# Lab 02a - Gestión de Suscripciones y RBAC con Azure CLI

## Introducción del Laboratorio

En este laboratorio se aprende sobre control de acceso basado en roles (RBAC) usando Azure CLI. Se implementa permisos y ámbitos para controlar acciones de identidades y simplificar la gestión de suscripciones usando grupos de administración.

**Tiempo estimado:** 30 minutos  
**Región recomendada:** East US

## Escenario del Lab

Implementar funcionalidad para simplificar la gestión de recursos Azure:

- Crear un grupo de administración que incluya todas las suscripciones Azure

- Otorgar permisos para solicitudes de soporte limitados a:

- Crear y administrar máquinas virtuales

- Crear tickets de solicitud de soporte (sin agregar proveedores Azure)

## Prerrequisitos

### Instalación y Configuración Inicial

# 1. Verificar instalación de Azure CLI  
az --version  
  
# 2. Verificar mi suscripción activa  
az account show  
  
# 3. Listar todas las suscripciones disponibles  
az account list --output table  
  
# 4. Establecer suscripción por defecto (si es necesario)  
# az account set --subscription "<nombre-o-id-suscripcion>"

## Tarea 1: Implementar Grupos de Administración

### 1.1 Verificar permisos en Microsoft Entra ID

# Obtener información del tenant actual  
## -> El siguiente comando necesita “extensiones account” (aceptar o rechazar, luego continuará)  
az account tenant list  
  
# Verificar permisos de gestión de acceso (requiere permisos de administrador)  
az rest --method GET --url "https://graph.microsoft.com/v1.0/organization" --query "value[0].{displayName:displayName, id:id}"

En se muestra parcialmente la sesión de trabajo de los comandos ejecutados

A screen shot of a computer

AI-generated content may be incorrect.

Captura : Verificando permisos

### 1.2 Crear Grupo de Administración

# Crear nuevo grupo de administración  
az account management-group create \  
 --name "az104-mg1" \  
 --display-name "az104-mg1"  
  
# Verificar creación del grupo  
az account management-group show --name "az104-mg1"  
  
# Listar todos los grupos de administración para confirmar  
az account management-group list --output table

A black screen with white text

AI-generated content may be incorrect.

Captura 2: Creación de grupo de administración

### 1.3 Agregar Suscripción al Grupo de Administración

# Obtener ID de la suscripción actual  
SUBSCRIPTION\_ID=$(az account show --query id --output tsv)  
echo "Subscription ID: $SUBSCRIPTION\_ID"  
  
# Agregar suscripción al grupo de administración  
az account management-group subscription add \  
 --name "az104-mg1" \  
 --subscription "$SUBSCRIPTION\_ID"  
  
# Verificar que la suscripción se agregó correctamente  
az account management-group show --name "az104-mg1" --expand –recurse

A screenshot of a computer program

AI-generated content may be incorrect.

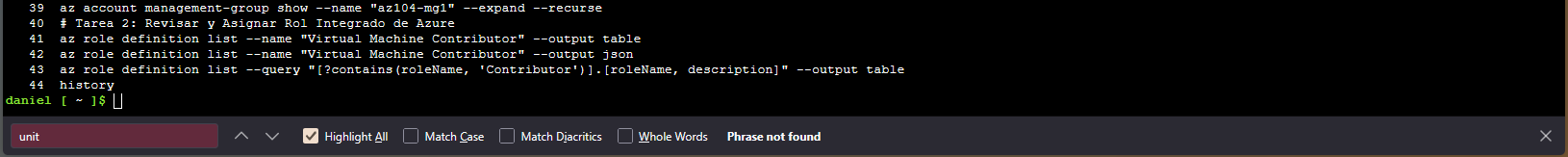
Captura 3: Agregando suscripción al grupo de administración

## Tarea 2: Revisar y Asignar Rol Integrado de Azure

### 2.1 Explorar Roles Integrados

# Listar roles integrados más comunes  
az role definition list --name "Virtual Machine Contributor" --output table  
  
# Ver detalles completos del rol Virtual Machine Contributor  
az role definition list --name "Virtual Machine Contributor" --output json  
  
# Listar otros roles útiles para referencia  
az role definition list --query "[?contains(roleName, 'Contributor')].[roleName, description]" --output table

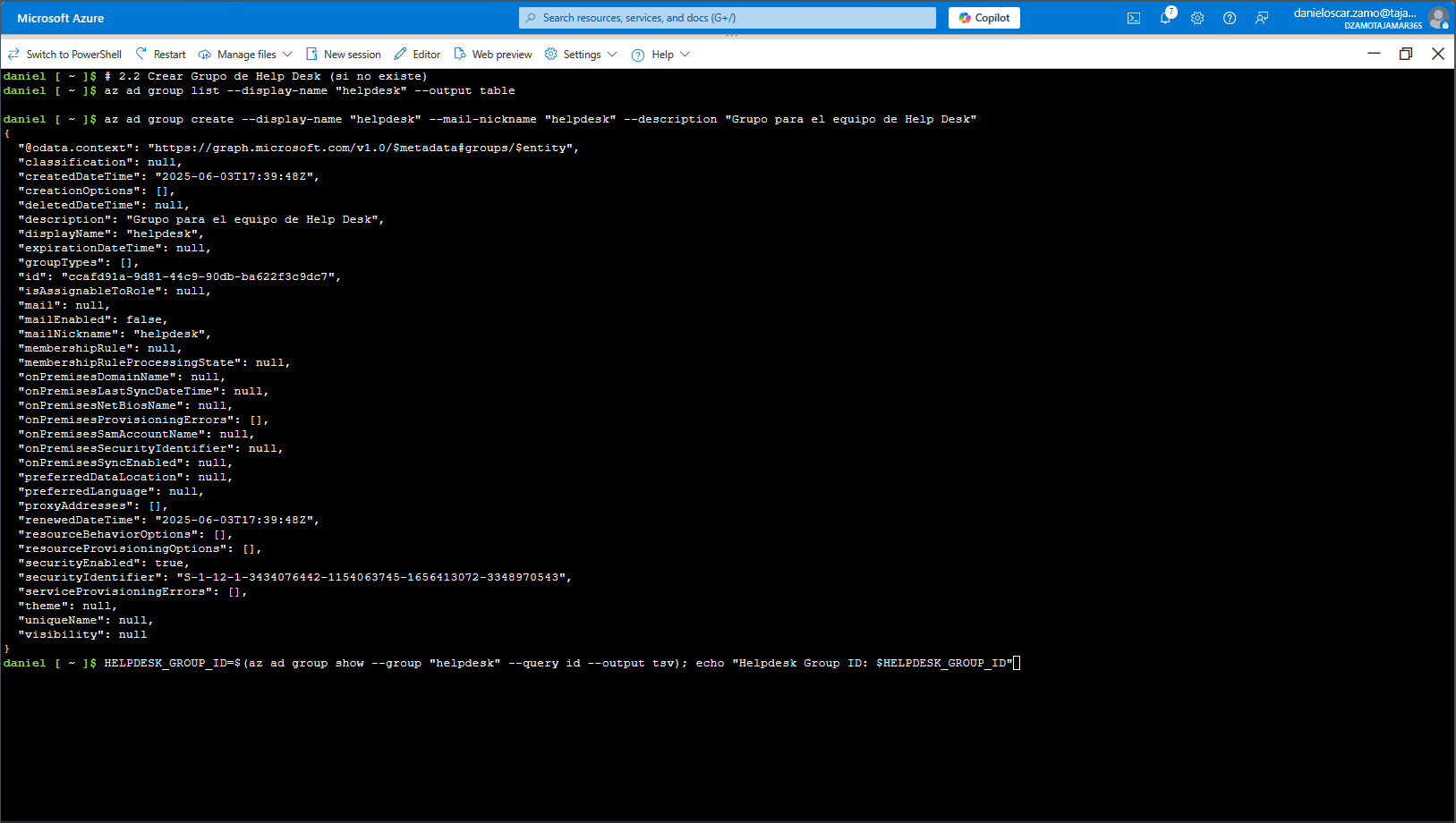
En Captura 4 se muestra el historial de los comandos ejecutados en este item, por verificar antes de asignar el rol.



Captura 4: Historial de revisión y detalles de los roles

### 2.2 Crear Grupo de Help Desk (si no existe)

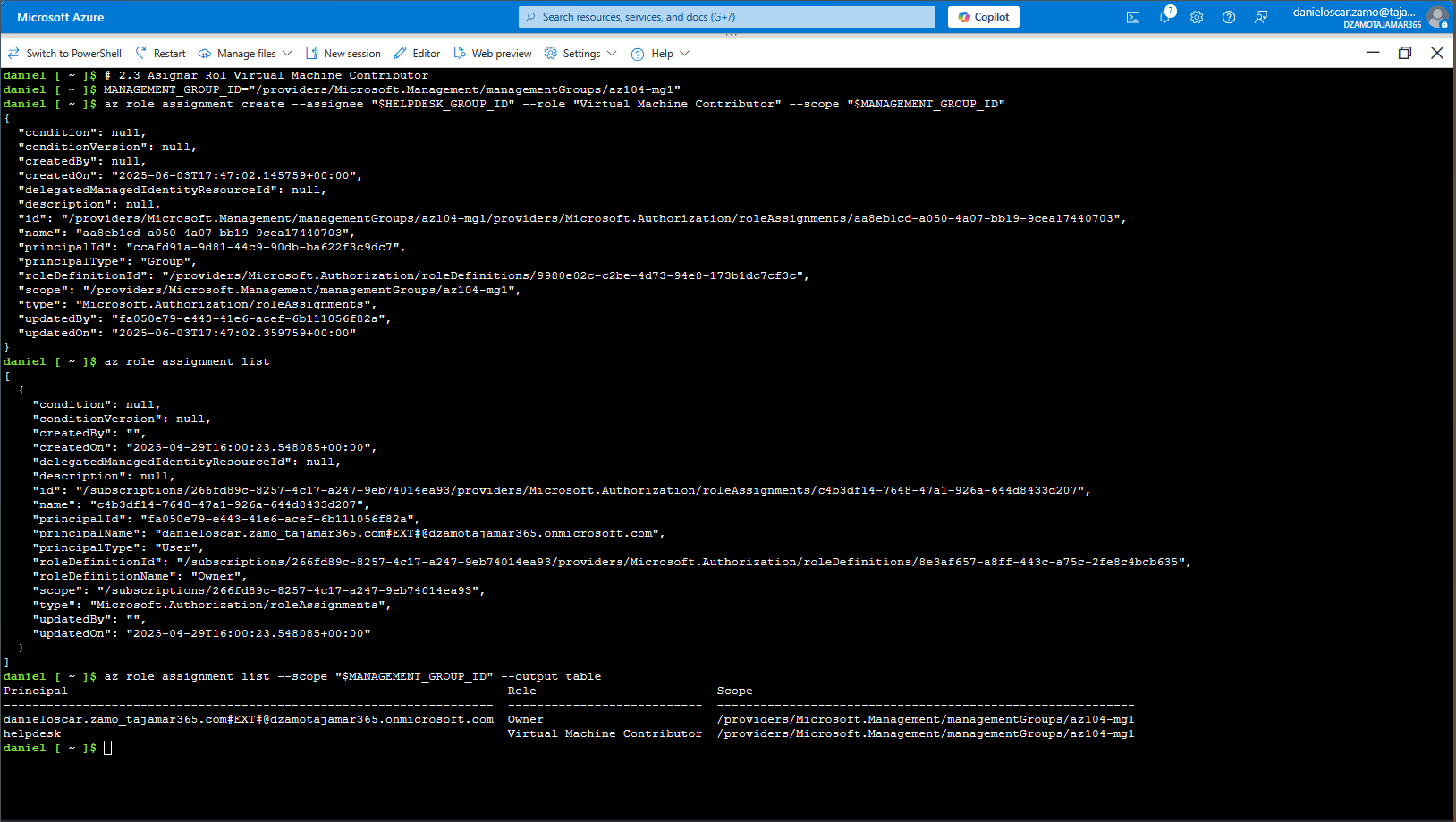
# Verificar si el grupo helpdesk existe  
az ad group list --display-name "helpdesk" --output table  
  
# Si no existe, crear el grupo helpdesk  
az ad group create \  
 --display-name "helpdesk" \  
 --mail-nickname "helpdesk" \  
 --description "Grupo para el equipo de Help Desk"  
  
# Obtener el Object ID del grupo helpdesk  
HELPDESK\_GROUP\_ID=$(az ad group show --group "helpdesk" --query id --output tsv)  
echo "Helpdesk Group ID: $HELPDESK\_GROUP\_ID"



Captura 5: Creación grupo Help Desk

### 2.3 Asignar Rol Virtual Machine Contributor

# Obtener el ID del grupo de administración  
MANAGEMENT\_GROUP\_ID="/providers/Microsoft.Management/managementGroups/az104-mg1"  
  
# Asignar rol Virtual Machine Contributor al grupo helpdesk en el grupo de administración  
az role assignment create \  
 --assignee "$HELPDESK\_GROUP\_ID" \  
 --role "Virtual Machine Contributor" \  
 --scope "$MANAGEMENT\_GROUP\_ID"  
  
# Verificar la asignación de rol  
az role assignment list \  
 --scope "$MANAGEMENT\_GROUP\_ID" \  
 --output table



Captura 6: Asignación del Rol Virtual Machine Contributor

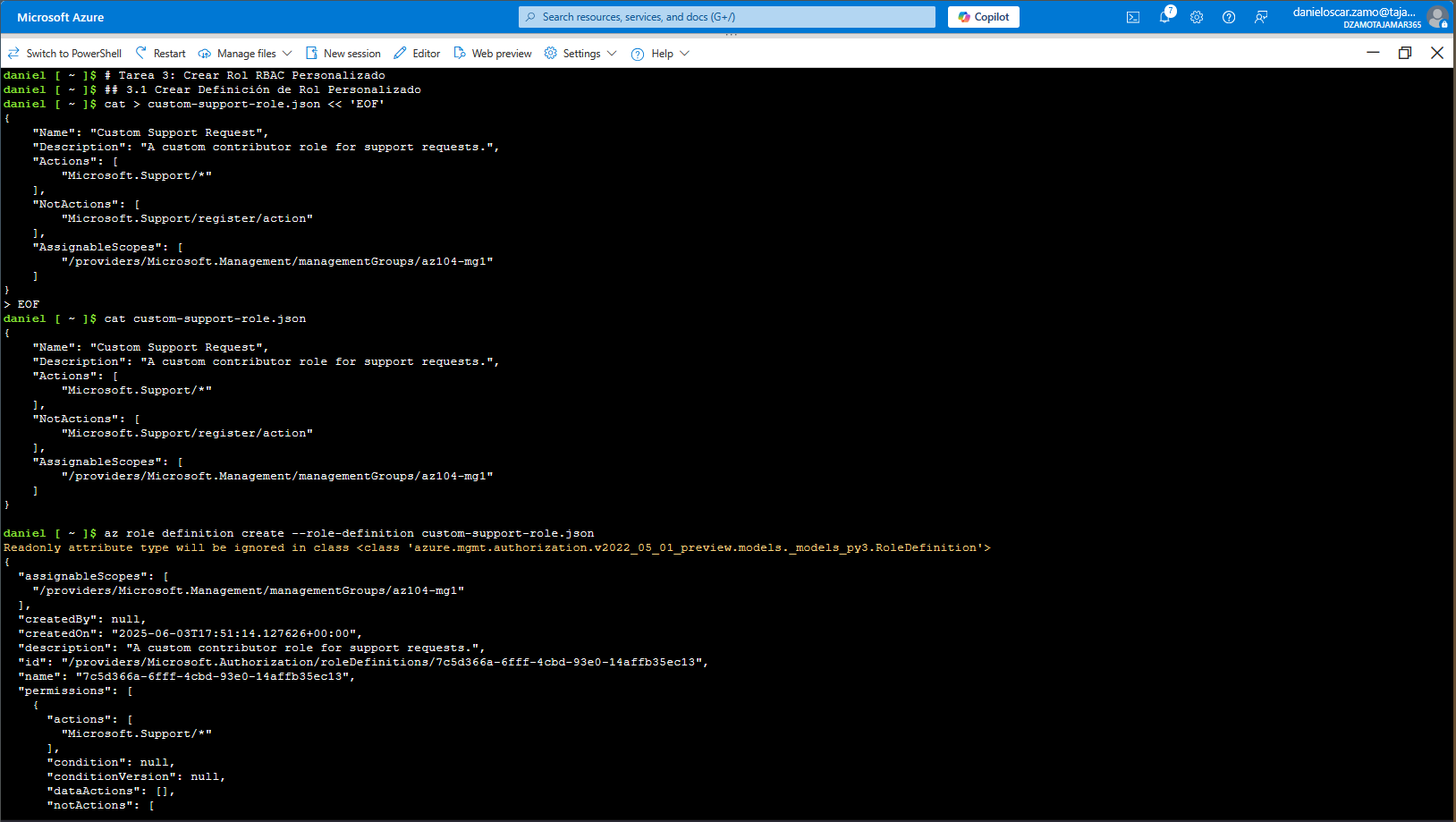
## Tarea 3: Crear Rol RBAC Personalizado

### 3.1 Crear Definición de Rol Personalizado

# Crear archivo JSON para el rol personalizado  
cat > custom-support-role.json << 'EOF'  
{  
 "Name": "Custom Support Request",  
 "Description": "A custom contributor role for support requests.",  
 "Actions": [  
 "Microsoft.Support/\*"  
 ],  
 "NotActions": [  
 "Microsoft.Support/register/action"  
 ],  
 "AssignableScopes": [  
 "/providers/Microsoft.Management/managementGroups/az104-mg1"  
 ]  
}  
EOF  
  
# Mostrar el contenido del archivo creado  
cat custom-support-role.json

### 3.2 Crear el Rol Personalizado

# Crear el rol personalizado usando el archivo JSON  
az role definition create --role-definition custom-support-role.json  
  
# Verificar que el rol se creó correctamente  
az role definition list --name "Custom Support Request" --output table  
  
# Ver detalles completos del rol personalizado  
az role definition list --name "Custom Support Request" --output json



Captura 7: Creación del rol personalizado

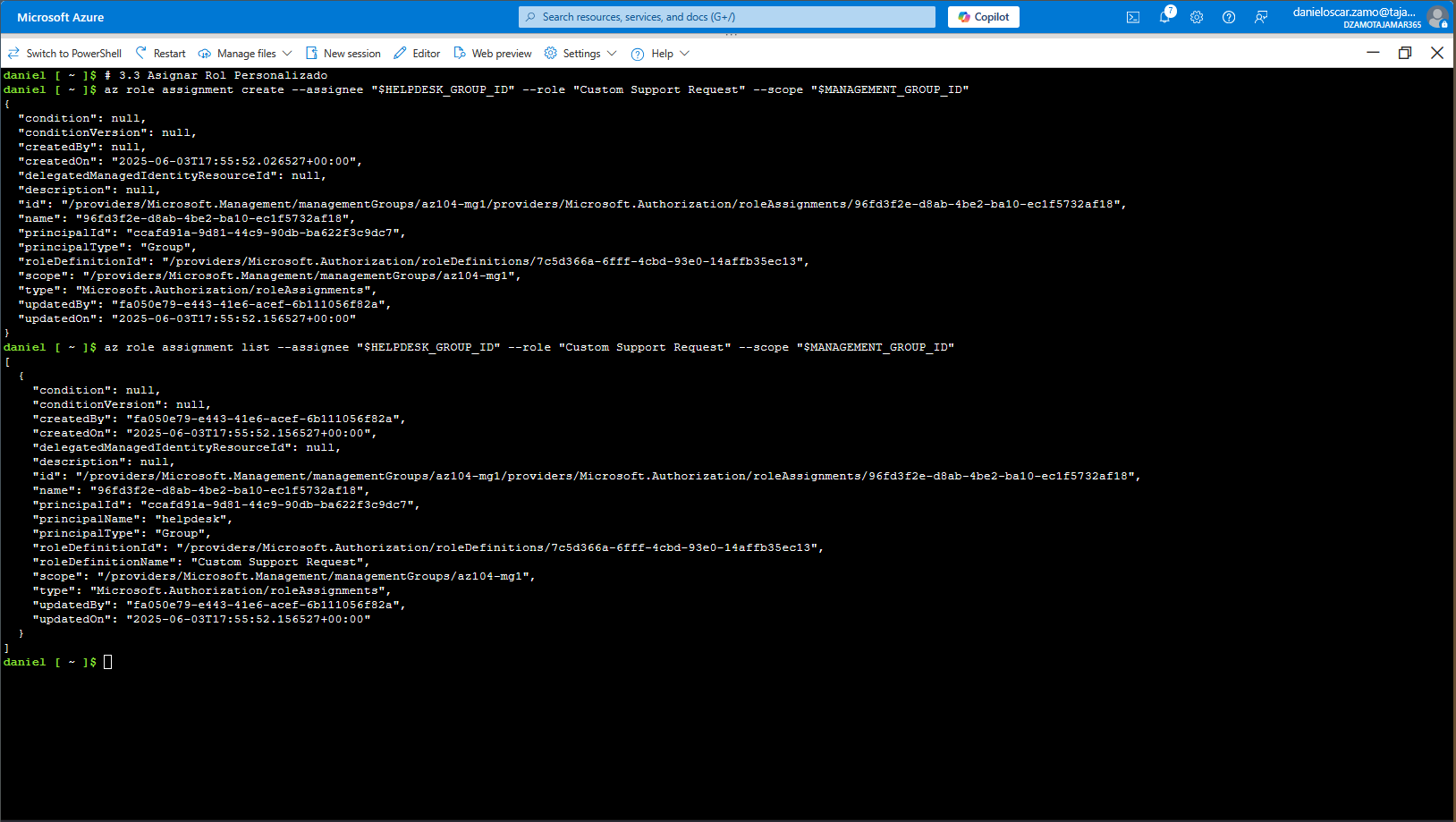
A computer screen shot of a black screen

AI-generated content may be incorrect.

Captura 8: verificación y ver detalles del rol personalizado

### 3.3 Asignar Rol Personalizado

# Asignar el rol personalizado al grupo helpdesk  
az role assignment create \  
 --assignee "$HELPDESK\_GROUP\_ID" \  
 --role "Custom Support Request" \  
 --scope "$MANAGEMENT\_GROUP\_ID"  
  
# Verificar todas las asignaciones de roles para el grupo de administración  
az role assignment list \  
 --scope "$MANAGEMENT\_GROUP\_ID" \  
 --output table



Captura 9: Asignación del rol a Help Desk y verificación

## Tarea 4: Monitorear Asignaciones de Roles con Activity Log

### 4.1 Consultar Activity Log

# Consultar actividades de creación de roles personalizados  
az role definition list --custom-role-only true --output table

# Verificar asignaciones de rolesecho "=== VERIFICACIÓN DIRECTA DE ASIGNACIONES ==="  
az role assignment list \  
 --scope "/providers/Microsoft.Management/managementGroups/az104-mg1" \  
 --output table  
  
# Ver detalles completos de las asignaciones  
az role assignment list \  
 --scope "/providers/Microsoft.Management/managementGroups/az104-mg1" \  
 --query "[].{Assignee:principalName, Role:roleDefinitionName, Scope:scope, Type:principalType}" \  
 --output table

# Debug: Ver todos los eventos recientes (últimas 2 horas)  
az monitor activity-log list \  
 --start-time $(date -u -d '2 hours ago' +%Y-%m-%dT%H:%M:%SZ) \  
 --output table   
  
# Debug: Ver estructura completa de un evento de Activity Logaz monitor activity-log list \  
 --max-events 1 \  
 --output json

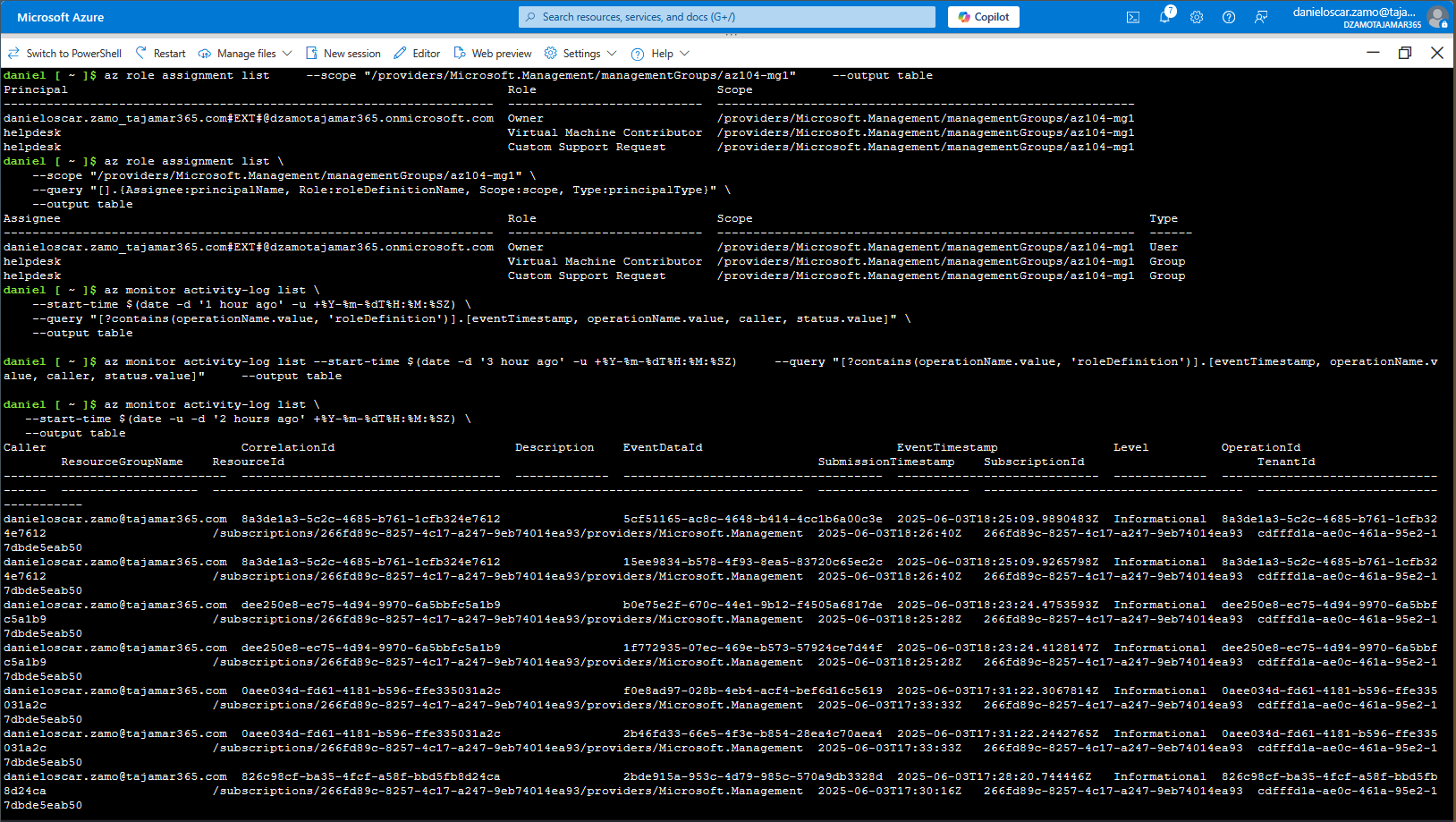
# Los siguientes son también utilizando Activity Log (Puede tardar en aparecer)

## Buscar específicamente eventos de creación de roles  
az monitor activity-log list \  
 --start-time $(date -u -d '4 hours ago' +%Y-%m-%dT%H:%M:%SZ) \  
 --query "[?contains(operationName.value, 'roleDefinitions/write')].[eventTimestamp, operationName.value, caller, status.value]" \  
 --output table

## Buscar todos los eventos relacionados con definiciones de roles  
az monitor activity-log list \  
 --start-time $(date -u -d '4 hours ago' +%Y-%m-%dT%H:%M:%SZ) \  
 --query "[?contains(operationName.value, 'roleDefinition')].[eventTimestamp, operationName.value, caller, status.value]" \  
 --output table

# Actividades de definiciones de roles (crear/modificar roles personalizados)  
az monitor activity-log list \  
 --start-time $(date -u -d '2 hours ago' +%Y-%m-%dT%H:%M:%SZ) \  
 --query "[?contains(operationName.value, 'roleDefinition')].[eventTimestamp, operationName.value, caller, status.value]" \  
 --output table

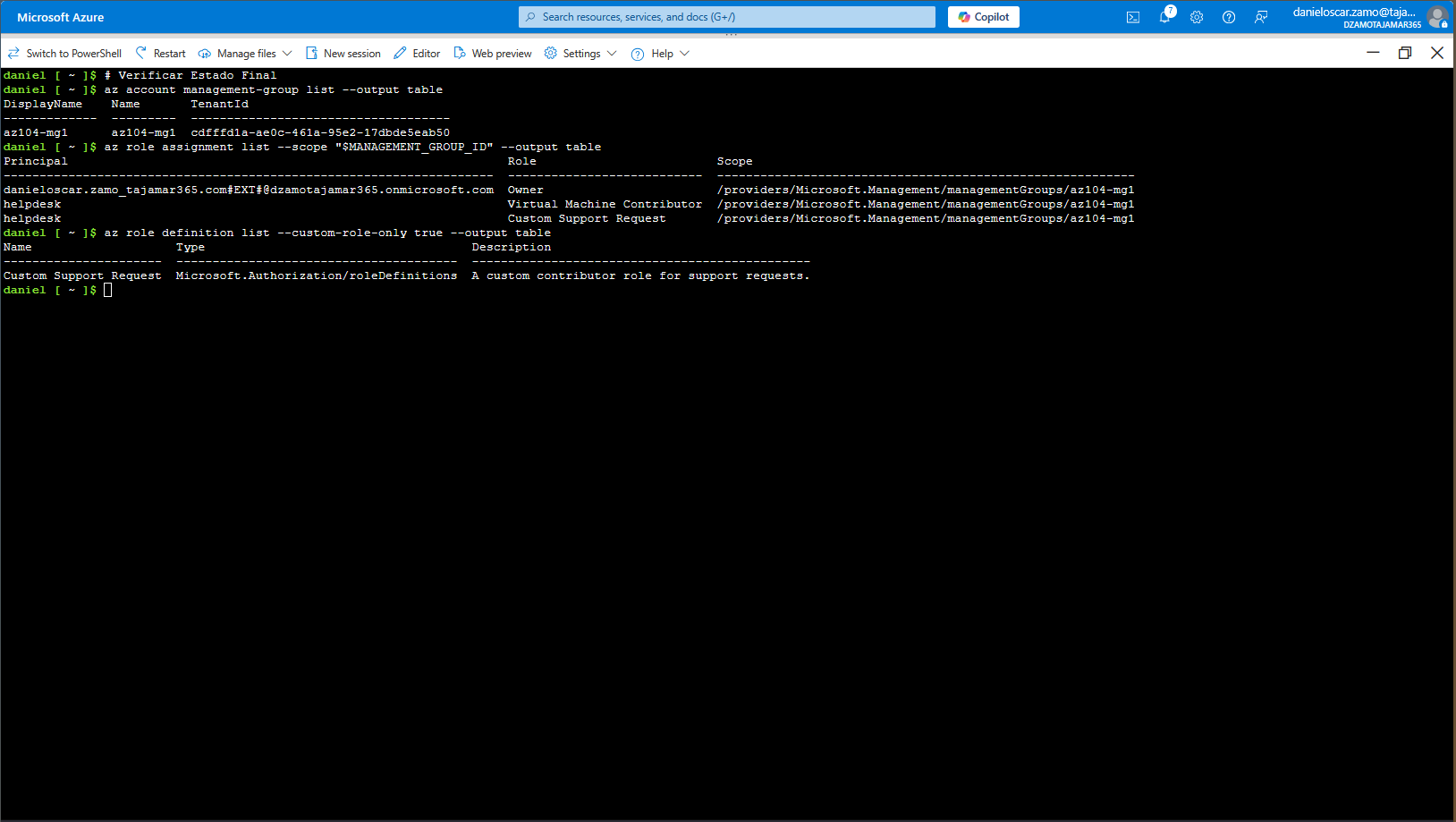
# Todos los eventos de autorización (más amplio)  
az monitor activity-log list \  
 --start-time $(date -u -d '2 hours ago' +%Y-%m-%dT%H:%M:%SZ) \  
 --query "[?resourceProviderName.value == 'Microsoft.Authorization'].[eventTimestamp, operationName.value, caller, status.value]" \  
 --output table



Captura 10: Verificación de asignación de roles y otras consultas

### 4.2 Verificar Estado Final

# Resumen de grupos de administración  
echo "=== GRUPOS DE ADMINISTRACIÓN ==="  
az account management-group list --output table  
  
# Resumen de asignaciones de roles  
echo -e "\n=== ASIGNACIONES DE ROLES ==="  
az role assignment list \  
 --scope "$MANAGEMENT\_GROUP\_ID" \  
 --output table  
  
# Resumen de roles personalizados  
echo -e "\n=== ROLES PERSONALIZADOS ==="  
az role definition list \  
 --custom-role-only true \  
 --output table



Captura 11: Verificación estado final

## Verificación y Pruebas

### Verificar Permisos del Grupo Helpdesk

# Listar todos los permisos efectivos para el grupo helpdesk  
az role assignment list \  
 --assignee "$HELPDESK\_GROUP\_ID" \  
 --all \  
 --output table  
  
# Verificar permisos específicos de VM  
az role assignment list \  
 --assignee "$HELPDESK\_GROUP\_ID" \  
 --role "Virtual Machine Contributor" \  
 --output table  
  
# Verificar permisos de soporte personalizado  
az role assignment list \  
 --assignee "$HELPDESK\_GROUP\_ID" \  
 --role "Custom Support Request" \  
 --output table

## Limpieza de Recursos

### Eliminar Asignaciones de Roles

# Eliminar asignación de Virtual Machine Contributor  
az role assignment delete \  
 --assignee "$HELPDESK\_GROUP\_ID" \  
 --role "Virtual Machine Contributor" \  
 --scope "$MANAGEMENT\_GROUP\_ID"  
  
# Eliminar asignación de Custom Support Request  
az role assignment delete \  
 --assignee "$HELPDESK\_GROUP\_ID" \  
 --role "Custom Support Request" \  
 --scope "$MANAGEMENT\_GROUP\_ID"

### Eliminar Rol Personalizado

# Eliminar rol personalizado  
az role definition delete --name "Custom Support Request"

### Eliminar Grupo de Administración

# Remover suscripción del grupo de administración  
az account management-group subscription remove \  
 --name "az104-mg1" \  
 --subscription "$SUBSCRIPTION\_ID"  
  
# Eliminar grupo de administración  
az account management-group delete --name "az104-mg1"

### Eliminar Grupo Helpdesk (opcional)

# Eliminar grupo helpdesk si se creó para este lab  
az ad group delete --group "helpdesk"

### Limpiar Archivos Temporales

# Eliminar archivo JSON temporal  
rm -f custom-support-role.json

## Scripts de Utilidad

### Script de Verificación Completa

#!/bin/bash  
# Crear script de verificación  
cat > verify-lab.sh << 'EOF'  
#!/bin/bash  
  
echo "=== VERIFICACIÓN DEL LABORATORIO ==="  
  
# Variables  
HELPDESK\_GROUP\_ID=$(az ad group show --group "helpdesk" --query id --output tsv 2>/dev/null)  
MANAGEMENT\_GROUP\_ID="/providers/Microsoft.Management/managementGroups/az104-mg1"  
  
echo -e "\n1. Verificando grupo de administración..."  
az account management-group show --name "az104-mg1" --query "{name:name, displayName:displayName}" --output table  
  
echo -e "\n2. Verificando grupo helpdesk..."  
if [ -z "$HELPDESK\_GROUP\_ID" ]; then  
 echo "❌ Grupo helpdesk no encontrado"  
else  
 echo "✅ Grupo helpdesk encontrado: $HELPDESK\_GROUP\_ID"  
fi  
  
echo -e "\n3. Verificando asignaciones de roles..."  
az role assignment list --scope "$MANAGEMENT\_GROUP\_ID" --output table  
  
echo -e "\n4. Verificando roles personalizados..."  
az role definition list --name "Custom Support Request" --query "[].{Name:roleName, Description:description}" --output table  
  
echo -e "\n=== VERIFICACIÓN COMPLETADA ==="  
EOF  
  
chmod +x verify-lab.sh

## Comandos de Referencia Rápida

# Ver ayuda para grupos de administración  
az account management-group --help  
  
# Ver ayuda para asignaciones de roles  
az role assignment --help  
  
# Ver ayuda para definiciones de roles  
az role definition --help  
  
# Ver ayuda para grupos de Azure AD  
az ad group --help  
  
# Ver ayuda para Activity Log  
az monitor activity-log --help

## Puntos Clave del Laboratorio

* **Grupos de Administración**: Organizan lógicamente las suscripciones y permiten herencia de RBAC y políticas
* **Roles Integrados**: Azure proporciona roles predefinidos como “Virtual Machine Contributor”
* **Roles Personalizados**: Se pueden crear roles específicos siguiendo el principio del menor privilegio
* **Asignaciones de Roles**: Se asignan a grupos (mejor práctica) en lugar de usuarios individuales
* **Monitoreo**: El Activity Log permite rastrear cambios en asignaciones y definiciones de roles
* **Ámbitos**: Los permisos se pueden aplicar a diferentes niveles (suscripción, grupo de administración, etc.)

## Extensión del Aprendizaje

Para profundizar en estos conceptos, puedes:

1. **Explorar más roles integrados**: az role definition list --output table
2. **Crear políticas de Azure**: Complementar RBAC con Azure Policy
3. **Implementar Privileged Identity Management (PIM)**: Para acceso just-in-time
4. **Automatizar con plantillas ARM**: Codificar la infraestructura de RBAC

**¡Felicitaciones!** Has completado el laboratorio de gestión de suscripciones y RBAC usando Azure CLI.