MC2MC

Azure Governance – 101

Azure Governance - 101

Vaibhav Gujral

https://vaibhavgujral.com/

About Me

- 14+ years of experience across designing and developing enterprise-class applications
- Microsoft Certified Azure Solutions Architect Expert
- Cloud Architect at Kiewit
- Organizer, Omaha Azure User Group
- Listed among the “Top 50 Microsoft Azure Blogs, Websites & Influencers in 2020”
- Speaker | Blogger
- #AzureHeroes Community & Content Hero
- http://www.vaibhavgujral.com
- @vabgujral
- linkedin.com/in/vaibhavgujral/

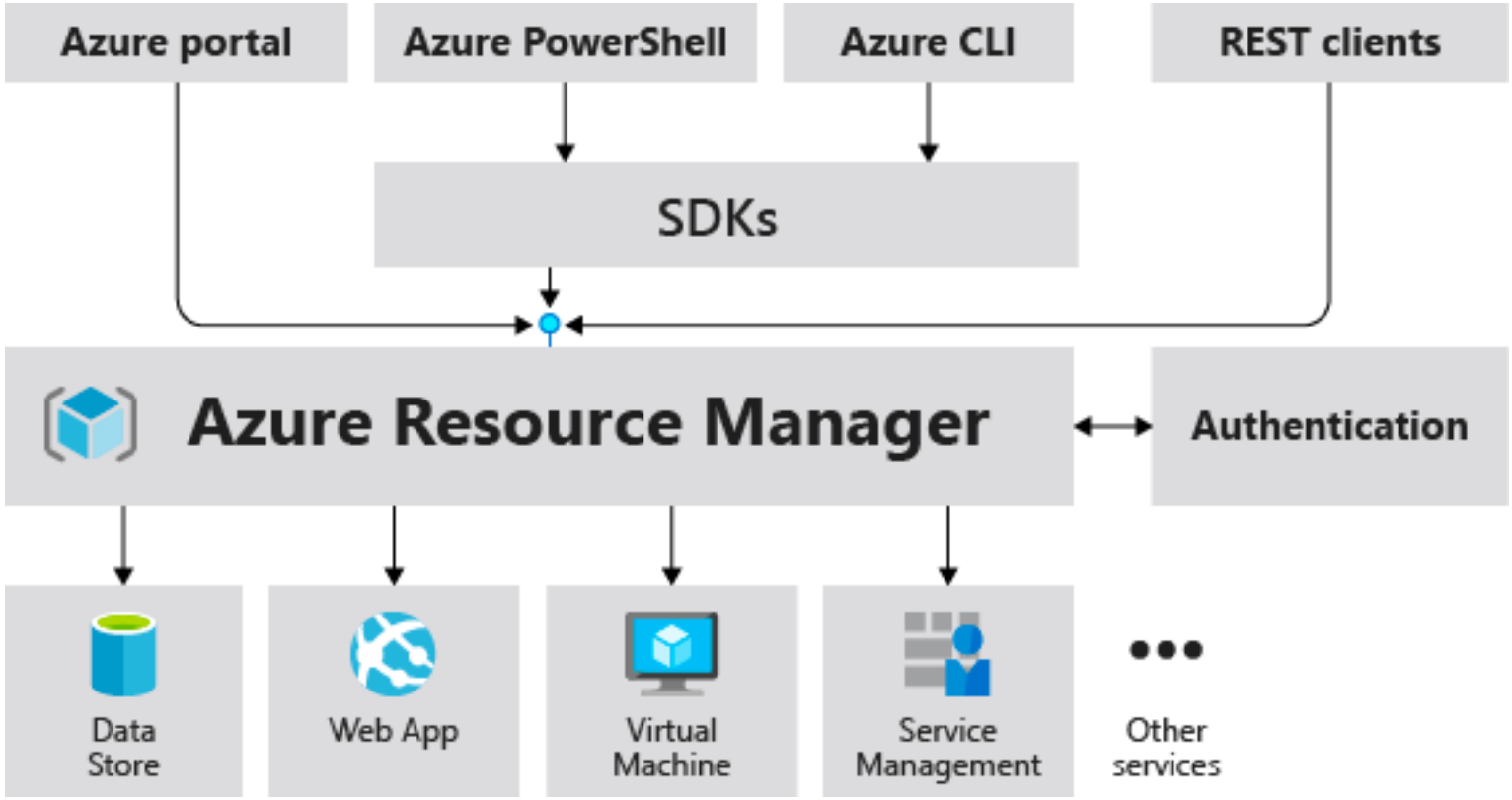
Agenda

- Azure Resource Manager
- Azure Resource Hierarchy / Scopes
- Azure Management Groups / Subscriptions / Resource Groups
- Azure Policies
- Azure Role-based access control
- Azure Resource Graph
- Azure Blueprints
- Azure Cost Management

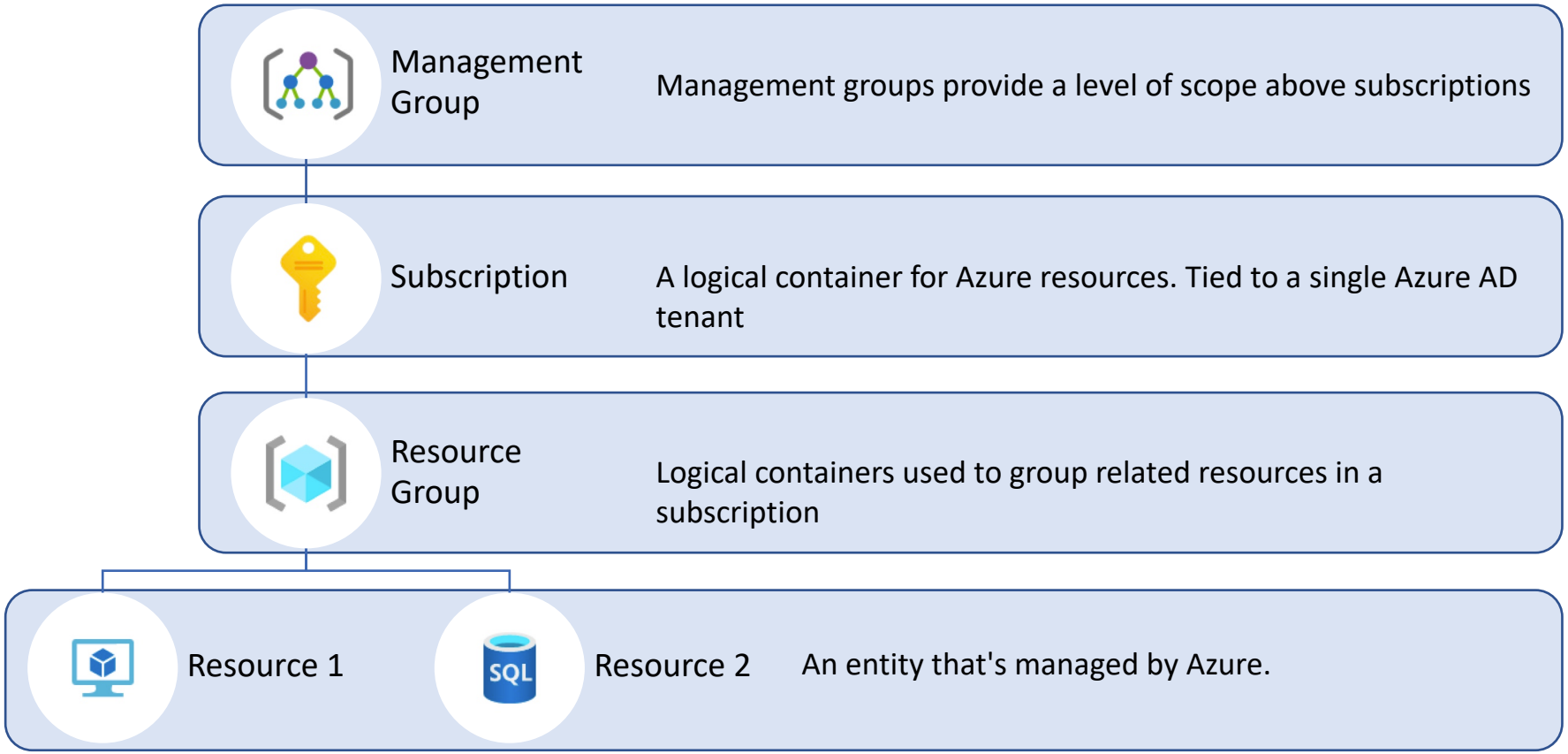
Azure Resource Manager (ARM)

