

 tajamar.	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	

Administración de la gobernanza mediante Azure Policy

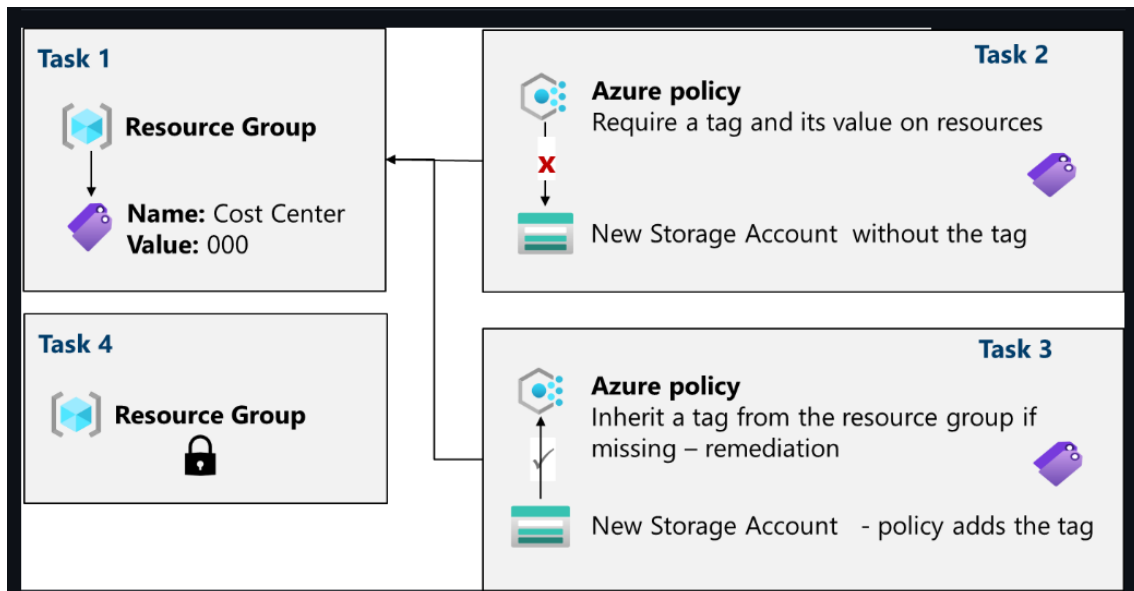
	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	


Contenido

Esquema del laboratorio	3
Asignar etiquetas a través de Azure Portal	4
Exigir tags mediante una instancia de Azure Policy	5
Aplicar tags a través de una instancia de Azure Policy	10
Configurar y probar los locs en recursos.	14

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	

Esquema del laboratorio



	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	

Asignar etiquetas a través de Azure Portal

Home > Resource Manager | Resource groups >

Create a resource group ...

Basics **Tags** Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Subscription * ⓘ Azure for Students ▼

Resource group name * ⓘ az104-rg2


Region * ⓘ (US) East US ▼

Home > Resource Manager | Resource groups >


Create a resource group ...

Basics **Tags** Review + create

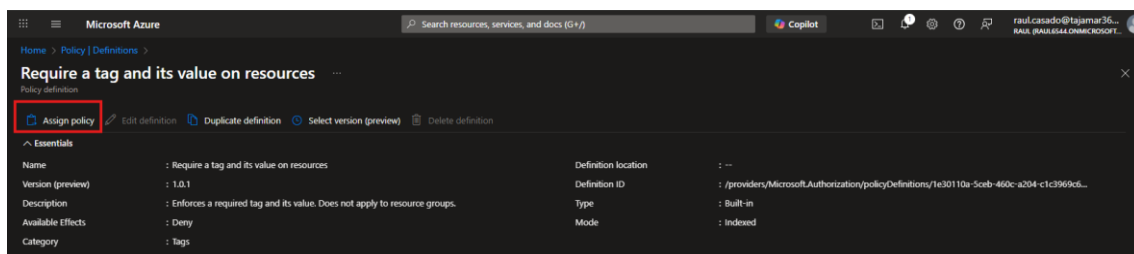
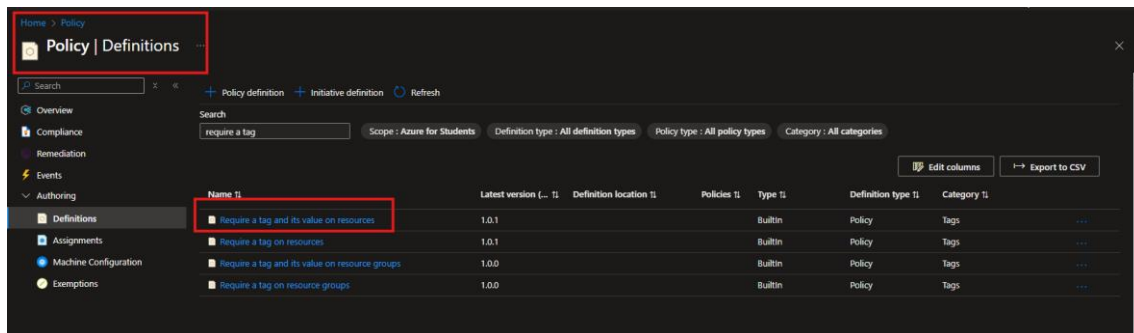
Apply tags to your Azure resources to logically organize them by categories. A tag consists of a key (name) and a value. Tag names are case-insensitive and tag values are case-sensitive. [Learn more](#)

