Azure Cloud Hardening Lab

Author: Alan Chavez  
Date: May 2025  
Version: 1.0

# 1. Executive Summary

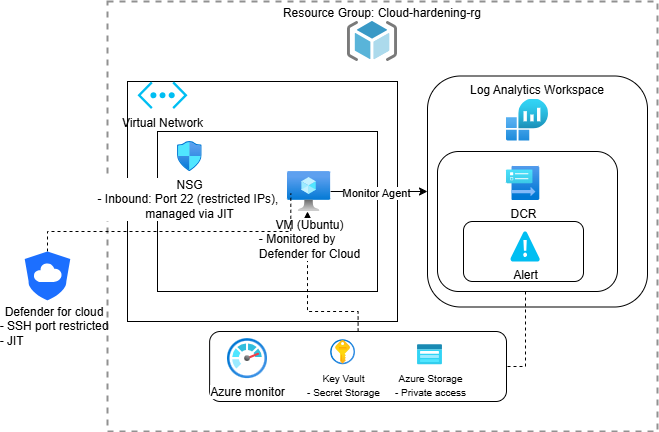
This report documents the implementation of a cloud hardening lab using Microsoft Azure. The goal was to secure an Ubuntu virtual machine by implementing Just-In-Time (JIT) access, restricted NSG rules, and centralized monitoring via Azure-native tools such as Azure Monitor and Log Analytics. The lab demonstrates best practices in cloud security monitoring and alerting.

# 2. Objectives

- Harden access to a VM using JIT and NSG.  
- Monitor cloud resources with Azure Monitor.  
- Set up centralized logging and alerting.  
- Detect suspicious activity such as SSH brute-force attempts.

# 3. Architecture Overview

The following diagram illustrates the core components of the cloud hardening lab.



# 4. Implementation Steps

1. Create Resource Group and Virtual Network

A screenshot of a computer

AI-generated content may be incorrect.

Why? Essential for good hygiene, it makes it easier to manage, monitor, secure resources together

A screenshot of a computer

AI-generated content may be incorrect.

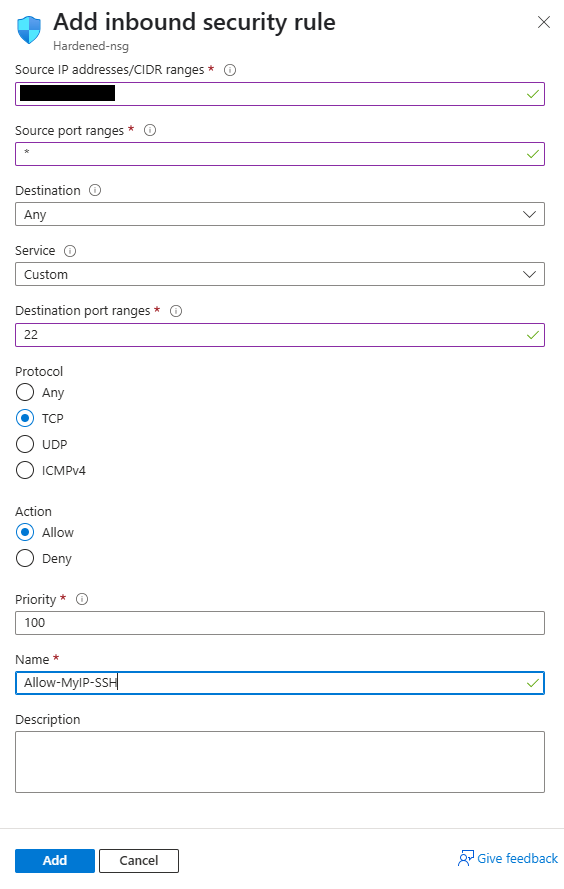
Why? Created a dedicated NSG to tightly control traffic flow into the hardened VM.