- Resource manager provides template based repeatable deployment model for all Azure resources
- Within Resource Manager, resources can be grouped, deployed, managed and monitored as a resource group
- Reusable/linkable JSON template
- Mark one resource dependable on another
- Supports tagging of resources
- Microsoft recommends all the new Azure resources should be created using ARM

Azure Resource Manager (ARM)



Scopes / Resource Hierarchy



Management Groups

- Group subscriptions into containers called as Management Groups
- Management groups provide a level of scope above subscriptions
- Management groups can be nested
- Removes the need to manage/govern individual subscriptions
- Tenant root group is always created by default and cannot be changed or deleted
- Name of a management group cannot be changed after creation
- All the policies that you define in a management group gets applied to all the underlying management groups and subscriptions
- To delete a management group, first move all the subscriptions out of it

Subscription

- An Azure subscription is a logical container for Azure resources
- Each Azure resource can be associated with only one subscription
- Each azure subscription is linked to an Azure Active Directory tenant
- An Azure subscription is linked to an Azure offer which defines the pricing and other benefits
- An Azure Subscription acts as a boundary of scale with defined scale limits
- An Azure subscription also acts as an administrative boundary

Azure Account Offer Types

- **Free Account**
- Sign up for a free trial at https://azure.microsoft.com/en-us/free/ to receive 200$ free credit for one month.
- Certain services are free for 12 months and 25+ services are always free.
- **Pay-As-You-Go Account**
- Create a pay-as-you-go account directly -or- convert your free account to pay-as-you-go account.
- Can be cancelled at any time.
- Credit card on file is billed on a monthly basis.
- **Visual Studio Subscribers**
- $50 or $150 credit per month

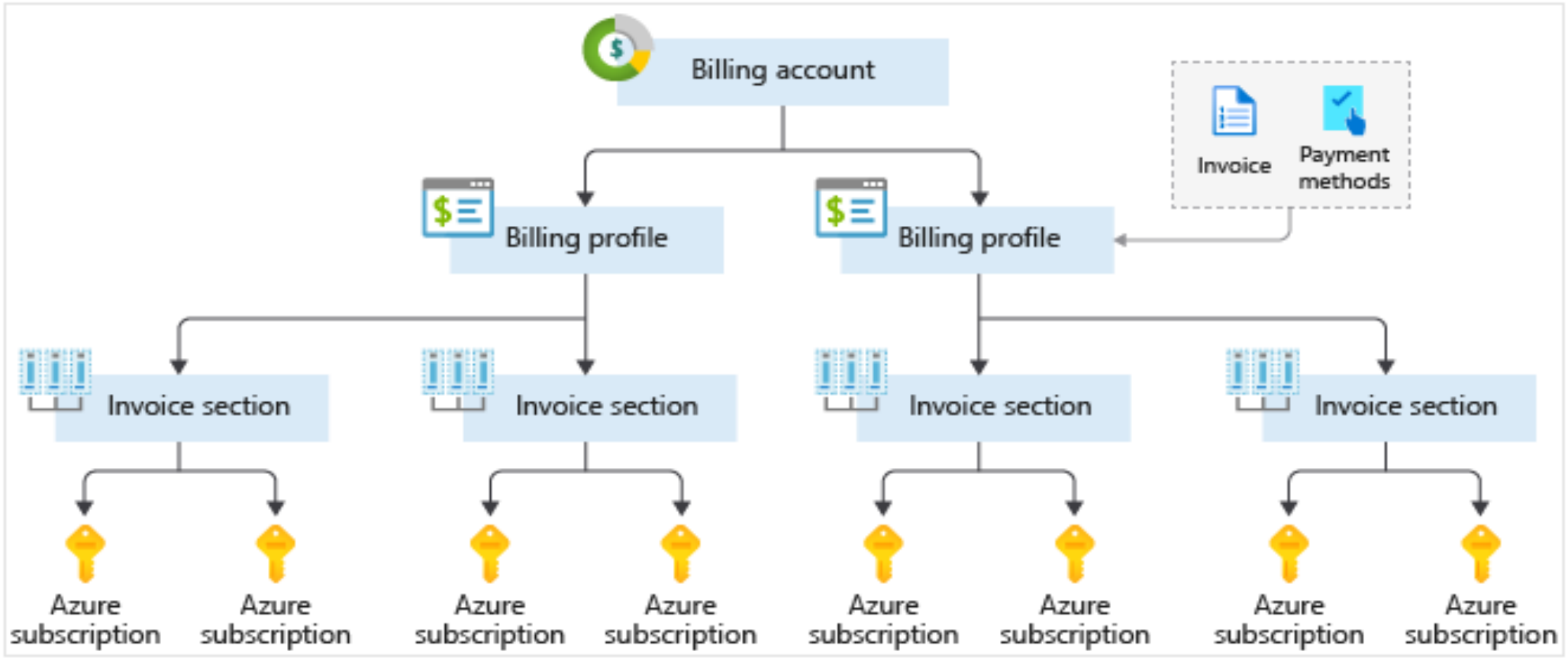
Azure Billing Account Types

- **Microsoft Online Services Program**: A individual billing account for a Microsoft Online Services Program is created when you sign up for Azure through the Azure website.
- **Enterprise Agreement**: A billing account for an Enterprise Agreement is created when your organization signs an Enterprise Agreement (EA) to use Azure.
- **Microsoft Customer Agreement**: A billing account for a Microsoft Customer Agreement is created when your organization works with a Microsoft representative to sign a Microsoft Customer Agreement.

Azure Account vs Azure Subscription?

- **Azure Billing Account**
- A billing account is created when you sign up to use Azure.
- Billing account is used to manage invoices, payments, and track costs.
- You can have access to multiple billing accounts.
- **Azure Subscription**
- An Azure subscription is a logical container used to provision resources in Azure.
- When you sign up for an account, an Azure subscription is created by default.
- There can be multiple subscriptions under an account.
- Any resource that you create in Azure must be created within a subscription.

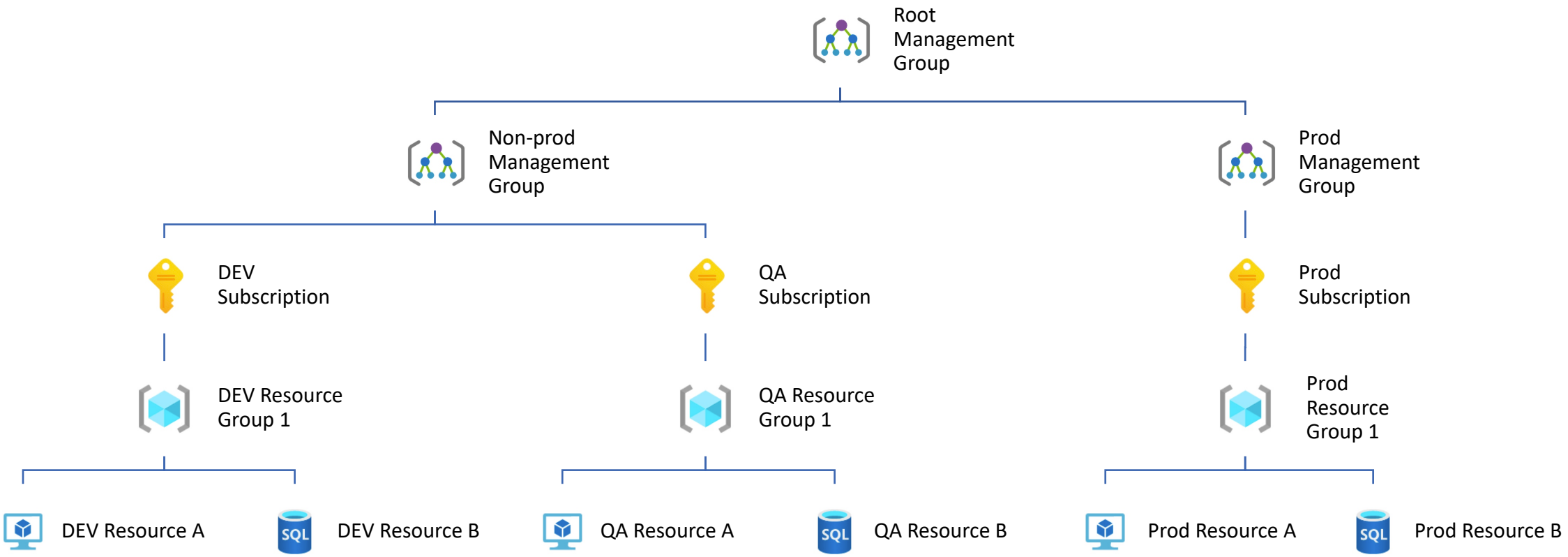
Azure Account Structure



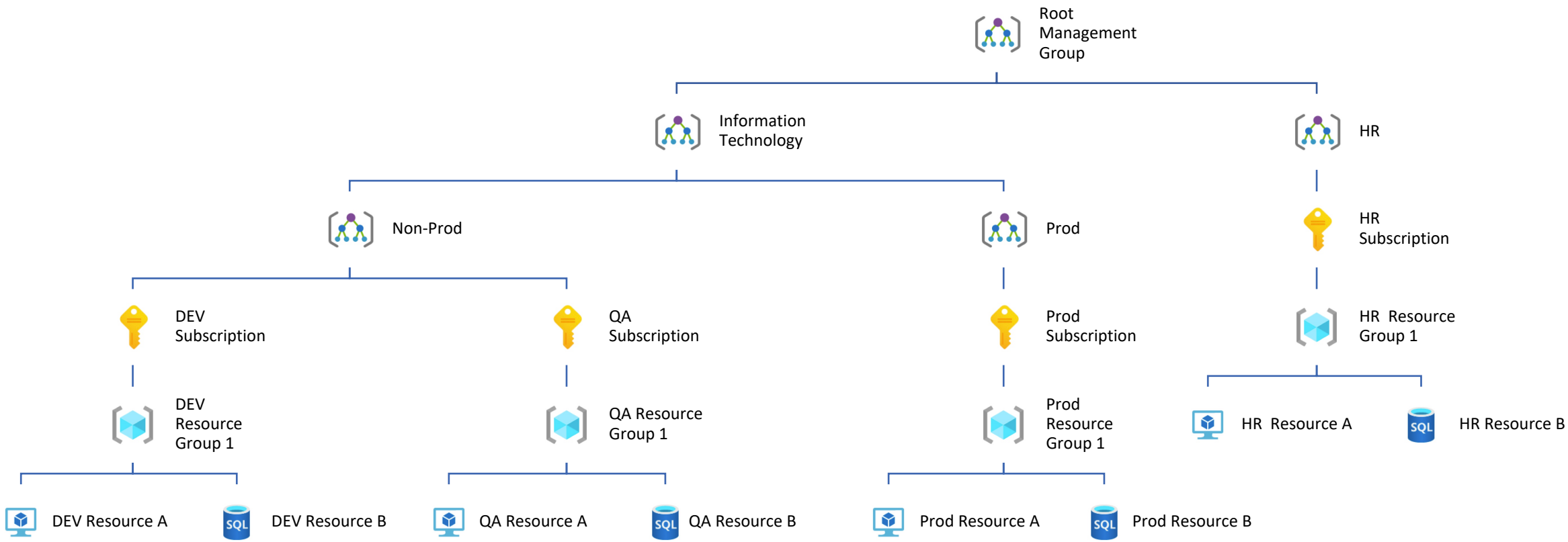
Resource Groups

- Under ARM, all the resources are grouped into a Resource Group
- All of the resources in a resource group share the same lifecycle
- A resource can only be assigned to one group at a time
- Most types of resource can be moved to a different resource group at any time
- The resources in a resource group can be in different regions
- You can use a resource group to control access for the resources therein

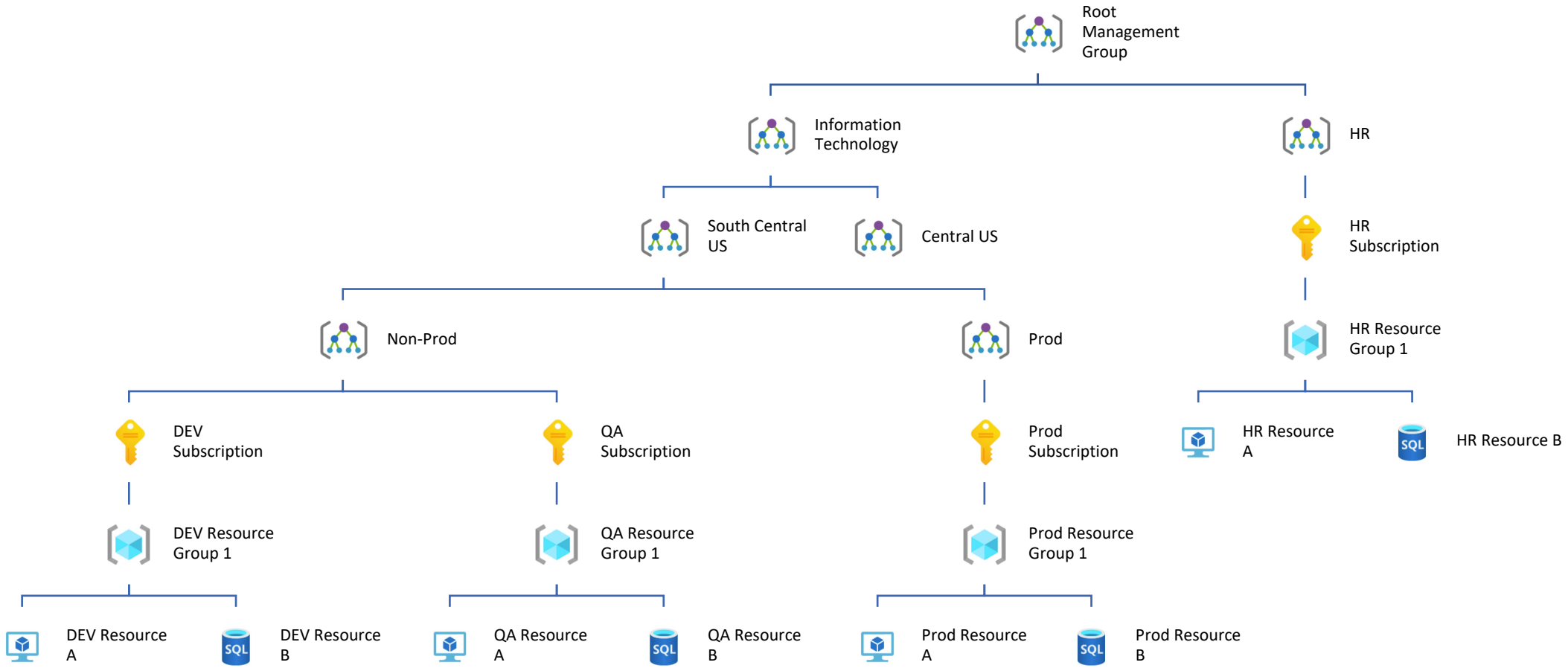
Scopes / Resource Hierarchy



Scopes / Resource Hierarchy



Scopes / Resource Hierarchy



Demo - 1

Azure resource hierarchy

Azure Policy

Defines set of rules for enforcing organizational standards and assessing compliance

Scans Azure Resources and provides compliance reports in a dashboard

Supports remediation

Examples –

- Allowed resource types
- Allowed Locations
- Allowed Virtual Machines SKUs

Azure Policy

Assignment Options –

1. Policy
2. Initiative – Group of policies

Three parts of a policy:

1. Policy Definition
2. Policy Assignment
3. Policy Parameters

List of Built-in Policies: https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies

Azure Policy

Assignment Options –

1. Policy
2. Initiative – Group of policies

Three parts of an initiative:

1. Initiative Definition
2. Initiative Assignment
3. Initiative Parameters

List of Built-in Initiatives: https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-initiatives

