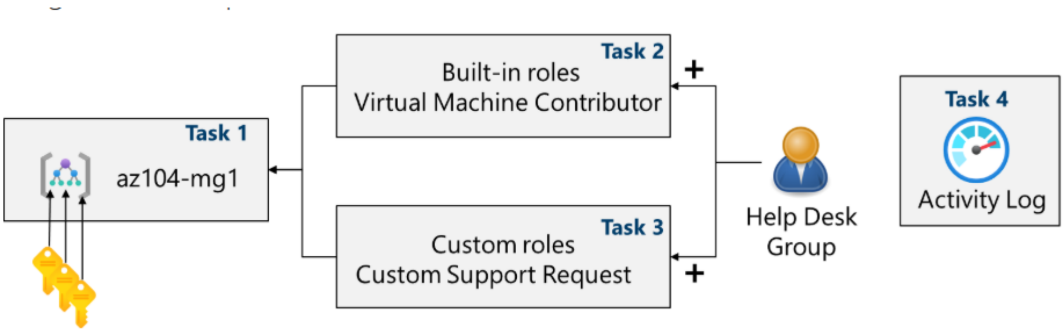
tajamar.	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #2a	

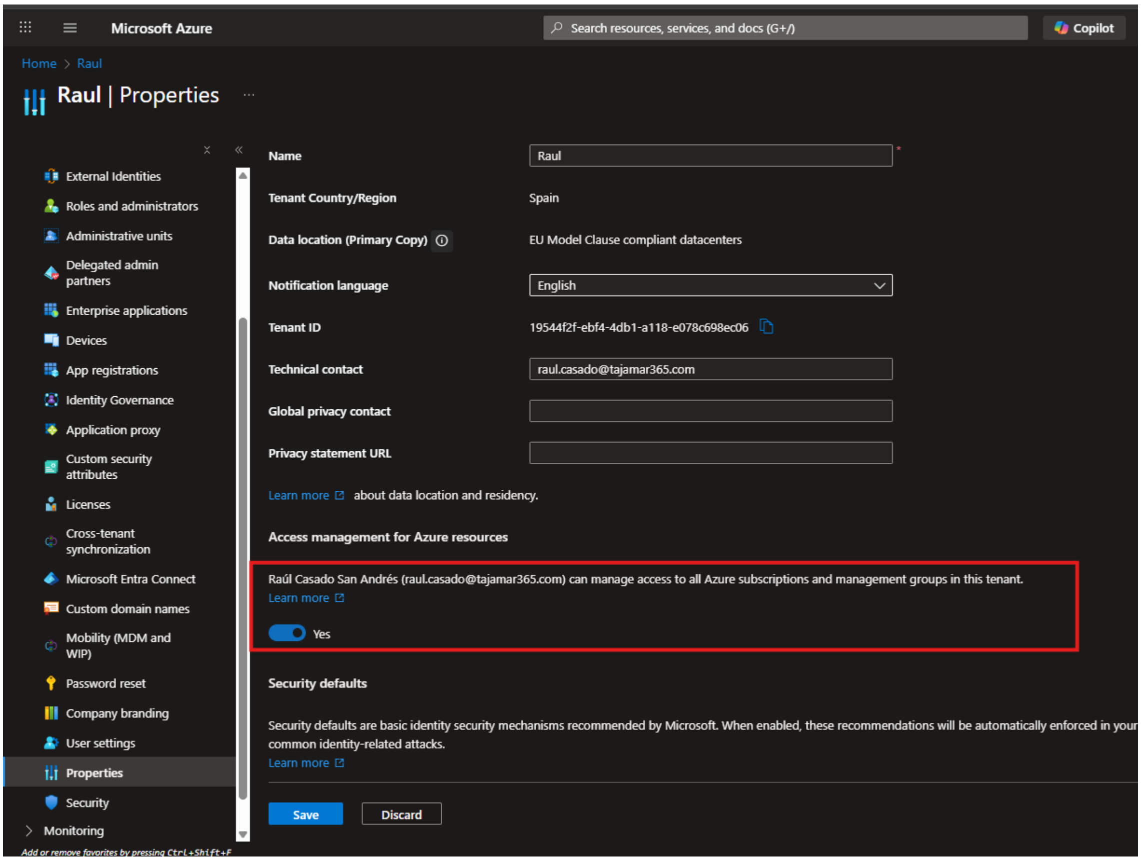
Administrar suscripciones y RBAC

Contenido

Esquema del laboratorio



Implementar grupos de administración



Name: Raul

Tenant Country/Region: Spain

Data location (Primary Copy): EU Model Clause compliant datacenters

Notification language: English

Tenant ID: 19544f2f-ebf4-4db1-a118-e078c698ec06

Technical contact: raul.casado@tajamar365.com

Global privacy contact:

Privacy statement URL:

Learn more about data location and residency.

Access management for Azure resources

