

Securing virtual machines

Case study

A small business that provides IT services has a number of systems hosted in Microsoft Azure. The backend systems are hosted on Azure virtual machines, and they need to be securely configured and protected from threats.

You have been hired as a security engineer to put together a testing environment using the many different Microsoft security services. This testing environment will form the basis for how production VMs will be protected in the future for this IT services provider.

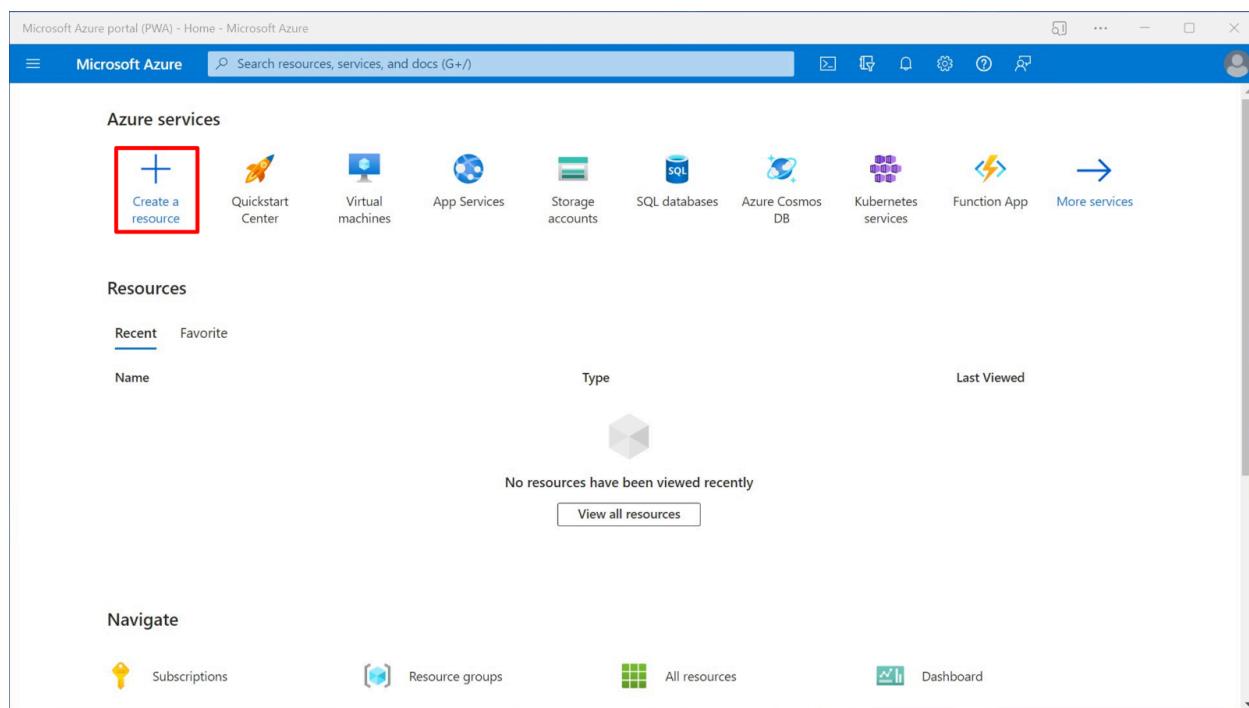
Your employer would like you to set up protection for a virtual machine in Azure using JIT, Azure Bastion, and Azure Standard Firewall. Once this has been set up, they would also like you to configure Microsoft Sentinel to monitor the testing environment before it is deployed on the production network.

Instructions

Step 1: Virtual machine setup

To start building a testing environment a virtual machine is needed first. Deploy a virtual machine in a new resource group. No public IP will be needed for this VM as Azure Bastion will be used for remote access. Revisit the video about [Spinning up a virtual machine](#) for a reminder on how to create virtual machines.

1. Sign into the [Azure portal](#) with your credentials.
2. In the Azure portal menu, select the **Create a resource** button located on the left-hand side of the screen.



The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo, a search bar, and various icons for account management and help. Below the header, the main content area is divided into sections:

- Azure services:** A row of icons for different Azure services, with the "Create a resource" button (a plus sign inside a red square) highlighted by a red box.
- Resources:** A table showing recent resources. The columns are "Name", "Type", and "Last Viewed". It displays a single entry: "No resources have been viewed recently".
- Navigation:** A footer section with links for "Subscriptions", "Resource groups", "All resources", and "Dashboard".