Name	Value	Resource
Cost Center ▼	: 000 ▼	Resource group 
▼	: ▼	Resource group

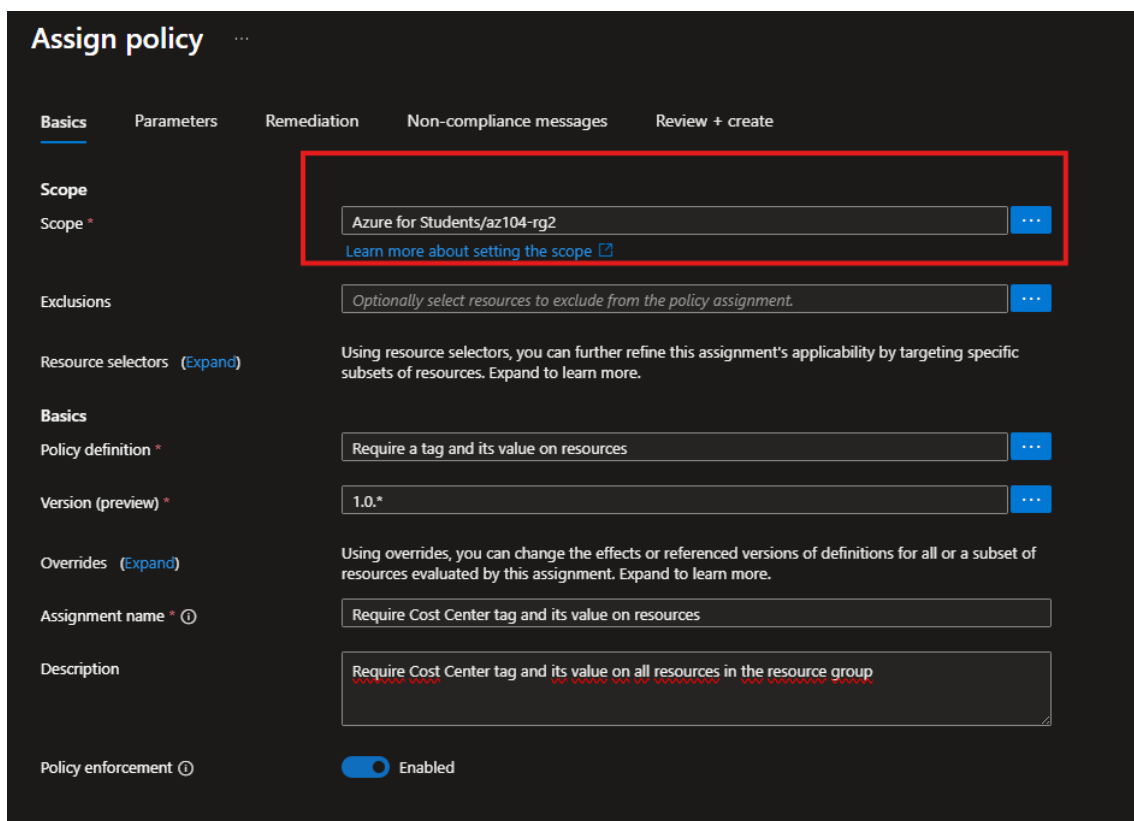
Creamos un nuevo grupo de recursos llamado az104-rg2, dentro de la pestaña Tags, creamos un tag y se lo asignamos al grupo de recursos.


	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	

Exigir tags mediante una instancia de Azure Policy

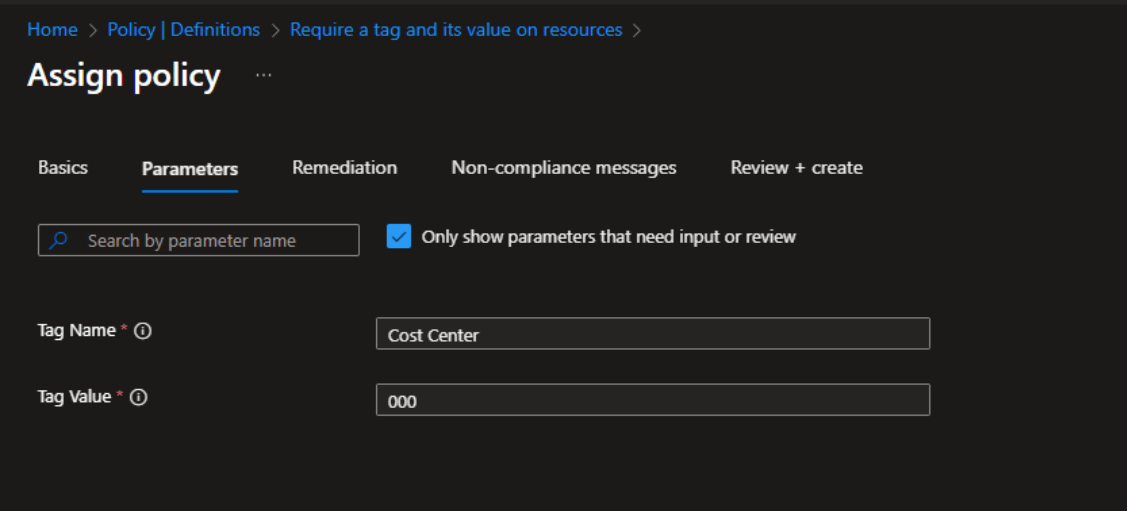


Dentro de la pestaña policy, filtramos por la política que queremos aplicar, clickamos en ella y asignamos la política a la suscripción o grupo de recursos que queremos que se aplique.



	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	

Definimos sobre que suscripción y el grupo de recursos donde se va a aplicar la política.



Home > Policy | Definitions > Require a tag and its value on resources >

Assign policy ...

Basics **Parameters** Remediation Non-compliance messages Review + create

☒ Only show parameters that need input or review

Tag Name * ⓘ

Tag Value * ⓘ


Configuramos la política para requerir que todos los recursos tengan:

Tag Name (Nombre de etiqueta): Cost Center

Tag Value (Valor de la etiqueta): 000

Si el recurso NO tiene esta etiqueta o tiene un valor diferente:

- Puede **bloquear** la creación/modificación del recurso (modo Deny)
- Puede **marcar** el recurso como no conforme (modo Audit)
- Puede **agregar automáticamente** la etiqueta (modo Modify/Append)

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	

Home > Policy | Definitions > Require a tag and its value on resources >

Assign policy ...

Basics Parameters Remediation Non-compliance messages Review + create

Basics

Scope	Azure for Students/az104-rg2
Exclusions	--
Policy definition	Require a tag and its value on resources
Assignment name	Require Cost Center tag and its value on resources
Version (preview)	1.0.*
Description	Require Cost Center tag and its value on all resources in the resource group
Policy enforcement	Default
Assigned by	Raúl Casado San Andrés

Advanced

Resource selectors	No selectors associated with this assignment.
Overrides	No overrides associated with this assignment.