2. Deploy Ubuntu VM with SSH & JIT enabled

A screenshot of a computer

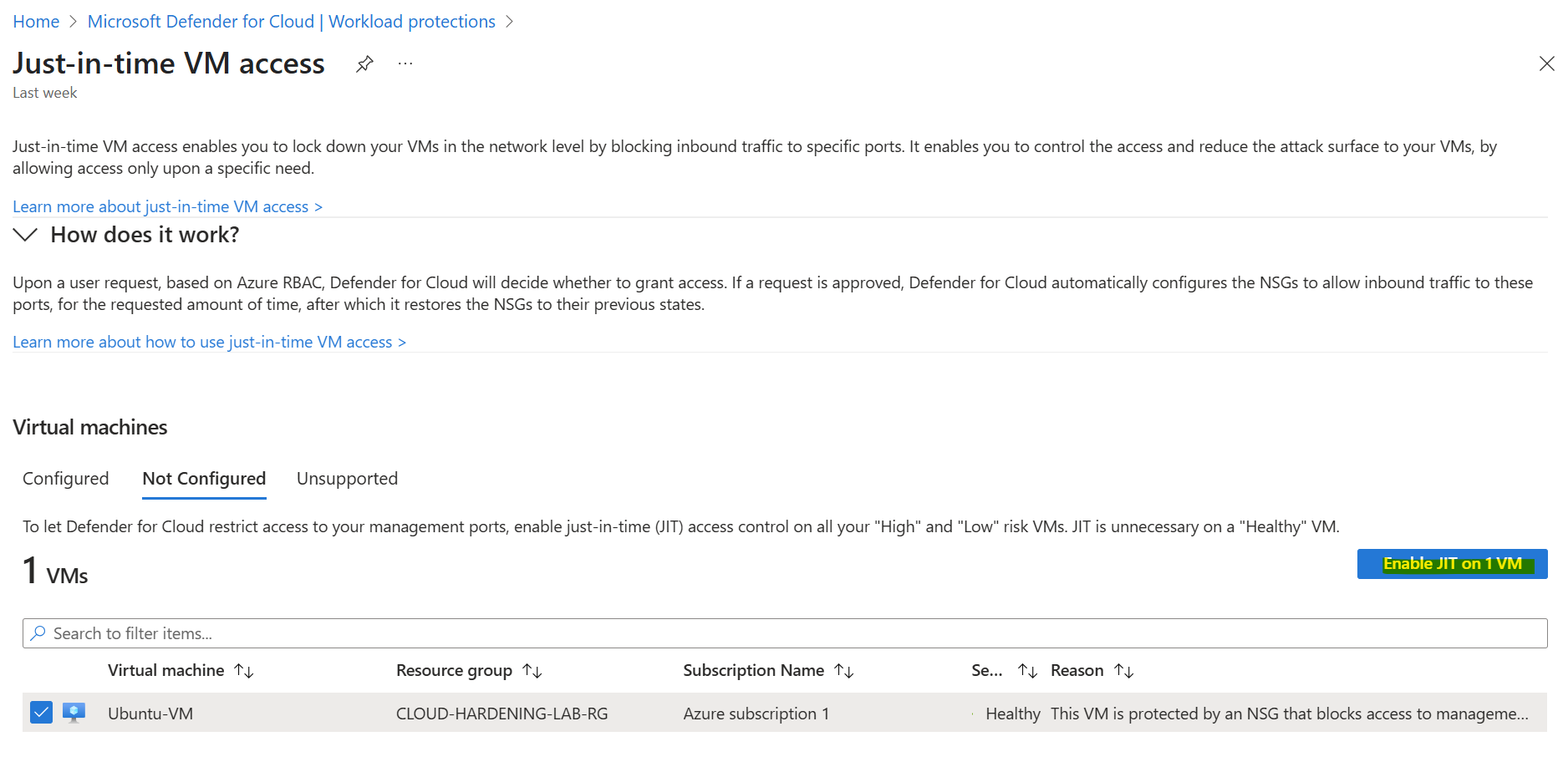
AI-generated content may be incorrect.

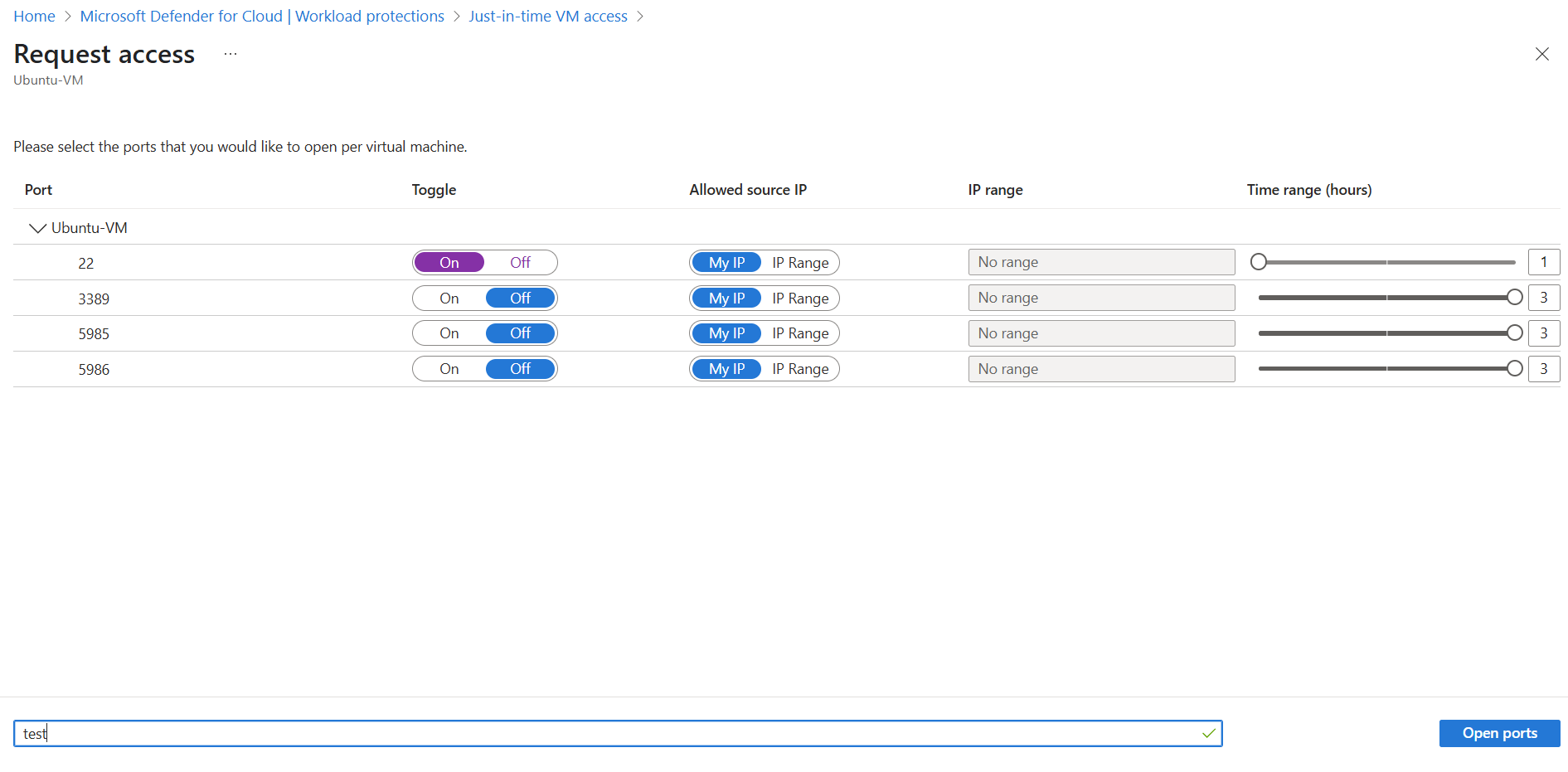
3. Configure NSG with port 22 restrictions



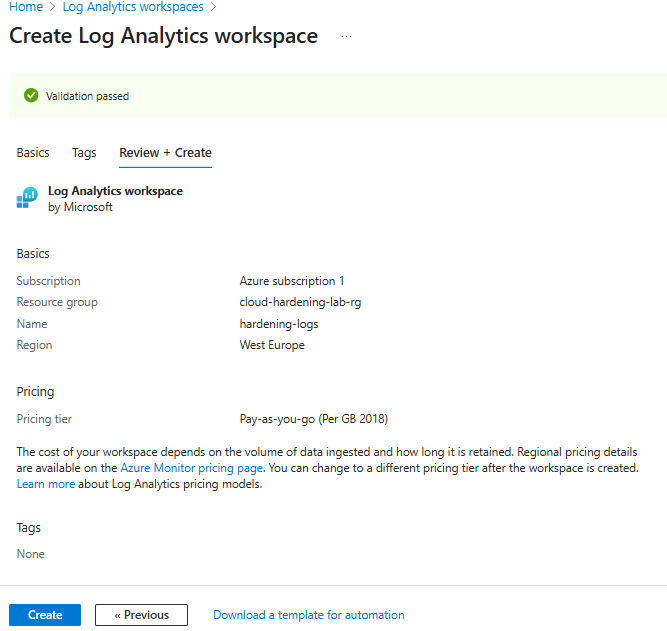
Restricted inbound management traffic to only trusted IP address.

