BAIT 3273 Cloud Computing

Week 12

Apply and monitor infrastructure standards with Azure Policy

Lesson Objectives:

- Apply policies to control and audit resource creation
- Learn how role-based security can calibrate access to your resources
- Understand Microsoft's policies and privacy guarantees
- Learn how to monitor your resources

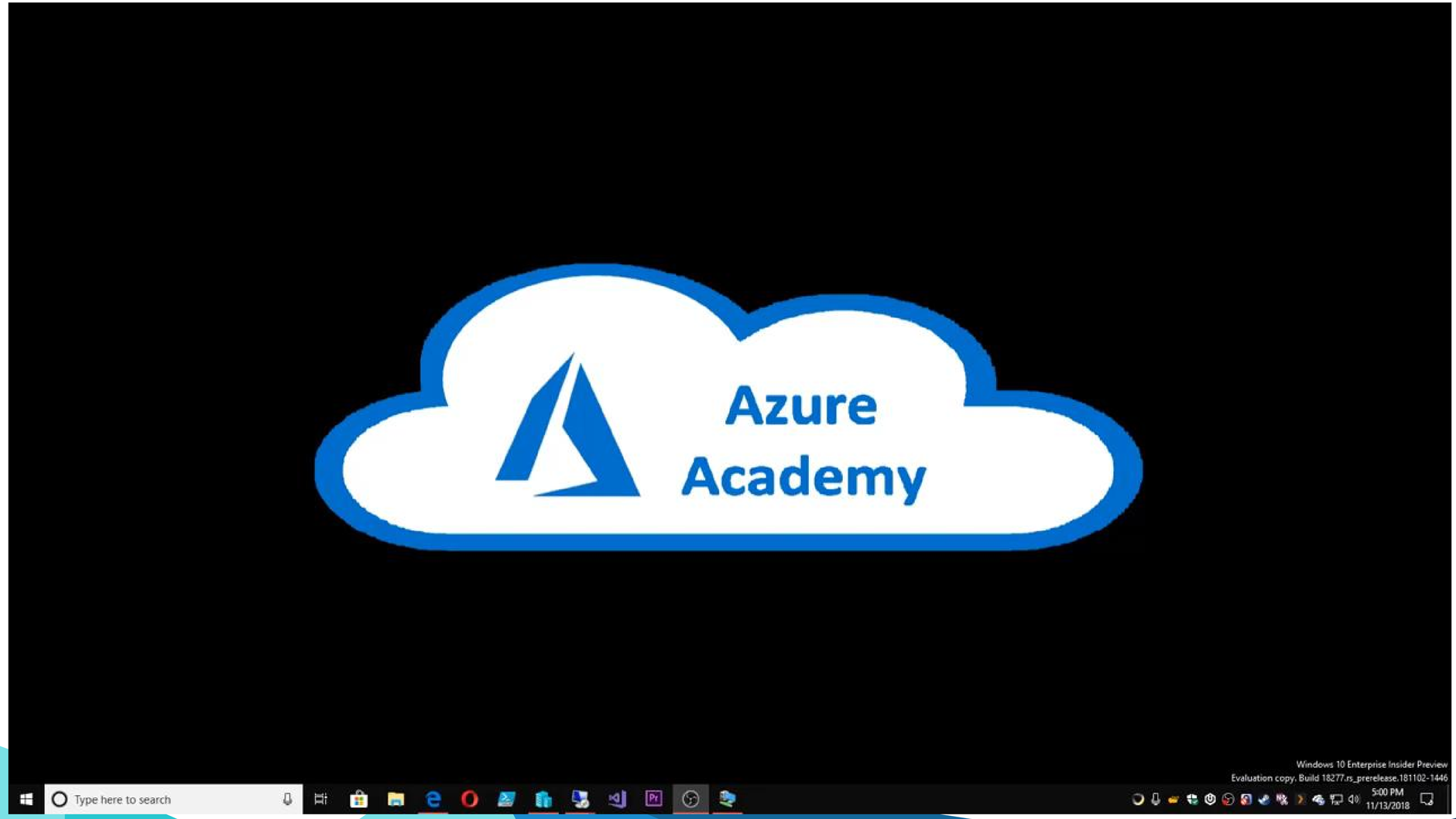
Introduction

Governance is important when:

- You have multiple engineering teams working in Azure
- You have multiple subscriptions in your tenant
- You have regulatory requirements that must be enforced
- You want to ensure standards are followed for all IT allocated resources

Azure provides several tools to enforce and validate the required standards. **Azure** also provides features to monitor resources utilization and performance.

Azure Governance



Define IT compliance with Azure Policy

Azure Policy

- An Azure service for creating, assigning, and managing policies.
- The policies enforce different rules upon the resources to ensure those resources stay compliant with the corporate standards and service level agreements.
- Azure Policy evaluates resources for noncompliance with assigned policies.

Azure Policy

[redacted]

Create a policy

Applying policy consists of following steps:

1. Create a policy definition
2. Assign a definition to a scope of resources
3. View policy evaluation results

What is a policy definition?

- A policy definition disclose on what to evaluate and what action to take.
  - E.g. Prevent the creation of a particular storage type
- The following table shows some common policy definitions that can be applied.

Policy definition	Description
Allowed Storage Account SKUs	This policy definition has a set of conditions/rules that determine whether a storage account that is being deployed is within a set of SKU sizes. Its effect is to deny all storage accounts that do not adhere to the set of defined SKU sizes.
Allowed Resource Type	This policy definition has a set of conditions/rules to specify the resource types that your organization can deploy. Its effect is to deny all resources that are not part of this defined list.
Allowed Locations	This policy enables you to restrict the locations that your organization can specify when deploying resources. Its effect is used to enforce your geographic compliance requirements.
Allowed Virtual Machine SKUs	This policy enables you to specify a set of VM SKUs that your organization can deploy.

Example of a Compute policy

JSON

Copy

```
{
  "if": {
    "allOf": [
      {
        "field": "type",
        "equals": "Microsoft.Compute/virtualMachines"
      },
      {
        "not": {
          "field": "Microsoft.Compute/virtualMachines/sku.name",
          "in": "[parameters('listOfAllowedSKUs')]"
        }
      }
    ]
  },
  "then": {
    "effect": "Deny"
  }
}
```

Apply an Azure policy

- To apply a policy, we can either use Azure portal or command-line tools by adding the 'Microsoft.PolicyInsights' extension.

PowerShell Copy

```powershell
# Register the resource provider if it's not already registered
Register-AzResourceProvider -ProviderNamespace 'Microsoft.PolicyInsights'
```

After registering the provider, a policy assignment can be created. For example:

PowerShell Copy

```powershell
# Get a reference to the resource group that will be the scope of the assignment
$rg = Get-AzResourceGroup -Name '<resourceGroupName>'

# Get a reference to the built-in policy definition that will be assigned
$definition = Get-AzPolicyDefinition | Where-Object { $_.Properties.DisplayName -eq 'Audit VMs that do not use

# Create the policy assignment with the built-in definition against your resource group
New-AzPolicyAssignment -Name 'audit-vm-manageddisks' -DisplayName 'Audit VMs without managed disks Assignment'
```

Azure Policy Demo

Govern your Azure environment

Use Azure Policy to enforce tags for resource creation

Pantelis Apostolidis
Solutions Architect @ Office Line SA
Microsoft Azure MVP

Microsoft Most Valuable Professional

Microsoft Certified Azure Solutions Architect Expert

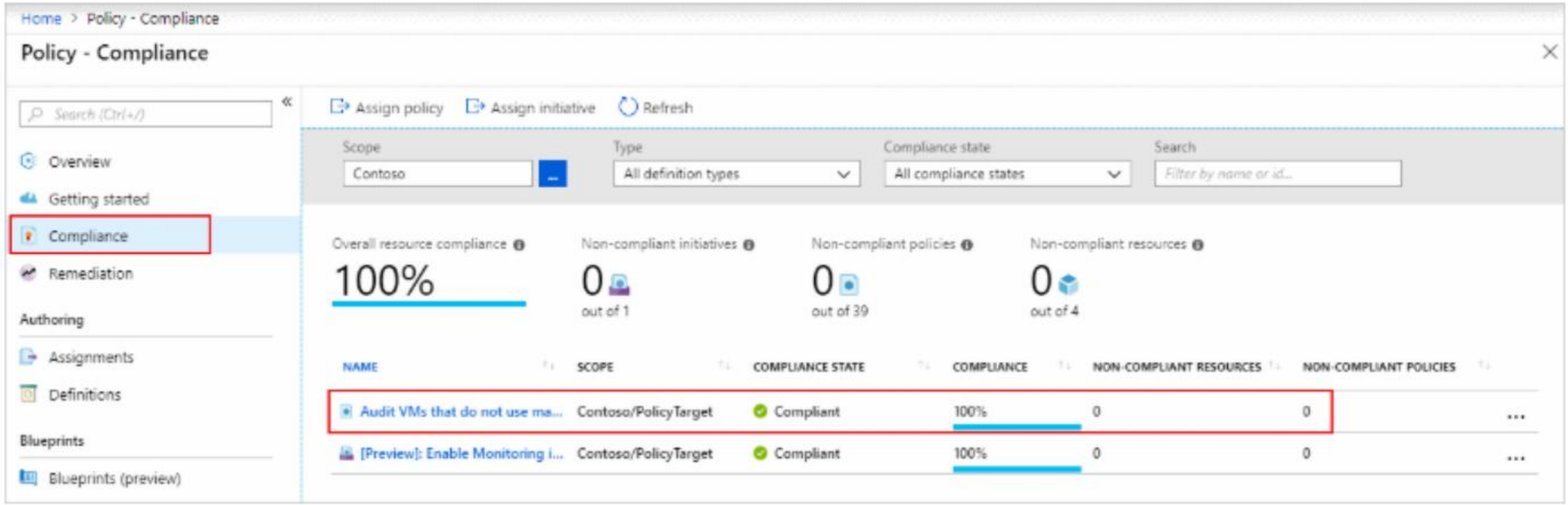
Microsoft 365 Certified Enterprise Administrator Expert

