

ASSIGNMENT TWO: MICROSOFT DEFENDER FOR CLOUD

WRITEUP

BY CS-CNS03-23082 – ABUOR ISABELLA MERCY

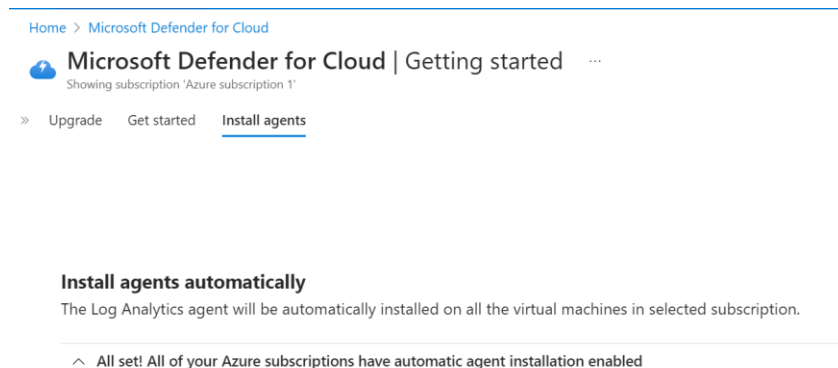
INTRODUCTION

This lab is a continuation of the previous lab exercise which takes us on a journey for azure security center which will be performing three different tasks. One in which we configure Microsoft Defender for Cloud, the second task focused on reviewing the Microsoft Defender for Cloud recommendations and lastly the third task was on implementing the Microsoft Defender for Cloud recommendation to enable Just-in-time VM Access. The following is a descriptive writeup on how the above task were achieved.

Task 1: Configure Microsoft Defender for Cloud

In this task, we configured Microsoft Defender for Cloud by clicking upgrade to the getting started blade Microsoft Defender for Cloud section.

After that on the Microsoft Defender for Cloud, Getting started blade, in the Install agents tab, we installed agents.



We then selected the workspaces with enhanced security features section is visible » turn on the Microsoft Defender plan by selecting your Log Analytics Workspace, then click the large Blue Upgrade button.

Home > Microsoft Defender for Cloud




Microsoft Defender for Cloud | Getting started ...

Showing subscription 'Azure subscription 1'


>> **Upgrade** Get started Install agents

Enable Defender for Cloud on 1 workspaces

<input checked="" type="checkbox"/>	Name	↑↓	Total resources	Microsoft Defender plan
<input checked="" type="checkbox"/>	 student		1	Off

Upgrade

We then navigated to Microsoft Defender for Cloud and clicked Environment Settings under the Management settings, clicked on the relevant subscription to Enable all Microsoft Defender for Cloud Plans.

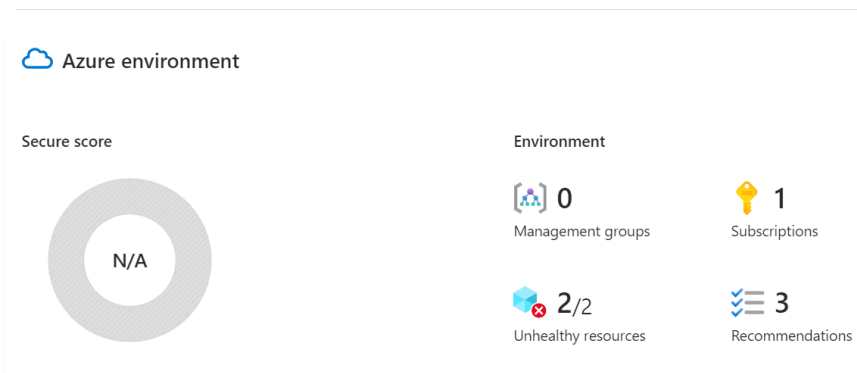
 Defender for Cloud plans will be enabled on 2 resources in this subscription

^ Select Defender plan by resource type **Enable all**

Task 2: Review the Microsoft Defender for Cloud recommendation

This task describes a step by step process on reviewing and confirming the Microsoft Defender for Cloud recommendations.

On the Microsoft Defender for Cloud | Overview blade, review the Secure Score tile.



On the Inventory blade, select the myVM entry. On the Resource health blade, on the Recommendations tab, review the list of recommendations for myVM.

Home > Microsoft Defender for Cloud | Overview > Inventory >

Resource health

myvm

virtual machine

4

Active recommendations

0

Active alerts

Resource information

Subscription

Azure subscription 1

Resource Group

az500lab131415

Environment

Azure

Location

eastus

Recommendations

Alerts

Installed applications

Secrets

Search

More (2)

Severity	Description	Status
High	Endpoint protection should be installed on machines	Healthy
High	Management ports of virtual machines should be protected with just-in-time net	Unhealthy
High	Internet-facing virtual machines should be protected with network security group	N/A - Unspe...
High	Adaptive application controls for defining safe applications should be enabled or	N/A - Unspe...

Task 3: Implement the Microsoft Defender for Cloud recommendation to enable Just-in-time VM Access

In this task, we implemented the Microsoft Defender for Cloud recommendation to enable Just-in-time VM Access on the virtual machine. Through the Microsoft Defender for Cloud in the overview blade and selected the Workload protections under Cloud Security tile.

On the Workload protections blade, in the Advanced protection section, click the Just-in-time VM access tile. On the Just-in-time VM access blade, under the Virtual machines section, select Not Configured and then click the myVM entry and enable JIT on VM option.

Home > Microsoft Defender for Cloud | Overview > Workload protections >

Just-in-time VM access

Last week

Upon a user request, based on Azure RBAC, Defender for Cloud will decide whether to grant access. If a request is approved, Defender for Cloud automatically configures the NSGs to allow inbound traffic to these ports, for the requested amount of time, after which it restores the NSGs to their previous states.

Learn more about how to use just-in-time VM access >

Virtual machines

Configured

Not Configured

Unsupported

To let Defender for Cloud restrict access to your management ports, enable just-in-time (JIT) access control on all your "High" and "Low" risk VMs. JIT is unnecessary on a "Healthy" VM.

2 VMs

Enable JIT on 1 VM

Search to filter items...

Virtual machine	Resource group	Subscription Name	Se...	Reason
<input type="checkbox"/> az500-10-vm1	AZ500LAB10	Azure subscription 1	High	This VM is protected by an NSG that allows access to managem...
<input checked="" type="checkbox"/> myVM	AZ500LAB131415	Azure subscription 1	High	This VM is protected by an NSG that allows access to managem...

On the JIT VM access configuration blade, on the far right of the row referencing the port 22, click the ellipsis button and then click Delete and then Save.

JIT VM access configuration

myVM



+ Add Save X Discard

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)	
22 (Recommended)	Any	Per request	N/A	3 hours	Delete ...
3389 (Recommended)	Any	Per request	N/A	3 hours	...
5985 (Recommended)	Any	Per request	N/A	3 hours	...

CONCLUSION

In conclusion, learning how to work the Microsoft defender to add extra protection against potential problems. This helps us spot where our setup might be at risk. The last task is all about putting this advice into action by turning on something called Just-in-time VM Access, which makes sure our virtual machines are only accessible when needed. These tasks together give us a strong grasp of how to make our Azure environment more secure. By finishing this journey, we've not only learned more but also gained practical skills to keep our Azure setup safe from new security issues.