3. Next, search for “virtual network” in the search bar, select **Virtual machine** from the results and then select **Create**.

Microsoft Azure portal (PWA) - Marketplace - Microsoft Azure

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

Home > Create a resource > Marketplace

Get Started Service Providers Management Private Marketplace Private Offer Management My Marketplace Favorites Recently created Private products Categories Compute (2538) IT & Management Tools (1692) Developer Tools (1418)

virtual machine

Pricing : All Operating System : All Publisher Type : All Product Type : All

Azure services only

Showing 1 to 20 of 7271 results for 'virtual machine'. Clear search

Tile view

Virtual machine
Microsoft Azure Service
Azure Virtual Machines provide on-demand, high-scale, secure and virtualized infrastructure using either Linux or Windows operating systems.

Virtual machine scale set
Microsoft Azure Service
Deploy multiple instances of a single image.

Free account virtual machine
Microsoft Azure Service
Azure free account users get up to 1500 free virtual machine hours each month.

Free account virtual machine
Microsoft Azure Service
Azure free account users get up to 1500 free virtual machine hours each month.

Create Create Create Create

Is Marketplace helpful?

4. In the **Basics** tab of the **Create a virtual machine** wizard, fill out the following information:

- Subscription: select your subscription.
- Resource group: **Create new** and enter "Services_Test" as the name of the new resource group.
- Name: Enter "ServicesVM" as the name of the virtual machine.
- Region: Select the region that is closest to you.
- Image: **Windows Server 2022 Datacenter: Azure Edition.**

Microsoft Azure portal (PWA) - Create a virtual machine - Microsoft Azure

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

Home > Create a resource > Marketplace >

Create a virtual machine

Subscription * (New) Services_Test

Resource group * Create new

Instance details

Virtual machine name * ServicesVM

Region * (US) East US

Availability options No infrastructure redundancy required

Security type Trusted launch virtual machines

Image * Windows Server 2022 Datacenter: Azure Edition - x64 Gen2

VM architecture x64

Review + create < Previous Next : Disks > Give feedback

Scroll down and complete the rest of the details.

- Size: **Standard_DS1_v2**
- Username: **AzAdmin**
- Password: **P@\$\$@1234567**
- Confirm password: **P@\$\$@1234567**

Microsoft Azure portal (PWA) - Create a virtual machine - Microsoft Azure

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

Home > Create a resource > Marketplace >

Create a virtual machine

Run with Azure Spot discount

Size * Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (\$91.98/month)

Administrator account

Username * AzAdmin

Password * *****

Confirm password * *****

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * None

Select inbound ports * RDP (3389)