Parameters

Tag Name	Cost Center
Tag Value	000


Remediation

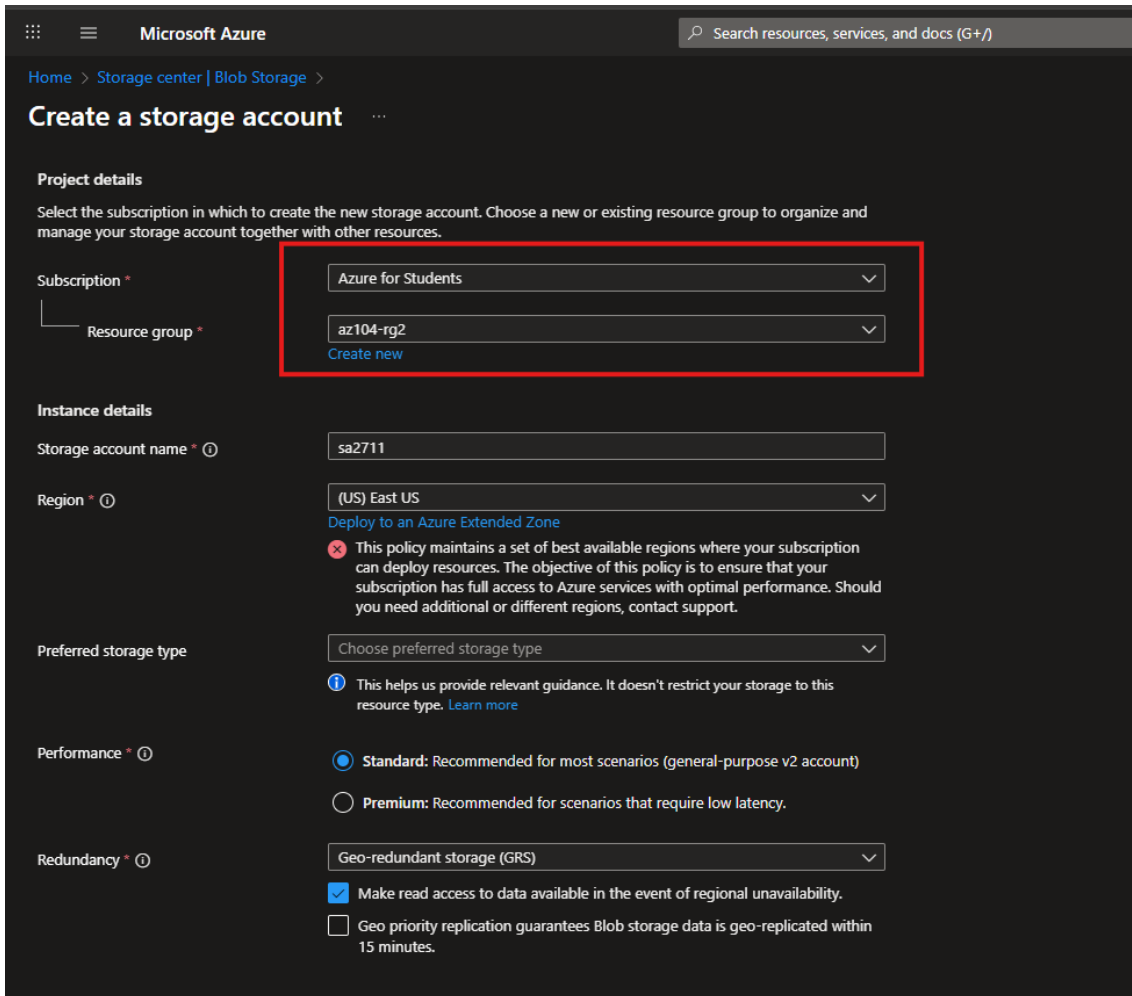
Create a Managed Identity	No managed identity associated with this assignment.
---------------------------	--

Non-compliance messages

Non-compliance messages	No non-compliance messages associated with this assignment.
-------------------------	---

Resumen de la política que hemos creado.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	



Microsoft Azure

Search resources, services, and docs (G+)

Home > Storage center | Blob Storage >

Create a storage account

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.


Subscription * ▼ Azure for Students

Resource group * ▼ az104-rg2
[Create new](#)


Instance details

Storage account name * ⓘ sa2711

Region * ⓘ (US) East US ▼
[Deploy to an Azure Extended Zone](#)

 This policy maintains a set of best available regions where your subscription can deploy resources. The objective of this policy is to ensure that your subscription has full access to Azure services with optimal performance. Should you need additional or different regions, contact support.

Preferred storage type ▼ Choose preferred storage type

 This helps us provide relevant guidance. It doesn't restrict your storage to this resource type. [Learn more](#)

Performance * ⓘ

☒ **Standard:** Recommended for most scenarios (general-purpose v2 account)


☐ **Premium:** Recommended for scenarios that require low latency.

