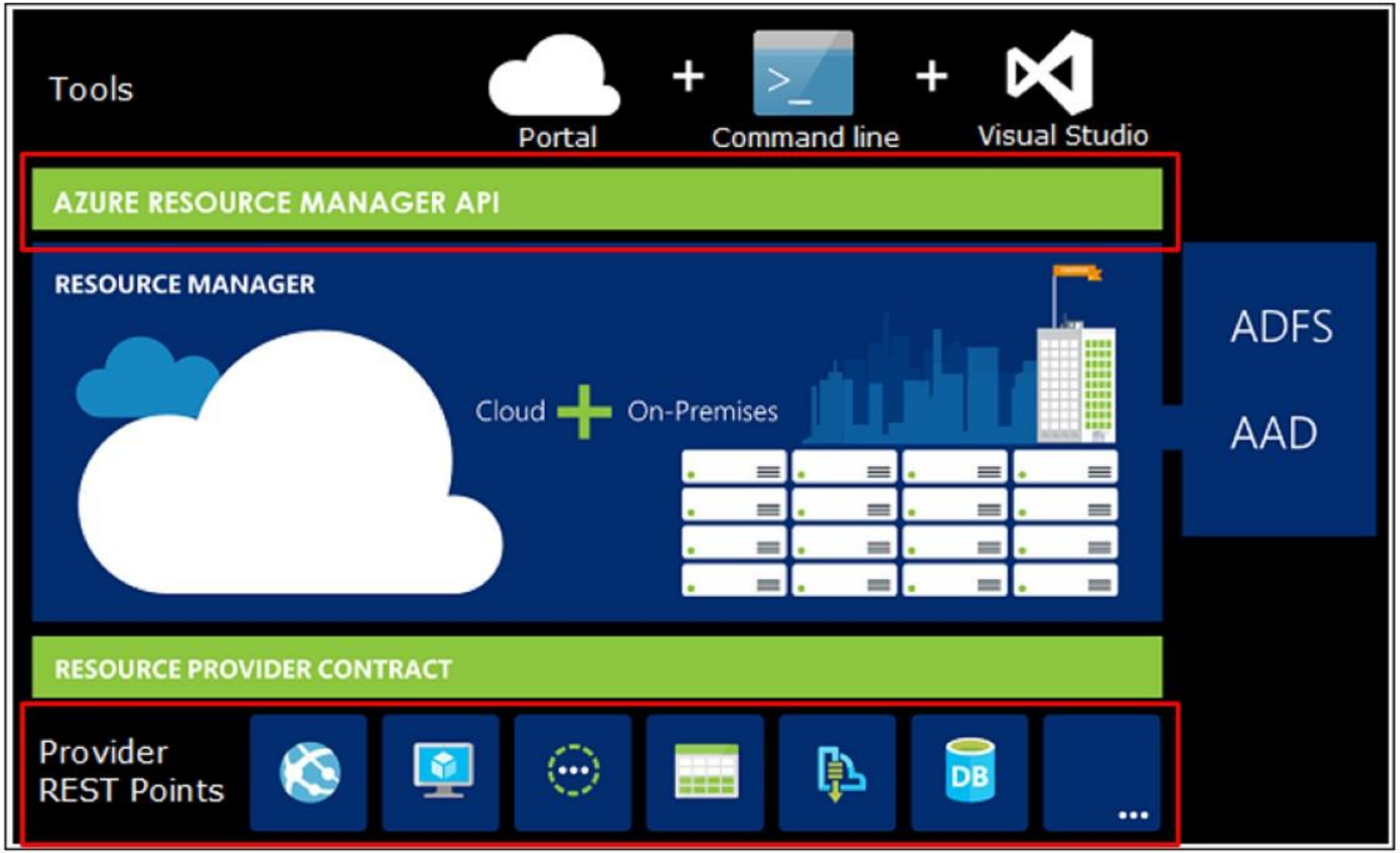
Azure Resource Manager

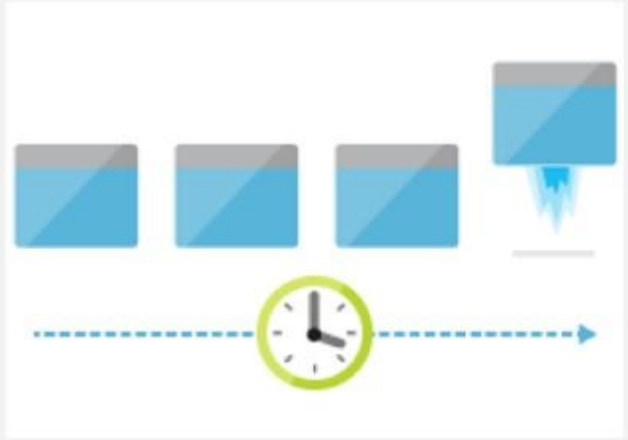
What is Azure Resource Manager?