Azure Policy

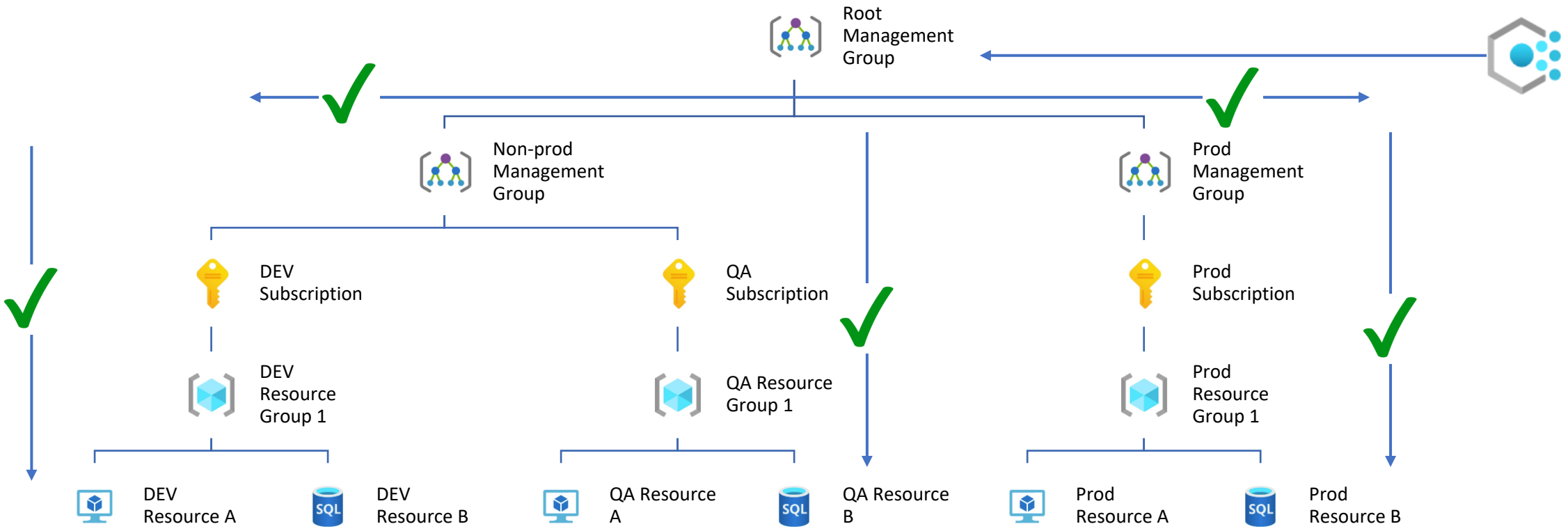
```
{
  "properties": {
    "displayName": "Allowed virtual machine size SKUs",
    "policyType": "BuiltIn",
    "mode": "Indexed",
    "description": "This policy enables you to specify a set of virtual machine size SKUs that your organization can deploy.",
    "metadata": {
      "version": "1.0.1",
      "category": "Compute"
    },
    "parameters": {
      "listOfAllowedSKUs": {
        "type": "Array",
        "metadata": {
          "description": "The list of size SKUs that can be specified for virtual machines.",
          "displayName": "Allowed Size SKUs",
          "strongType": "VMSKUs"
        }
      }
    },
    "policyRule": {
      "if": {
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Compute/virtualMachines"
          },
          {
            "not": {
              "field": "Microsoft.Compute/virtualMachines/sku.name",
              "in": "[parameters('listOfAllowedSKUs')]"
            }
          }
        ]
      },
      "then": {
        "effect": "Deny"
      }
```

Azure Policy

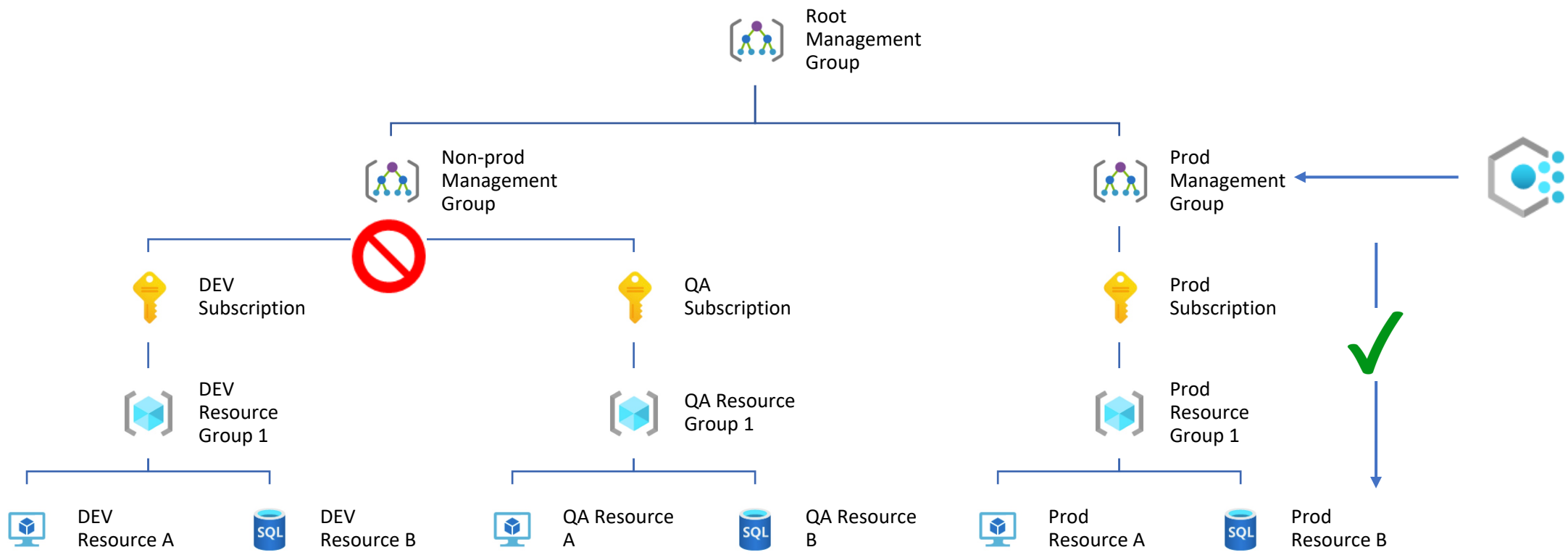
Effects of an Azure Policy:

1. Append
2. Audit
3. AuditIfNotExists
4. Deny
5. DeployIfNotExists
6. Disabled
7. Modify

Scopes / Resource Hierarchy



Scopes / Resource Hierarchy



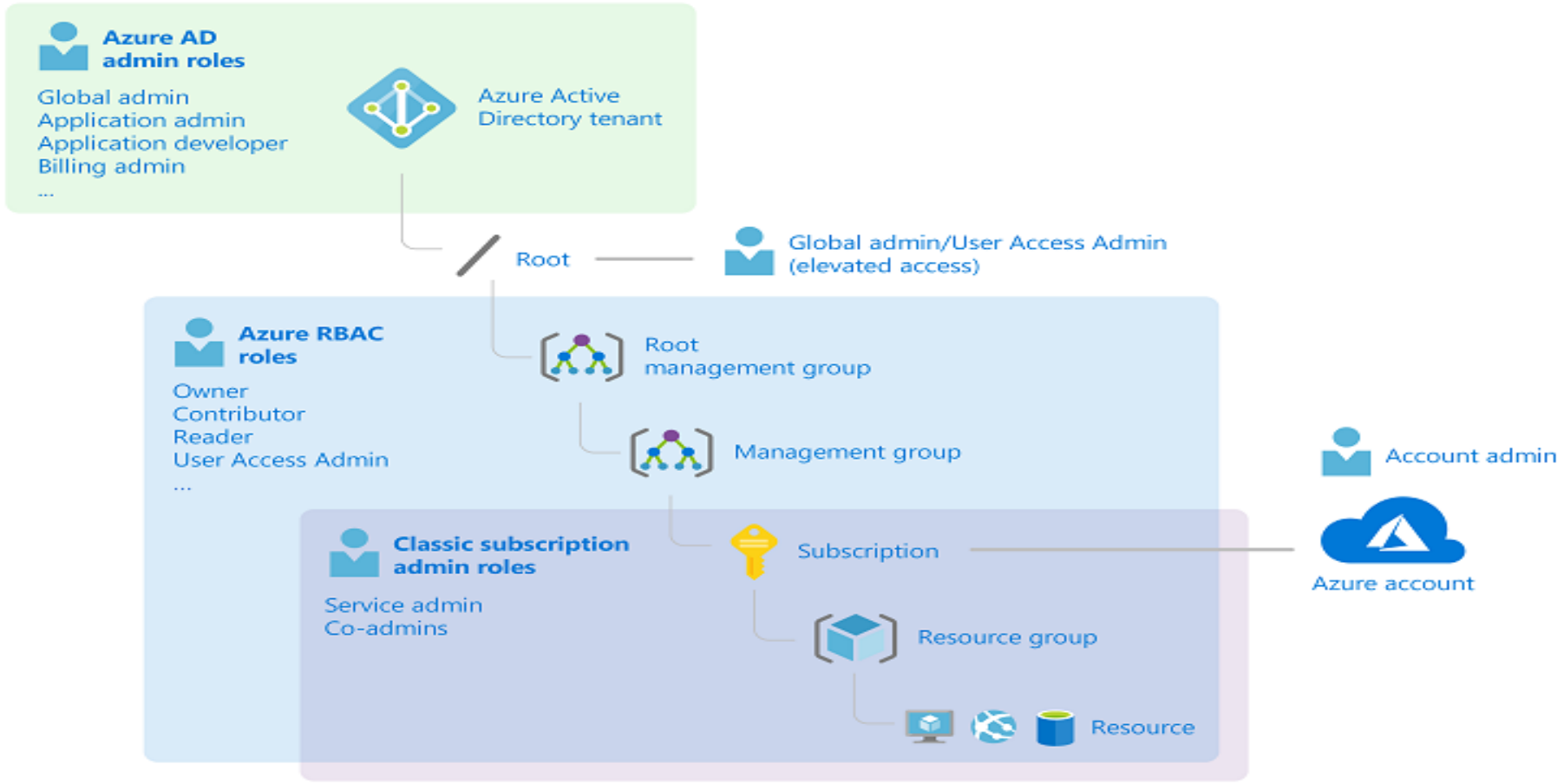
Demo - 2

Azure Policies

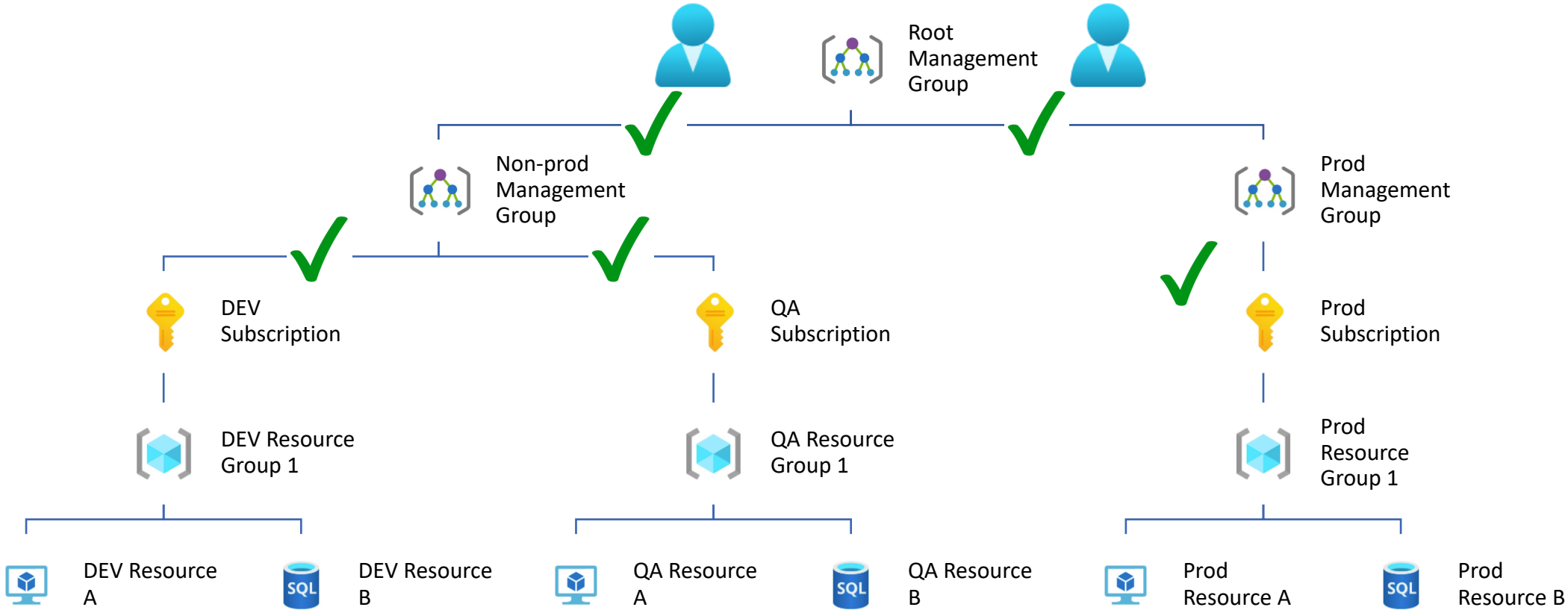
Azure Role based Access Control

- Fine-grained control over the operations and scope with which a user can perform an action
- Supported roles-
  - Owner
  - Reader
  - SQL DB contributor
  - SQL Security Manager
  - Storage Account Contributor
  - VM Contributor
  - Custom Roles
- Applies to any security principal like user, group and service principal
- Different roles from Azure Active Directory roles

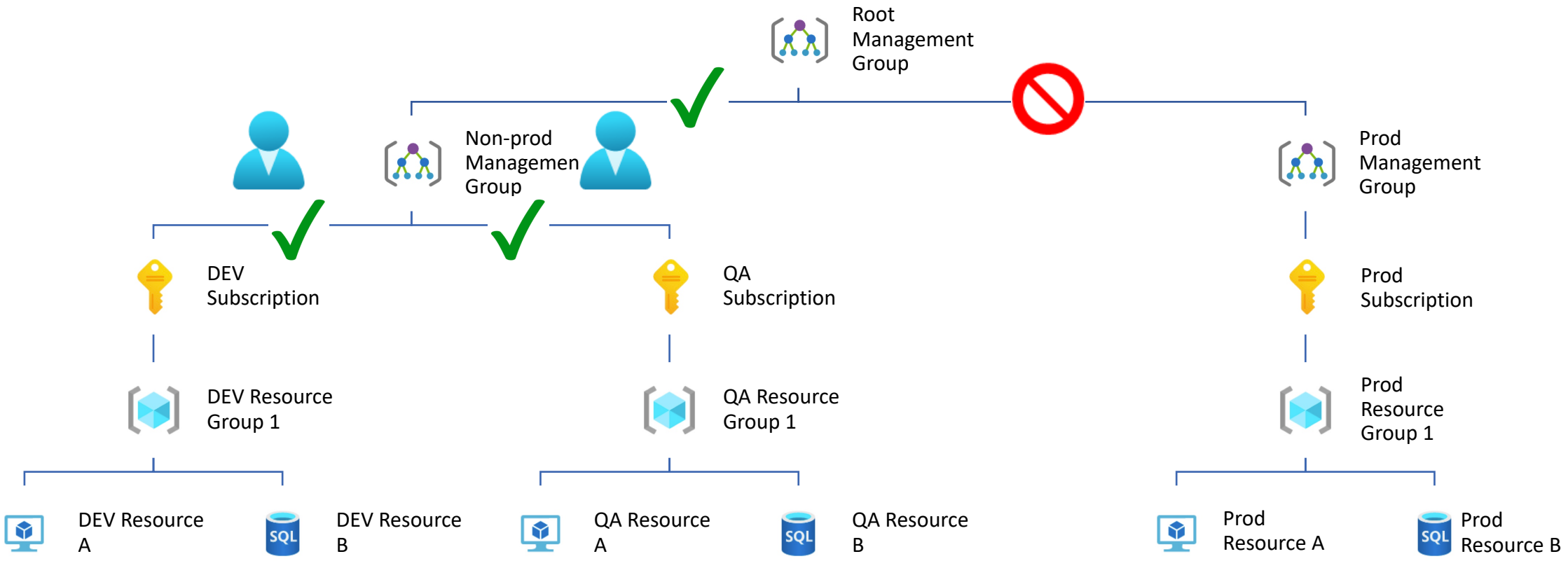
Role based Access Control



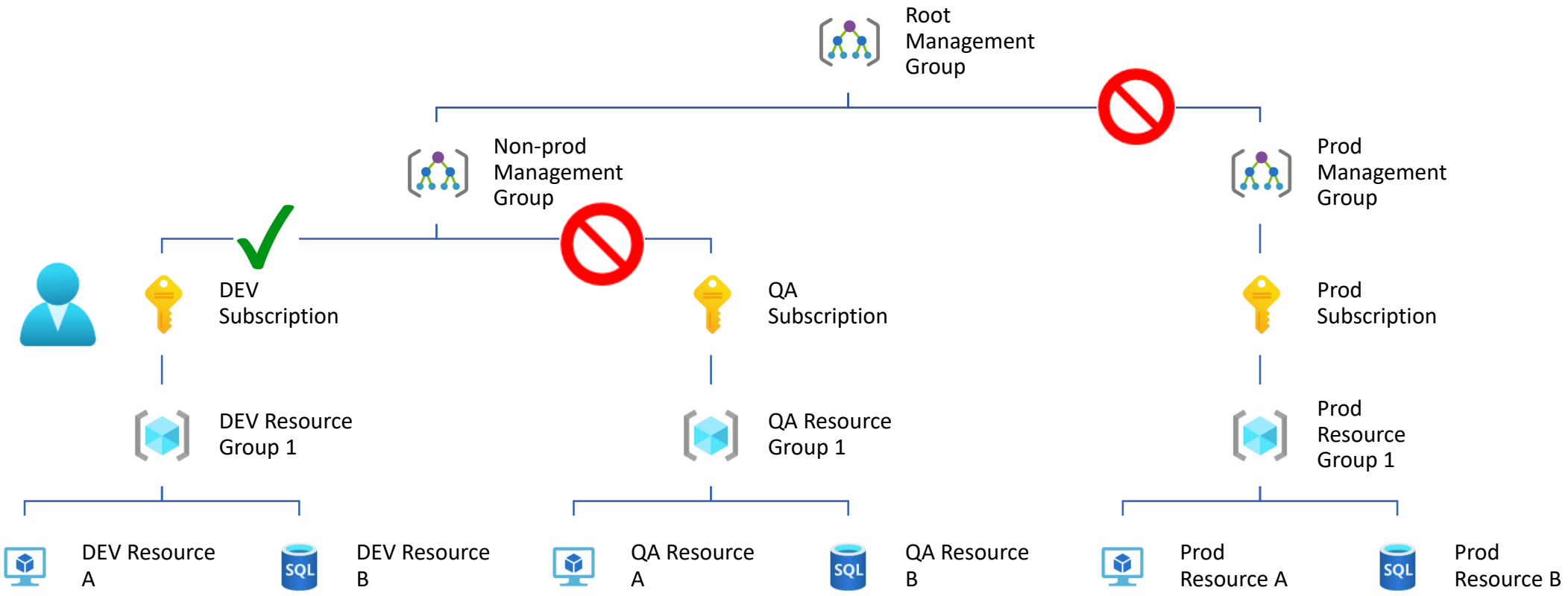
Role based Access Control



Role based Access Control



Role based Access Control



DEMO - 3

Role-based access control

Azure Blueprints

Blueprints offer a declarative way to orchestrate the deployment of artifacts enabling quick repeatable creation of fully governed environments. Artifacts include:

1. Role Assignments (RBAC)
2. Policy Assignments (Azure Policies)
3. ARM templates
4. Resource groups

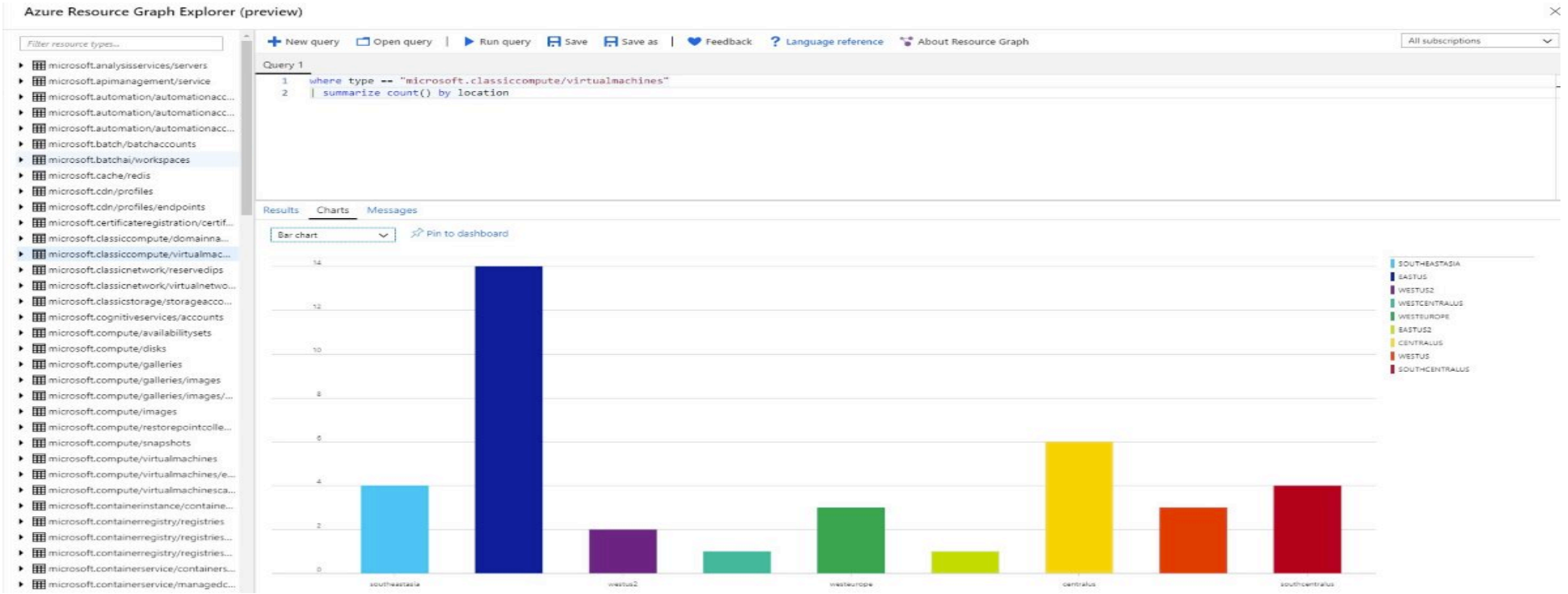
Lifecycle –

1. Create and Edit
2. Publish

Azure Resource Graphs

Powerful resource exploration tool

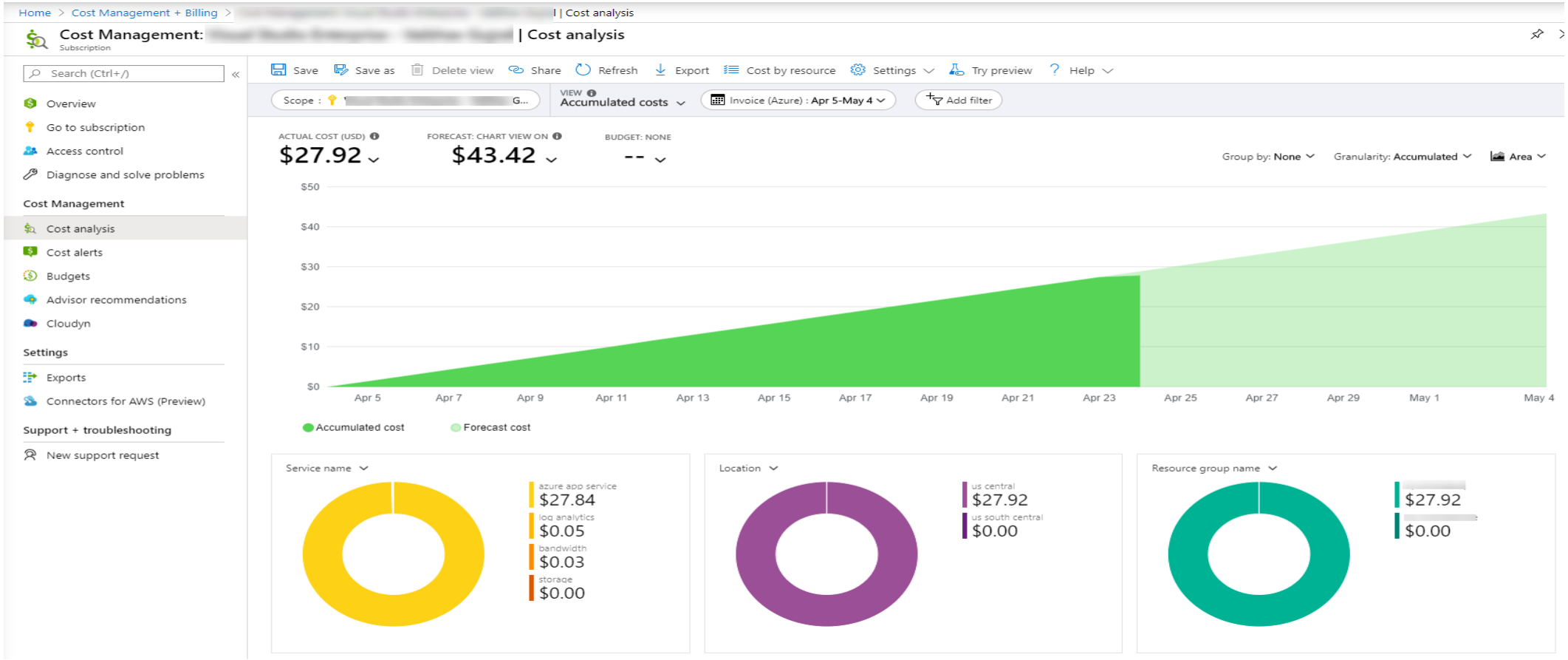
Uses a query language based on Kusto Query Language