Raúl Casado San Andrés (raul.casado@tajamar365.com) can manage access to all Azure subscriptions and management groups in this tenant.
Learn more

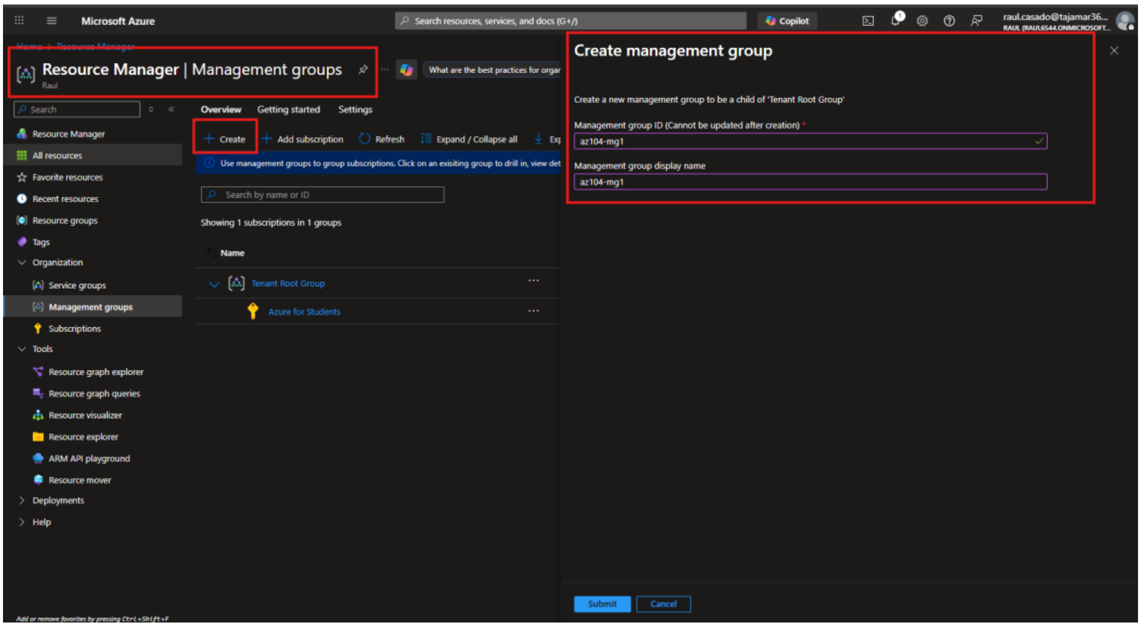
● Yes

Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your common identity-related attacks.
Learn more

Raul Casado San Andrés (raul.casado@tegamar365.com) puede gestionar el acceso a todas las suscripciones y grupos de administración de Azure en este tenant

El toggle está activado (Yes), lo que significa que tengo permisos elevados como administrador global



Use management groups to group subscriptions. Click on an exisiting group to drill in, view det