Benefits of Azure Resource Manager

- Deploy, Manage and Monitor all resources in a solution as a group
- Repeatedly deploy a solution throughout the development cycle
- Use declarative templates or imperative scripts across public or private cloud
- Define dependencies between resources so they are deployed in the correct order
- Role based access control with all resources
- Use tags to provide further taxonomy of resource groups

What can you do with Resource Manager?



Deploy

Organize

Control

Tooling for Azure Resource Manager

- Azure Management Portal

- Visual Studio

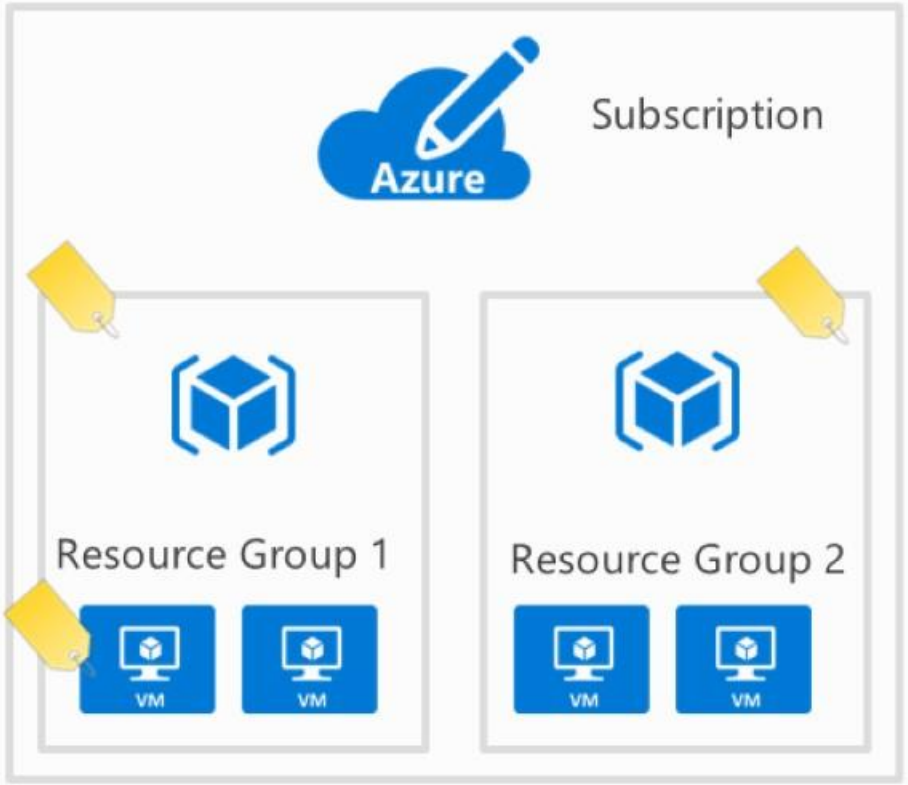
- PowerShell or Azure CLI

- Custom Code calling ARM API

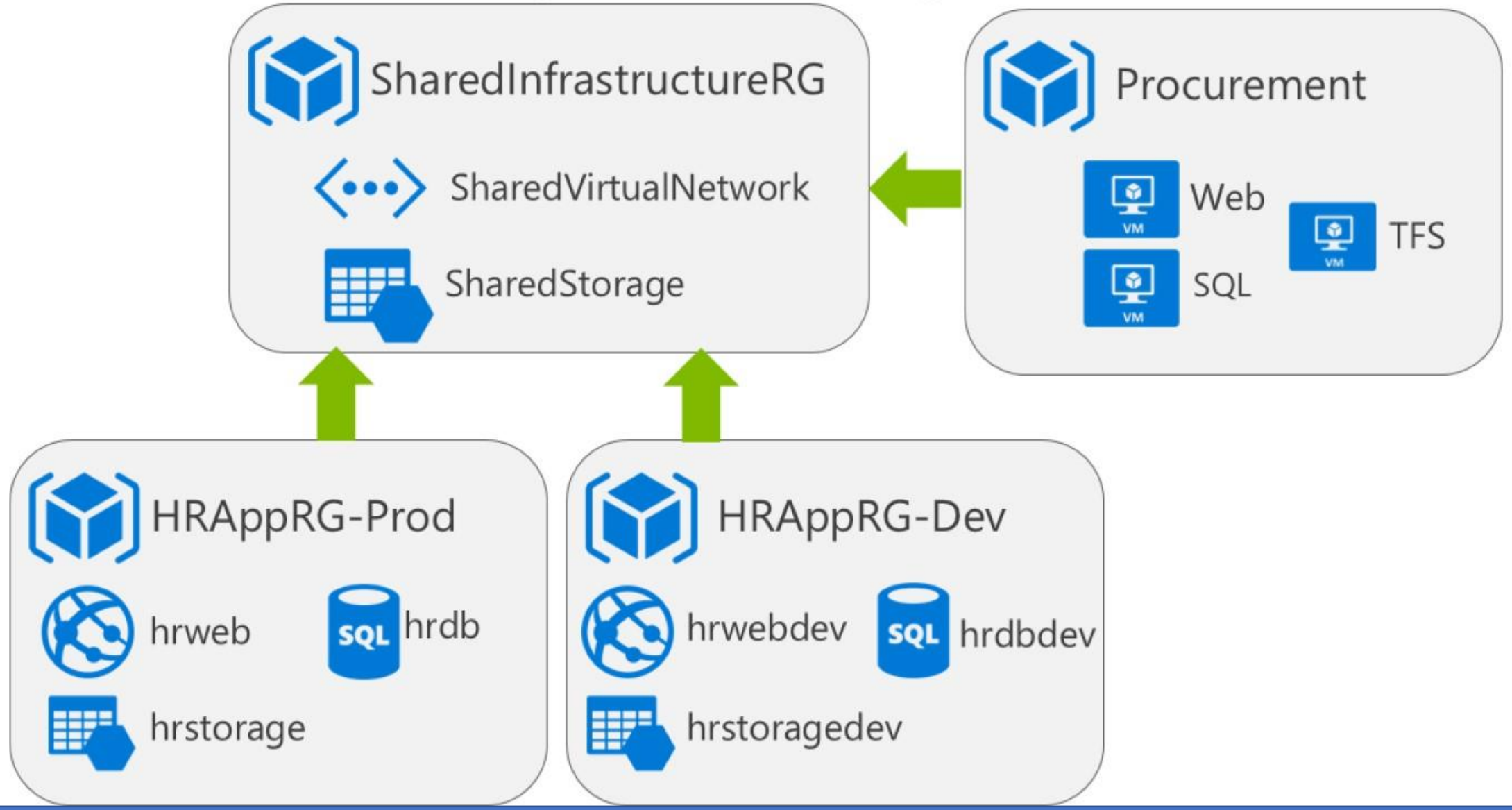
Organizing Resources

Resource Organization

- Why worry about organization?
  - Resource Management
  - Security boundaries (RBAC)
  - Billing Scope
    - Subscription
    - Resource Group
    - Tag



Resource Group Planning



Azure Resource Tags

environment: production
cost-center: marketing

Resource Tags

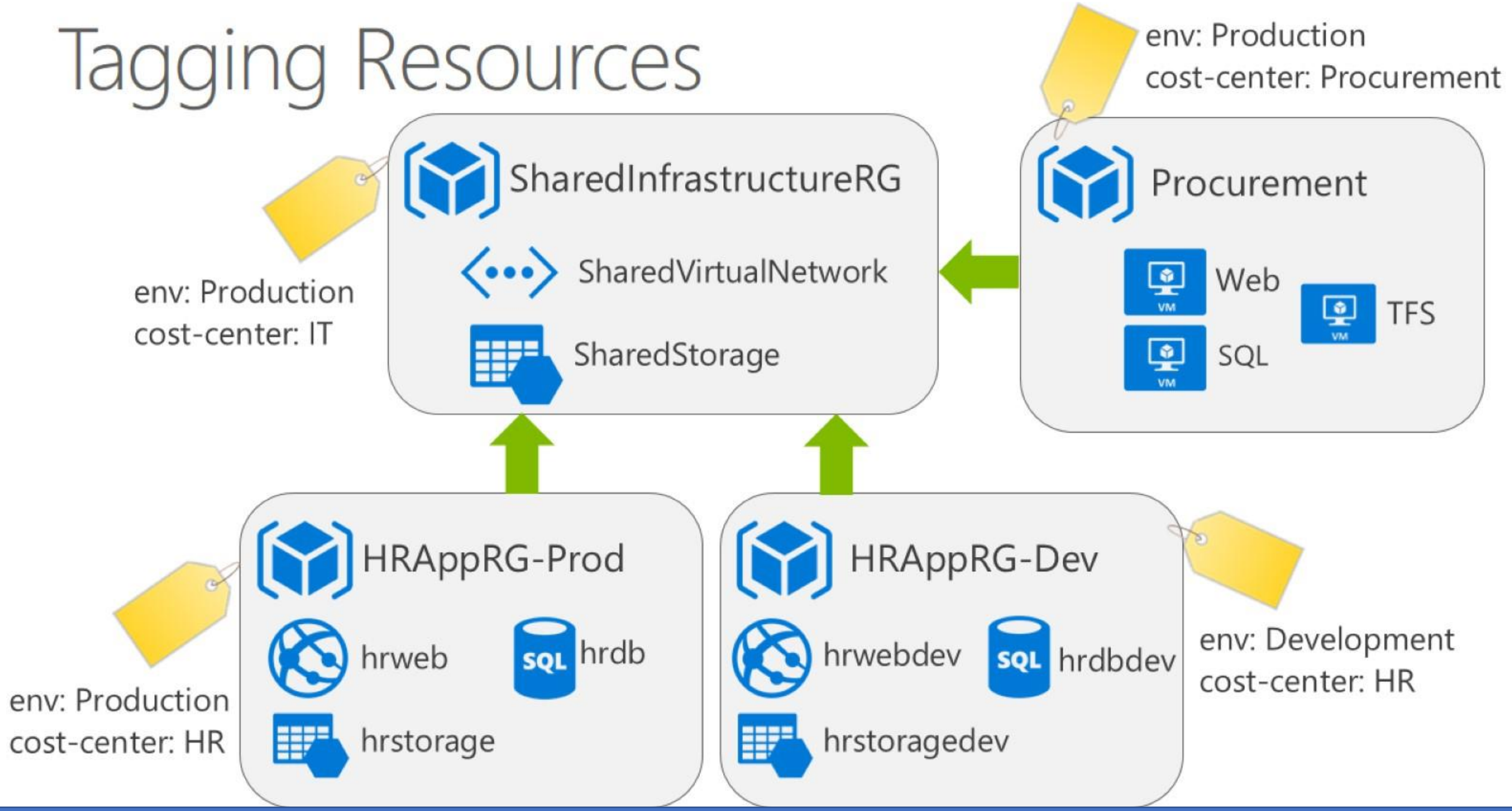
Name-value pairs assigned to resources or resource groups

Subscription-wide taxonomy

Each resource can have up to 15 tags

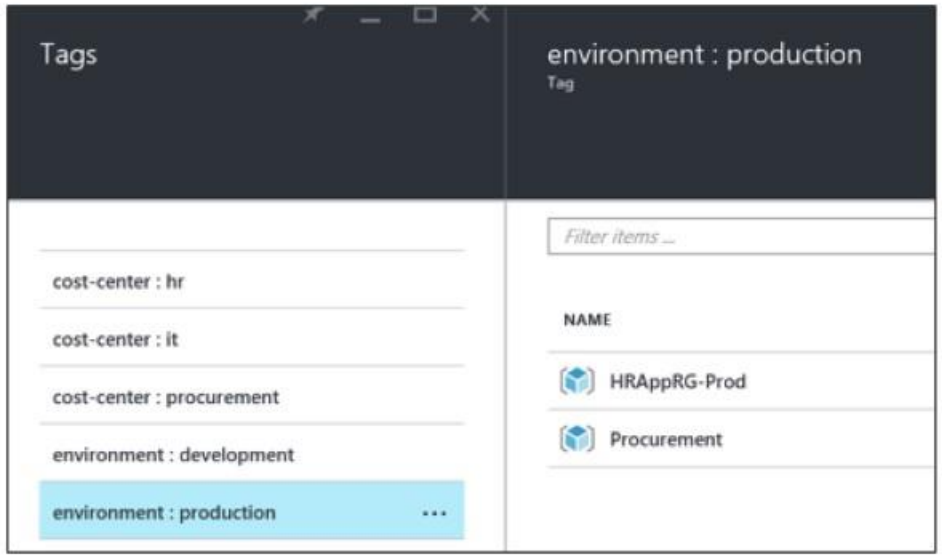
Tags roll up to your Azure bill

Tagging Resources



Viewing Resources by Tags

- View Resource Groups by Tag with the portal or the command line




```
PS C:\Users\        > Find-AzureRmResourceGroup -Tag @{ Name="cost-center"; Value="hr" }

Id         : /subscriptions/                                    /resourceGroups/HRAppRG-Dev
Name       : HRAppRG-Dev
Location   : westus
Tags       : @{Environment=development; Cost-center=hr}
Properties : @{ProvisioningState=Succeeded}

Id         : /subscriptions/                                    /resourceGroups/HRAppRG-Prod
Name       : HRAppRG-Prod
Location   : westus
Tags       : @{Environment=production; Cost-center=hr}
Properties : @{ProvisioningState=Succeeded}
```

```
az group update -n HRDEV --set
tags.ENV=DEVELOPMENT --set tags.CostCenter=HR
```

Charge Back

- Resource Groups and Tags are exported via CSV with your Azure Bill

Daily Usage						
Usage Date	Meter Category	Unit	Consume	Resource Gr	nstance 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"}"

Moving Resources

- Not all services support moving between subscriptions or resource groups
- It's important to do the planning up front on where and how resources are organized

Current resources that are supported
https://azure.microsoft.com/en-us/documentation/articles/resource-group-move-resources/

Resource Locks

Resource Lock Overview

- Used to prevent accidental deletion
- Scope
  - Subscription
  - Resource Group
  - Resource
- Locks are inherited by child resources

Setting Resource Locks

- PowerShell

```
New-AzureRmResourceLock -LockLevel CanNotDelete `
                        -LockName LockVM -ResourceName MyVM `
                        -ResourceType Microsoft.Compute/virtualMachines
```

- Template

```
"resources": [
{
   "name": "[concat(parameters('lockedResource'), '/Microsoft.Authorization/myLock')]",
   "type": "Microsoft.Storage/storageAccounts/providers/locks",
   "apiVersion": "2015-01-01",
   "properties": {
     "level": "CannotDelete"
    }
}
```

- CLI

```
az lock create -n ReadOnlyLock -g OpsTrainingOSS_RG --lock-type ReadOnly
```

s

DEMO

Microsoft Azure

Using Tags to Organize Resources

Role Based Access Control (RBAC)

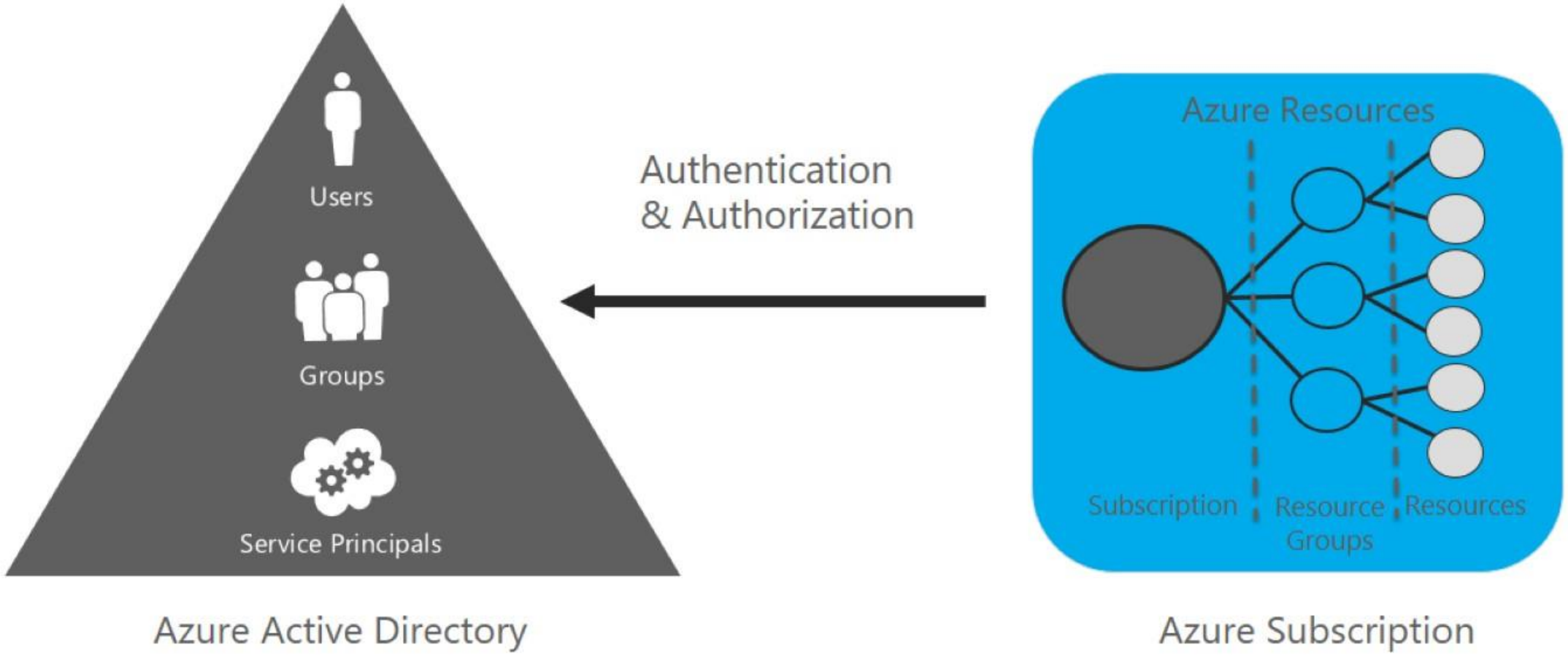
Role Based Access Control (RBAC)

In systems security, role based access control is an approach to restricting system access to authorized users

Azure RBAC

- It is the capability to control cloud resources access between employees at resource level and which actions they can perform
- Subscription is no longer access management boundary
- Access is granted to users and groups
- Supported on the new Azure Portal only
- In order to enforce RBAC, user cannot be granted co-administrator of the subscription from the current management portal

Identity Comes from Azure AD

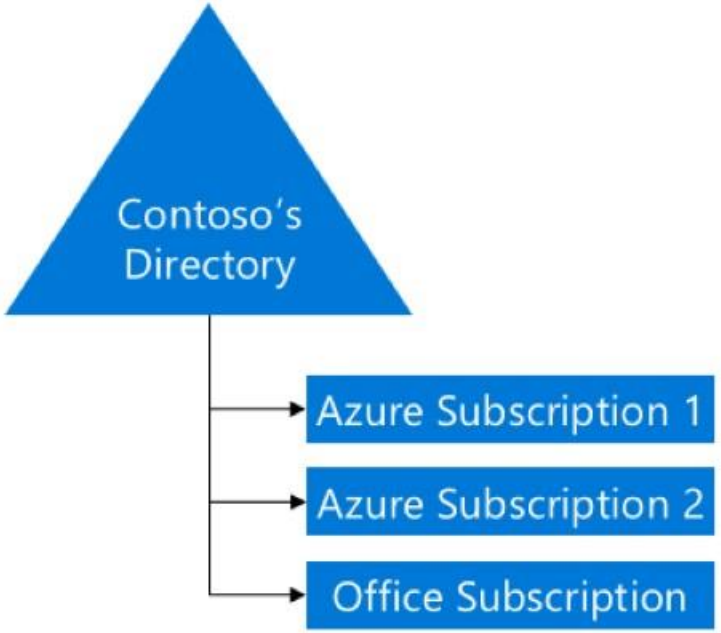


Azure Active Directory

Azure Subscription

Azure AD and Azure Subscriptions

- AAD is used for organizational identity
  - Directory admins can apply identity, authentication and authorization policies for apps and azure is modeled as an app that belongs to the directory
- Applied to Azure subscriptions:
  - Every Azure subscription belongs to a directory (n:1)
  - Even if you sign up with an MSA, you get a directory
- A subscription's directory:
  - Limits the work accounts that may be added as a co-admin or RBAC role
  - Contains policies that impact authentication & authorization for the subscription
  - Directory global admins of the directory have the ability to access subscription