Review + create < Previous Next : Disks > Give feedback

5. Select Next: Disks.

Microsoft Azure portal (PWA) - Create a virtual machine - Microsoft Azure

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

Home > Create a resource > Marketplace >

Create a virtual machine

Run with Azure Spot discount

Size *

Administrator account

Username *

Password *

Confirm password *

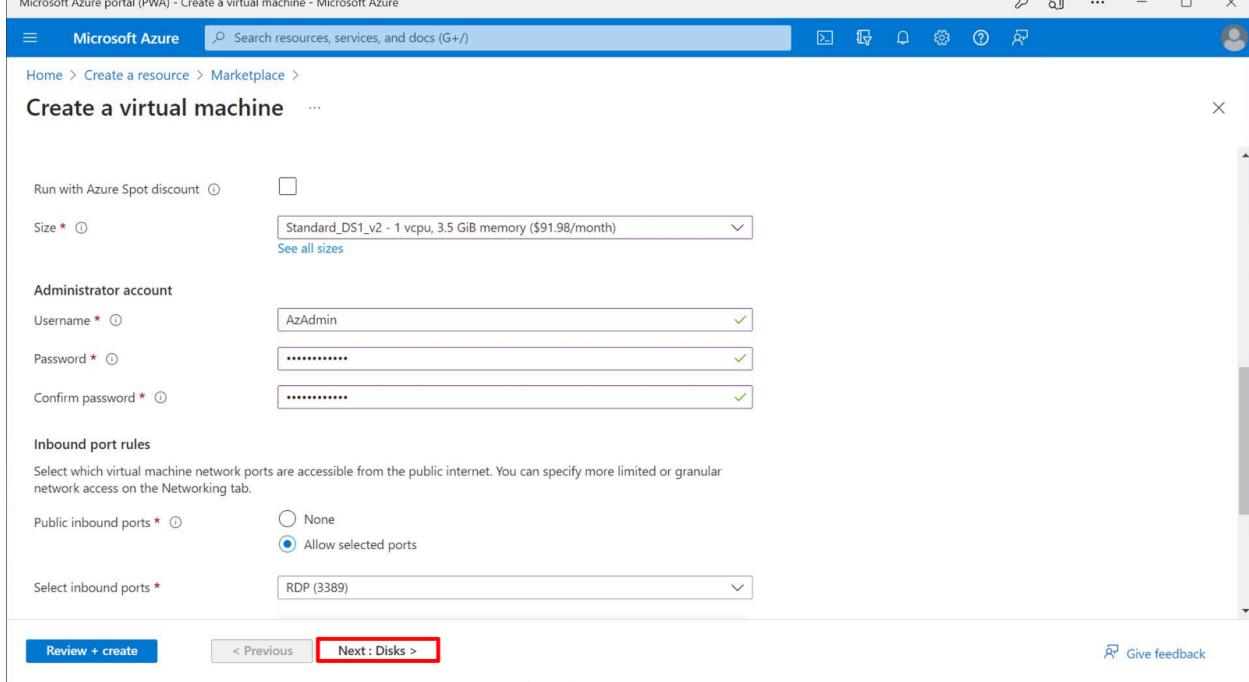
Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * None Allow selected ports

Select inbound ports *

Review + create **< Previous** **Next : Disks >** **Give feedback**



6. Select Next: Networking.

Microsoft Azure portal (PWA) - Create a virtual machine - Microsoft Azure

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

Home > Create a resource > Marketplace >

Create a virtual machine

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host
Encryption at host is not registered for the selected subscription.
[Learn more about enabling this feature](#)