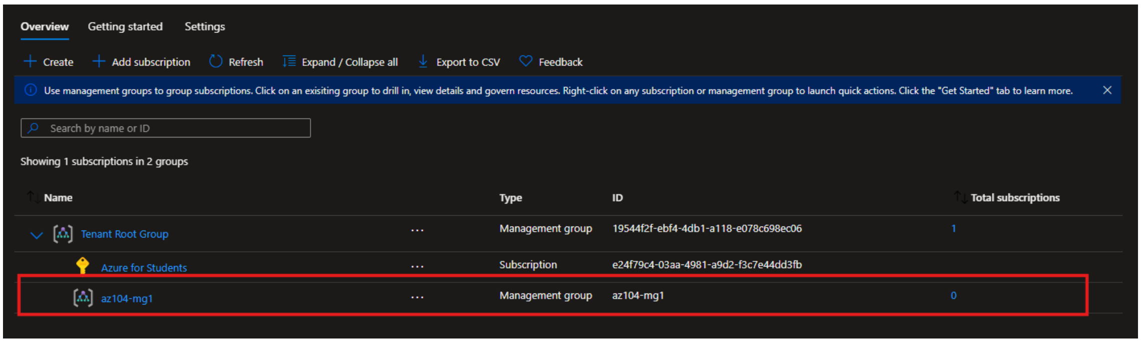
Showing 1 subscriptions in 1 groups

Create management group

Create a new management group to be a child of 'Tenant Root Group'

Management group ID (Cannot be updated after creation) *: az104-mg1

Management group display name: az104-mg1



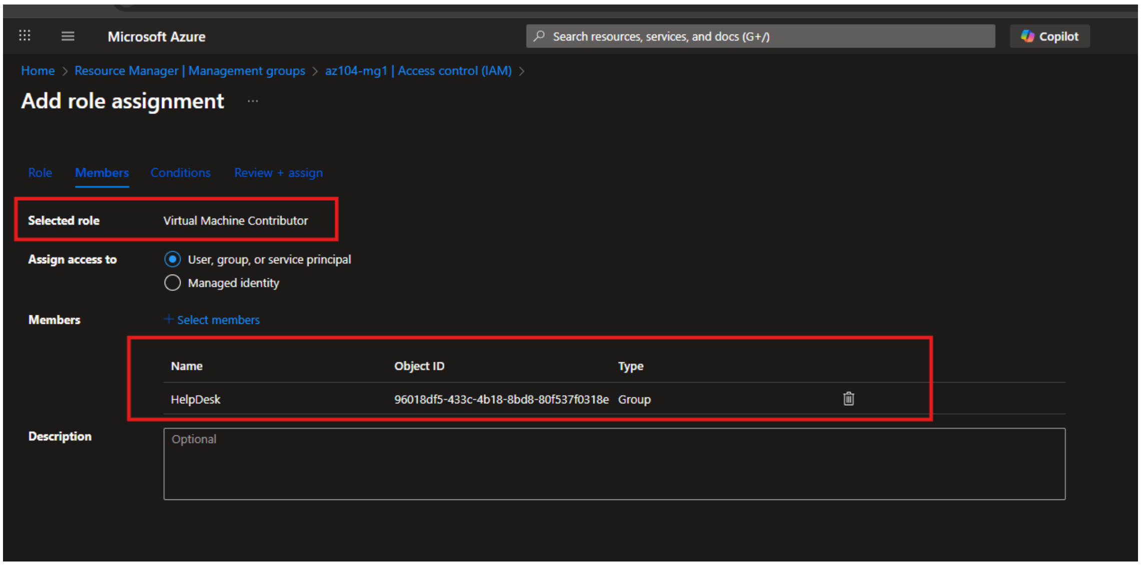
Use management groups to group subscriptions. Click on an exisiting group to drill in, view details and govern resources. Right-click on any subscription or management group to launch quick actions. Click the "Get Started" tab to learn more.