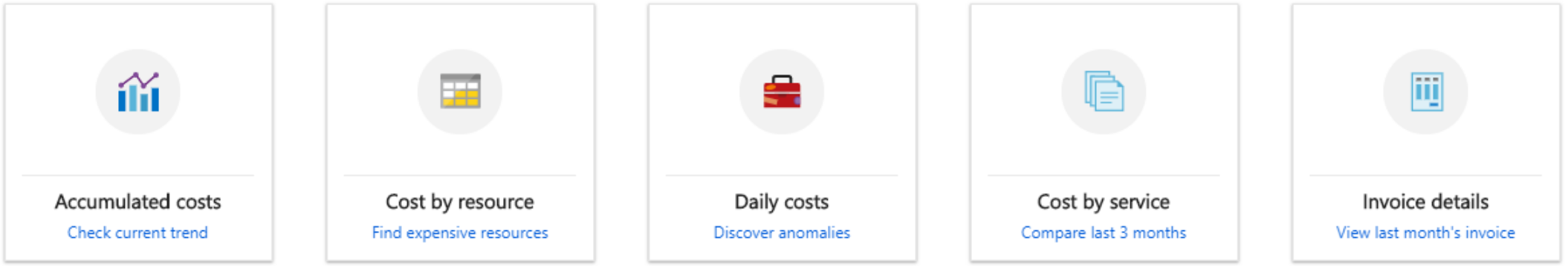
Demo - 4

Azure Resource graph

Azure Cost Management



Azure Cost Management



Tags

Tags can be applied to logically organize Azure resources into taxonomy

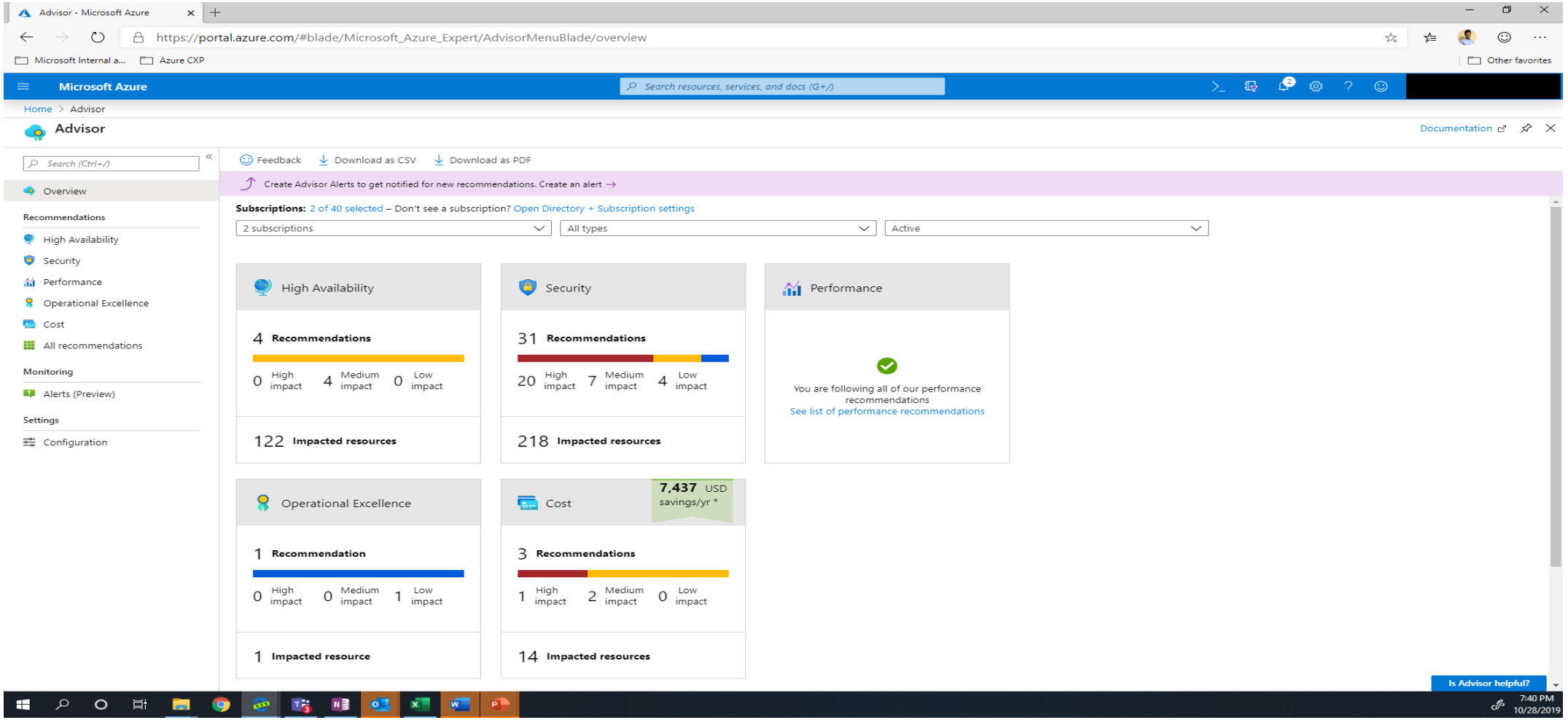
Tags can be applied to –

1. Subscriptions
2. Resource Groups
3. Resources

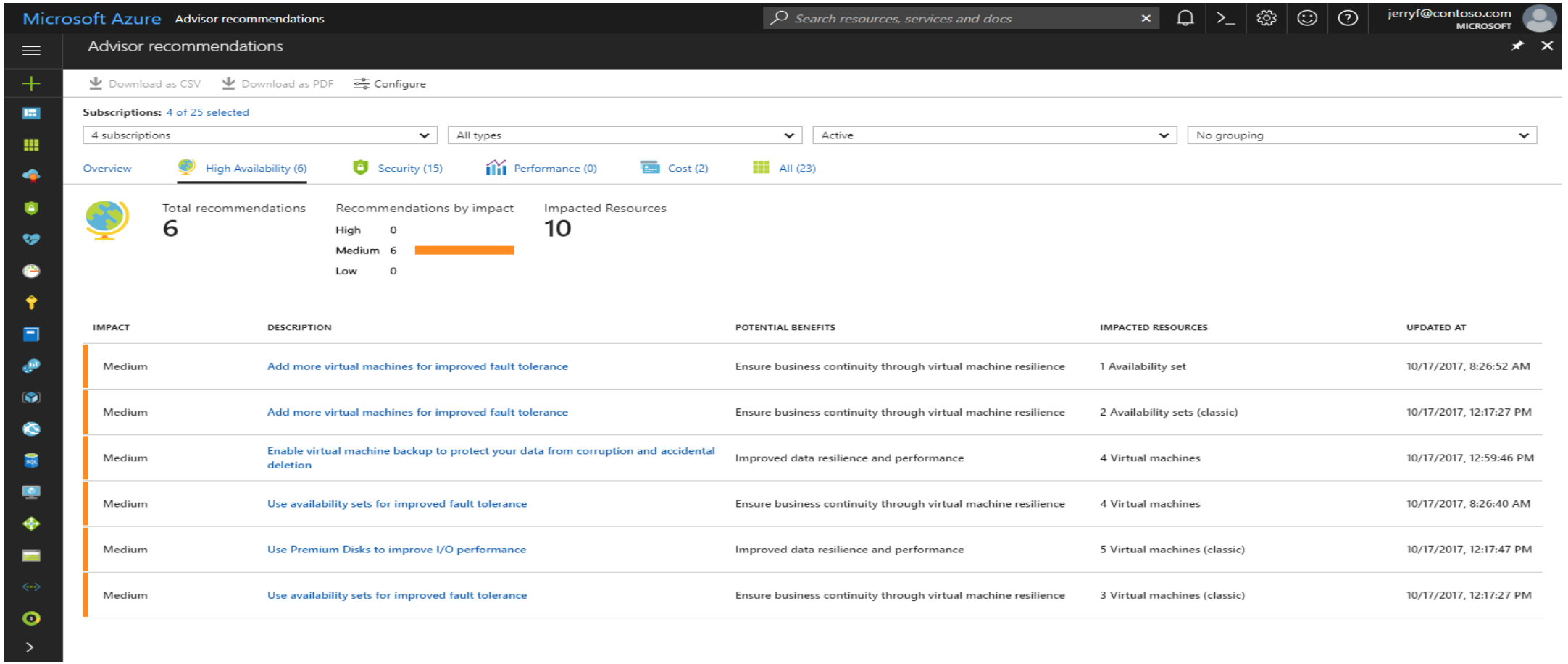
Examples – costcenter, env, owner, department

Tagging Decision Guide - https://bit.ly/30BR7Sx

Azure Advisor



Azure Advisor



IMPACT	DESCRIPTION	POTENTIAL BENEFITS	IMPACTED RESOURCES	UPDATED AT
Medium	Add more virtual machines for improved fault tolerance	Ensure business continuity through virtual machine resilience	1 Availability set	10/17/2017, 8:26:52 AM
Medium	Add more virtual machines for improved fault tolerance	Ensure business continuity through virtual machine resilience	2 Availability sets (classic)	10/17/2017, 12:17:27 PM
Medium	Enable virtual machine backup to protect your data from corruption and accidental deletion	Improved data resilience and performance	4 Virtual machines	10/17/2017, 12:59:46 PM
Medium	Use availability sets for improved fault tolerance	Ensure business continuity through virtual machine resilience	4 Virtual machines	10/17/2017, 8:26:40 AM
Medium	Use Premium Disks to improve I/O performance	Improved data resilience and performance	5 Virtual machines (classic)	10/17/2017, 12:17:47 PM
Medium	Use availability sets for improved fault tolerance	Ensure business continuity through virtual machine resilience	3 Virtual machines (classic)	10/17/2017, 12:17:27 PM

Demo - 5

Azure Cost management

Resource Locks

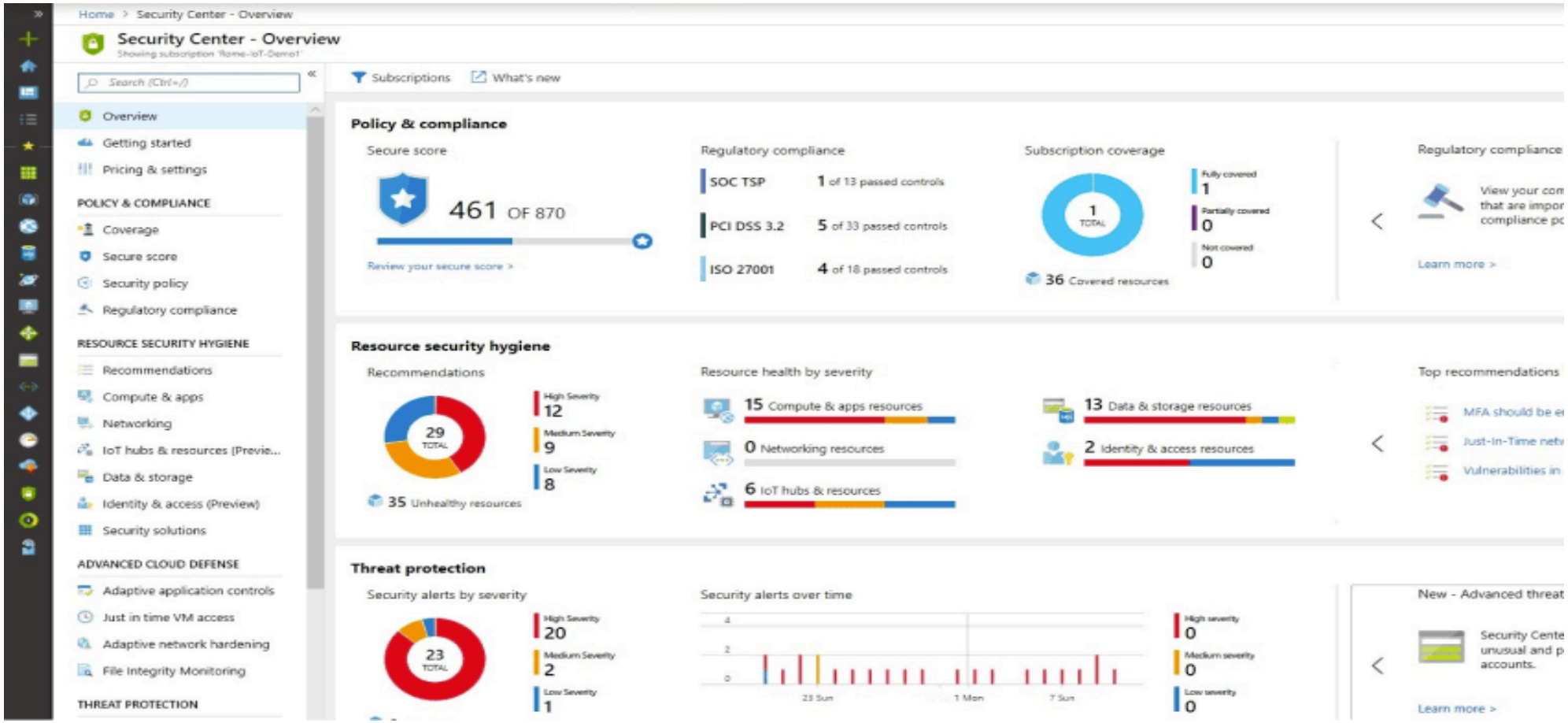
Lock resources to prevent accidental deletion or modification

Two Lock levels:

- CanNotDelete – Authorized users can read and modify but cannot delete the resource
- ReadOnly – Authorized users can read a resource but cannot delete or update

Only an Owner or User Access Administrator can create or delete resource locks

Azure Security Center



Resources for further reading

1. Cloud Adoption Framework: https://azure.microsoft.com/en-us/cloud-adoption-framework/
2. Azure Governance: https://azure.microsoft.com/en-us/solutions/governance/
3. Azure Architecture Center: https://docs.microsoft.com/en-us/azure/architecture/
4. Microsoft Azure Documentation: https://docs.microsoft.com/en-us/azure/

Q&A


thank
you