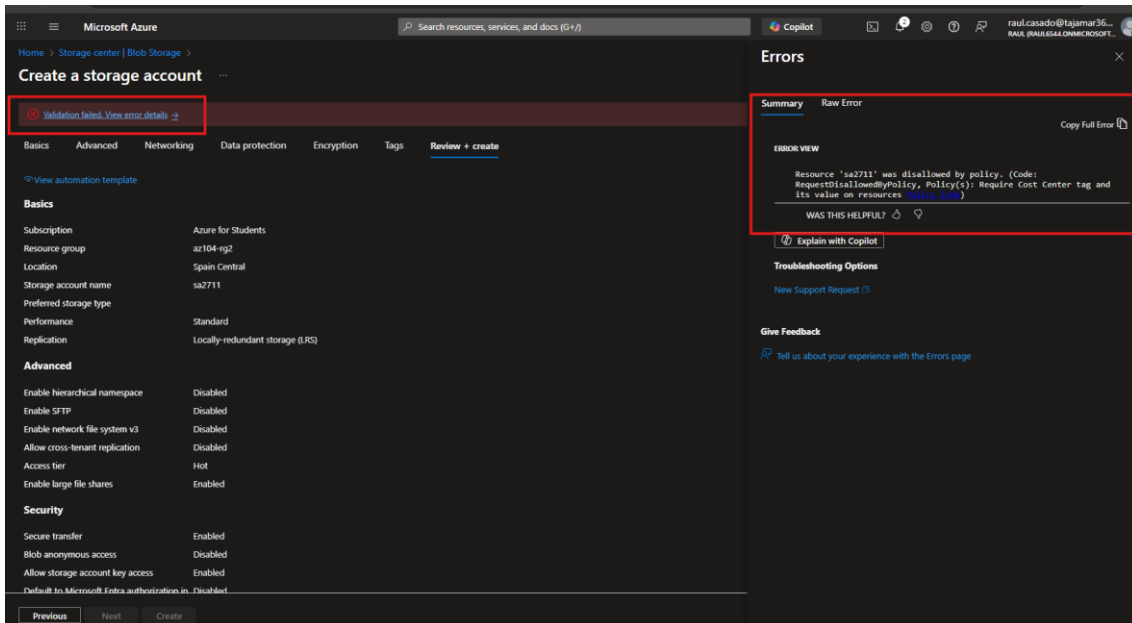
Redundancy * ⓘ ▼ Geo-redundant storage (GRS)

☒ Make read access to data available in the event of regional unavailability.

☐ Geo priority replication guarantees Blob storage data is geo-replicated within 15 minutes.

Creamos una cuenta de almacenamiento dentro del grupo de recursos en el que hemos aplicado la política.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	



The screenshot shows the Microsoft Azure portal interface. On the left, the 'Create a storage account' wizard is in the 'Review + create' step. A red box highlights a validation error message: 'Validation failed. View error details →'. The error details panel on the right shows the following message:


```

ERROR VIEW
Resource 'sa2711' was disallowed by policy. (Code: RequestDisallowedByPolicy, Policy(s): Require Cost Center tag and its value on resources: https://aka.ms/reqcc)
WAS THIS HELPFUL?
Explain with Copilot
Troubleshooting Options
New Support Request
Give Feedback
Tell us about your experience with the Errors page

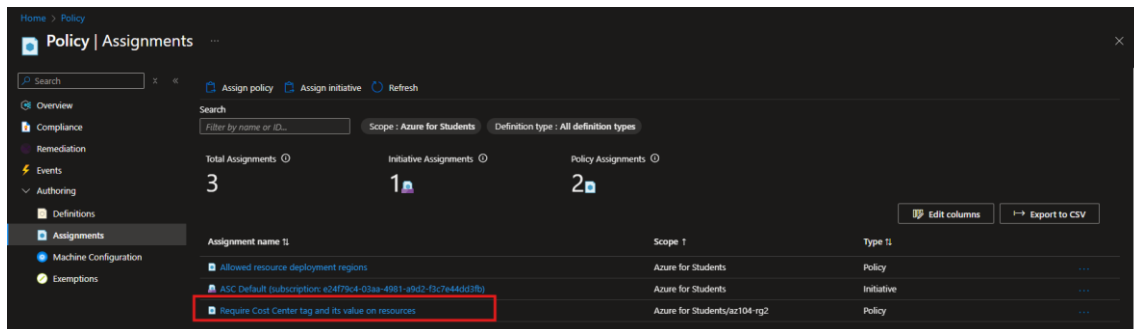
```

The error message indicates that the resource 'sa2711' was disallowed by policy because it does not have the required 'Cost Center' tag. The policy is 'Require Cost Center tag and its value on resources'.

Al momento de crear la cuenta de almacenamiento, como no le hemos aplicado ningún tag al momento de su configuración nos da un error, que no cumple con las políticas para este grupo de recursos.

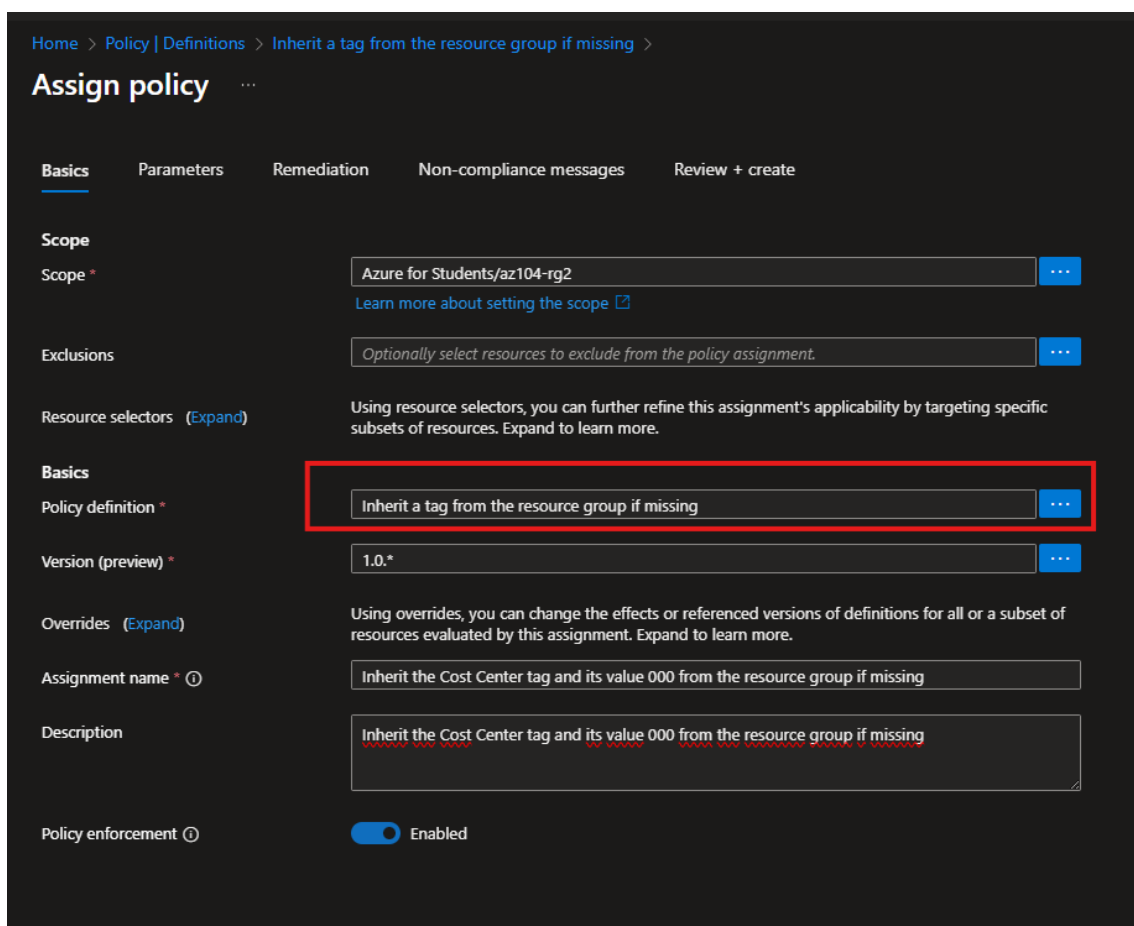
	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	

Aplicar tags a través de una instancia de Azure Policy




Dentro de policy | assignments encontramos todas las políticas que están activas.

Vamos a quitar la que hemos creado anteriormente.



Creamos una nueva política aplicada al grupo de recursos az104-rg2, este caso trata de una política para que los recursos que se creen hereden el tag del grupo de recursos si les falta.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	

Home > Policy | Definitions > Inherit a tag from the resource group if missing >

Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Search by parameter name ☒ Only show parameters that need input or review

Tag Name * ⓘ

Home > Policy | Definitions > Inherit a tag from the resource group if missing >

Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task after the policy is assigned. For deployIfNotExists policies, the remediation task will deploy the specified template. For modify policies, the remediation task will edit tags on the existing resources.

☒ Create a remediation task

Policy to remediate

Managed Identity
Policies with the deployIfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, choose between an existing user assigned managed identity or creating a system assigned managed identity. [Learn more about Managed Identity.](#)


Create a Managed Identity ⓘ ☒

Type of Managed Identity ⓘ ☒ System assigned managed identity ☐ User assigned managed identity

System assigned identity location

Permissions
This identity will also be given the following permissions:

ⓘ Role assignments (permissions) are created based on the role definitions specified in the policies.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	

Configuramos la política para que se aplique.