Showing 1 subscriptions in 2 groups

Name	Type	ID	Total subscriptions
Tenant Root Group	Management group	19544f2f-ebf4-4db1-a118-e078c698ec06	1
Azure for Students	Subscription	e24f79c4-03aa-4981-a9d2-f3c7e44dd3fb	
az104-mg1	Management group	az104-mg1	0

Buscamos management groups y creamos un nuevo grupo.

Revisar y asignar un rol de Azure integrado



Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home > Resource Manager | Management groups > az104-mg1 | Access control (IAM) >

Add role assignment ...

Role | Members | Conditions | Review + assign

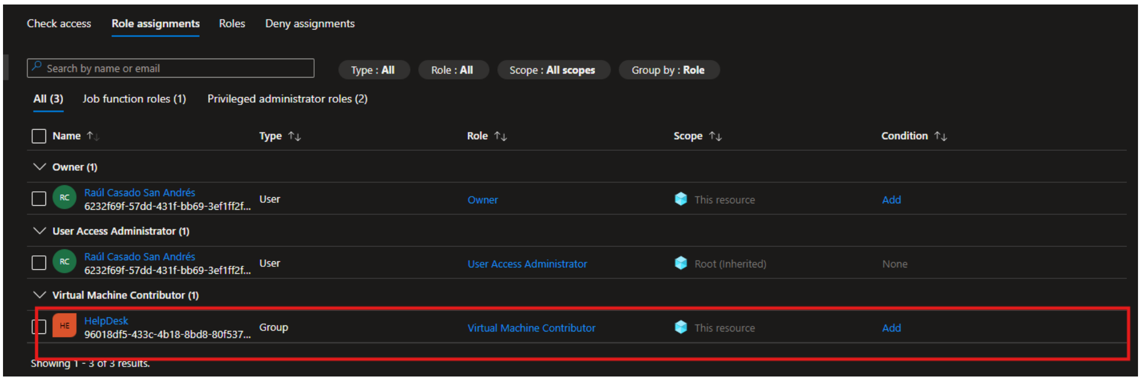
Selected role: Virtual Machine Contributor

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

Name	Object ID	Type
HelpDesk	96018df5-433c-4b18-8bd8-80f537f0318e	Group

Description: Optional



Check access | Role assignments | Roles | Deny assignments

Search by name or email

Type : **All** | Role : **All** | Scope : **All scopes** | Group by : **Role**

All (3) | Job function roles (1) | Privileged administrator roles (2)

Name	Type	Role	Scope	Condition
Owner (1)				
Raúl Casado San Andrés 6232f69f-57dd-431f-bb69-3ef1ff2f...	User	Owner	This resource	Add
User Access Administrator (1)				
Raúl Casado San Andrés 6232f69f-57dd-431f-bb69-3ef1ff2f...	User	User Access Administrator	Root (Inherited)	None
Virtual Machine Contributor (1)				
HelpDesk 96018df5-433c-4b18-8bd8-80f537...	Group	Virtual Machine Contributor	This resource	Add

Showing 1 - 3 of 3 results.

Seleccionamos el az104-mg1 management group.

Seleccionamos Access control (IAM) , y después Roles.

