

Laboratorio 02a: Administrar suscripciones y RBAC

Manual de laboratorio del estudiante

Escenario de laboratorio

Para mejorar la administración de los recursos de Azure en Contoso, se le asignó la tarea de implementar la siguiente funcionalidad:

- crear un grupo de administración que incluiría todas las suscripciones de Azure de Contoso
- otorgar permisos para enviar solicitudes de soporte para todas las suscripciones en el grupo de administración a un usuario designado de Azure Active Directory. Los permisos de ese usuario deben limitarse solo a:
 - crear tickets de solicitud de soporte
 - ver grupos de recursos

Objetivos

En este laboratorio, podrá:

- Tarea 1: Implementar grupos de gestión
- Tarea 2: crear roles RBAC personalizados
- Tarea 3: Asignar roles de RBAC

Tiempo estimado: 30 minutos

Instrucciones

Ejercicio 1

Tarea 1: Implementar grupos de gestión

En esta tarea, creará y configurará grupos de administración.

1. Inicie sesión en [Azure Portal](#) .
2. Busque y seleccione **Grupos de administración** y luego, en la hoja **Grupos de administración** , haga clic en + **Agregar grupo de administración** .

Nota : Si no ha creado previamente grupos de administración, seleccione **Comenzar a usar grupos de administración**

3. Cree un grupo de administración con la siguiente configuración:

Ajuste	Valor
ID del grupo de administración	az104-02-mg1
Nombre para mostrar del grupo de administración	az104-02-mg1

4. En la lista de grupos de administración, haga clic en la entrada que representa el grupo de administración recién creado y luego muestre sus **detalles** .
5. En la hoja **az104-02-mg1** , haga clic en + **Agregar suscripción** y agregue la suscripción que está usando en este laboratorio al grupo de administración.

Nota : Copie el ID de su suscripción de Azure en el Portapapeles. Lo necesitará en la siguiente tarea.

Tarea 2: crear roles RBAC personalizados

En esta tarea, creará una definición de un rol RBAC personalizado.

1. Desde la computadora del laboratorio, abra el archivo **\ Allfiles \ Labs \ 02 \ az104-02a-customRoleDefinition.json** en el Bloc de notas y revise su contenido:
2. {
3. " Nombre " : " Colaborador de solicitud de soporte (personalizado) "
4. " IsCustom " : true ,
5. " Descripción " : " Permite crear solicitudes de soporte " ,

```

6.      " Acciones " : [
7.          " Microsoft.Resources / subscriptions / resourceGroups / read " ,
8.          " Microsoft.Support/* "
9.      ],
10.     " NotActions " : [
11.     ],
12.     " AssignableScopes " : [
13.         " /providers/Microsoft.Management/managementGroups/az104-02-mg1 "
14.     ],
15.     " / subscriptions / SUBSCRIPTION_ID "
16. ]
17. }

```

16. Reemplace el SUBSCRIPTION_ID marcador de posición en el archivo JSON con el ID de suscripción que copió en el Portapapeles y guarde el cambio.

17. En Azure Portal, abra el panel de **Cloud Shell** haciendo clic en el icono de la barra de herramientas directamente a la derecha del cuadro de texto de búsqueda.

18. Si se le solicita que seleccione **Bash** o **PowerShell** , seleccione **PowerShell** .

Nota : Si es la primera vez que inicia **Cloud Shell** y aparece el mensaje **No tiene almacenamiento activado** , seleccione la suscripción que está usando en este lab y haga clic en **Crear almacenamiento** .

19. En la barra de herramientas del panel de Cloud Shell, haga clic en el ícono **Cargar / Descargar archivos** , en el menú desplegable, haga clic en **Cargar** y cargue el archivo **\ Allfiles \ Labs \ 02 \ az104-02a-customRoleDefinition.json** en el directorio de inicio de Cloud Shell .

20. Desde el panel de Cloud Shell, ejecute lo siguiente para crear la definición de función personalizada:

```

Nueva-AzRoleDefinition - InputFile $ HOME / az104 - 02a -
customRoleDefinition.json

```

21. Cierre el panel de Cloud Shell.

Tarea 3: Asignar roles de RBAC

En esta tarea, creará un usuario de Azure Active Directory, asignará el rol de RBAC que creó en la tarea anterior a ese usuario y verificará que el usuario pueda realizar la tarea especificada en la definición de rol de RBAC.

1. En Azure Portal, busque y seleccione **Azure Active Directory** , en la hoja de Azure Active Directory, haga clic en **Usuarios** y luego en **+ Nuevo usuario** .

