Azure: Role-Base Access Control Architecture Diagram

Scenario

You have been asked to create a proof of concept showing how Azure users and groups are created. Also, how role-based access control is used to assign roles to groups. Specifically, you need to:

Create a Senior Admins group containing the user account of Joseph Price as its member.

Create a Junior Admins group containing the user account of Isabel Garcia as its member.

Create a Service Desk group containing the user account of Dylan Williams as its member.

Assign the Virtual Machine Contributor role to the Service Desk group.

A screenshot of a computer

Description automatically generated

**Objective 1**: Create the Senior Admins group with the user account Joseph Price as its member.

Task 1: Use the Azure portal to create a user account for Joseph Price.

* Start a browser session and sign-in to the Azure portal https://portal.azure.com/.
* On the Overview blade of the Microsoft Entra ID tenant, in the Manage section, select Users, and then select + New user.
* On the New User blade, ensure that the Create user option is selected, and specify the following settings:

Setting Value

User name: Joseph

Name: Joseph Price

* Ensure that the Auto-generate password is selected, select the Show password checkbox to identify the automatically generated password. You would need to provide this password, along with the user name to Joseph.
* Click Create.

**Task2: Use the Azure portal to create a Senior Admins group and add the user account of Joseph Price to the group. And configure it as the group owner.**

* In the Azure portal, navigate back to the blade displaying your Microsoft Entra ID tenant.
* In the Manage section, click Groups, and then select + New group.
* On the New Group blade, specify the following settings (leave others with their default values):

Setting Value

Group type: Security

Group name: Senior Admins

Membership type: Assigned

* Click the No owners selected link, on the Add owners blade, select Joseph Price, and click Select.
* Click the No members selected link, on the Add members blade, select Joseph Price, and click Select.
* Back on the New Group blade, click Create.

**Result:** Used the Azure Portal to create a user, a group, and assigned the user to the group.

A white background with text

Description automatically generated with medium confidence

**Objective 2: Create a Junior Admins group containing the user account of Isabel Garcia as its member.**

**Task 1: Use PowerShell to create a user account for Isabel Garcia.**

* Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select PowerShell and Create storage.
* In the PowerShell session within the Cloud Shell pane, run the following to create a password profile object:

**$passwordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile**

* In the PowerShell session within the Cloud Shell pane, run the following to set the value of the password within the profile object:

**$passwordProfile.Password = "Pa55w.rd1234"**

* In the PowerShell session within the Cloud Shell pane, run the following to connect to Microsoft Entra ID:

**Connect-AzureAD**

* In the PowerShell session within the Cloud Shell pane, run the following to identify the name of your Microsoft Entra tenant:

**$domainName = ((Get-AzureAdTenantDetail).VerifiedDomains)[0].Name**

A screen shot of a computer screen

Description automatically generated

* In the PowerShell session within the Cloud Shell pane, run the following to create a user account for Isabel Garcia:

**New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true -MailNickName 'Isabel'**

* In the PowerShell session within the Cloud Shell pane, run the following to list Microsoft Entra ID users (the accounts of Joseph and Isabel should appear on the listed):

**Get-AzureADUser**

A blue screen with white text

Description automatically generated

**Task2: Use PowerShell to create the Junior Admins group and add the user account of Isabel Garcia to the group by using PowerShell.**

* In the same PowerShell session within the Cloud Shell pane, run the following to create a new security group named Junior Admins:

**New-AzureADGroup -DisplayName 'Junior Admins' -MailEnabled $false -SecurityEnabled $true -MailNickName JuniorAdmins**

* In the PowerShell session within the Cloud Shell pane, run the following to list the groups in your Microsoft Entra tenant (the list should include the Senior Admins and Junior Admins groups):

**Get-AzureADGroup**

A blue screen with text

Description automatically generated

* In the PowerShell session within the Cloud Shell pane, run the following to obtain a reference to the user account of Isabel Garcia:

**$user = Get-AzureADUser -Filter "MailNickName eq 'Isabel'"**

* In the PowerShell session within the Cloud Shell pane, run the following to add the user account of Isabel to the Junior Admins group:

**Add-AzADGroupMember -MemberUserPrincipalName $user.userPrincipalName -TargetGroupDisplayName "Junior Admins"**

* In the PowerShell session within the Cloud Shell pane, run the following to verify that the Junior Admins group contains the user account of Isabel:

**Get-AzADGroupMember -GroupDisplayName "Junior Admins"**

**Result:** Used PowerShell to create a user and a group account, and added the user account to the group account.

A screen shot of a computer code

Description automatically generated

A white background with text

Description automatically generated with medium confidence

**Objective 3**: **Create a Service Desk group containing the user account of Dylan Williams as its member. Using Bash on the CLI.**

**Task 1: Use Azure CLI to create a user account for Dylan Williams.**

* In the drop-down menu in the upper-left corner of the Cloud Shell pane, select Bash, and, when prompted, click Confirm.
* In the Bash session within the Cloud Shell pane, run the following to identify the name of Microsoft Entra tenant:

**DOMAINNAME=$(az ad signed-in-user show --query 'userPrincipalName' | cut -d '@' -f 2 | sed 's/\"//')**

* In the Bash session within the Cloud Shell pane, run the following to create a user, Dylan Williams. Use *yourdomain*.

**az ad user create --display-name "Dylan Williams" --password "Pa55w.rd1234" --user-principal-name Dylan@$DOMAINNAME**

A screenshot of a computer

Description automatically generated

* In the Bash session within the Cloud Shell pane, run the following to list Microsoft Entra ID user accounts (the list should include user accounts of Joseph, Isabel, and Dylan)

**az ad user list --output table**

A computer screen with white text

Description automatically generated

**Task 2: Use Azure CLI to create the Service Desk group and add the user account of Dylan to the group.**

* In this task, create the Service Desk group and assign Dylan to the group.
* In the same Bash session within the Cloud Shell pane, run the following to create a new security group named Service Desk.

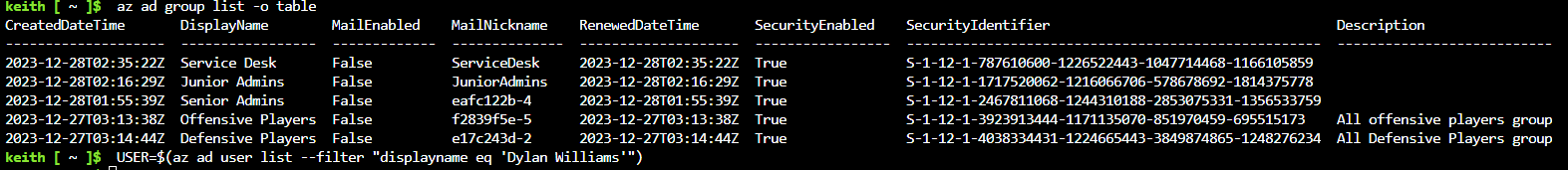
**az ad group create --display-name "Service Desk" --mail-nickname "ServiceDesk"**

A screenshot of a computer screen

Description automatically generated

* In the Bash session within the Cloud Shell pane, run the following to list the Microsoft Entra ID groups (the list should include Service Desk, Senior Admins, and Junior Admins groups):

**az ad group list -o table**



* In the Bash session within the Cloud Shell pane, run the following to obtain a reference to the user account of Dylan Williams:

**USER=$(az ad user list --filter "displayname eq 'Dylan Williams'")**

* In the Bash session within the Cloud Shell pane, run the following to obtain the objectId property of the user account of Dylan Williams:

**OBJECTID=$(echo $USER | jq '.[].id' | tr -d '"')**

* In the Bash session within the Cloud Shell pane, run the following to add the user account of Dylan to the Service Desk group:

**az ad group member add --group "Service Desk" --member-id $OBJECTID**

* In the Bash session within the Cloud Shell pane, run the following to list members of the Service Desk group and verify that it includes the user account of Dylan:

**az ad group member list --group "Service Desk"**

**Result:** Using Azure CLI a user and a group accounts were created, and added the user account to the group.

A computer screen shot of a group of code

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Objective 4: Assign the Virtual Machine Contributor role to the Service Desk group.**

**Task 1: Create a resource group**

* In the Azure portal, in the Search text box at the top of the Azure portal page, type Resource groups and press the Enter key.
* On the Resource groups blade, click + Create and specify the following settings:

Setting Value

Subscription name: the name of your Azure subscription

Resource group name: AZ500Lab01

Location: East US

Click Review + create and then Create.

**Task 2: Assign the Service Desk Virtual Machine Contributor permissions.**

* On the Resource groups blade, click the AZ500LAB01 resource group entry.
* On the AZ500Lab01 blade, click Access control (IAM) in the middle pane.
* On the AZ500Lab01 | Access control (IAM) blade, click + Add and then, in the drop-down menu, click Add role assignment.
* On the Add role assignment blade, specify the following settings and click Next after each step:

Setting Value

Role in the search tab: Virtual Machine Contributor

Assign access to (Under Members Pane) User, group, or service principal

Select (+Select Members): Service Desk

* Click Review + assign twice to create the role assignment.
* From the Access control (IAM) blade, select Role assignments.
* On the AZ500Lab01 | Access control (IAM) blade, on the Check access tab, in the Search by name or email address text box, type Dylan Williams.
* In the list of search results, select the user account of Dylan Williams and, on the Dylan Williams assignments - AZ500Lab01 blade, view the newly created assignment.

A screenshot of a computer

Description automatically generated

* Repeat the same last two steps to check access for Joseph Price.

A screenshot of a computer

Description automatically generated

**Delete resources from the CLI:**

* In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal.
* In the drop-down menu in the upper-left corner of the Cloud Shell pane, select PowerShell, and, when prompted, click Confirm.
* In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

**Remove-AzResourceGroup -Name "AZ500LAB01" -Force -AsJob**

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated