Practical exam AZ-104 part 1

This exam is composed by two parts:

1º Role-Based Access Control (6 points over 10)

2º Azure policy (4 points over 10)

All parts are independent of each other and will be scored independently.

**Remarks:**

It is important that you take **screenshots** during each process of solving the exercises, as well as **commenting** on what you are doing at all times, differentiating your comments from the exam statement using the **Spanish** language and a different color or a marker.

You are allowed to access information on the Internet or **your** own class notes. But any attempt to communicate with a classmate or external person, if detected, implies failing the exam with a 0 and the risk of being dropped from the master's degree.

Before starting the exam, each student will have to create in their server account, in the AZ-104 folder, a new folder with the name "Examen P1". You will place a copy of the exam document (“Examen Práctico 1 AZ-104.docx”) in this folder, rename it as “Surname1 Surname2, Names” and it will be the document you will use to take the exam from the very beginning.

During the entire time of the exam, the student will make a video of the full screen of their computer. This recording can be requested at any time after the exam and must be kept by the student for 2 weeks after the exam. After two weeks it can be deleted.

When it is time to finish the exam, students will be prompted to save the document and close it. Attach the file in the exam task.

First Part: Role-Based Access Control

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.

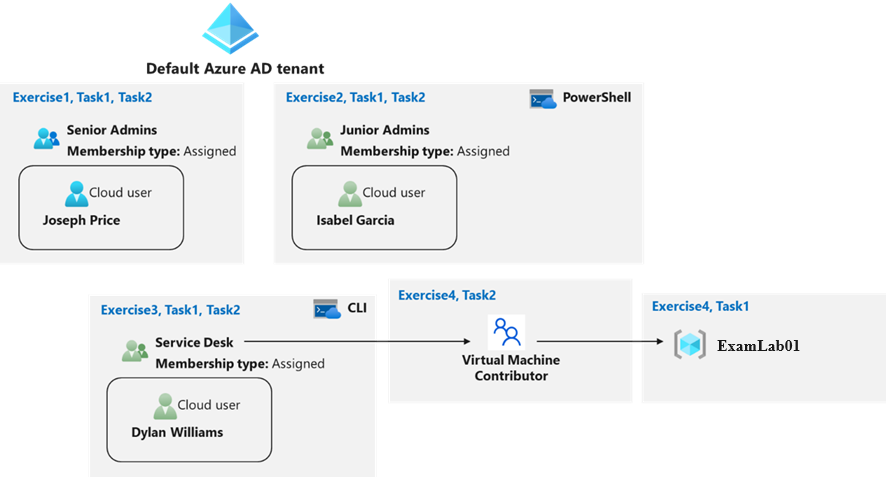
For all the resources in this lab, we are using the **East US** region. Verify with your instructor this is the region to use for class.

Objectives

In this exercise, you will complete the following exercises:

* Exercise 1: Create the Senior Admins group with the user account Joseph Price as its member (the Azure portal).
* Exercise 2: Create the Junior Admins group with the user account Isabel Garcia as its member (PowerShell).
* Exercise 3: Create the Service Desk group with the user Dylan Williams as its member (Azure CLI).
* Exercise 4: Assign the Virtual Machine Contributor role to the Service Desk group.

Role-Based Access Control architecture diagram



Instructions

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

Estimated timing: 20 minutes.

In this exercise, you will complete the following tasks:

* Task 1: Use the Azure portal to create a user account for Joseph Price.
* Task 2: Use the Azure portal to create a Senior Admins group and add the user account of Joseph Price to the group.

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

In this task, you will create a user account for Joseph Price.

1. Start a browser session and sign-in to the Azure portal **https://portal.azure.com/**.

**Note**: Sign into the Azure portal using an account that has the Owner or Contributor role in the Azure subscription you are using for this lab and the Global Administrator role in the Azure AD tenant associated with that subscription.

1. In the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Microsoft Entra ID** and press the **Enter** key.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. On the **Overview** blade of the Azure Active Directory tenant, in the **Manage** section, select **Users**, and then select **+ New user**.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

1. On the **New User** blade, ensure that the **Create new user** option is selected, and specify the following settings:

| Setting | Value |
| --- | --- |
| User principal name | **Joseph** |
| Mail nickname | **Joseph** |
| Display name | **Joseph Price** |
| Password | **Scooby123456** |

1. Ensure that the **Auto-generate password** is not selected and the **Account enabled** is selected.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Click **Create**.

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

1. Refresh the **Users | All users** blade to verify the new user was created in your Azure AD tenant.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Task2: Use the Azure portal to create a Senior Admins group and add the user account of Joseph Price to the group.

In this task, you will create the *Senior Admins* group, add the user account of Joseph Price to the group, and configure it as the group owner.

1. In the Azure portal, navigate back to the blade displaying your Azure Active Directory tenant.
2. In the **Manage** section, click **Groups**, and then select **+ New group**.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. 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** |

Imagen que contiene Aplicación

Descripción generada automáticamente

1. Click the **No owners selected** link, on the **Add owners** blade, select **Joseph Price**, and click **Select**.
2. Click the **No members selected** link, on the **Add members** blade, select **Joseph Price**, and click **Select**.

Diagrama

Descripción generada automáticamente

1. Back on the **New Group** blade, click **Create**.

Result: You used the Azure Portal to create a user and a group and assigned the user to the group.

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

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

Estimated timing: 20 minutes.

In this exercise, you will complete the following tasks:

* Task 1: Use PowerShell to create a user account for Isabel Garcia.
* Task 2: Use PowerShell to create the Junior Admins group and add the user account of Isabel Garcia to the group.

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

In this task, you will create a user account for Isabel Garcia by using PowerShell.

1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select **PowerShell** and **Create storage**.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente Interfaz de usuario gráfica, Texto, Aplicación

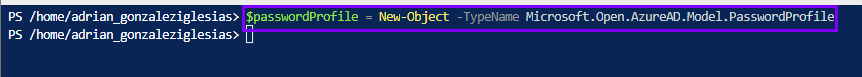
Descripción generada automáticamente

1. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.

**Note**: To paste copied text into the Cloud Shell, right-click within the pane window and select **Paste**. Alternatively, you can use the **Shift+Insert** key combination.

1. 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



1. 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 = "Scooby123456"

Imagen que contiene Patrón de fondo

Descripción generada automáticamente

1. In the PowerShell session within the Cloud Shell pane, run the following to connect to Azure Active Directory:

Connect-AzureAD

Texto

Descripción generada automáticamente

1. In the PowerShell session within the Cloud Shell pane, run the following to identify the name of your Azure AD tenant:

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



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

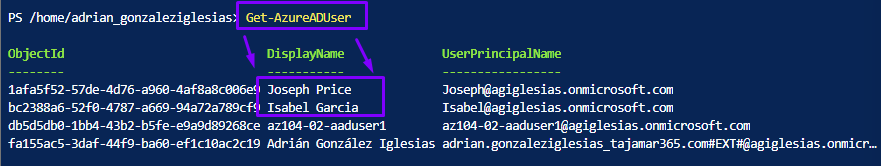
New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true -MailNickName 'Isabel'

Captura de pantalla con letras

Descripción generada automáticamente

1. In the PowerShell session within the Cloud Shell pane, run the following to list Azure AD users (the accounts of Joseph and Isabel should appear on the listed):

Get-AzureADUser



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

In this task, you will create the Junior Admins group and add the user account of Isabel Garcia to the group by using PowerShell.

1. 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

1. In the PowerShell session within the Cloud Shell pane, run the following to list the groups in your Azure AD tenant (the list should include the Senior Admins and Junior Admins groups):

Get-AzureADGroup

Texto

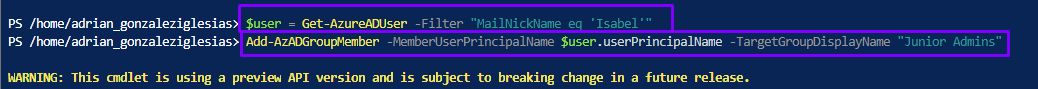
Descripción generada automáticamente

1. 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'"

1. 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"



1. 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: You used PowerShell to create a user and a group account and added the user account to the group account.

