



## Securing Azure with Defender and JIT

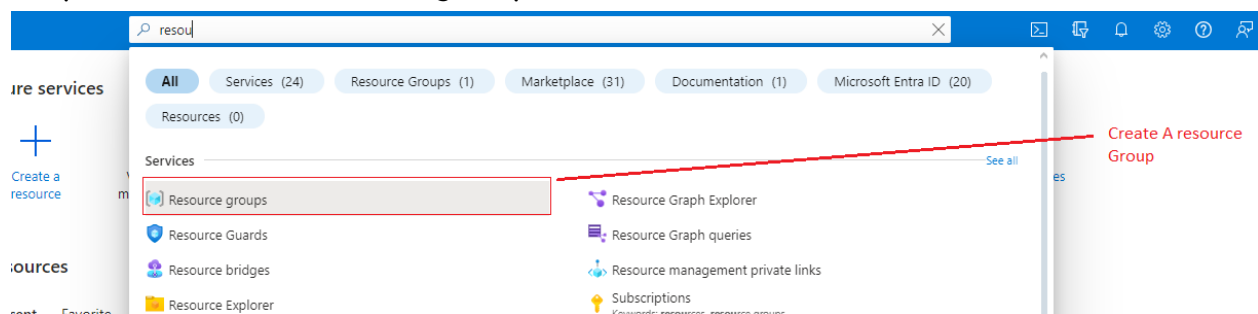
Empowering Azure Defenses: A Step-by-Step Guide to Implement Microsoft Defender for Cloud and Just-in-time Virtual Machine Access!

### Scenario:

An organization has deployed virtual machines (VMs) on Azure to run business-critical applications. These VMs are accessible over the internet, and there is a potential threat of brute-force attacks on the Remote Desktop Protocol (RDP) port (3389). We will secure such VM using JIT and MS defender

### Implementation:

#### Step 1: Create a resource group



## Step 1.1: Name the resourceGroup

### Create a resource group ...

Basics Tags Review + create

**Resource group** - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

#### Project details

Subscription \* ⓘ

Azure subscription 1

Resource group \* ⓘ

JIT\_VM

#### Resource details

Region \* ⓘ

(US) East US

Select resourceGroup  
Name

Review + create

< Previous

Next : Tags >

## Step 2: Enable Microsoft Defender for Cloud

**Microsoft Defender for Cloud | Environment settings**

Showing subscription 'Azure subscription 1'

Search

General

- Overview
- Getting started
- Recommendations
- Attack path analysis
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Data security
- Firewall Manager
- DevOps security

Management

- Environment settings**

Buttons: Add environment, Refresh, Guides & Feedback, Cost estimator, Defender Plans Coverage

Metrics:

- Azure subscriptions: 1
- AWS accounts: 0
- GCP projects: 0
- GitHub connectors: 0
- AzureDevOps connectors: 0
- GitLab connectors: 0

0 Total issues

0 GCP Projects, 0 AWS Accounts, 0 AzureDevOps Connectors

Search by name

Environments == All Standards == All Coverage == All Connectivity status == All

Collapse all

Name	Total resources	Connectivity status	Defender coverage
Azure			
Tenant Root Group (1 of 1 subscriptions)	1		
Azure subscription 1	1		0/12 plans

### Step 2.1 Enable all to enable all the plans for Microsoft Defender for Cloud.

**Settings | Defender plans**

Azure subscription 1

Search

Save Settings & monitoring

Settings

- Defender plans**
- Security policies
- Email notifications
- Workflow automation
- Continuous export

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free <a href="#">Details &gt;</a>		Full	Off On
Defender CSPM	\$5/Billable resource/Month <a href="#">Details &gt;</a>	1 resources	Full <a href="#">Settings &gt;</a>	Off On

Cloud Workload Protection (CWP)

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (\$15/Server/Month) <a href="#">Change plan &gt;</a>	0 servers	Full <a href="#">Settings &gt;</a>	Off On
App Service	\$15/Instance/Month <a href="#">Details &gt;</a>	0 instances	Full	Off On
Databases	Selected: 0/4 <a href="#">Select types &gt;</a>	Protected: 0/0 instances	Full <a href="#">Settings &gt;</a>	Off On
Storage	\$10/Storage account/month \$0.15/GB scanned for On-Upload Malware Scanning (configural) <a href="#">Details &gt;</a>	1 storage accounts	Full <a href="#">Settings &gt;</a>	Off On
Containers	\$7/VM core/Month <a href="#">Details &gt;</a>	0 container registries; 0 kubernetes cores	Full <a href="#">Settings &gt;</a>	Off On
Key Vault	\$0.25/Vault/Month <a href="#">Details &gt;</a>	0 key vaults	Full	Off On
Resource Manager	\$5/Subscription/Month <a href="#">Details &gt;</a>		Full	Off On
APIs	Plan 1 (Free until February 2024) <a href="#">Details &gt;</a>	0 Azure API Management services	Action required	Off On

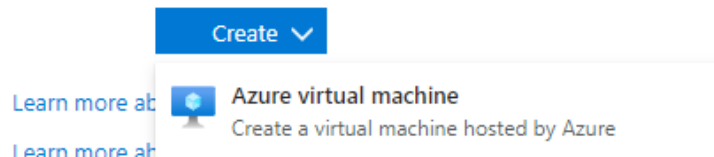
All Plans are enabled

Name	Total resources	Connectivity status	Defender coverage
Azure			
Tenant Root Group (1 of 1 subscriptions)	1		
Azure subscription 1	1		12/12 plans

Step3: Make a VM in East US with x64, set RDP (3389) for inbound, and enable JIT.

