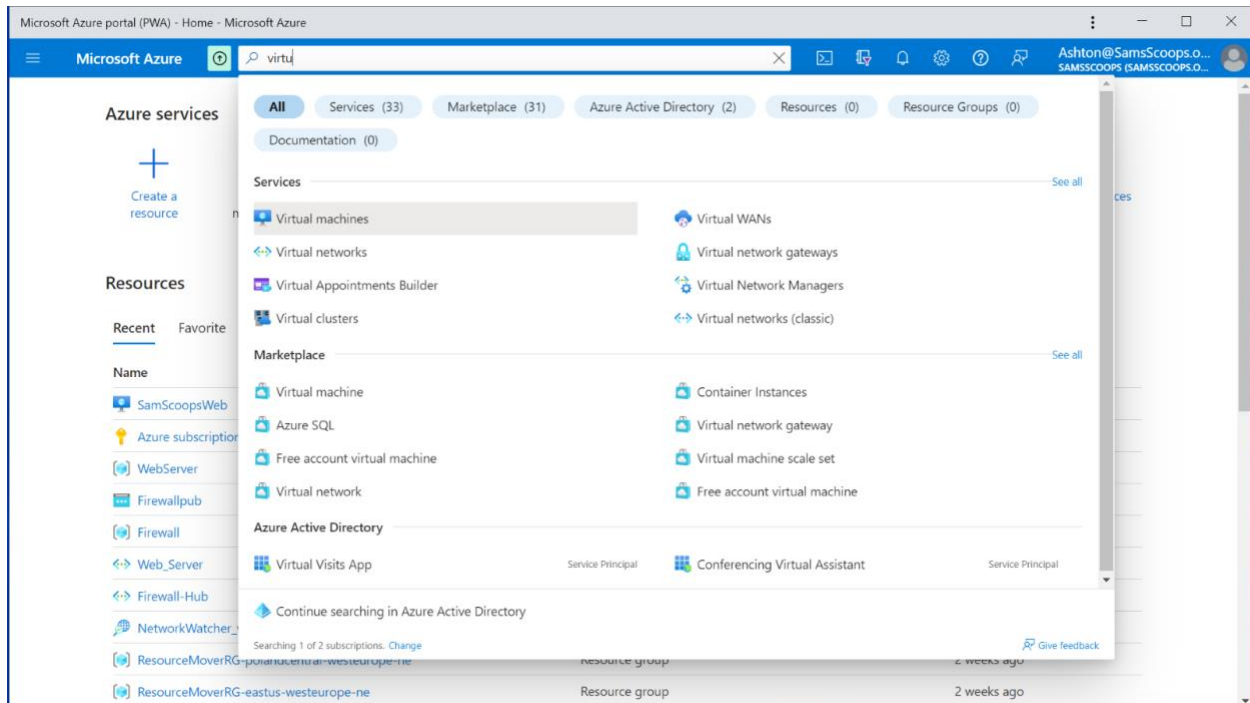


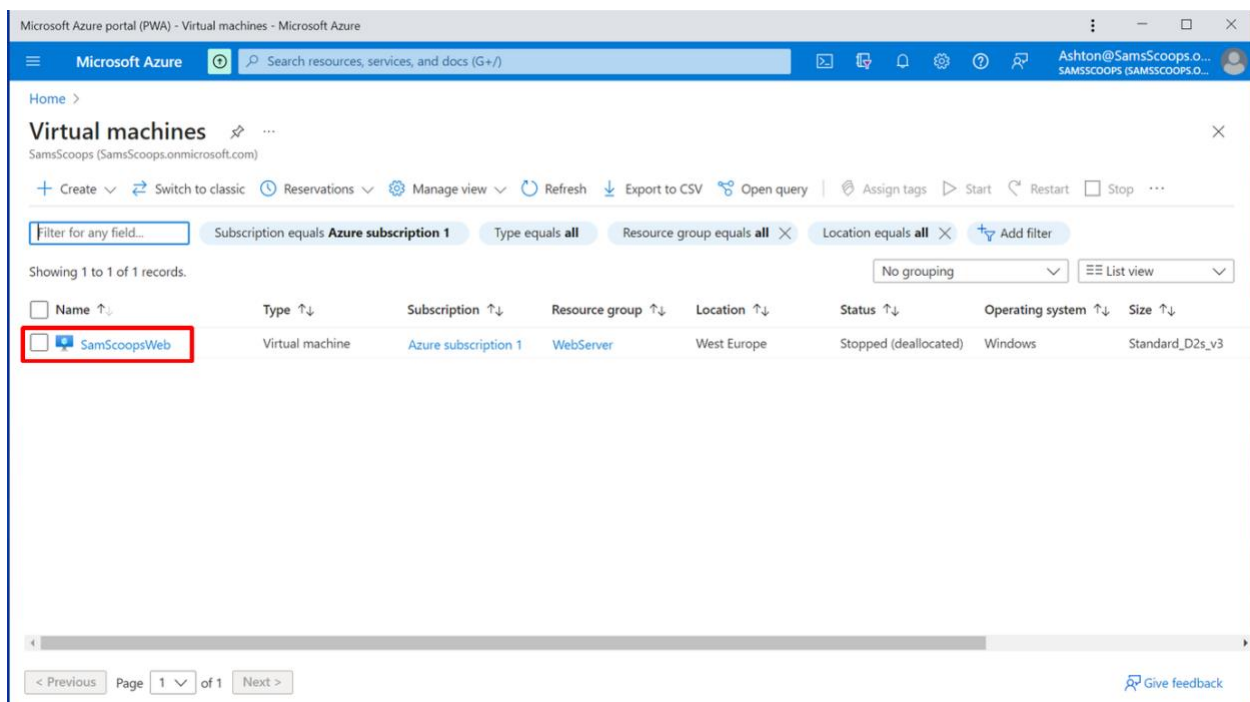
# Just-In-Time Configuration in Cloud

## Step 1: Enable