Interfaz de usuario gráfica, Texto, Sitio web

Descripción generada automáticamente

Exercise 3: Create a Service Desk group containing the user account of Dylan Williams as its member.

Estimated timing: 20 minutes.

In this exercise, you will complete the following tasks:

* Task 1: Use Azure CLI to create a user account for Dylan Williams.
* Task 2: Use Azure CLI to create the Service Desk group and add the user account of Dylan to the group.

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

In this task, you will create a user account for Dylan Williams.

1. In the drop-down menu in the upper-left corner of the Cloud Shell pane, select **Bash**, and, when prompted, click **Confirm**.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. In the Bash session within the Cloud Shell pane, run the following to identify the name of your Azure AD tenant:

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



1. 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 "Scooby123456" --user-principal-name Dylan@$DOMAINNAME

Captura de pantalla de computadora

Descripción generada automáticamente

1. In the Bash session within the Cloud Shell pane, run the following to list Azure AD user accounts (the list should include user accounts of Joseph, Isabel, and Dylan)

az ad user list --output table

Captura de pantalla de un celular

Descripción generada automáticamente

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

In this task, you will create the Service Desk group and assign Dylan to the group.

1. In the same Bash session within the Cloud Shell pane, run the following to create a new security group named Service Desk.

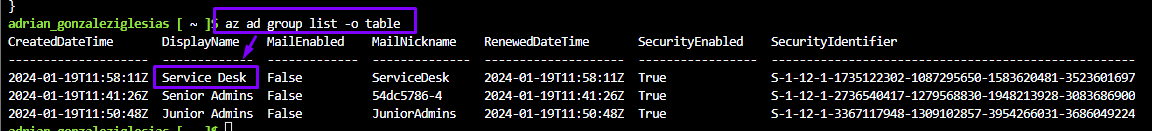
az ad group create --display-name "Service Desk" --mail-nickname "ServiceDesk"

Captura de pantalla de un celular

Descripción generada automáticamente

1. In the Bash session within the Cloud Shell pane, run the following to list the Azure AD groups (the list should include Service Desk, Senior Admins, and Junior Admins groups):

az ad group list -o table



1. 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'")

1. 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 '"')

1. 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



1. 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"

Texto

Descripción generada automáticamente

1. Close the Cloud Shell pane.

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

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

Estimated timing: 20 minutes.

In this exercise, you will complete the following tasks:

* Task 1: Create a resource group.
* Task 2: Assign the Service Desk Virtual Machine Contributor permissions to the resource group.

Task 1: Create a resource group

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

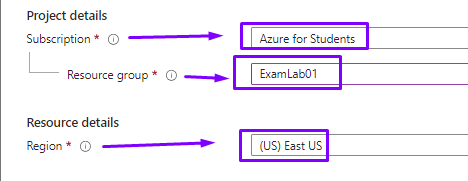
| Setting | Value |
| --- | --- |
| Subscription name | the name of your Azure subscription |
| Resource group name | **ExamLab01** |
| Location | **East US** |

Interfaz de usuario gráfica

Descripción generada automáticamente

Diagrama

Descripción generada automáticamente



1. Click **Review + create** and then **Create**.

**Note**: Wait for the resource group to deploy. Use the **Notification** icon (top right) to track progress of the deployment status.

Imagen que contiene Gráfico de líneas

Descripción generada automáticamente

1. Back on the **Resource groups** blade, refresh the page and verify your new resource group appears in the list of resource groups.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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

1. On the **Resource groups** blade, click the **ExamLab01** resource group entry.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. On the **ExamLab01** blade, click **Access control (IAM)** in the middle pane.
2. On the **ExamLab01 | Access control (IAM)** blade, click **+ Add** and then, in the drop-down menu, click **Add role assignment**.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente con confianza media

| 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** |

1. On the **Add role assignment** blade, specify the following settings and click **Next** after each step:

Diagrama

Descripción generada automáticamente

1. Click **Review + assign** twice to create the role assignment.

Diagrama

Descripción generada automáticamente con confianza baja

1. From the **Access control (IAM)** blade, select **Role assignments**.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

1. On the **ExamLab01 | Access control (IAM)** blade, on the **Check access** tab, in the **Search by name or email address** text box, type **Dylan Williams**.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente con confianza media

1. In the list of search results, select the user account of Dylan Williams and, on the **Dylan Williams assignments - ExamLab01** blade, view the newly created assignment.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Close the **Dylan Williams assignments - ExamLab01** blade.
2. Repeat the same last two steps to check access for **Joseph Price**.

