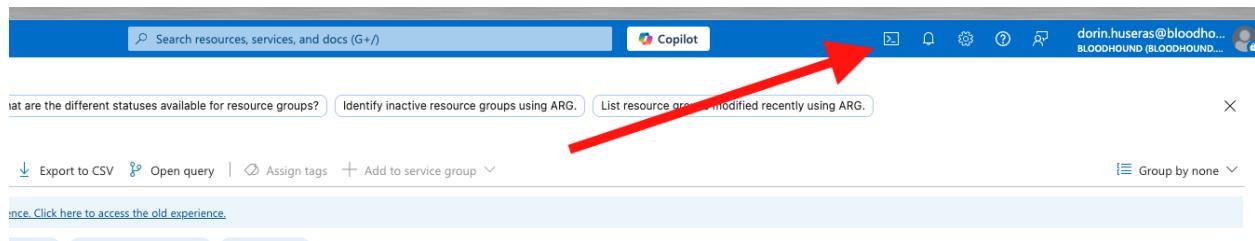


# Create a resource group

## 1. Sign in to Azure Portal

- Navigate to <https://portal.azure.com/>
- Log in with your Azure account.
- Click on the cloud shell button



A screenshot of the Azure portal interface. At the top, there is a search bar, a Copilot button, and a user profile. Below the search bar, there are three cards: "What are the different statuses available for resource groups?", "Identify inactive resource groups using ARG.", and "List resource groups modified recently using ARG.". A red arrow points from the text above to the "Cloud Shell" button, which is located in the top right corner of the main content area. The content area shows a table with columns like "Name", "Status", and "Last modified". At the bottom, there are filter options and a command prompt window containing the command: "az group create --name [yourusername]-rg --location westeurope".

- Run the command:

```
az group create --name [yourusername]-rg --location westeurope
```

## Steps to Create a Resource Lock for a Resource Group

Azure resource locks help prevent accidental deletion or modification of resources. Here are the steps to create a resource lock for a resource group in the Azure Portal:

## 2. Sign in to Azure Portal

- Navigate to <https://portal.azure.com/>
- Log in with your Azure account.

## 3. Select Resource Groups

- In the search bar at the top, type and select “Resource groups”.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar with the placeholder "resource groups". Below it, a navigation menu is open under "Services". The "All" tab is selected, showing "Services (37)" and "Marketplace (2)". Under "Services", there are links for "Resource groups", "Subscriptions", "Resource Manager", and "Marketplace". On the right side of the menu, there are sections for "Resource Manager" and "Marketplace".

#### 4. Choose your Resource Group [yourusername]-rg

- From the list of resource groups, click on [yourusername]-rg

#### 5. Navigate to Locks

- In the resource group blade, under the "Settings" section, click on "Locks".

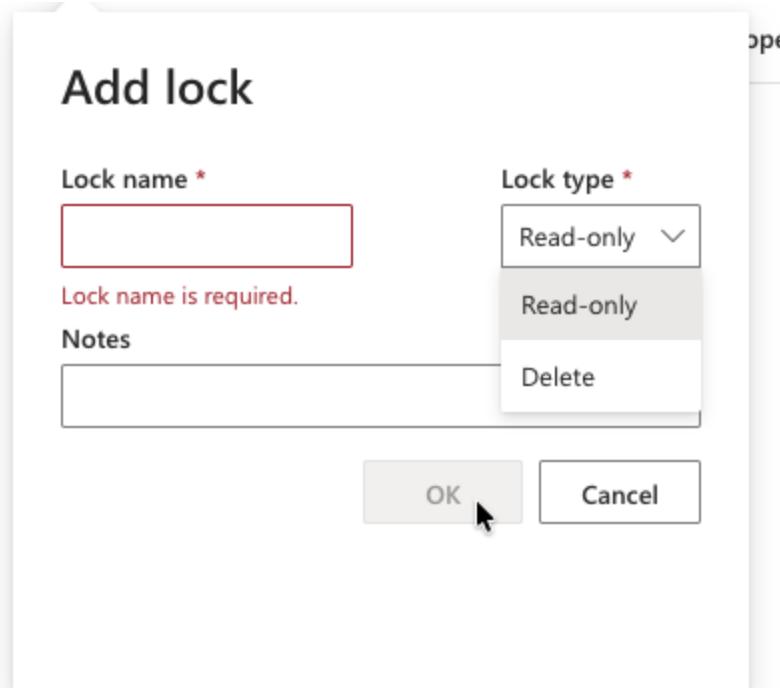
The screenshot shows the "dorinh-rg | Locks" blade. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings (Deployments, Security, Deployment stacks, Policies, Properties, Locks), and Cost Management. The main area shows a table titled "Locks" with columns: Lock name, Lock type, Scope, and Notes. A note at the bottom states "This resource has no locks." At the top of the blade, there are buttons for Search, Add, Refresh, and Feedback.

#### 6. Add a Lock

- Click on the "+ Add" button at the top of the "Locks" blade.

#### 7. Configure the Lock

- Lock name: Provide a unique name for your lock.
- Lock level: Choose between:
  - CanNotDelete:** This allows users to read and modify the resources but prevents them from deleting the resource group or any resources contained within.
  - ReadOnly:** This prevents users from modifying or deleting the resource group or any resources within.
  - Notes (Optional): Provide a description or rationale for the lock. This is especially useful for teams to understand the intent or importance of the lock.
  - Select **ReadOnly** lock.



8. **Save the Lock**
  - a. Click on the "OK" or "Create" button to create the lock.
9. **Verification**
  - a. After you create the lock, you should see it listed in the "Locks" blade for that resource group. This confirms that the lock has been applied to the resource group.

**Note:**

- Remember that while resource locks can prevent unintentional modification or deletion, they can also lead to **confusion** or **disruption** if team members aren't aware of them. Always communicate and document the purpose of resource locks.
- Users need appropriate permissions to **create** or **delete** resource locks. The two key permissions related to managing locks are **Microsoft.Authorization/locks/write** (to create or delete locks) and **Microsoft.Authorization/locks/read** (to view locks).

## Test the Resource lock

### Create a resource

1. Sign in to Azure Portal
2. Navigate to <https://portal.azure.com/>
3. Log in with your Azure account.
4. Click on the cloud shell button

Search resources, services, and docs (G+)

Copilot

Export to CSV | Open query | Assign tags | Add to service group

Group by none

5. Run the command:

```
az storage account create --resource-group [yourusername]-rg --name [yourusername]lab1uqsa --location westeurope --sku Standard_LRS
```

## Delete a resource with a lock

1. Navigate to <https://portal.azure.com/>
  - a. In the search bar, search for storage accounts

storage

All Services (23) Marketplace (31) More (4)

Services

Storage accounts Storage browser

2. Access the Storage account
  - a. Try to delete it
  - b. Observe the error message

dorinlab1uqsa Storage account

Storage is retiring support for TLS 1.0 and 1.1 starting Feb 3, 2026. If you

Overview Activity log Tags Diagnose and solve problems Access Control (IAM) Data migration Events Storage browser

Resource group (dorin-rg) Location (westerurope) Subscription (move) Subscription ID (8d82146a-0138-4a26-884b-37480942ecd8) Disk state (Available) Tags (edit) : Add tags

3. Modify the storage account
  - a. Create a new Container

The screenshot shows the Azure Storage center interface. On the left, there's a sidebar with various navigation options like Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Partner solutions, Resource visualizer, and Data storage. The 'Containers' option is selected. The main area shows a list of containers with a search bar and buttons for Add container, Upload, Refresh, Delete, Change access level, and Restore containers. A note at the bottom says 'Showing all 0 items' and 'No items found'. On the right, a modal window titled 'New container' is open. It has fields for 'Name' (set to 'testcontainer'), 'Anonymous access level' (set to 'Private (no anonymous access)'), and a note stating 'The access level is set to private because anonymous access is disabled on this storage account'. There's also an 'Advanced' section.

4. Click on "Save".
5. Review the Outcome
6. Observe the error message (if any) after attempting to save.
7. Delete the lock

