

Lock resources to prevent unexpected changes

- [Overview](#)
- [Problem](#)
- [Solution](#)
 - [Who can create or delete locks](#)
 - [You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.](#)
 - [Configure locks](#)
 - [Portal](#)

Overview

Platform:	Azure
Owner of this SOP:	Fully Managed POD A
Cloud Services:	Azure Resource Lock

Problem

Resource Lock enable & disable

tester	Reviewer
@ Ayush Tripathi	

Solution

As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

Who can create or delete locks

To create or delete management locks, you must have access to `Microsoft.Authorization/*` or `Microsoft.Authorization/locks/*` actions. Of the built-in roles, only **Owner** and **User Access Administrator** are granted those actions.

Please note:

Cloud Factory's default position is the **Owner** permission should be granted to customers who wish to manage resource locks.

In the situation where a customer does not wish owner permission to be granted, a more granular solution can be used as per the below process:

1. Update in-place an additional path to `assignableScopes` in the JSON for the "Resource Lock Manager" custom role. This means you can extend the custom roles usage to other scopes. Right now its assigned to `/subscriptions/65f41d0e-1076-40d7-956b-8c2694f8bf62/resourceGroups/it-npe-cleopatra_dev-arg`.
2. Create a new Azure AD group with members in it who wish to have Resource Lock Manager permissions.
`New-AzADGroup -DisplayName "azure-cleopatra-npe-arg-resourcelockmanager" -MailNickname "NotSet"`
`Add-AzADGroupMember -MemberUserPrincipalName "piyush.banerjee@bhp.com" -TargetGroupDisplayName "azure-cleopatra-npe-arg-resourcelockmanager"`
3. Create a new role assignment which assigns the group you created the Resource Lock Manager custom role on a scope
`New-AzRoleAssignment -ObjectId 5dc72535-e306-4255-8179-394d119ebb76 -Scope "/subscriptions/65f41d0e-1076-40d7-956b-8c2694f8bf62/resourceGroups/it-npe-cleopatra_dev-arg" -RoleDefinitionName "Resource Lock Manager"`

You can set the lock level to `CanNotDelete` or `ReadOnly`. In the portal, the locks are called Delete and Read-only respectively.

- `CanNotDelete` means authorized users can still read and modify a resource, but they can't delete the resource.

`ReadOnly` means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

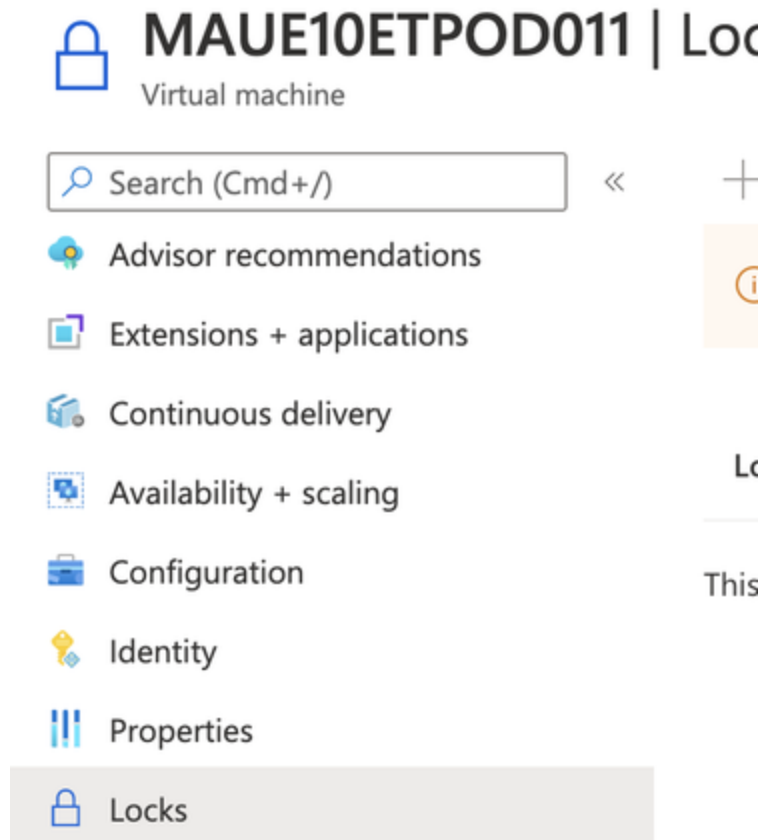
Lock inheritance

When you apply a lock at a parent scope, all resources within that scope inherit the same lock. Even resources you add later inherit the lock from the parent. The most restrictive lock in the inheritance takes precedence.

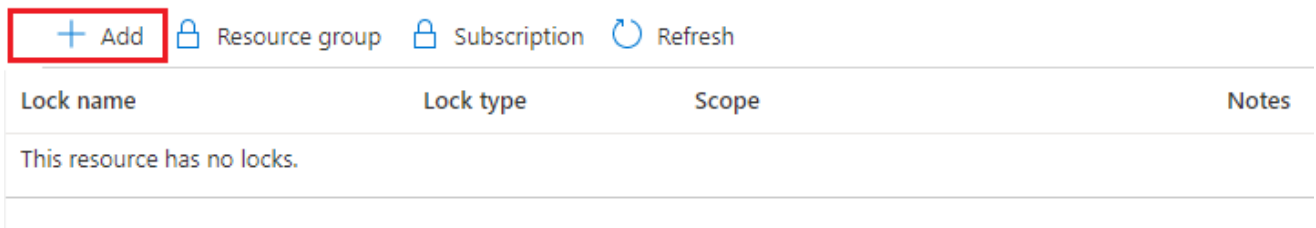
Configure locks

Portal

1. In the Settings blade for the resource, resource group, or subscription that you wish to lock, select **Locks**.



2. To add a lock, select **Add**. If you want to create a lock at a parent level, select the parent. The currently selected resource inherits the lock from the parent. For example, you could lock the resource group to apply a lock to all its resources.



3. Give the lock a name and lock level. Optionally, you can add notes that describe the lock.

[+ Add](#) [🔒 Resource group](#) [🔒 Subscription](#) [🔄 Refresh](#)

Add lock

Lock name

DatabaseServerLock ✓

Lock type

Delete ▼

Notes




Prevent deleting the database server.

OK

Cancel

4. To delete the lock, select the **Delete** button.

[+ Add](#) [🔒 Resource group](#) [🔒 Subscription](#) [🔄 Refresh](#)

Lock name	Lock type	Scope	Notes	
DatabaseServerLock	Delete	 databaseserverexample0503	Prevent deleting the database server.	 Edit  Delete