2. Cree un nuevo usuario con la siguiente configuración (deje a los demás con sus valores predeterminados):

Ajuste	Valor
Nombre de usuario	az104-02-aaduser1
Nombre	az104-02-aaduser1
Déjame crear la contraseña	habilitado
Contraseña inicial	Pa55w.rd124

3. **Nota : Copie al portapapeles el nombre de usuario** completo . Lo necesitará más adelante en este laboratorio.
4. En Azure Portal, vuelva al grupo de administración **az104-02-mg1** y muestre sus **detalles** .
5. Haga clic en **Control de acceso (IAM)** , haga clic en + **Agregar** seguido de **Asignación de rol** y asigne el rol **Colaborador de solicitud de soporte (personalizado)** a la cuenta de usuario recién creada.
6. Abra una ventana del explorador de **InPrivate** e **inicie** sesión en [Azure Portal](#) con la cuenta de usuario recién creada. Cuando se le solicite que actualice la contraseña, cambie la contraseña del usuario.

Nota : en lugar de escribir el nombre de usuario, puede pegar el contenido del Portapapeles.
7. En la ventana del explorador de **InPrivate** , en Azure Portal, busque y seleccione **Grupos de recursos** para verificar que el usuario az104-02-aaduser1 pueda ver todos los grupos de recursos.
8. En la ventana del explorador de **InPrivate** , en Azure Portal, busque y seleccione **Todos los recursos** para verificar que el usuario az104-02-aaduser1 no puede ver ningún recurso.
9. En la ventana del navegador **InPrivate** , en Azure Portal, busque y seleccione **Ayuda + soporte** y luego haga clic en + **Nueva solicitud de soporte** .

10. En la ventana del navegador **InPrivate** , en la pestaña **Básico** de **Ayuda + soporte - Nueva** hoja de **solicitud de soporte** , seleccione el tipo de problema de **Límites de suscripción y servicio (cuotas)** y tenga en cuenta que la suscripción que está utilizando en este laboratorio se enumera en la lista desplegable **Suscripción**- lista abajo.

Nota : La presencia de la suscripción que está usando en este laboratorio en la lista desplegable **Suscripción** indica que la cuenta que está usando tiene los permisos necesarios para crear la solicitud de soporte específica de la suscripción.

Nota : Si no ve la opción **Límites de suscripción y servicio (cuotas)** , cierre la sesión en Azure Portal y vuelva a iniciarla.

11. No continúe con la creación de la solicitud de soporte. En su lugar, cierre la sesión como usuario **az104-02-aaduser1** en Azure Portal y cierre la ventana del explorador de InPrivate.

Limpiar recursos

Nota : Recuerde eliminar cualquier recurso de Azure recién creado que ya no use.

Nota : Eliminar los recursos no utilizados garantiza que no verá cargos inesperados, aunque los recursos creados en este laboratorio no incurren en costos adicionales.

1. En Azure Portal, busque y seleccione **Azure Active Directory** , en la hoja de Azure Active Directory, haga clic en **Usuarios** .
2. En la hoja **Usuarios: todos los usuarios** , haga clic en **az104-02-aaduser1** .
3. En la **hoja az104-02-aaduser1 - Perfil** , copie el valor del atributo **ID** de **objeto** .
4. En Azure Portal, inicie una sesión de **PowerShell** dentro de **Cloud Shell** .
5. Desde el panel de Cloud Shell, ejecute lo siguiente para quitar la asignación de la definición de función personalizada (reemplace el [object_ID] marcador de posición con el valor del atributo de **ID de objeto** de la **cuenta de usuario de Azure Active Directory az104-02-aaduser1** que copió anteriormente en esta tarea):
6.

```
$ scope = ( Get-AzRoleAssignment - RoleDefinitionName ' Colaborador de solicitud de soporte (personalizado) ' ) .Scope
```
- 7.

```
Remove-AzRoleAssignment - ObjectId ' [object_ID] ' - RoleDefinitionName  
' Colaborador de solicitud de soporte (personalizado) ' - Alcance $  
scope
```

8. Desde el panel de Cloud Shell, ejecute lo siguiente para quitar la definición de función personalizada:

```
Remove-AzRoleDefinition - Nombre ' Colaborador de solicitud de soporte  
(personalizado) ' - Fuerza
```

9. En Azure Portal, vuelva a la hoja **Usuarios: todos los usuarios** de **Azure Active Directory** y elimine la cuenta de usuario **az104-02-aaduser1** .
10. En Azure Portal, navegue hasta el grupo de administración **az104-02-mg1** y muestre sus **detalles** .
11. Haga clic con el botón derecho en el icono de **puntos suspensivos** a la derecha de la entrada que representa su suscripción de Azure y haga clic en **Mover** .
12. En la hoja **Mover** , seleccione el grupo de administración del que originalmente formaba parte la suscripción y haga clic en **Guardar** .

Nota : Este es el **grupo de administración Tenant Root** , a menos que haya creado una jerarquía de grupos de administración personalizada antes de ejecutar este laboratorio.

1. Vuelva a la hoja **Grupos de administración** , haga clic con el botón derecho en el icono de **puntos suspensivos** a la derecha del grupo de administración **az104-02-mg1** y haga clic en **Eliminar** .

revisión

En este laboratorio, tiene:

- Grupos de gestión implementados
- Se crearon roles RBAC personalizados
- Roles RBAC asignados