4. Enable Microsoft Defender for Cloud & JIT



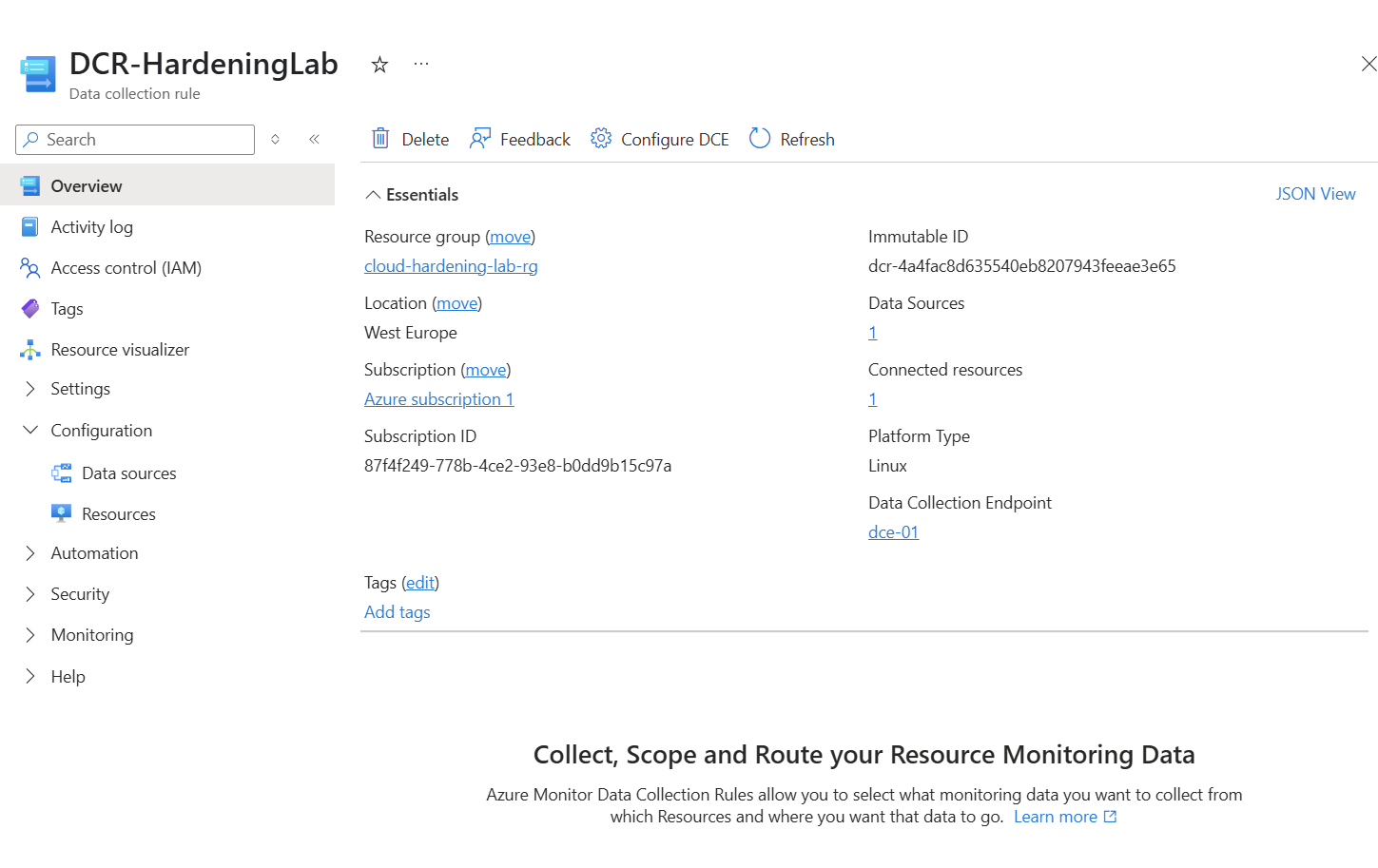


5. Link the VM to Log Analytics Workspace



Why: Created a Log Analytics workspace (hardening-logs) to centralize VM telemetry and support alerting.

6. Create Data Collection Rules and Alerts



Why? DCRs are required when using Azure Monitor Agent — they define what to collect, from where, and where to send it.

7. Monitor Virtual Machine

A screenshot of a computer

AI-generated content may be incorrect.

Why? Connect VM to Log Analytics and enabled Insights to monitor CPU, memory, disk, and security events in real time

8. Create Alert for SSH brute-force attempts

Screens screenshot of a computer

AI-generated content may be incorrect.

9. Execution

Local VM triggering Alert

A screen shot of a computer

AI-generated content may be incorrect.

Monitor > Alerts > Fired Alerts

A screenshot of a computer

AI-generated content may be incorrect.

This alert simulates real-world brute-force detection and prepares for automated response actions in future phases.

# 5. Security Considerations

- Just-In-Time (JIT) access limits open ports  
- NSG rules restrict exposure to specific IPs  
- Monitoring agents provide visibility into logs and metrics  
- Alerting helps detect brute-force or suspicious behavior

# 6. Findings / Results

Alerts successfully triggered for SSH brute-force attempts. Key Vault and Storage activity logs were monitored via Azure Monitor. NSG logs showed minimal external access due to JIT restrictions.

# 7. Conclusion

This lab successfully demonstrated Azure cloud security best practices. Future improvements could include integration with Microsoft Sentinel, additional resource types, and automated alert response.

# 8. Appendix

- Alert rule definitions - <https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview>   
- Log samples - <https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-tutorial>   
- GitHub link to project repo - <https://github.com/akaheric/Cybersecurity-Lab-Portafolio/tree/main/azure-cloud-labs/hardening-lab>