OS disk

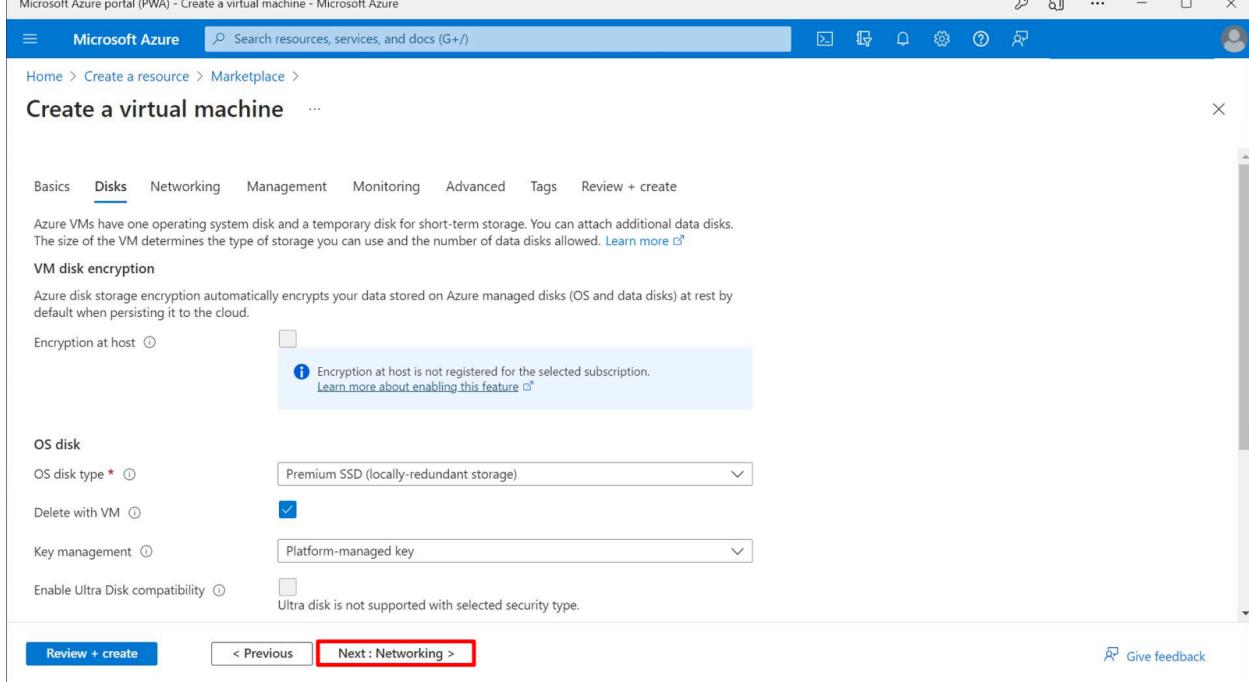
OS disk type *

Delete with VM

Key management

Enable Ultra Disk compatibility
Ultra disk is not supported with selected security type.

Review + create **< Previous** **Next : Networking >** **Give feedback**



7. Select Create New for the virtual network.

Microsoft Azure portal (PWA) - Create a virtual machine - Microsoft Azure

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

Home > Create a resource > Marketplace >

Create a virtual machine

Networking

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	(new) ServicesVM-vnet
	Create new
Subnet *	(new) default (10.0.0.0/24)
Public IP	(new) ServicesVM-ip
NIC network security group	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports *	<input type="radio"/> None Add

[Review + create](#) < Previous Next : Management > [Give feedback](#)

8. Fill in the following details on the **Create virtual network** page:

- Name: "Services_Test_Network"
- Address space address range: **172.16.0.0/16**
- Subnets Subnet name: "VMs"
- Subnets Address range: **172.16.1.0/24**

9. Select **OK**.

Microsoft Azure portal (PWA) - Create virtual network - Microsoft Azure

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

Home > Create a resource > Marketplace >

Create a virtual machine

Networking

Basics Disks Networking Management Monitoring

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	(new) ServicesVM-vnet
	Create new
Subnet *	(new) default (10.0.0.0/24)
Public IP	(new) ServicesVM-ip
NIC network security group	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports *	<input type="radio"/> None Add

Create virtual network

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network which is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or your on-premises network. [Learn more](#)

Name * **Services_Test_Network**

Address space

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

<input type="checkbox"/> Address range *	Addresses	Overlap
<input checked="" type="checkbox"/> 172.16.0.0/16	172.16.0.0 - 172.16.255.255 (65536 addresses)	None
	(0 Addresses)	None

Subnets

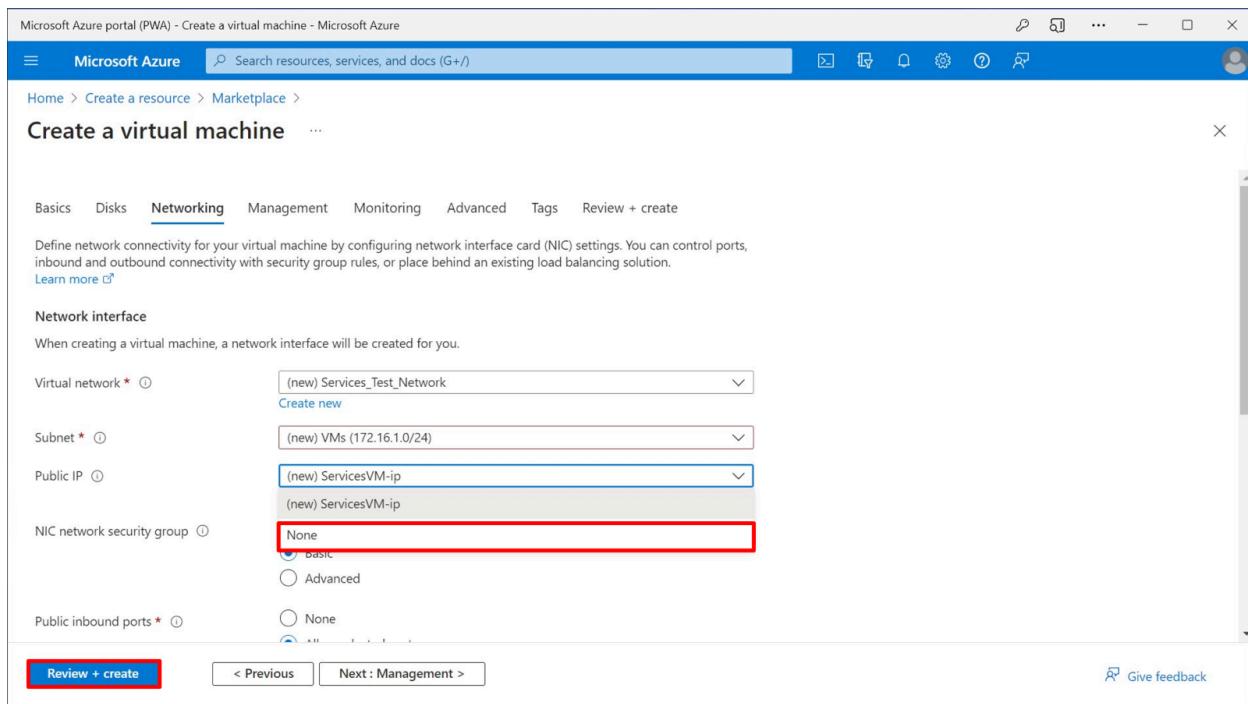
The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.