Azure Defender for cloud

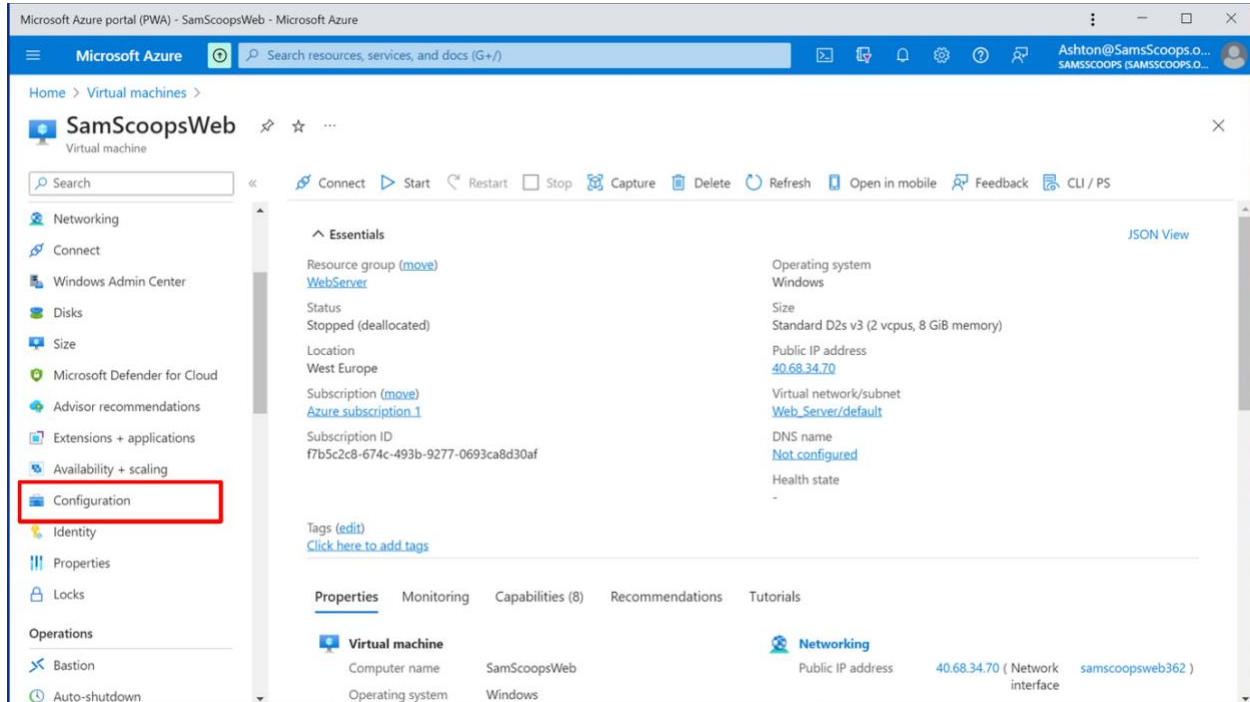
I started by selecting virtual machines from the home page of azure account.