## No virtual machines to display

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.



## Step 3.1

### Create a virtual machine ...

#### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Resource group \* ⓘ  [Create new](#)

#### Instance details

Virtual machine name \* ⓘ  ✓

Region \* ⓘ

Availability options ⓘ

Availability zone \* ⓘ

✓ You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type ⓘ  [Configure security features](#)

Image \* ⓘ  [See all images](#) | [Configure VM generation](#)

VM architecture ⓘ ☐ Arm64 ☒ x64

Select inbound ports \*

## 3.2 Enable JIT Access

Go to Config from settings; under Just-in-time VM access, enable it. When done, a notification will appear. On Config page, choose Open Microsoft Defender for Cloud.


[Home](#) > [CreateVm-MicrosoftWindowsServer.WindowsServer-201-20240105024545 | Overview](#) > [VirtualMachineForJIT](#)

### VirtualMachineForJIT | Configuration ☆ ⋮


Virtual machine

 confi × «

#### Settings

 Configuration



#### Operations

 Configuration management

#### Just-in-time VM access

To improve security, enable a just-in-time access.

[Enable just-in-time](#)

 Just-in-time VM access secures your VM's management ports and grants access on-demand, for a limited time period, to pre-approved IP addresses. [Learn more about just-in-time access](#) 

#### Just-in-time VM access

Just-in-time VM access (JIT) is enabled. To disable JIT, modify the configuration, or request access.

[Open Microsoft Defender for Cloud](#)

Step 3.3:  
On the Request access page of your VM, Toggle On the port (e.g., Remote Desktop port 3389). Set hours to keep it open. After time expires, the port(s) close, and access is denied.

Virtual machines

Configured Not Configured Unsupported

VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.

1 VMs

Request access

Search to filter items...

Virtual machine	Approved	Last access	Connection details	Last user
<input type="checkbox"/> VirtualMachineForJIT	0 Requests	N/A	-	N/A

Step 3.4 Choose VM, then request access to open management port

Virtual machines

Configured Not Configured Unsupported

VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.

1 VMs

Request access

Search to filter items...

Virtual machine	Approved	Last access	Connection details	Last user
<input checked="" type="checkbox"/> VirtualMachineForJIT	0 Requests	N/A	-	N/A

# Request access

VirtualMachineForJIT

Please select the ports that you would like to open per virtual machine.

Port

Toggle

VirtualMachineForJIT

3389

On Off

Final step VM is live to test and play

Virtual machines

Configured Not Configured Unsupported

VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.

1 VMs

Request access

Search to filter items...

Virtual machi...	Approved	Last access	Connection det...	Last user
<input type="checkbox"/> VirtualMachineFor...	1 Requests	Active now	Ports: 3389	live.com#muham...

# Lastly Don't Forget to disable Defender trail

Defender CSPM

\$5/Billable resource/Month  
[Details >](#)

2 resources ⓘ

Off

On

Cloud Workload Protection (CWP)

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (\$15/Server/Month) ⓘ <a href="#">Change plan &gt;</a>	1 servers		<div>Off</div> <div>On</div>
App Service	\$15/Instance/Month ⓘ <a href="#">Details &gt;</a>	0 instances		<div>Off</div> <div>On</div>
Databases	Selected: 0/4 ⓘ <a href="#">Select types &gt;</a>	Protected: 0/0 instances		<div>Off</div> <div>On</div>
Storage	\$10/Storage account/month \$0.15/GB scanned for On-Upload Malware Scanning (configura <a href="#">Details &gt;</a>	1 storage accounts		<div>Off</div> <div>On</div>
Containers	\$7/VM core/Month ⓘ <a href="#">Details &gt;</a>	0 container registries; 0 kubernetes cores		<div>Off</div> <div>On</div>
Key Vault	\$0.25/Vault/Month <a href="#">Details &gt;</a>	0 key vaults		<div>Off</div> <div>On</div>
Resource Manager	\$5/Subscription/Month ⓘ <a href="#">Details &gt;</a>			<div>Off</div> <div>On</div>
APIs	Plan 1 (Free until February 2024) ⓘ <a href="#">Details &gt;</a>	0 Azure API Management services		<div>Off</div> <div>On</div>

# Delete resource

Ontology-based Cy... Series and Parallel Ci... How to Secure Dock... Page Not Found | D... Page Not Found | D...

Microsoft Azure

Search resources, services, and docs (G+)

PowerShell

Requesting a Cloud Shell.Succeeded.  
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI  
Type "help" to learn about Cloud Shell

MOTD: SqlServer has been updated to Version 22!

VERBOSE: Authenticating to Azure ...  
VERBOSE: Building your Azure drive ...  
PS /home/muhammad> Remove-AzResourceGroup -Name "JIT\_VM" -Force -AsJob

Id	Name	PSJobTypeName	State	HasMoreData	Location	Command
2	Long Running O...	AzureLongRunni...	Running	True	localhost	Remove-AzResourceGroup

PS /home/muhammad>