**Microsoft Azure Fundamentals: Azure RBAC & Azure Policy**

**Azure Role-based Access Control (RBAC)**

* Determines Azure resource management capabilities
* Delegates access control
* Roles are collections of related permissions
  + Built-in roles
  + Custom roles

**Built-in Azure RBAC Roles**

Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

KI-generierte Inhalte können fehlerhaft sein.

**RBAC Role Assignment**

* User
* Group
* Service principal
* Managed identity

**RBAC Assignment Scopes**

* Management group, subscription
* Resource group
* Individual resource

**RBAC Inherited Role Assignment**

**Ein Bild, das Text, Software, Screenshot, Computersymbol enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Custom Azure RBAC Role Creation**

Create custom JSON role file 🡪 Create custom role from file

* PowerShell: New-AzRoleDefinition
* CLI: az role defintion create

**Custom RBAC Role JSON Definition File**

**Ein Bild, das Text, Screenshot, Schrift enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Managing RBAC Using the Azure Portal**

Storage Account 🡪 sbdemo1103 🡪 Access Control (IAM)

**Managing RBAC Using the CLI**

$store = az storage account show -g sbdemo1103 -n sbdemo1103 | ConvertFrom-Json

$store

Cls

Az role definition list --scope $store.id

Az role assignment create --role „Storage Blob Data Reader“ --assignee [max.mustermann@gmail.com](mailto:max.mustermann@gmail.com) --scope $store.id

**Managing RBAC Using PowerShell**

$store = Get-AzStorageAccount -ResourceGroupName sbdemo1103 -Name sbdemo1103

$store

Cls

Get-AzRoleDefinition -Scope $store.id

New-AzRoleAssignment -RoleDefinitionName „Storage Blob Data Reader“ -SignInName [max.mustermann@gmail.com](mailto:max.mustermann@gmail.com) -Scope $store.id

**Creating a Custom RBAC Role**

Subscriptions 🡪 „Pay-As-You-Go“ 🡪 Access control (IAM) 🡪 Add (Custom Role)

Sbdemo1103 (storage account) 🡪 Access Control (IAM) 🡪 Add role assignment

**Managing Azure AD Roles**

Microsoft Entra ID

Default Directory 🡪 Roles and administrators

Default Directory 🡪 Users 🡪 Assigned roles 🡪 Add assignments

**Azure Policy**

* Cloud resource control (deployment, configuration, settings)
* Built-in and custom policies; more granular than RBAC

Ein Bild, das Text, Schrift, Screenshot enthält.

KI-generierte Inhalte können fehlerhaft sein.

Ein Bild, das Text, Screenshot, Visitenkarte, Diagramm enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Azure Policy Effects**

* Append
* Audit
* AuditIfNotExist
* DeployIfNotExists
* Deny
* Modify

**Azure Policy Initiatives**

* Policies are organized into a „group“ (initiative)
* The policy „group“ gets assigned to a scope
* Example:
  + Harden regional Azure resources
  + Ensure VM disk encryption is enabled
  + Ensure endpoint protection is enabled

**Azure Policy Management**

Portal

Command line interface(CLI)

PowerShell

**Assigning Azure Policies Using the Portal**

Policy 🡪 Assignments 🡪Assign Policy

**Assigning Azure Policies Using the CLI**

$subscriptionId = az account show --query „id“ --output tsv

$subscriptionId

Cls

$policy = az policy definition list --query „[?displayName==“Inherit a tag from the resource group if missing“]“ | ConvertFrom-Json

$policy

Cls

Az policy assignment create --name „sbdemo110“ --display-name „Assign Tag Inheritance Policy“ --scope /subscription/$subscriptionId --policy $policy.name --params „{\“tagName\“:{\“value\“:\“environment\“}}“ --mis-system-assigned --location eastus

**Assigning Azure Policies Using PowerShell**

$subscription = Get-AzContex

$subscriptionId = $subscription.Subscript.Id

$subscriptionId

Cls

$policy = Get-AzPolicyDefinition | Where-Object { $\_.Properties.DiplayName -eq „inherit a tag from the resource group if missing“ }

$policy

Cls

New-AzPolicyAssignment -Name „sbdemo1111“ -DisplayName „Assign Inheritance Policy for Tags“ -Scope /subsription/$subscriptionId -PolicyDefinition $policy -IdentityType SystemAssigned --Location EastUS

Tagname: environment

**Creating and Assigning a Custom Policy**

Policy 🡪 Definitions 🡪 Policy definition

Policy 🡪 Definitions 🡪 Assing

**Managing Policy Initiatives**

Policy 🡪 Definitions 🡪 Initiative definitions

**Using Azure Service Trust Portal**

Documentation of microsoft implementations