<input type="checkbox"/> Subnet name	Address range	Addresses
<input checked="" type="checkbox"/> VMs	172.16.1.0/24	172.16.1.0 - 172.16.1.255 (256 addresses)
	(0 Addresses)	None

[Review + create](#) < Previous Next : Management > [OK](#) [Discard](#)

10. For public IP select **None**.

11. Select the **Review + create** button to review the settings.



Microsoft Azure portal (PWA) - Create a virtual machine - Microsoft Azure

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

Home > Create a resource > Marketplace >

Create a virtual machine ...

Networking

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
[Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * (new) Services_Test_Network
Create new

Subnet * (new) VMs (172.16.1.0/24)

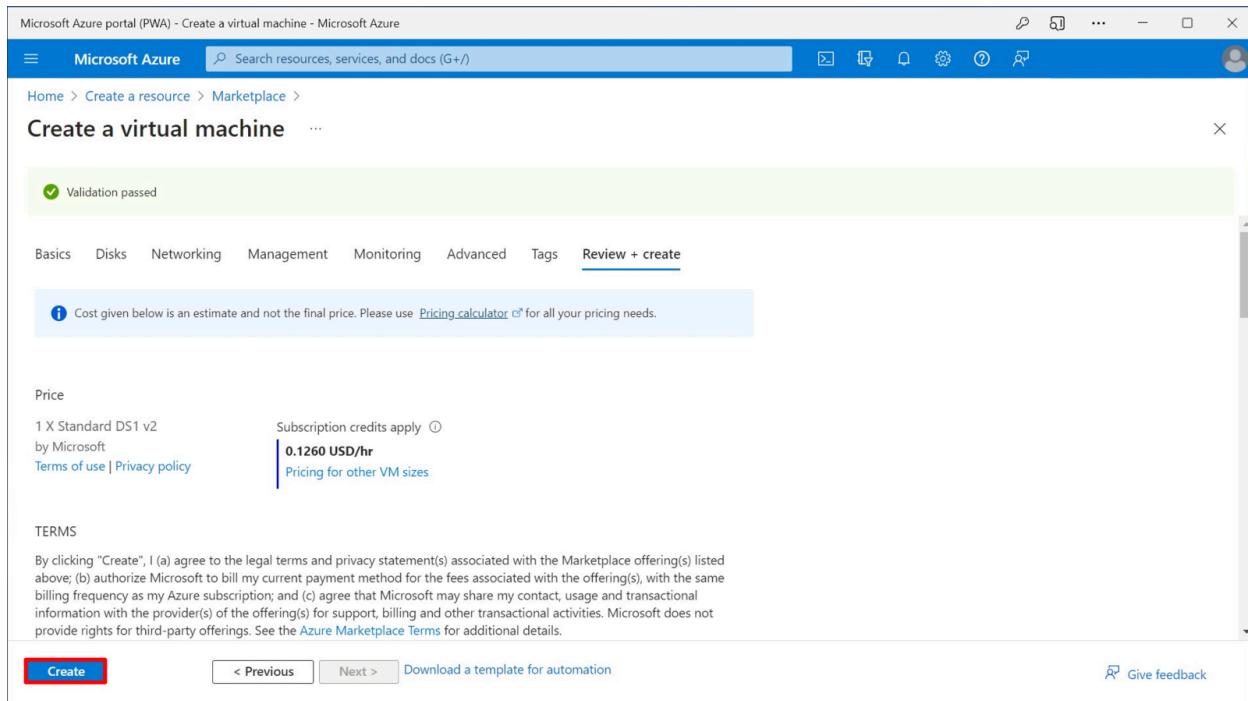
Public IP (new) ServicesVM-ip
(new) ServicesVM-ip