Home > Storage center | Blob Storage >

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * Azure for Students

Resource group * az104-rg2 [Create new](#)

Instance details

Storage account name * sa2711

Region * (Europe) Spain Central [Deploy to an Azure Extended Zone](#)

Preferred storage type Choose preferred storage type


i This helps us provide relevant guidance. It doesn't restrict your storage to this resource type. [Learn more](#)

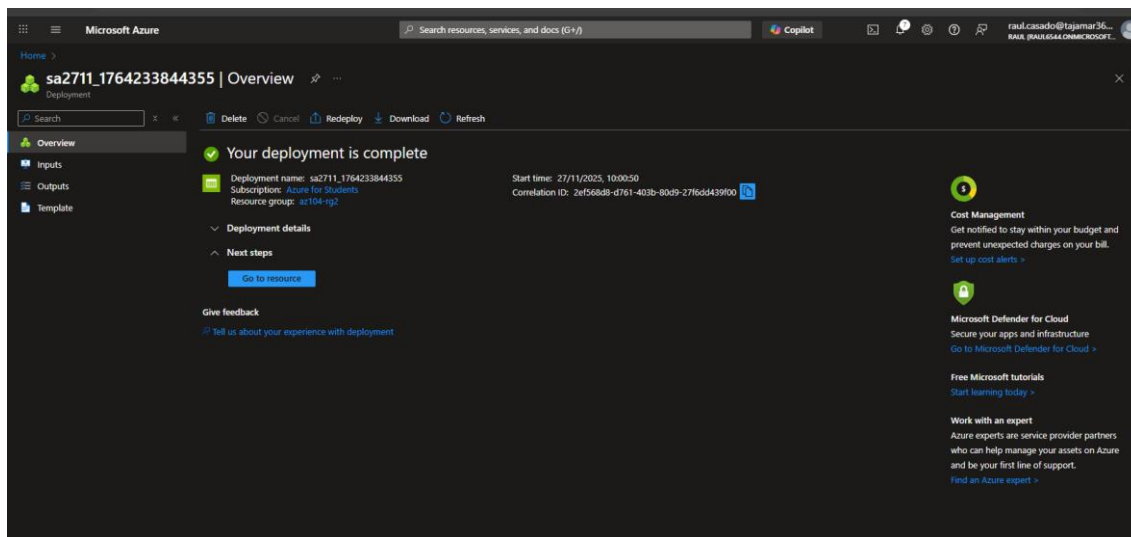
Performance * ☒ Standard: Recommended for most scenarios (general-purpose v2 account) ☐ Premium: Recommended for scenarios that require low latency.

Redundancy * Locally-redundant storage (LRS)

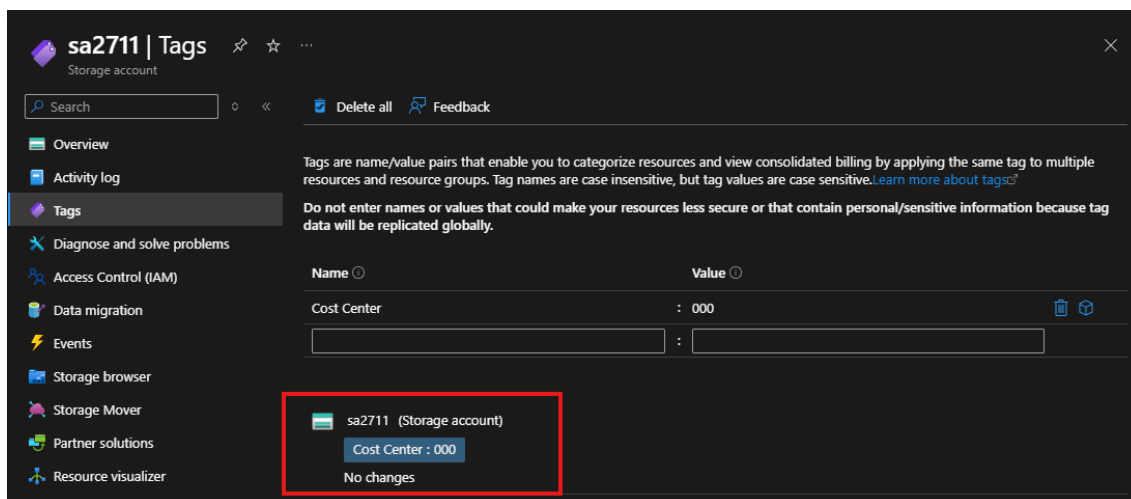
Previous Next Review + create

Creamos otra cuenta de almacenamiento.