Result: You have assigned and checked RBAC permissions.

Interfaz de usuario gráfica, Texto, Aplicación, Teams

Descripción generada automáticamente

**Clean up resources.**

Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs.

1. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal.
2. In the drop-down menu in the upper-left corner of the Cloud Shell pane, select **PowerShell**, and, when prompted, click **Confirm**.
3. 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 "ExamLab01" -Force -AsJob

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

1. Close the **Cloud Shell** pane.

Second: Azure Policy

Scenario

You have been asked to create a proof of concept showing how Azure policy can be used. Specifically, you need to:

* Create an Allowed Locations policy that ensures resource are only created in a specific region.
* Test to ensure resources are only created in the Allowed location

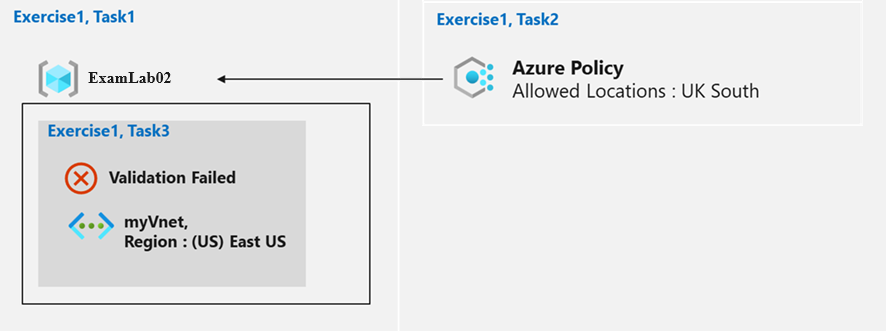
For all the resources in this lab, we are using the **East US** region. Verify with your instructor this is the region to use for class.

Objectives

In this exercise, you will complete the following:

* Exercise 1: Implement Azure Policy.

Azure Policy diagram



Instructions

Exercise 1: Implement Azure Policy

Estimated timing: 40 minutes.

In this exercise, you will complete the following tasks:

* Task 1: Create an Azure resource group.
* Task 2: Create an Allowed Locations policy assignment.
* Task 3: Verify the Allowed Locations policy assignment is working.

Task 1: Create a resource group for the lab.

In this task, you will create a resource group for the lab.

1. Sign-in to the Azure portal **https://portal.azure.com/**.

**Note**: Sign into the Azure portal using an account that has the Owner or Contributor role in the Azure subscription you are using for this lab.

1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select **PowerShell** and **Create storage**.
2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. In the PowerShell session within the Cloud Shell pane, run the following to create a resource group (verify with your instructor regarding the value of the location parameter):

New-AzResourceGroup -Name ExamLab02 -Location 'East US'

Confirm

Provided resource group already exists. Are you sure you want to update it?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Interfaz de usuario gráfica, Texto, Correo electrónico

Descripción generada automáticamente

1. In the PowerShell session within the Cloud Shell pane, type **Y** and press the Enter key.
2. In the PowerShell session within the Cloud Shell pane, run the following to list resource groups to verify that the new resource group was created:

Get-AzResourceGroup | format-table

Texto

Descripción generada automáticamente

1. Close the **Cloud Shell**.

Task 2: Create an Allowed Locations policy assignment.

In this task, you will create an Allowed Locations policy assignment and specify which Azure regions the policy can use.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Policy** and press the **Enter** key.
2. On the **Policy** blade, in the **Authoring** section, select **Definitions**.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente Diagrama

Descripción generada automáticamente

1. Take a minute to browse the built-in definitions. Use the **Category** drop-down to filter the list of policies.
2. In the **Search** text box, type **Allowed locations**.

