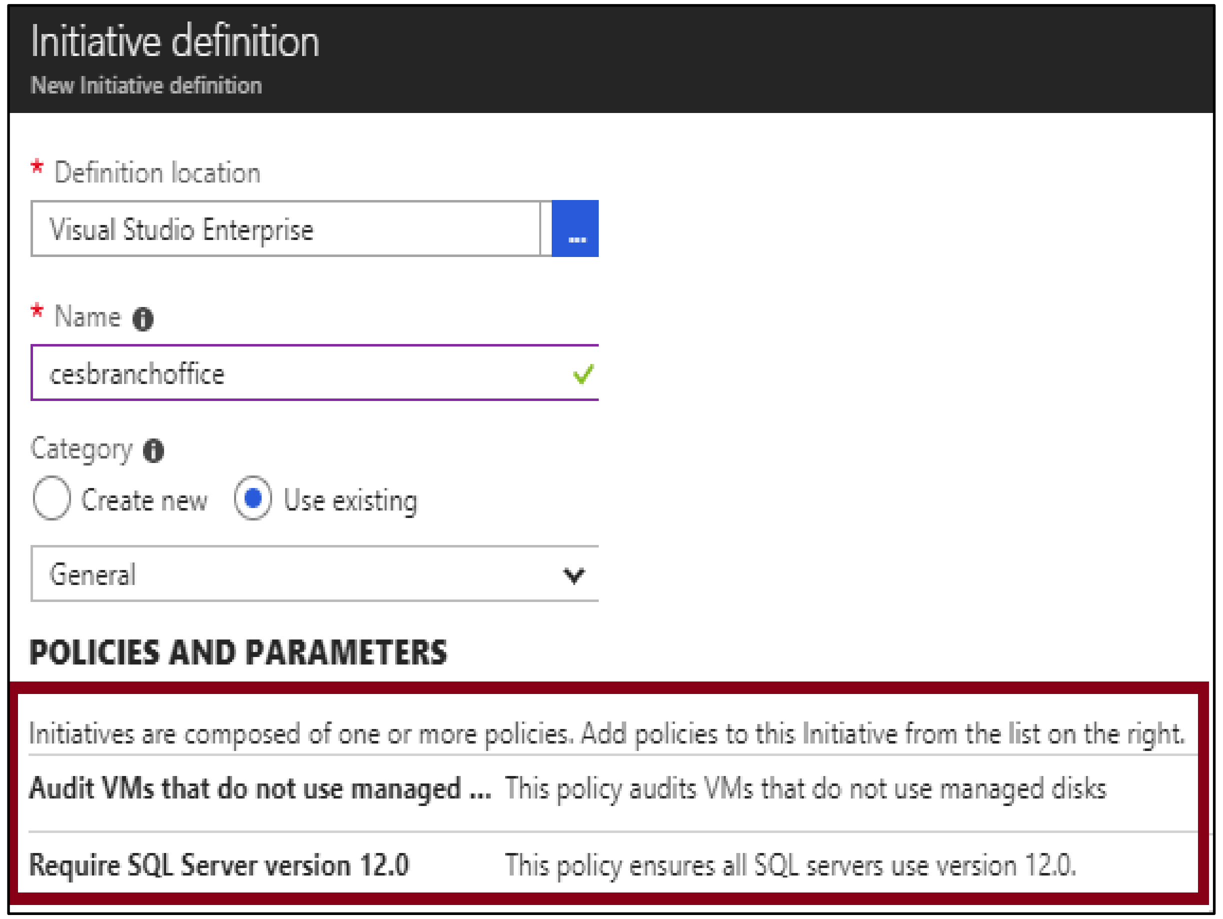


NAME	DEFI...	POLI...	TYPE	DEFINITIO...	CATEGORY
[Preview]: Enable Monitoring in Azure Security Ce...		38	Built-in	Initiative	Security Center
Audit enabling of diagnostic logs in Azure Data L...			Built-in	Policy	Data Lake
Audit VMs that do not use managed disks			Built-in	Policy	Compute
[Preview]: Deploy default OMS VM Extension for ...			Built-in	Policy	Compute
[Preview]: Monitor unencrypted VM Disks in Secu...			Built-in	Policy	Security Center
Audit resource location matches resource group l...			Built-in	Policy	General
Audit transparent data encryption status			Built-in	Policy	SQL
Audit use of classic virtual machines			Built-in	Policy	Compute

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

Create Initiative Definitions

There are steps to create initiative definitions:



Initiative definition
New Initiative definition

* Definition location
Visual Studio Enterprise

* Name
cesbranchoffice ✓

Category
○ Create new ● Use existing

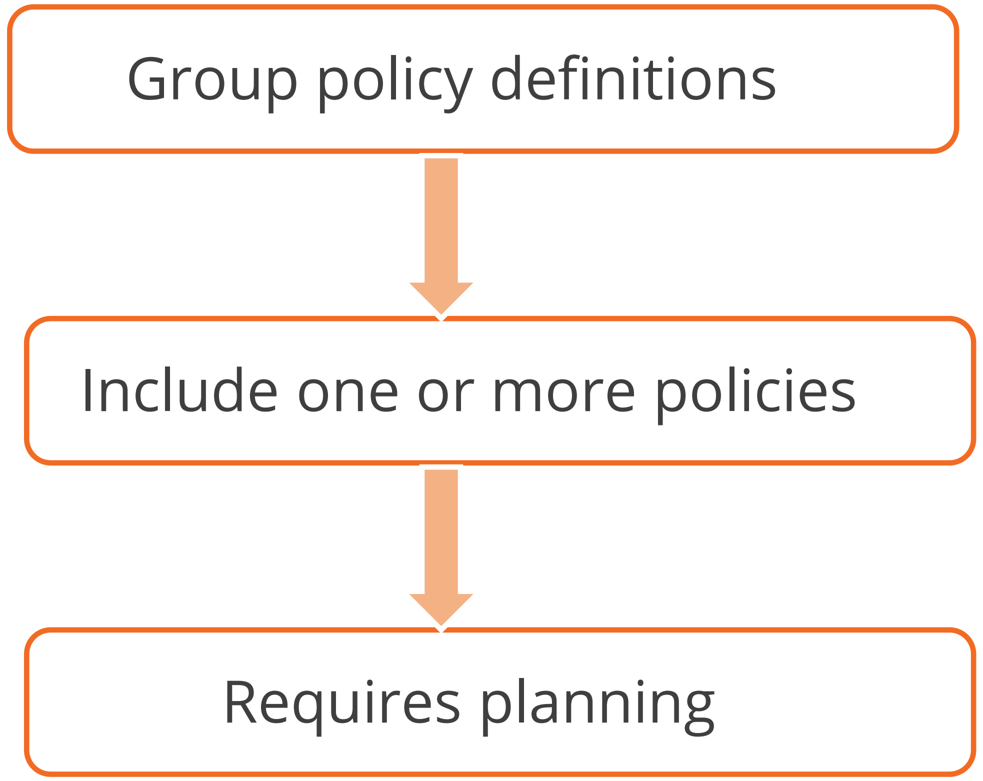
General

POLICIES AND PARAMETERS

Initiatives are composed of one or more policies. Add policies to this Initiative from the list on the right.

Audit VMs that do not use managed ... This policy audits VMs that do not use managed disks

Require SQL Server version 12.0 This policy ensures all SQL servers use version 12.0.



Group policy definitions

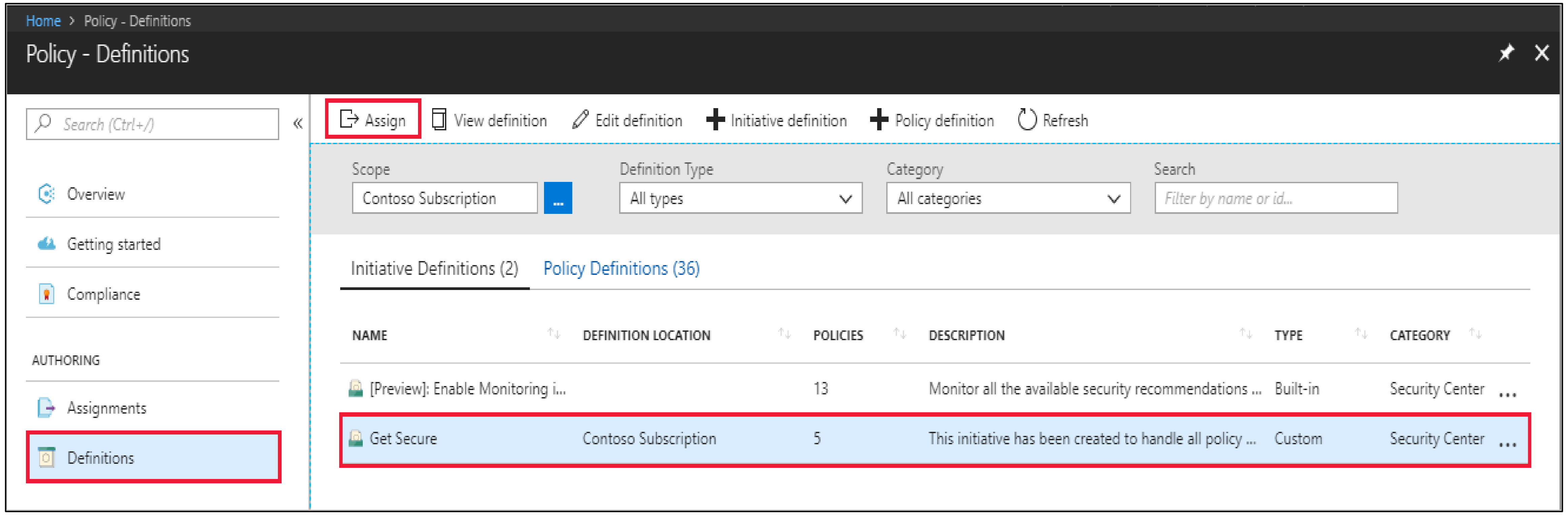
Include one or more policies

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



Scope: Contoso Subscription

Definition Type: All types

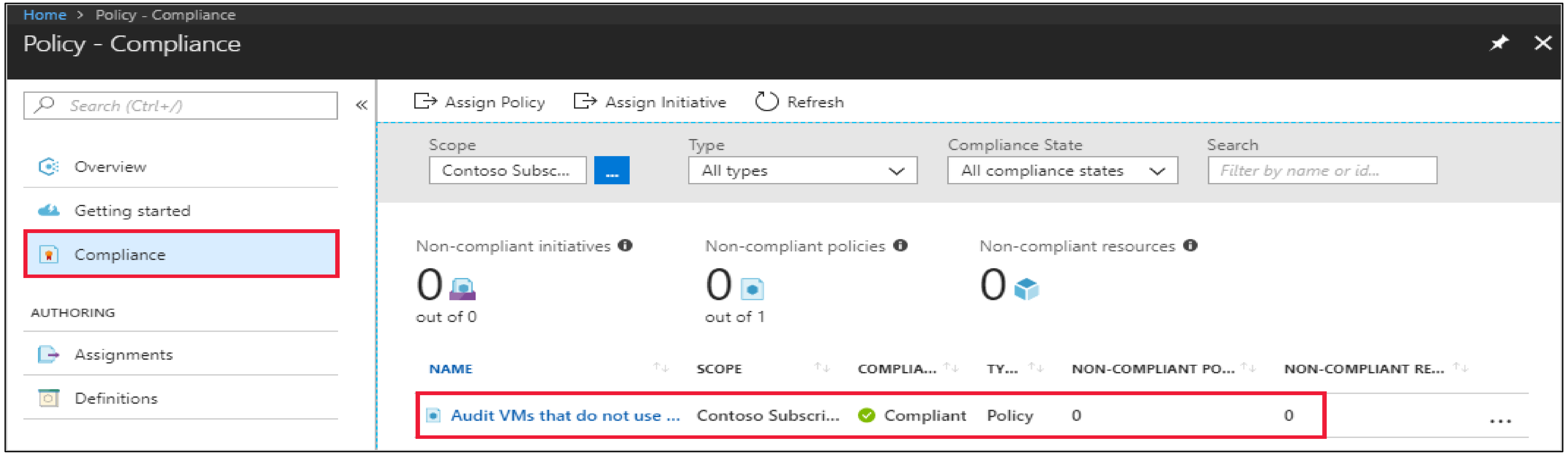
Category: All categories

Search: Filter by name or id...

NAME	DEFINITION LOCATION	POLICIES	DESCRIPTION	TYPE	CATEGORY
[Preview]: Enable Monitoring i...		13	Monitor all the available security recommendations ...	Built-in	Security Center
Get Secure	Contoso Subscription	5	This initiative has been created to handle all policy ...	Custom	Security Center

Note: An initiative definition can have up to 100 policies.

Determine Compliance



Scope: Contoso Subsc...

Type: All types

Compliance State: All compliance states

Search: Filter by name or id...

Non-compliant initiatives: 0 out of 0

Non-compliant policies: 0 out of 1

Non-compliant resources: 0

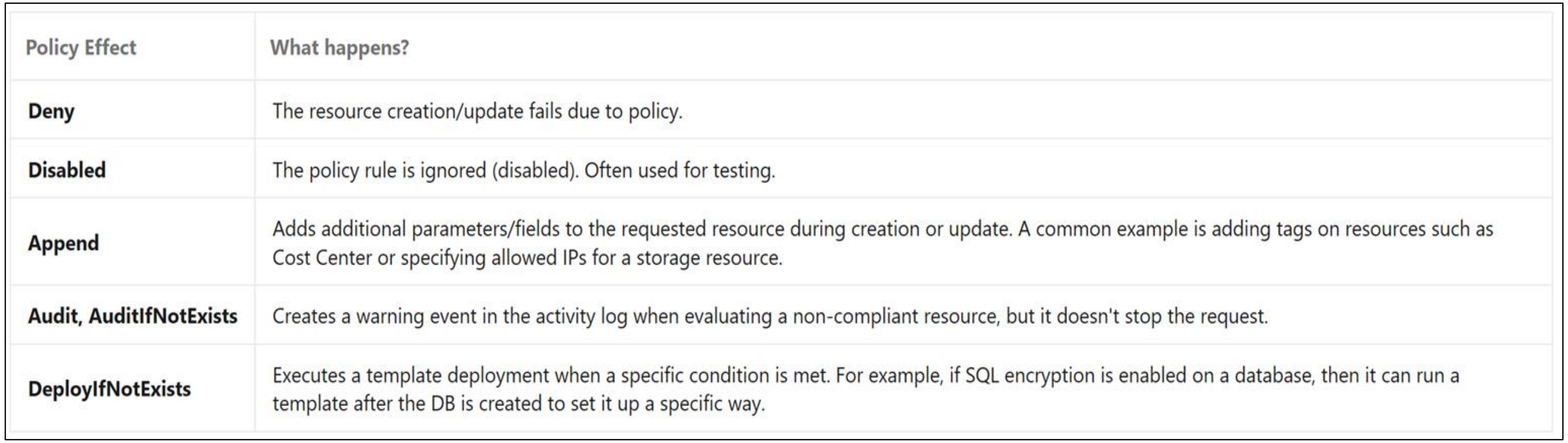
NAME	SCOPE	COMPLIA...	TY...	NON-COMPLIANT PO...	NON-COMPLIANT RE...
Audit VMs that do not use ...	Contoso Subscri...	✓ Compliant	Policy	0	0

Non-compliant initiatives

- **Non-compliant policies:** It is the number of policy assignments with at least one non-compliant resource.
- **Non-compliant resources:** Once a condition is evaluated against the existing resources and found to be true, 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.

- Azure Policy evaluates the requests to create or update a resource through Azure resource manager.
- Policy processes several of the effects before handing the request to the appropriate Resource Provider to avoid violating 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 a new Policy definition page
4. Add information on 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

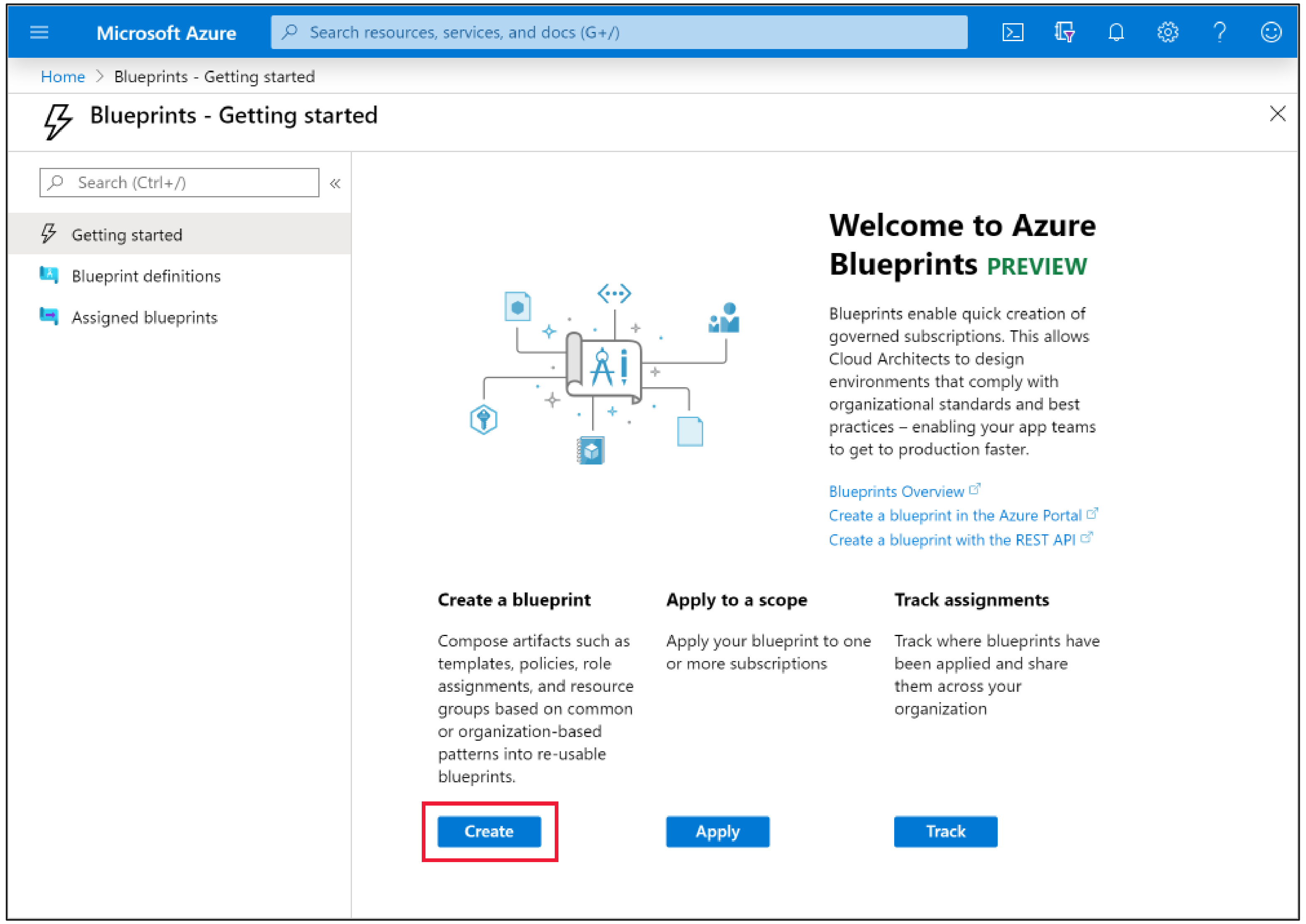
Steps to assign a policy assignment:

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



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Blueprints - Getting started
Blueprints - Getting started
Search (Ctrl+/)
Getting started
Blueprint definitions
Assigned blueprints

Welcome to Azure Blueprints PREVIEW

Blueprints enable quick creation of governed subscriptions. This allows Cloud Architects to design environments that comply with organizational standards and best practices – enabling your app teams to get to production faster.

Blueprints Overview
Create a blueprint in the Azure Portal
Create a blueprint with the REST API

Create a blueprint

Compose artifacts such as templates, policies, role assignments, and resource groups based on common or organization-based patterns into re-usable blueprints.

Apply to a scope

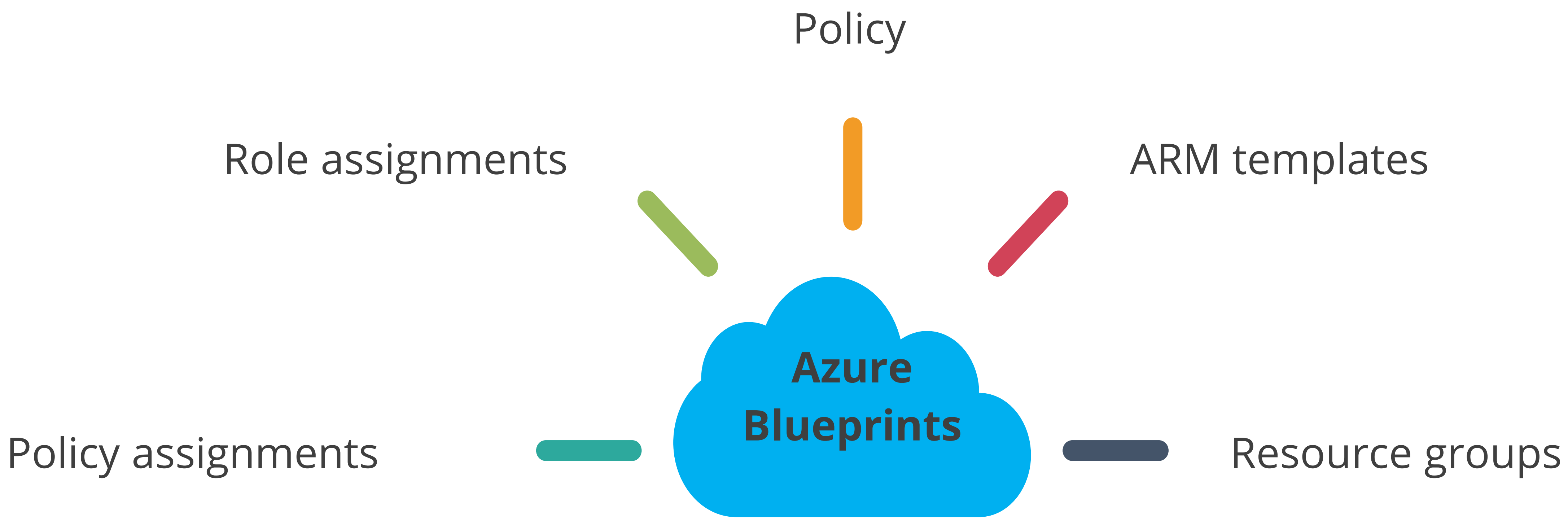
Apply your blueprint to one or more subscriptions

Track assignments

Track where blueprints have been applied and share them across your organization

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 new environments with the trust within organizational compliance
Helps to bring the resources to compliance through bulk remediation for existing resources and automatic remediation for new resources	Duplicates objects across various Azure regions which ensure low latency, high availability, and consistent access to the user's blueprint objects regardless of the region

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 are a declarative way to orchestrate the deployment of artifacts such as policy, ARM templates, and resource groups.
- Applying governance strategies to analyze different areas of Azure management areas.

Design Governance

Duration: 10 min.

Project Agenda: Design a solution for governance with respect to the given scenario

Description: You work as a cloud architect in a Fortune 500 organization.