	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	



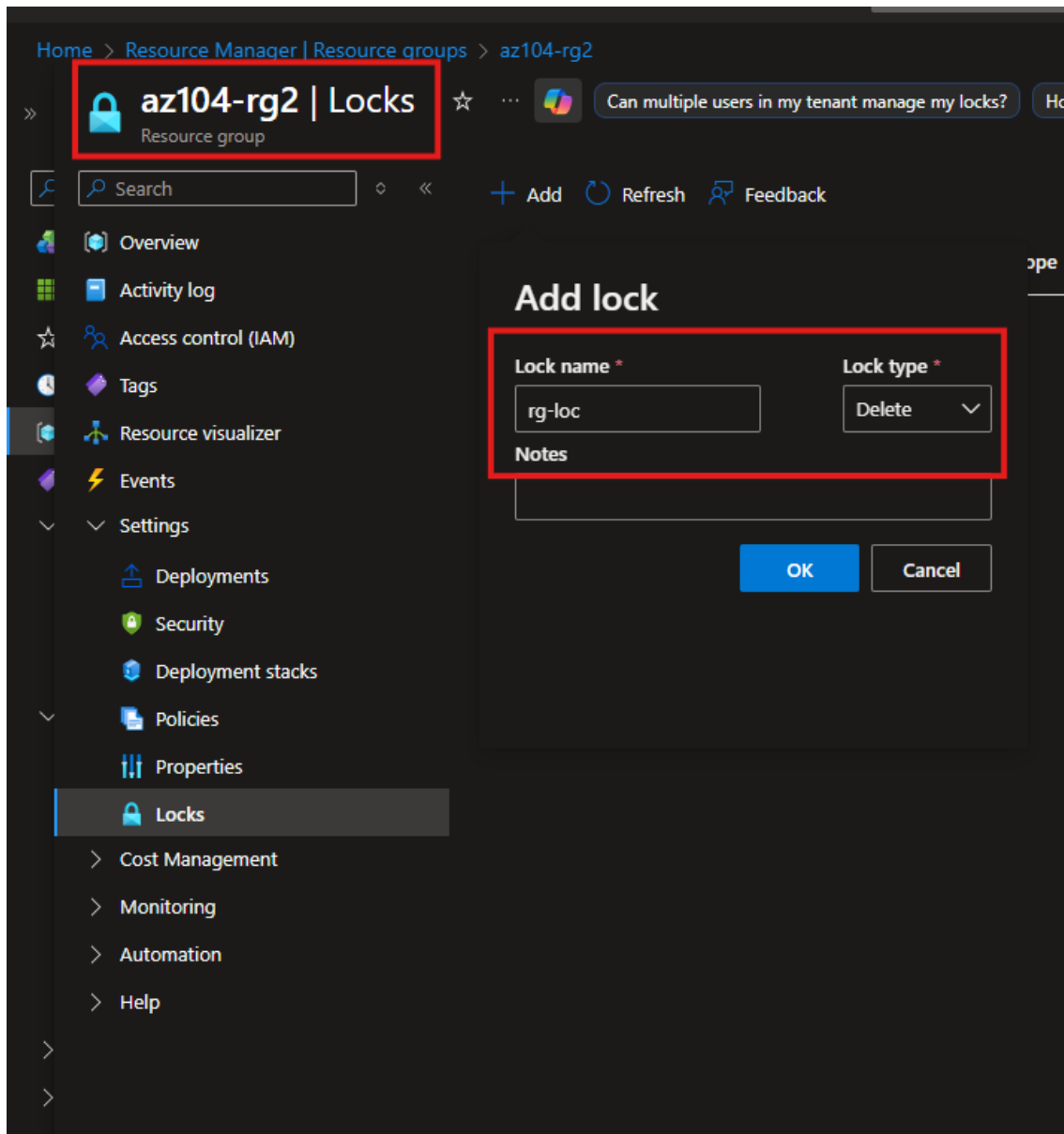
Se crea la cuenta.



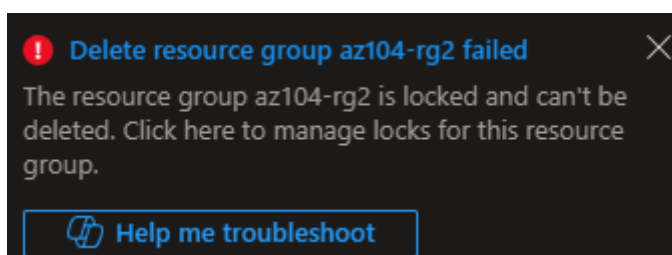
El tag se ha aplicado automáticamente.


	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	

Configurar y probar los locks en recursos.



Creamos el lock de delete en el grupo de recursos.



	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2b	

Al borrar nos da error.

```
PS /home/raul_casado> Remove-AzResourceGroup -name "az104-rg2"

Confirm
Are you sure you want to remove resource group 'az104-rg2'
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
True
PS /home/raul_casado> 
```

Vamos a utilizar az powershell para borrar el grupo de recursos, antes hemos tenido que quitar el lock.