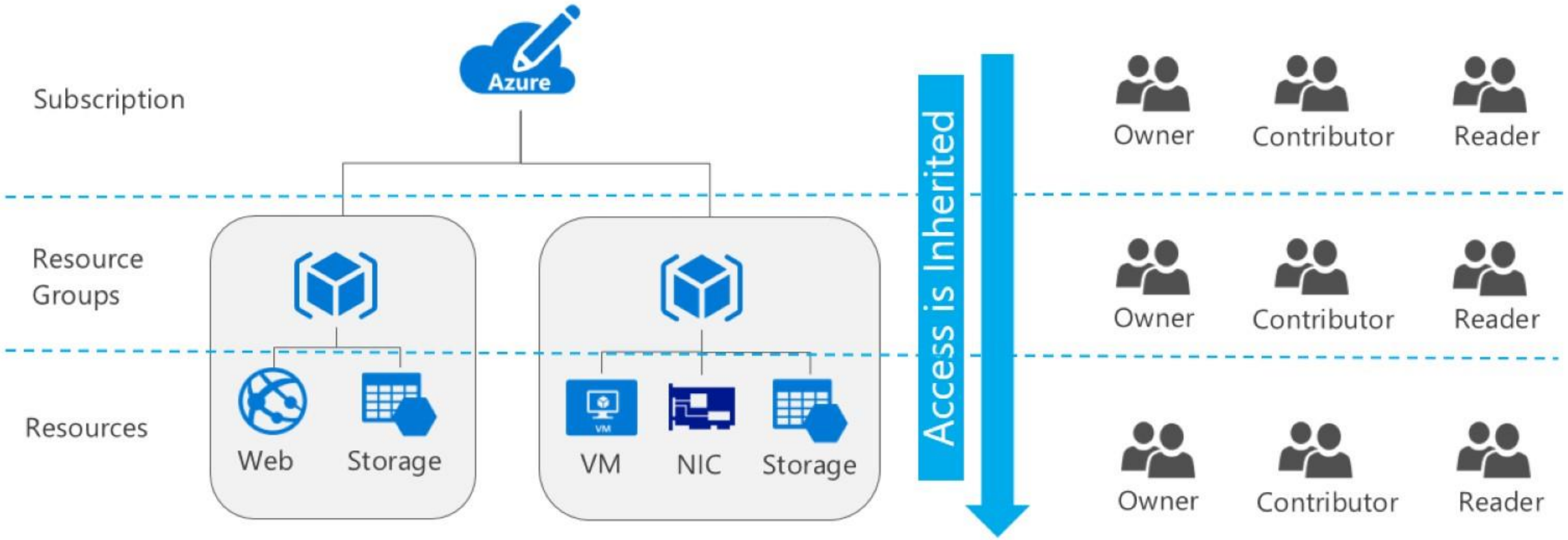
Roles

BUILT-IN ROLE	ACTIONS	NOT ACTIONS
Owner (allow all actions)	*	
Contributor (allow all actions except writing or deleting role assignments)	*	Microsoft.Authorization/*/Write, Microsoft.Authorization/*/Delete
Reader (allow all read actions)	*/Read	