**Note**: The **Allowed locations** policy allows you to restrict location of resources, not resource groups. To restrict locations of resource groups, you can use the **Allowed locations for resource groups** policy.

1. Click the **Allowed locations** policy definition to display its details.

**Note**: This policy definition takes an array of locations as parameters. A policy rule is an ‘if-then’ statement. The ‘if’ clause checks if the resource location is included in the parameter list, and if not, the ‘then’ clause denies the resource creation or, for existing resources, marks them as non-compliant.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. On the **Allowed locations** blade, click **Assign**.

Interfaz de usuario gráfica

Descripción generada automáticamente

1. On the **Basics** tab of the **Allowed locations** blade, click the Ellipsis (…) button next to the **Scope** text box and, on the **Scope** blade, specify the following settings:

| Setting | Value |
| --- | --- |
| Subscription | the name of you Azure subscription |
| Resource group | **ExamLab02** |

1. Click **Select**.

Imagen que contiene Aplicación

Descripción generada automáticamente Interfaz de usuario gráfica

Descripción generada automáticamente

1. On the **Allowed locations** blade, on the **Basics** tab, specify the following settings (leave others with their default values):

| Setting | Value |
| --- | --- |
| Assignment name | **Allow UK South for ExamLab02** |
| Description | **Allow resources to be created in UK South Only for ExamLab02** |
| Policy enforcement | **Enabled** |

1. Click **Next**.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente con confianza media

1. On the **Parameters** tab of the **Allowed locations** blade, in the **Allowed locations** drop-down list, select **UK South** as the only allowed location.

**Note**: You can select more than one location. If the policy required a different set of parameters, this tab would provide those selections.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Click **Review + create**, followed by **Create** to create the policy assignment.

**Note**: You will see a notification that the assignment was successful, and that the assignment might take around 30 minutes to complete.

**Note**: The reason the Azure policy assignment might take up to 30 minutes to take effect is that is has to replicate globally. Typically, this takes only a few minutes. If the next task fails, simply wait a few minutes and attempt its steps again.

Texto

Descripción generada automáticamente

Task 3: Test the Allowed Locations policy assignment

In this task, you will test the Allowed Locations policy assignment.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Virtual networks** and press the **Enter** key.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. On the **Virtual Networks** blade, click **+ Create**.

**Note**: First, you will try to create a virtual network in East US. Since this is not an allowed location, the request should be blocked.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente con confianza media

1. On the **Basics** tab of the **Create virtual network** blade, specify the following settings (leave others with their defualt values):

| Setting | Value |
| --- | --- |
| Resource group | **ExamLab02** |
| Name | **myVnet** |
| Region | **East US** |

Teams

Descripción generada automáticamente

1. Click **Review + create**.

Diagrama

Descripción generada automáticamente con confianza media

1. On the **Review + create** tab of the **Create virtual network** blade note the **Validation failed** message.

**Note**: If the **Validation Failed** warning does not appear, click **Previous** and wait a few more minutes.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. On the **Basics** tab, click the error message link to open the **Policy Assignment** blade. You will see the policy assignment that restricts the location.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Close the **Policy Assignment** blade, on the **Create virtual network** blade, click the **Basics** tab, and, in the **Region** drop-down list, select **UK South**.

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

1. Click **Review + create**, verify that validation passed, click **Create**, and verify that the virtual network was created successfully.

Exercise results: In this exercise, you learned to apply an Azure policy by selecting a built-in policy definitions and assigning it to a resource group.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Clean up resources.**

Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs.

1. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **Reconnect**.
2. 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 "ExamLab02" -Force -AsJob

Captura de pantalla de un celular

Descripción generada automáticamente

Sitio web

Descripción generada automáticamente

1. Close the **Cloud Shell** pane.
2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Policy** and press the **Enter** key.
3. In the Authoring section, select **Assignments**.
4. In the list of assignments, select the name of the **Allowed Locations** policy that you created in this lab.
5. On the policy assignment, select **Delete assignment**, and then select **Yes**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente