Resource Governance in Azure

Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

Azure Resource Manager locks

Azure Policy

Azure Resource Manager Locks

Azure Resource Locks

Azure resource locks are a feature of Azure Resource Manager

- Deployment and management service for Azure

Azure resource locks allows you to lock a resource to prevent accidental modification or deletion

- This is in addition to Azure role-based access control

RBAC in Azure vs. Entra ID

Entra ID Role-based Access Control	VS	Azure Role-based Access Control
Microsoft Entra roles control access to Microsoft Entra resources such as users, groups, and applications using the Microsoft Graph API		Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management

Two Lock Options

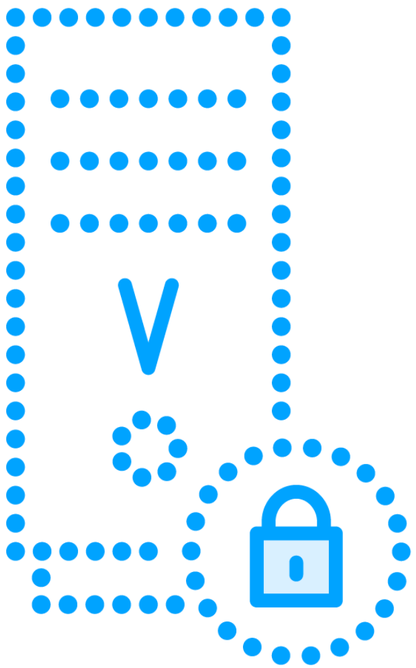
CanNotDelete

Authorized users can read and modify a resource – but cannot delete it

ReadOnly

Authorized users can read a resource – but cannot delete or update it

How Locks Are Applied



Locks can be applied to

- A subscription
- A resource group
- A resource

When a lock is applied at a parent scope all resources within that scope inherit the lock

- Even future resources

A resource can have more than one lock

- Most restrictive lock takes precedence

Locks Only Apply to Management Actions

A lock does not restrict the resource from operating normally

A SQL Server with a ReadOnly lock

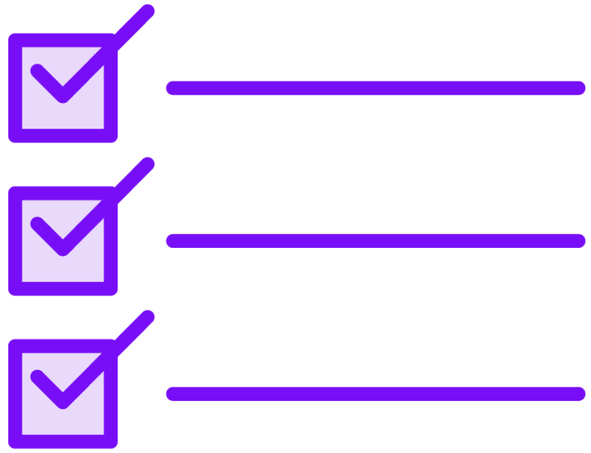
- You cannot modify or delete the server
- You can still create, update, or delete data in the databases on that server

Demo

Azure resource locks

Azure Policy

Azure Policy



Helps enforce organizational standards and assess compliance at scale

A policy is made of business rules

- JSON policy definitions

Multiple business rules can be grouped together to form an initiative

- Makes deployment easier

Can be deployed at multiple levels

- Subscriptions
- Resource groups
- Individual resources

Sample Policies

Azure Backup should be enabled for virtual machines

API app should only be accessible over HTTPS

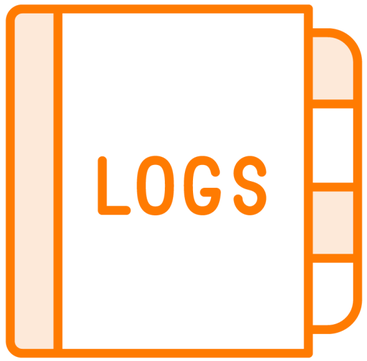
Allowed virtual machine size SKUs

Require a tag on resources

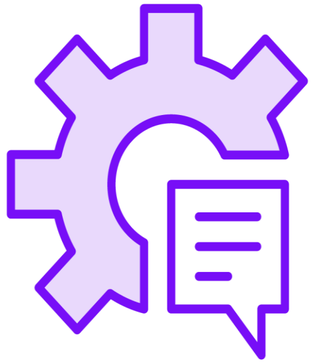
Resource logs in Logic apps should be enabled

Responses to a Non-compliant Resource

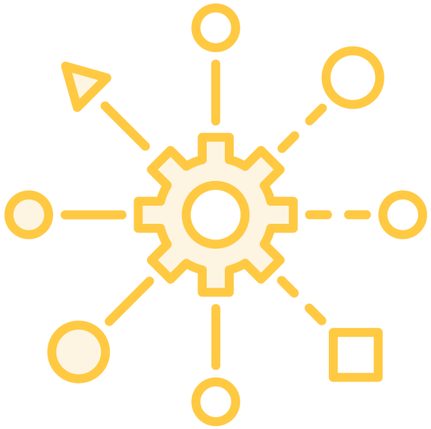
Deny a change to a resource



Log the change to the resource

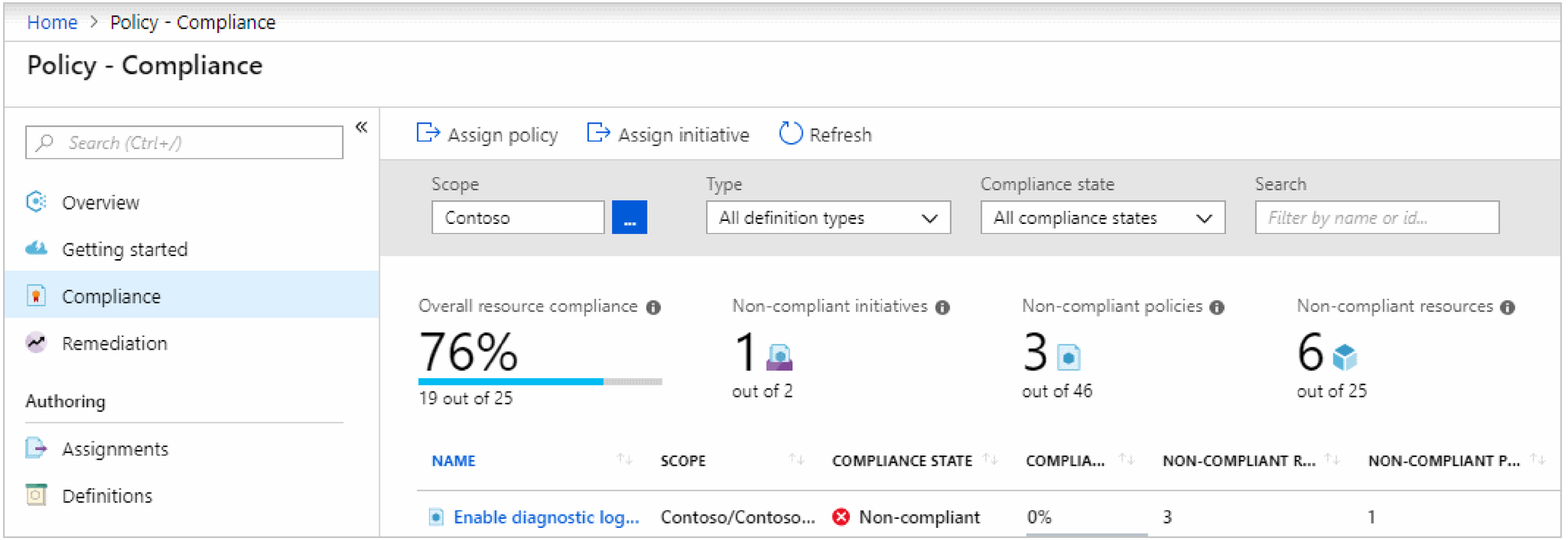


Alter a resource before or after a change



Deploy related compliant resources

Compliance Dashboard



Source: https://learn.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data

Module Conclusion

Azure Resource Manager locks

- Prevents accidental modification or deletion of resources

Azure Policy

- Enforce organizational standards and assess compliance at scale

Up Next:

Course Conclusion