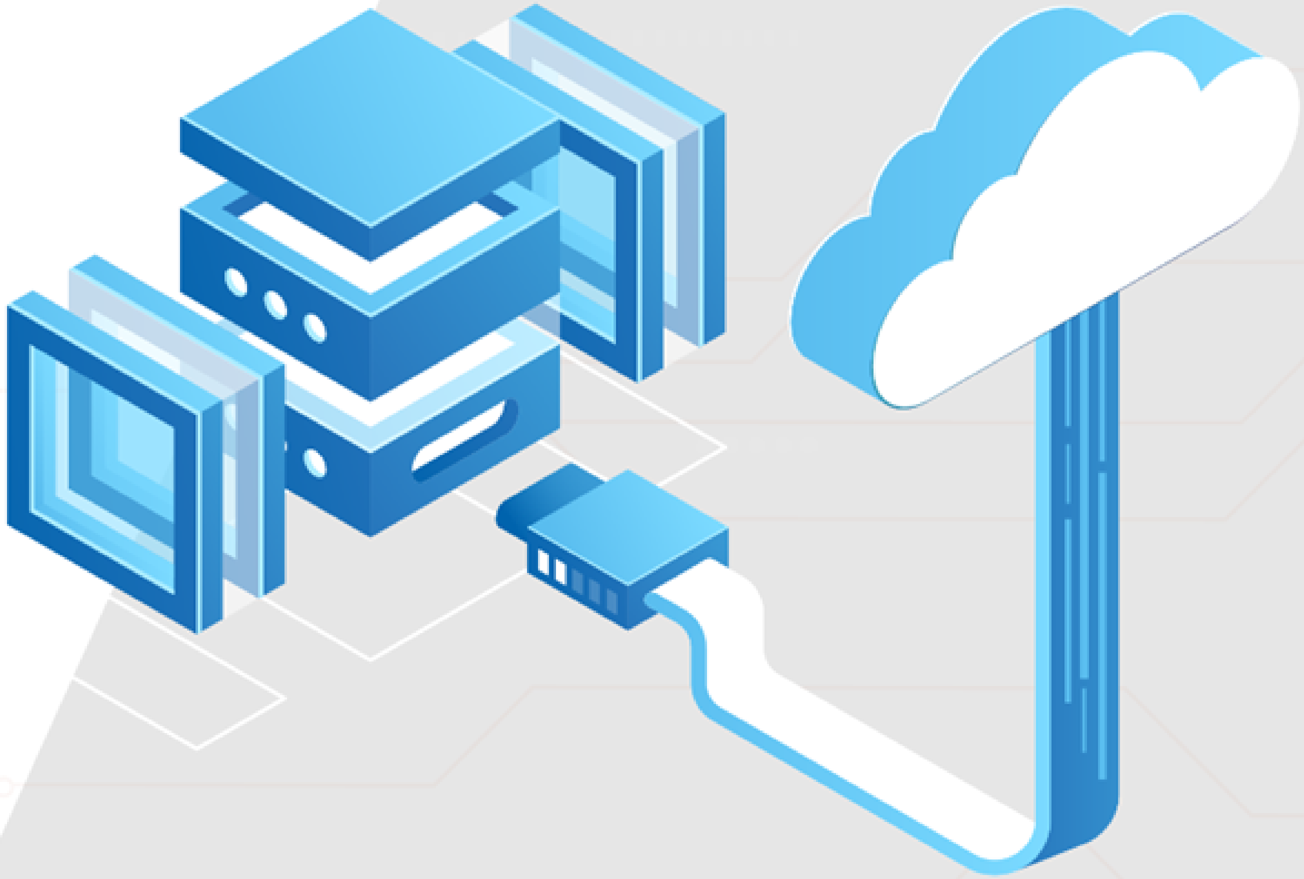
You need to design a solution for developers which will grant them the ability to provision certain Azure Resources, keeping the below requirements in mind:

- Allow only a certain size of VMs to be provisioned
- Allow storage account and VMs provisioning in only specific regions
- Do not allow the creation of a storage account if a secure transfer is not enabled

Perform the following:

1. Create users
2. Create a group
3. Create a resource group to assign policy as per the requirement
4. Assign a role to the created group at the resource group level
5. Assign the policies to resource group

LESSON-END PROJECT



Thank you