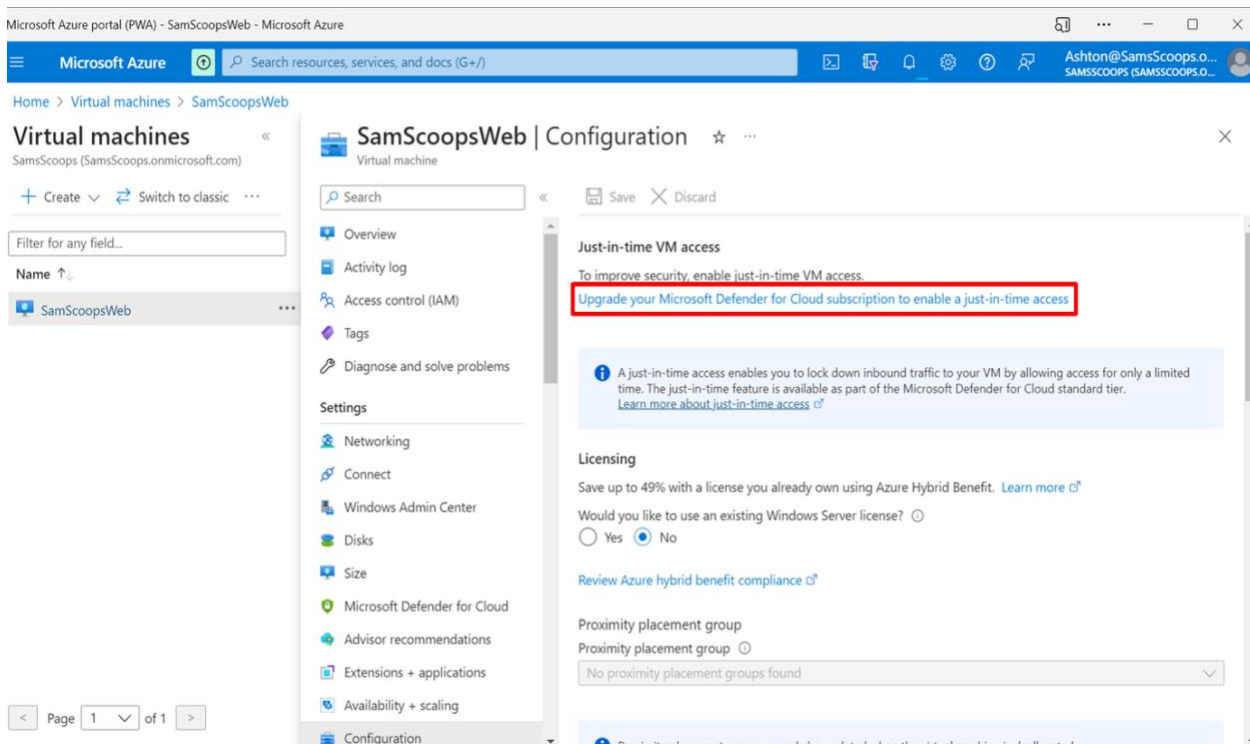
2. I choose the samscoopsweb machine because that is the machine that I want to create JIT.



3. Select **Configuration** from the left-hand side menu.



4. Select **Upgrade your Microsoft Defender for Cloud subscription to enable a just-in-time access.**



5. Select **Upgrade** on the **Microsoft Defender for Cloud** page.

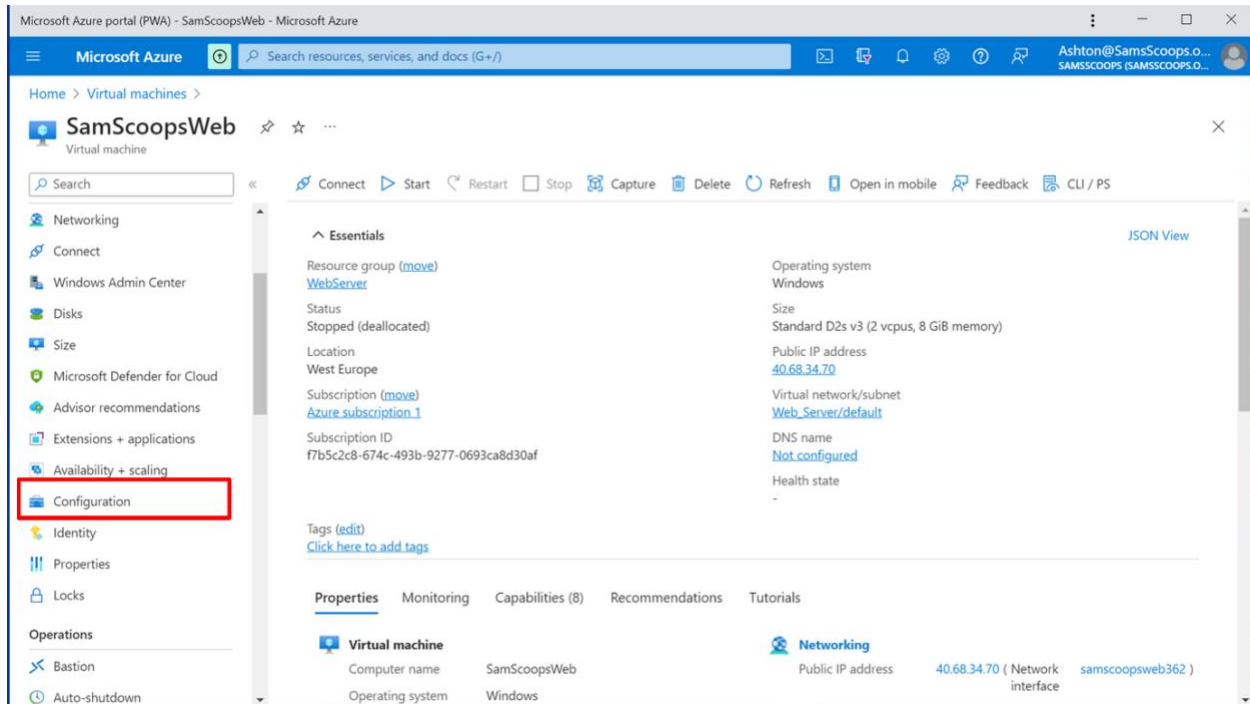
The screenshot shows the Microsoft Azure portal (PWA) for Microsoft Defender for Cloud. The breadcrumb trail is: Home > Virtual machines > SamScoopsWeb | Configuration > Microsoft Defender for Cloud. The page title is "Microsoft Defender for Cloud | Getting started". Below the title, it says "Showing subscription 'Azure subscription 1'". The left sidebar contains a search bar and a list of navigation items: Inventory, Cloud Security Explorer, Workbooks, Community, Diagnose and solve problems, Cloud Security (with sub-items: Security posture, Regulatory compliance, Workload protections, Firewall Manager, DevOps Security (Preview)), and Management (with sub-items: Environment settings, Security solutions, Workflow automation). The main content area has three tabs: "Upgrade" (selected), "Get started", and "Install agents". The "Upgrade" tab displays a large heading "Enable Microsoft Defender for Cloud's enhanced security features on your subscriptions." followed by "Get started with a 30-day free trial". Below this, it says "Upgrade to get advanced capabilities including hybrid support, networking, security policies, just-in-time administration and adaptive application controls. [Learn more >](#)". There are three feature cards: "Cloud security posture management", "Cloud workload protection for machines", and "Advanced threat protection for PaaS". At the bottom of the main content area, there is a red-bordered button labeled "Upgrade".

6. Select **continue without installing agents** on the right-hand side.

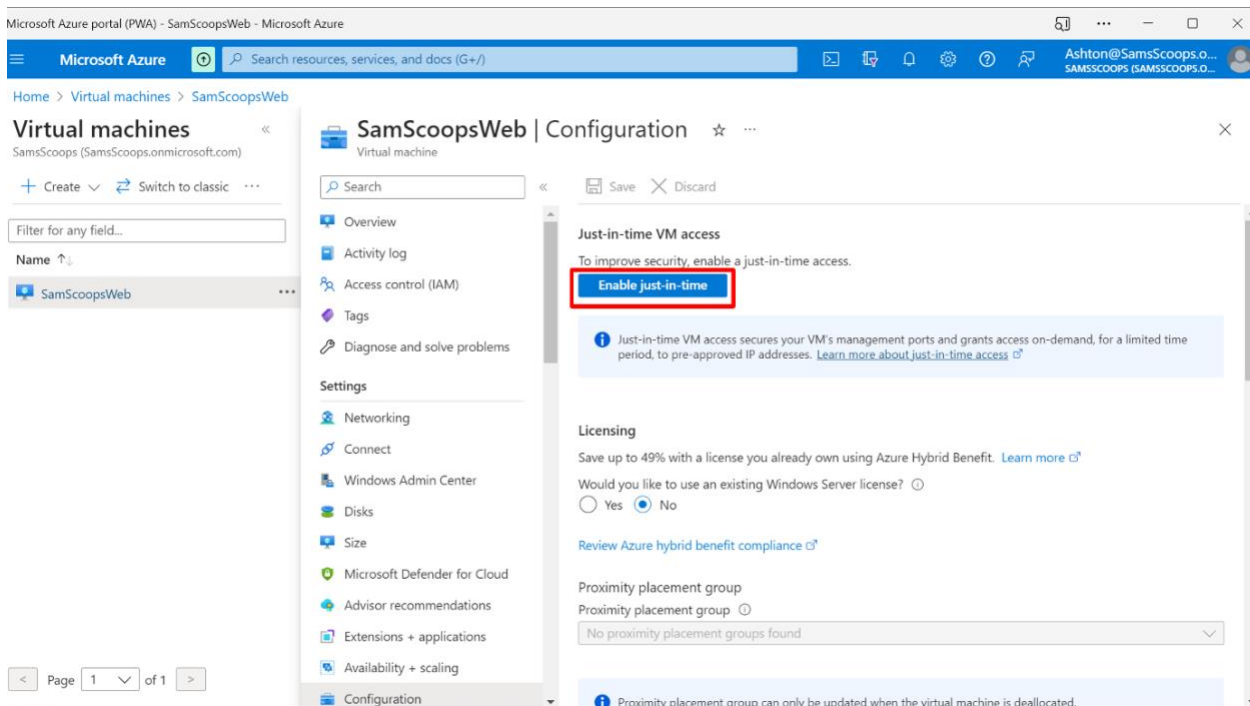
The screenshot shows the Microsoft Azure portal (PWA) for Microsoft Defender for Cloud, specifically the "Install agents" tab. The breadcrumb trail is: Home > Virtual machines > SamScoopsWeb | Configuration > Microsoft Defender for Cloud. The page title is "Microsoft Defender for Cloud | Getting started". Below the title, it says "Showing subscription 'Azure subscription 1'". The left sidebar is the same as in the previous screenshot. The main content area has three tabs: "Upgrade", "Get started", and "Install agents" (selected). The "Install agents" tab displays a large heading "Make the most of Defender for Cloud by enabling data collection agents". Below this, it says "To receive security alerts and recommendations, agents must be installed on your virtual machines for data collection. [Learn more >](#)". There are two main sections: "Install agents automatically" and "Continue without installing agents". The "Install agents automatically" section states "The Log Analytics agent will be automatically installed on all the virtual machines in selected subscription." and shows a status "All set! All of your Azure subscriptions have automatic agent installation enabled". The "Continue without installing agents" section states "Many important security features won't work if you don't install agents." and has a red-bordered button labeled "Continue without installing agents".

## Step 2: Enable JIT access

Moving on to create JIT access, select configuration for the panel on the left side.

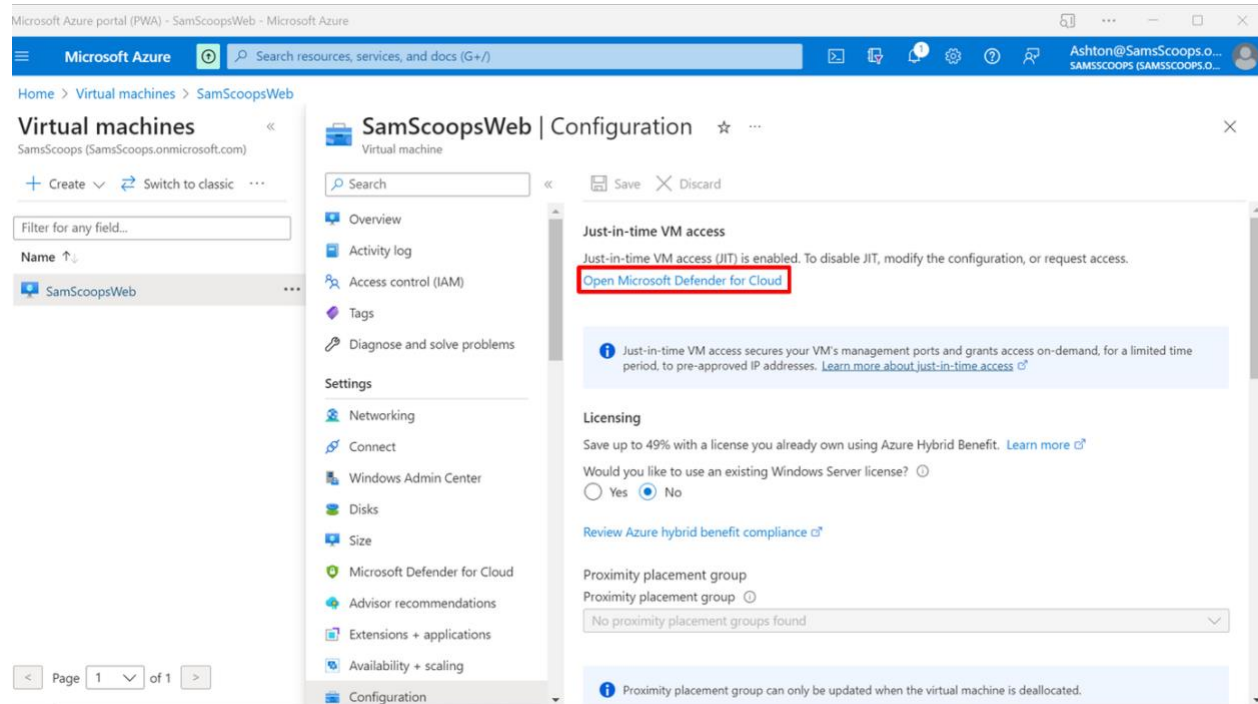


Select **Enable just-in-time**.

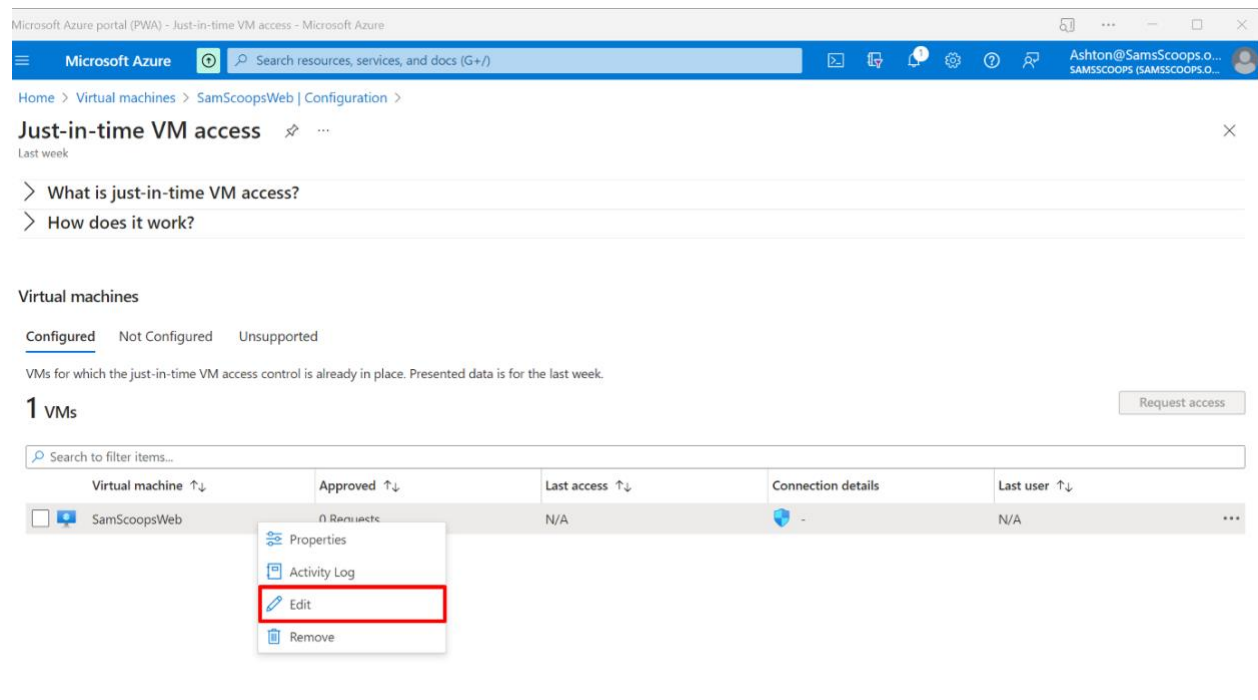


### Step 3: Configure JIT policies for SSH and RDP from Microsoft Defender for Cloud

From the SamScoopsWeb Configuration page select **Open Microsoft Defender for Cloud**.



From **Configured** tab, right-click on the VM to which you want to add a port, select Edit.





To add SSH select **Add** and add the port number for SSH which is **22**.

Microsoft Azure portal (PWA) - JIT VM access configuration - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+/I)

Home > Virtual machines > SamScoopsWeb | Configuration > Just-in-time VM access >

### JIT VM access configuration

SamScoopsWeb

**+ Add** Save 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)	
3389	Any	Per request	N/A	3 hours	...

Select **TCP** and leave the defaults.

Microsoft Azure portal (PWA) - Add port configuration - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+/I)

Home > Virtual machines > SamScoopsWeb | Configuration > Just-in-time VM access >

### JIT VM access configuration

SamScoopsWeb

**+ Add** Save Discard

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

Port	Protocol	Allowed source IPs	IP range
3389	Any	Per request	N/A

#### Add port configuration

Port \*  
22 ✓

Protocol  
Any TCP UDP

Allowed source IPs  
Per request CIDR block

IP addresses ⓘ

Max request time  
3 (hours)

Discard **OK**

Microsoft Azure portal (PWA) - JIT VM access configuration - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+/)

Ashton@SamsScoops.o... SAMSSCOOPS (SAMSSCOOPS.O...)

Home > Virtual machines > SamScoopsWeb | Configuration > Just-in-time VM access >

## JIT VM access configuration

SamScoopsWeb

+ Add Save 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)
3389	Any	Per request	N/A	3 hours
22	TCP	Per request	N/A	3 hours

## Step 4: Test remote access

To test, start the virtual machine,

Microsoft Azure portal (PWA) - SamScoopsWeb - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+/)

Ashton@SamsScoops.o... SAMSSCOOPS (SAMSSCOOPS.O...)

Home > Virtual machines >

## Virtual machines

SamScoops (SamsScoops.onmicrosoft.com)

+ Create Switch to classic

Filter for any field...

Name

SamScoopsWeb

### SamScoopsWeb

Virtual machine

Search

Connect Start Restart Stop Capture Delete Refresh

Advisor (1 of 5): Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources

#### Essentials

Resource group (move) [WebServer](#)

Operating system: Windows

Status: Stopped (deallocated)

Size: Standard D2s v3 (2 vcpus, 8 GiB memory)

Location: West Europe

Public IP address: [51.124.205.99](#)

Subscription (move) [Azure subscription 1](#)

Virtual network/subnet: [Web\\_Server/default](#)

Subscription ID: f7b5c2c8-674c-493b-9277-0693ca8d30af

DNS name: [Not configured](#)

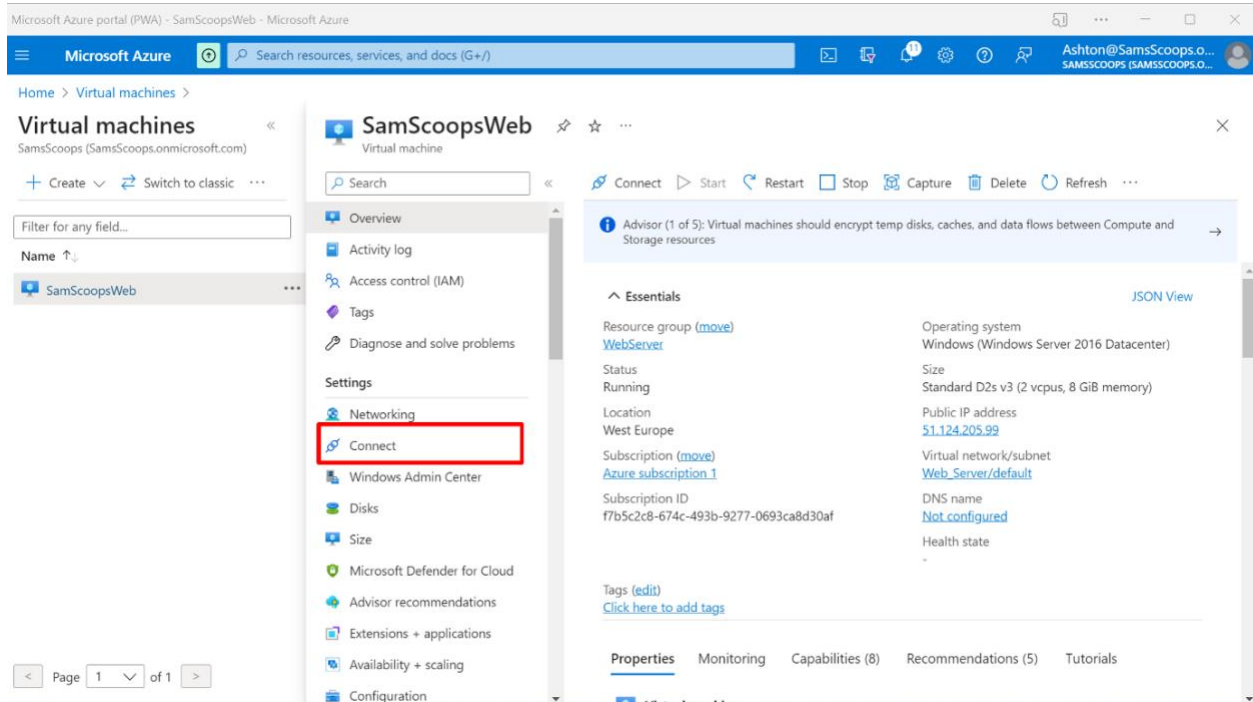
Health state: -

Tags (edit) [Click here to add tags](#)

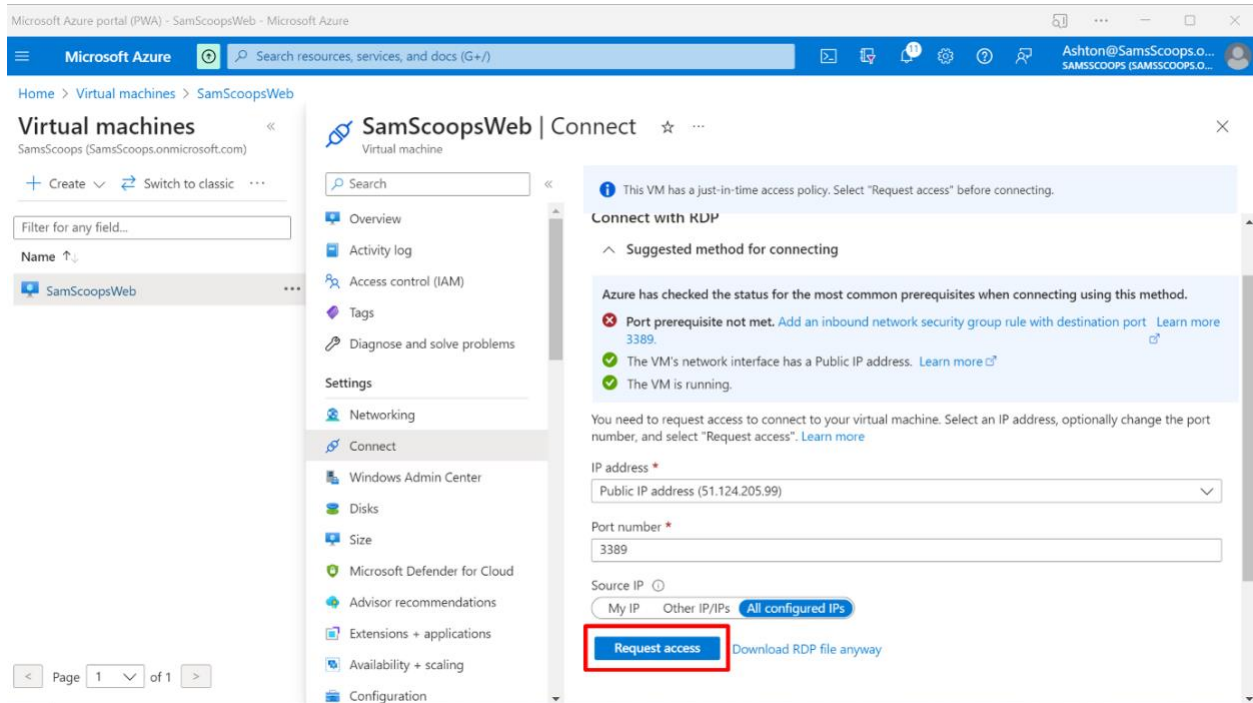
Properties Monitoring Capabilities (8) Recommendations (5) Tutorials

Page 1 of 1

6. Select **Connect** from the left-hand menu.



7. Select **Request access**.





8. Select **Download RDP file**.

Microsoft Azure portal (PWA) - SamScoopsWeb - Microsoft Azure

Home > Virtual machines > SamScoopsWeb

Virtual machines  
Samscoops (Samscoops.onmicrosoft.com)

Filter for any field...

Name ↑

SamScoopsWeb

Search

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems

Settings

Networking  
Connect  
Windows Admin Center  
Disks  
Size  
Microsoft Defender for Cloud  
Advisor recommendations  
Extensions + applications  
Availability + scaling  
Configuration

Connect with RDP

Suggested method for connecting

Azure has checked the status for the most common prerequisites when connecting using this method.

- Port prerequisite not met. Add an inbound network security group rule with destination port 3389. [Learn more](#)
- The VM's network interface has a Public IP address. [Learn more](#)
- The VM is running.

Just-in-time access approved. To connect to your virtual machine via RDP, download the RDP file.

IP address \*

Public IP address (51.124.205.99)

Port number

3389

Source IP

My IP Other IP/IPv6 All configured IPv6

**Download RDP File**

Can't connect?

9. Select the downloaded RDP file from your downloads folder.

10. Select **Connect**.

Remote Desktop Connection

The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

Publisher: **Unknown publisher**

Type: Remote Desktop Connection

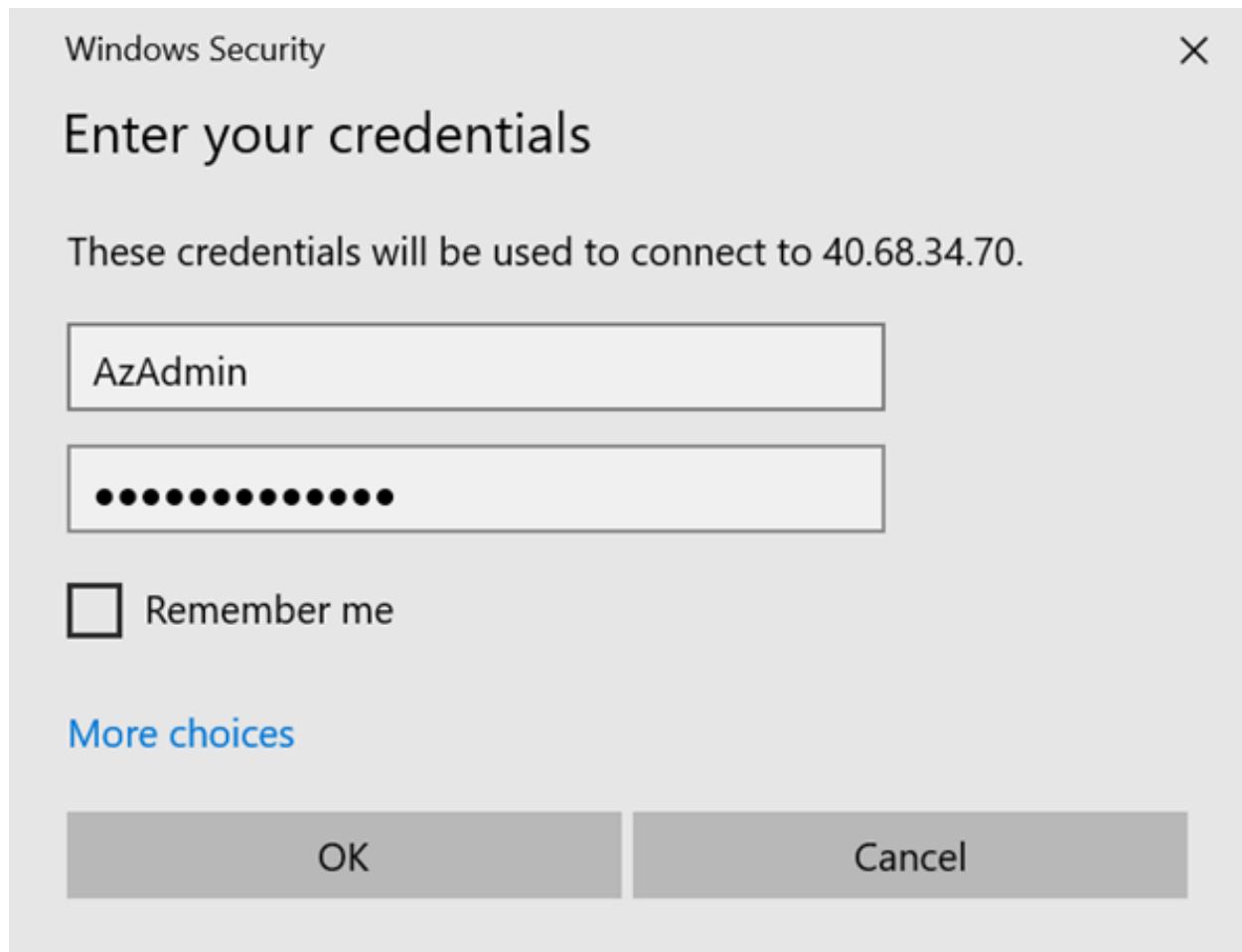
Remote computer: 40.68.34.70

☐ Don't ask me again for connections to this computer

Show Details

**Connect** Cancel

11. Enter the username **AzAdmin** and the password **P@\$\$@1234567** and select **OK**.



You have now connected to the webserver using JIT access and you should see a window like the one below.

(Ref: Microsoft Cybersecurity Professional Certificate)