AzureHeads

autoexec.gr

Identify non-compliant resources

- Policy definition that is applied can be used to identify resources that aren't compliant with the policy via the Azure portal.



Identify non-compliant resources

- Command-line tools can also be used to identify non-compliant resource group instead of using the Azure portal. For example:

PowerShell

Copy

```
Get-AzPolicyState -ResourceGroupName $rg.ResourceGroupName -PolicyAssignmentName 'audit-vm-manageddisks' -Filt
```

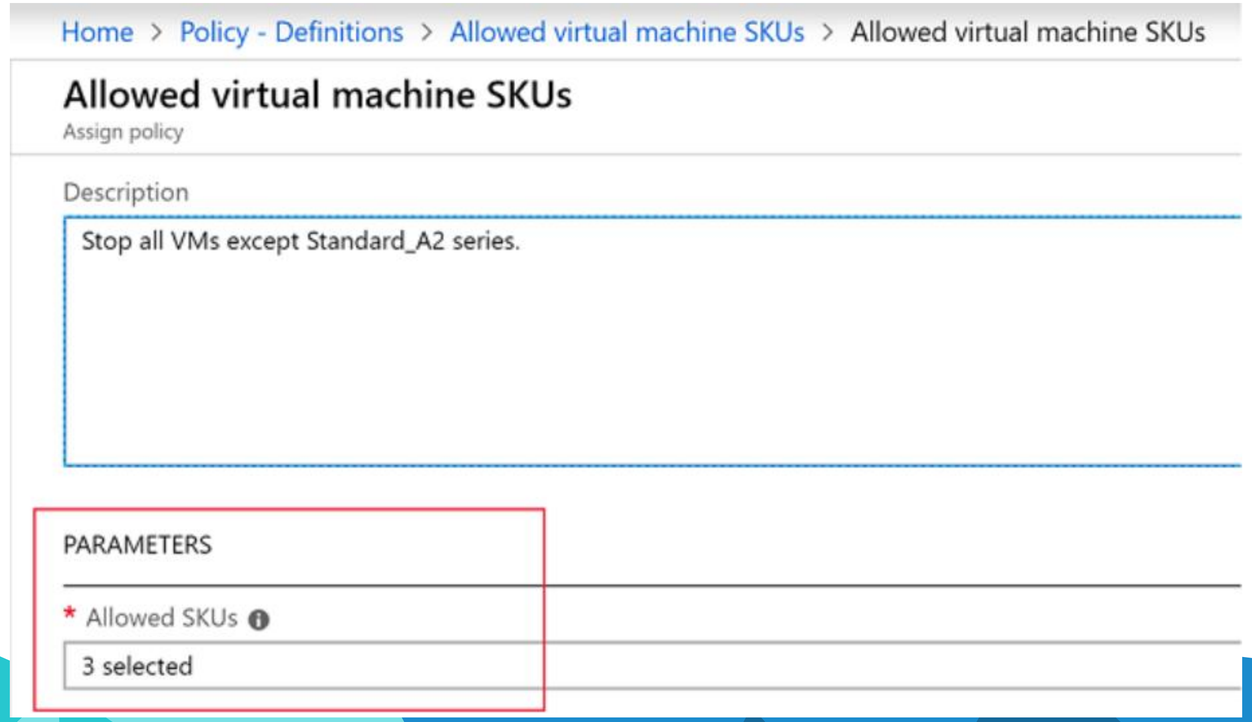
Output

Copy

```
Timestamp                   : 3/9/19 9:21:29 PM
ResourceId                  : /subscriptions/{subscriptionId}/resourcegroups/{resourceGroupName}/providers/Mic
PolicyAssignmentId          : /subscriptions/{subscriptionId}/providers/microsoft.authorization/policyassignme
PolicyDefinitionId          : /providers/Microsoft.Authorization/policyDefinitions/06a78e20-9358-41c9-923c-fb7
IsCompliant                 : False
SubscriptionId              : {subscriptionId}
ResourceType                : /Microsoft.Compute/virtualMachines
ResourceTags                : tbd
PolicyAssignmentName        : audit-vm-manageddisks
PolicyAssignmentOwner       : tbd
PolicyAssignmentScope       : /subscriptions/{subscriptionId}
PolicyDefinitionName        : 06a78e20-9358-41c9-923c-fb736d382a4d
PolicyDefinitionAction      : audit
PolicyDefinitionCategory    : Compute
ManagementGroupIds          : {managementGroupId}
```

Assign a definition to a scope of resources

- After each policy definition is created, they have to be assigned.
- A policy assignment is a policy definition that has been assigned to take place within a specific scope.
- The policies can be assigned through Azure portal or command-line tools.



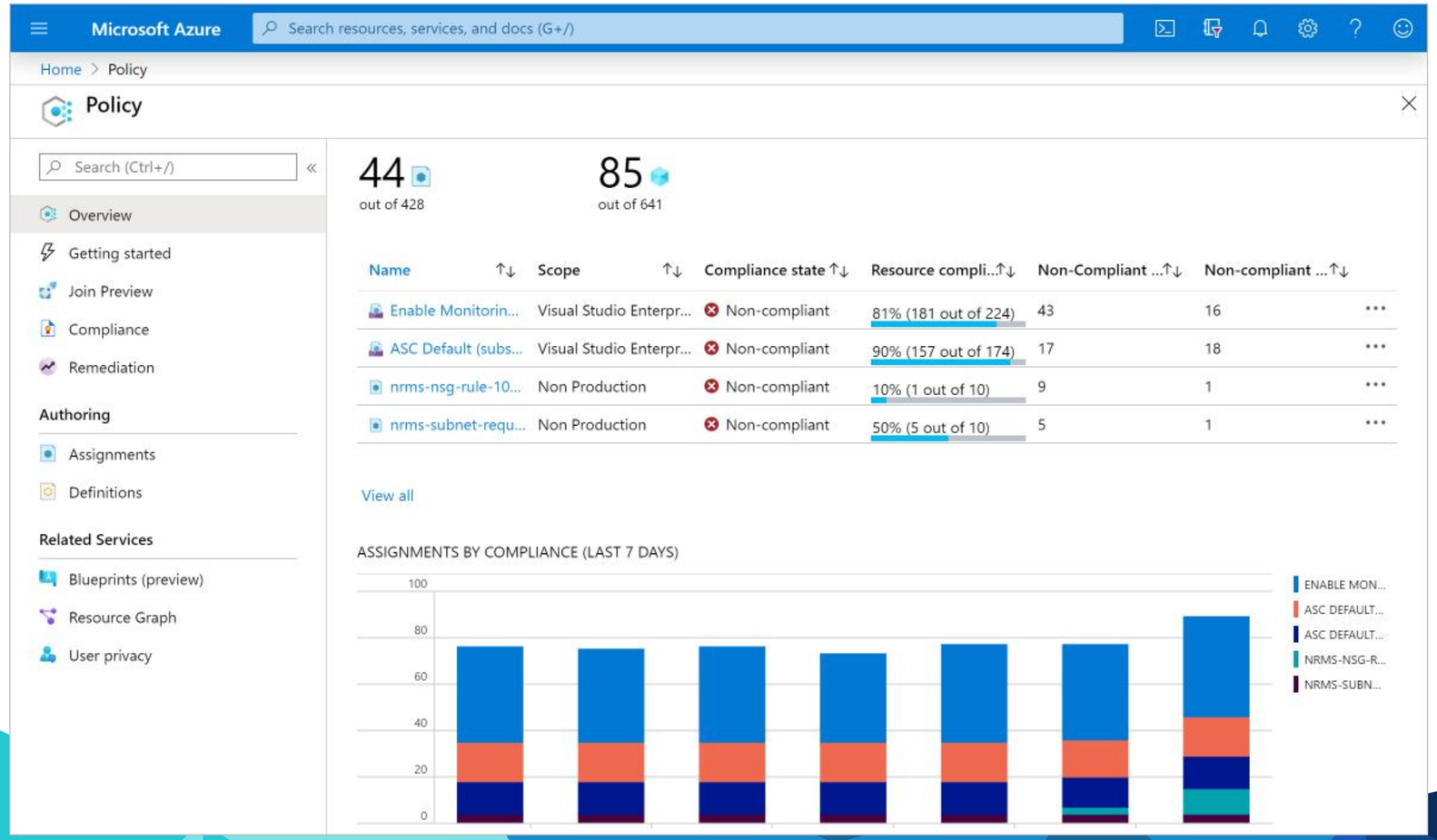
Policy effects

- Azure Policy will evaluate every request to create or update a resource.
- Each policy definition in Azure Policy is associated with an effect that determines what happens when the policy rule is matched.

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

View policy evaluation results

- Azure Policy can still allow a resource to be created even if it doesn't pass the validation.
- For situation like these, the result can be viewed through Azure Policy Portal



Azure Policy Compliance

Remove a policy assignment

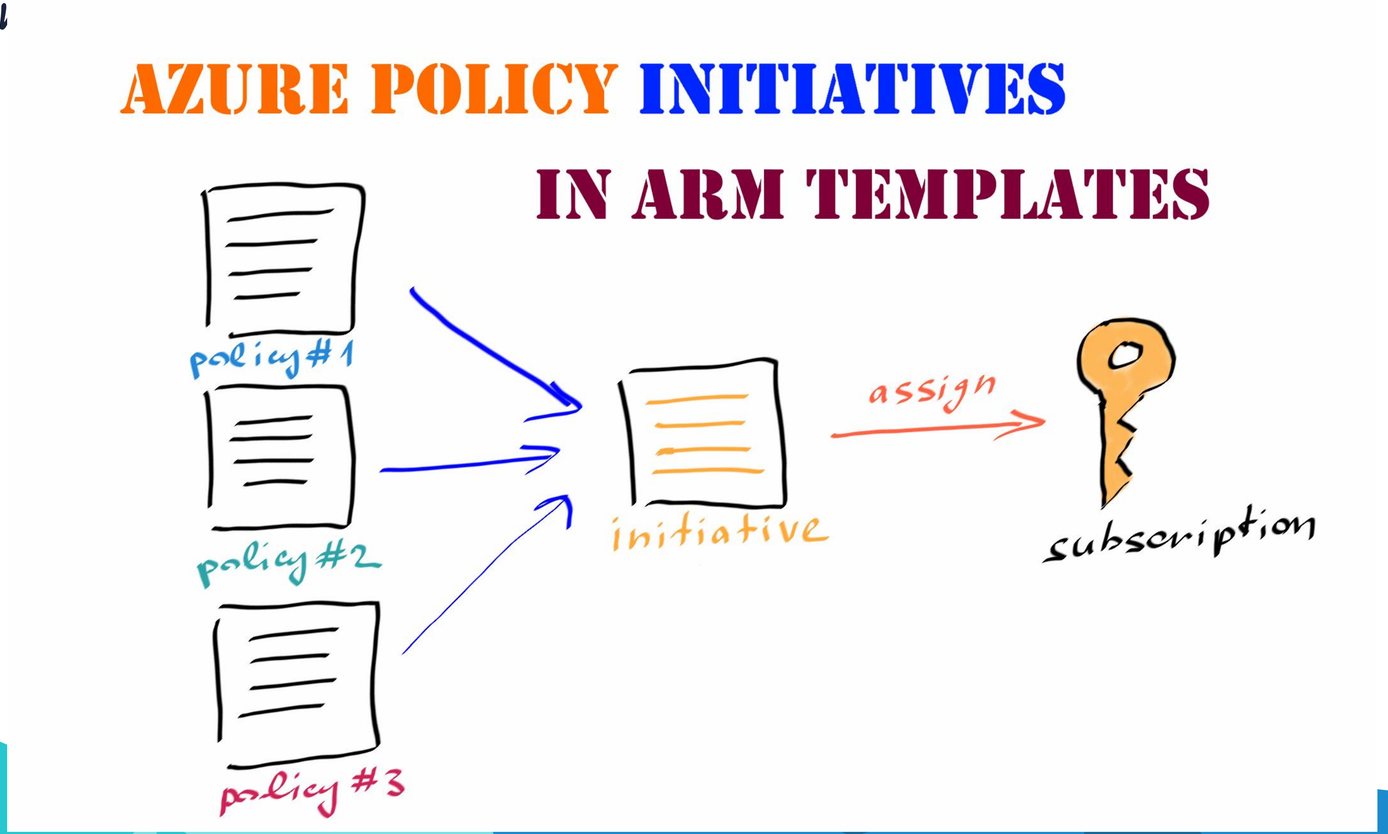
- When a policy is no longer required to be assigned, they can be removed through the Azure Portal or command-line tools as well. For example:

PowerShell Copy

```
Remove-AzPolicyAssignment -Name 'audit-vm-manageddisks' -Scope '/subscriptions/<subscriptionID>/resourceGroups
```

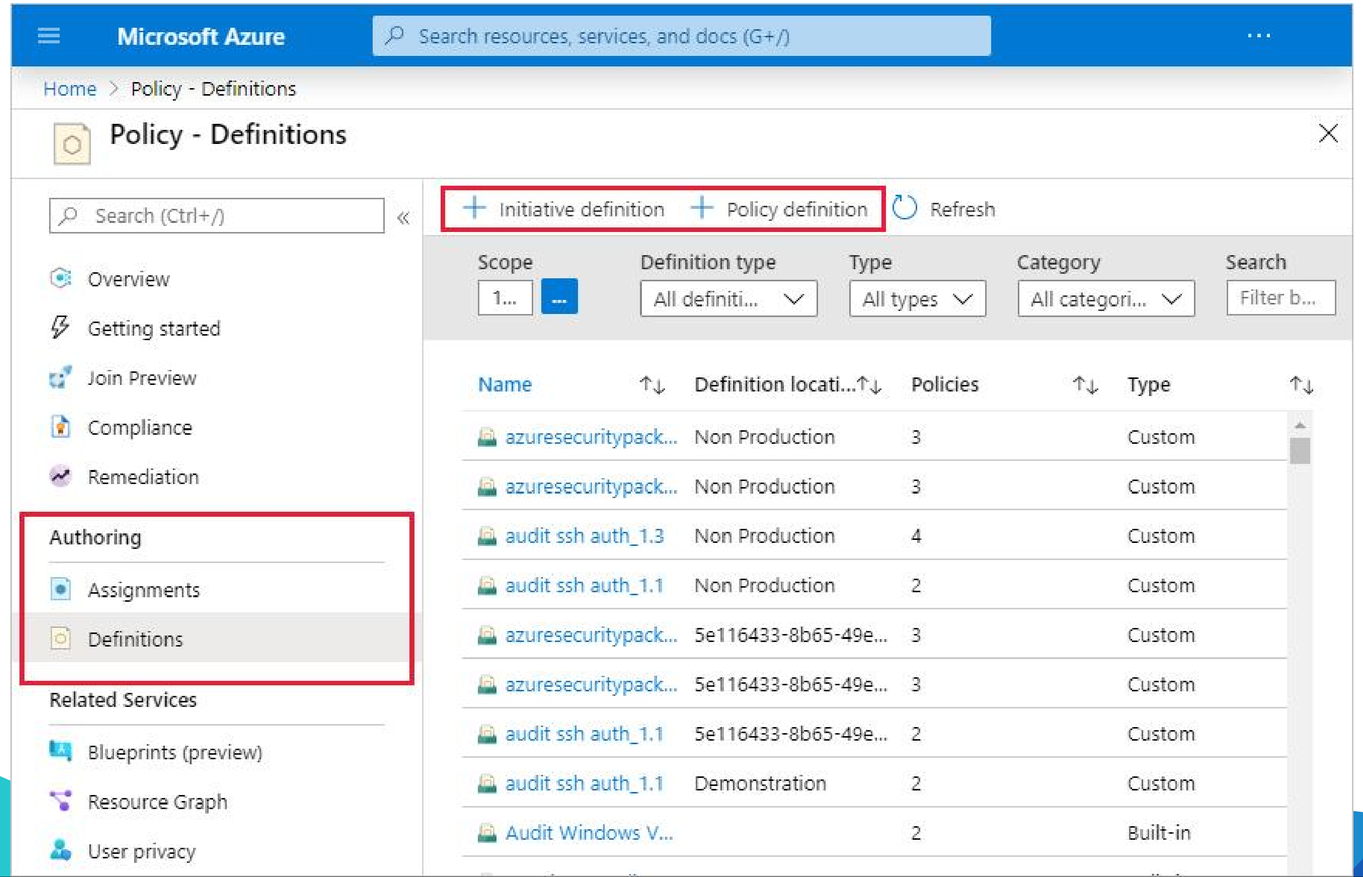
Organize policy with initiatives

- Initiatives work with policies in Azure Policy.
- Initiatives are used to manage and organize policies easily.
- Similar to how policy works, initiative involves definition and assignmen



Defining initiatives

- By defining initiatives, the process of managing and assigning policy definitions are simplified since the policies are grouped together.
- Initiatives can be defined through Azure Portal or command-line tools.



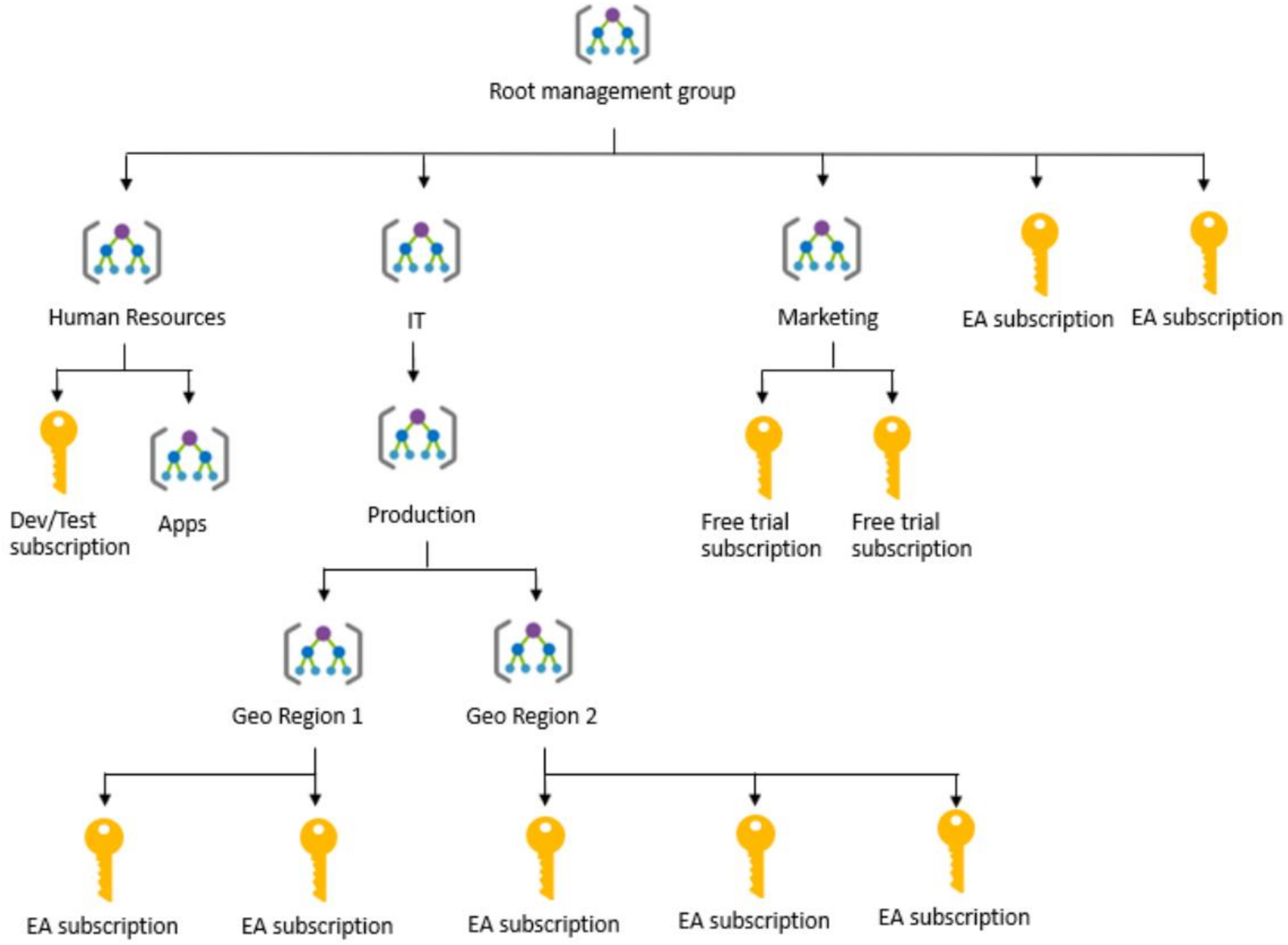
Understanding Initiatives

Enterprise governance management

- **Azure Management Groups** serve as containers for managing access, policies, and compliance across multiple Azure subscriptions.

- It allows organization to structure Azure resources into a hierarchy of collections where each subscription inherits the conditions applied to the management group that they are in.

Example of management



Azure Management Groups

Introducing Azure Management Groups

Make environment management easier by grouping subscriptions together

- Grouping subscriptions into logical groups allow for new organization models
- Inheritance allows for single assignment of controls that apply to all subscriptions
- Aggregated views above the subscription level

Create a hierarchy of management groups that fit your organization

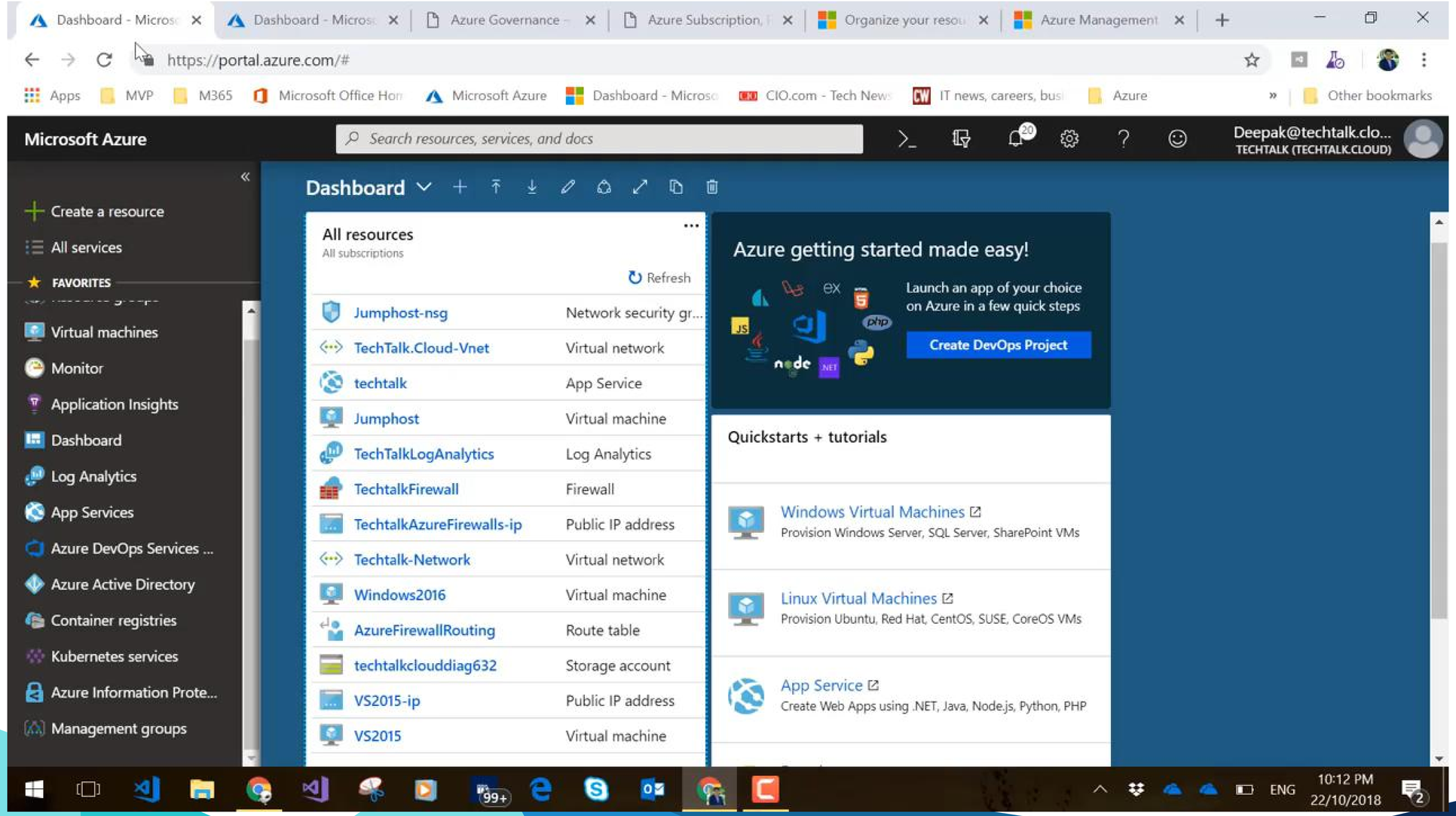
- Create a flexible hierarchy that can be updated quickly
- Hierarchy doesn't need to model the organizations billing hierarchy
- Can easily scale up or down depending on the organizational needs

Apply governance controls with policies and access controls along with other Azure services

- Azure Resource Manager (ARM) objects that allow integrations with other Azure services
- Azure services:
  - Azure Policy
  - RBAC
  - Azure Cost Management
  - Azure Blueprints
  - Azure Security Center

TALLAN

Azure Management Groups Demo



Thanks!