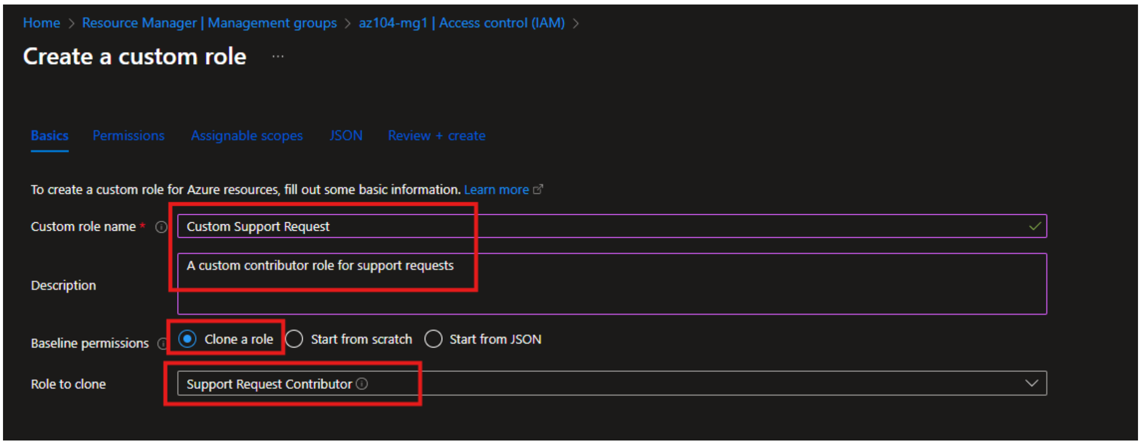
Seleccionamos Add, desde el menú desplegable y pulsamos Add role assignment.

En **Add role assignment** , buscamos y elegimos **Virtual Machine Contributor**.

En la pestaña de miembros añadimos el grupo helpdesk que hemos tenido que crear anteriormente.

Creamos el rol.

Crear un rol de RBAC personalizado



Home > Resource Manager | Management groups > az104-mg1 | Access control (IAM) >

Create a custom role ...

To create a custom role for Azure resources, fill out some basic information. Learn more

Custom role name * : Custom Support Request

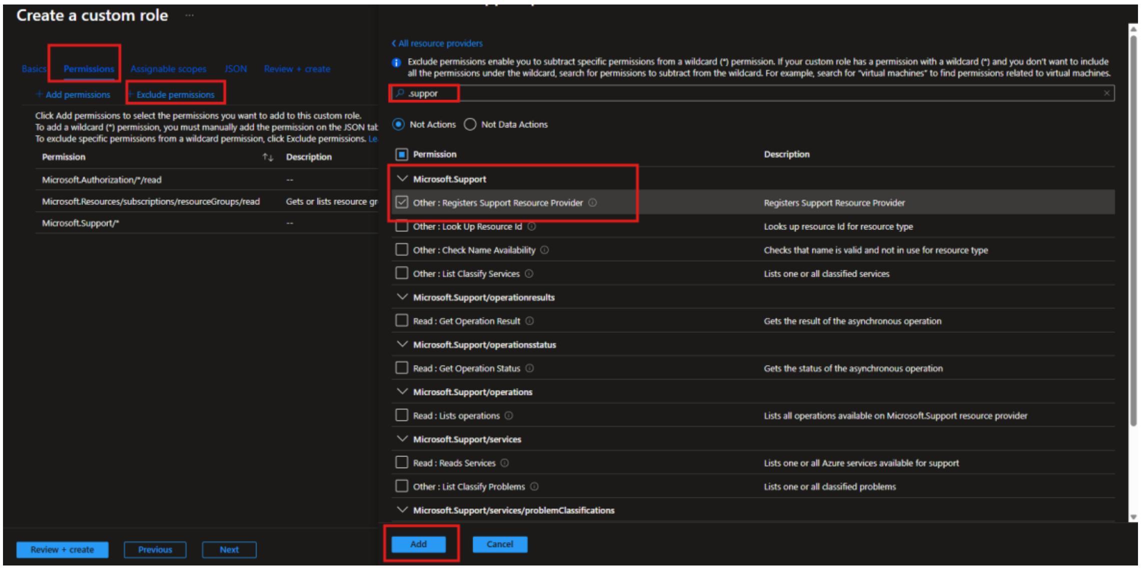
Description: A custom contributor role for support requests

Baseline permissions: ● Clone a role ○ Start from scratch ○ Start from JSON

Role to clone: Support Request Contributor

Creamos el rol personalizado y clonamos los permisos básicos de otro rol.