Custom Roles

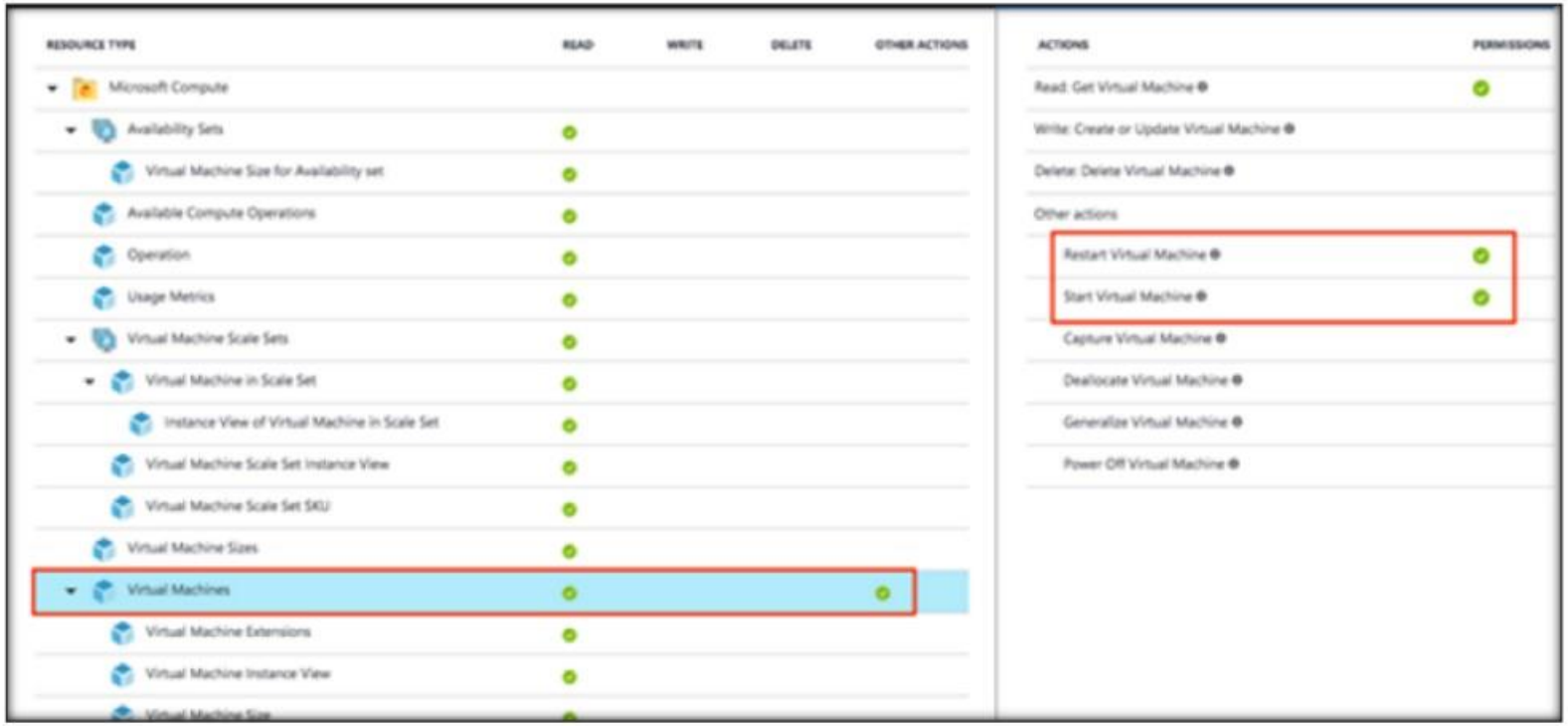
Custom roles can be created using RBAC command-line tools in Azure PowerShell, and Azure Command-Line Interface

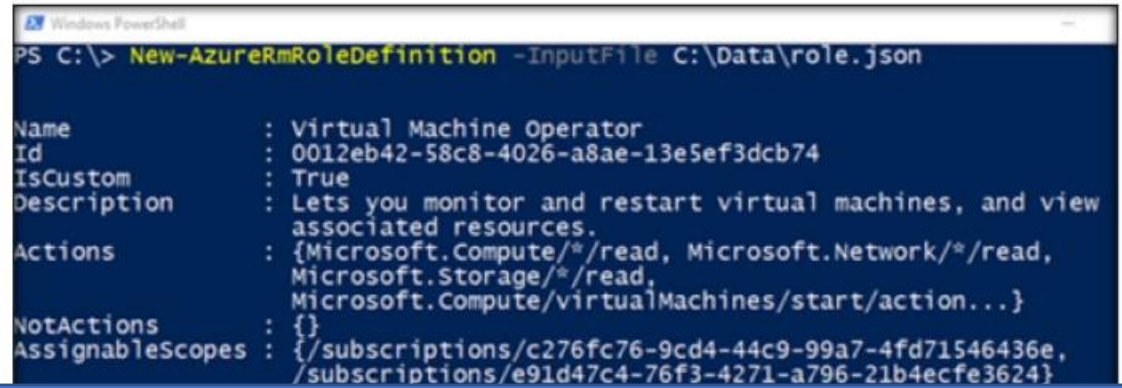
RBAC Scope and Access Inheritance



Creating a Custom Role

- Create custom "Roles" to allow or deny rights to Individuals or Groups
- Rights are "Hand Picked" from the Resource Providers
- Very Granular In Nature
- Created using PowerShell or AzureCLI





Auditing Role Assignment Changes

- Role assignment changes are captured in events where the ResourceProviderName is Microsoft.Authorization
- Azure Resource Manager provides the ability to restrict operations on resources through resource management locks
- Resource locks are policies which enforce a lock level at a particular scope