Son el conjunto mínimo de permisos que se otorgan por defecto a usuarios, grupos o servicios para realizar sus funciones básicas de manera segura.



Create a custom role ...

Click Add permissions to select the permissions you want to add to this custom role.
To add a wildcard (*) permission, you must manually add the permission on the JSON tab
To exclude specific permissions from a wildcard permission, click Exclude permissions. Le

Permission	Description
Microsoft.Authorization/*/read	--
Microsoft.Resources/subscriptions/resourceGroups/read	Gets or lists resource gr
Microsoft.Support/*	--

< All resource providers

Exclude permissions enable you to subtract specific permissions from a wildcard (*) permission. If your custom role has a permission with a wildcard (*) and you don't want to include all the permissions under the wildcard, search for permissions to subtract from the wildcard. For example, search for "virtual machines" to find permissions related to virtual machines.

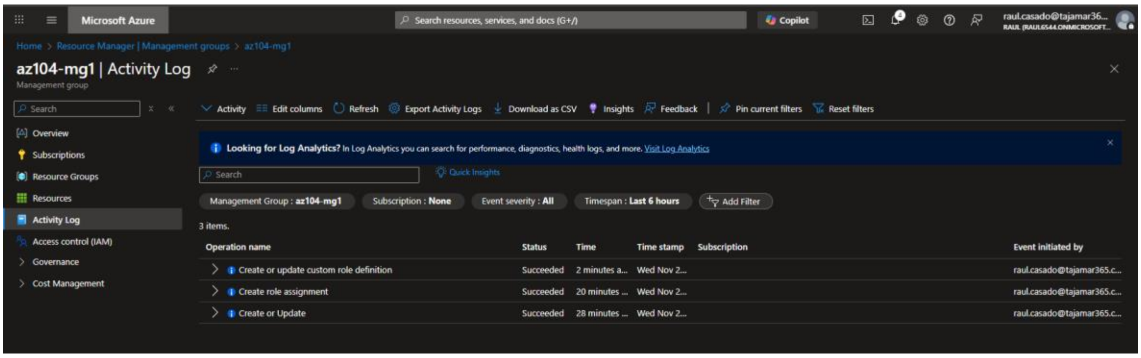
.suppor

● Not Actions ○ Not Data Actions

Permission	Description
Microsoft.Support	
☑ Other : Registers Support Resource Provider	Registers Support Resource Provider
□ Other : Look Up Resource Id	Looks up resource Id for resource type
□ Other : Check Name Availability	Checks that name is valid and not in use for resource type
□ Other : List Classify Services	Lists one or all classified services
Microsoft.Support/operationresults	
□ Read : Get Operation Result	Gets the result of the asynchronous operation
Microsoft.Support/operationsstatus	
□ Read : Get Operation Status	Gets the status of the asynchronous operation
Microsoft.Support/operations	
□ Read : Lists operations	Lists all operations available on Microsoft.Support resource provider
Microsoft.Support/services	
□ Read : Reads Services	Lists one or all Azure services available for support
□ Other : List Classify Problems	Lists one or all classified problems
Microsoft.Support/services/problemClassifications	

Denegamos los permisos de Registra el proveedor de recursos de soporte.

Supervisar la asignación de roles con el registro de actividades



az104-mg1 | Activity Log

Management group

Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. Visit Log Analytics

Management Group : **az104-mg1** Subscription : **None** Event severity : **All** Timespan : **Last 6 hours**

3 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Create or update custom role definition	Succeeded	2 minutes a...	Wed Nov 2...		raul.casado@tajamar365.c...
Create role assignment	Succeeded	20 minutes ...	Wed Nov 2...		raul.casado@tajamar365.c...
Create or Update	Succeeded	28 minutes ...	Wed Nov 2...		raul.casado@tajamar365.c...

Revisamos las actividades para las asignaciones de roles.