NIC network security group * None
 basic
 Advanced

Public inbound ports * (new) None

Review + create < Previous Next : Management > Give feedback

12. Select the **Create** button to create the virtual network.



Microsoft Azure portal (PWA) - Create a virtual machine - Microsoft Azure

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

Home > Create a resource > Marketplace >

Create a virtual machine ...

Validation passed

Review + create

Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.

Price

1 X Standard DS1 v2 by Microsoft Subscription credits apply
[Terms of use](#) | [Privacy policy](#) **0.1260 USD/hr** Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Create < Previous Next > Download a template for automation Give feedback

13. The virtual machine will now deploy.

Microsoft Azure portal (PWA) - CreateVm-MicrosoftWindowsServer.WindowsServer-202-20230706095433 - Microsoft Azure

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

Home > CreateVm-MicrosoftWindowsServer.WindowsServer-202-20230706095433 | Overview

Deployment

Search Delete Cancel Redeploy Download Refresh

Overview Deployment is in progress

Deployment name: CreateVm-MicrosoftWindowsServer.Win... Start time: 7/6/2023, 10:45:07 AM
Subscription: Azure subscription 1 (1094ab39-adb6-44d9-bf... Correlation ID: c2d56526-cd9e-4a4c-b8e8
Resource group: Services_Test

Inputs Outputs Template

Deployment details

Resource	Type	Status	Operation details
No results.			

Give feedback Tell us about your experience with deployment

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >

Step 2: Hub Network with VNet peering.

Create a hub network with VNet peering to the **Service_Test_Network**, all inside a new resource group ready for an Azure Standard firewall deployment. The activity about [Resource group and VNet creation](#) will help you to remember how to create a hub and perform VNet peering.

1. On the Azure home page, search and select the **Resource groups** service.

Microsoft Azure portal (PWA) - Home - Microsoft Azure

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

Resource

All Services (19) Resource Groups (2) Marketplace (31) Documentation (99+)

Azure Active Directory (11) Resources (0)

Services

Resource groups (highlighted with a red box)

Resource Graph Explorer
Resource Graph queries
Resource management private links
Subscriptions

Resource Guards
Resource bridges
Resource Explorer

Resource Groups

ResourceMoverRG-eastus-westeuropene
ResourceMoverRG-polandcentral-westeuropene

Marketplace

Resource group
Vault Platform
Resource Management Private Link
Resource Guard

Resource Scheduler
Concierge by CloudScope
Emissions.AI
LAMP on Ubuntu 22.04 LTS

See all

Continue searching in Azure Active Directory

Searching all subscriptions. Change

Give feedback

2. Select **Create**.

Microsoft Azure portal (PWA) - Resource groups - Microsoft Azure

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

Home > Resource groups

Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Location equals all Add filter

Showing 1 to 4 of 4 records.

Name	Subscription	Location
NetworkWatcherRG	Azure subscription 1	East US
ResourceMoverRG-eastus-westeuropene	Azure subscription 1	North Europe
ResourceMoverRG-polandcentral-westeuropene	Azure subscription 1	North Europe
Services_Test	Azure subscription 1	East US

No grouping List view

< Previous Page 1 of 1 Next > Give feedback

3. Select the following details:

- Resource group: "Service_Security"
- Virtual network name: "Services_Hub"

4. Select **Review + create**, and then **Create**.

Microsoft Azure portal (PWA) - Create virtual network - Microsoft Azure

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

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Project details

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

Subscription * Azure subscription 1 (1094ab39-adb6-44d9-bfe6-51c9ea920f2e)

Resource group * Services_Security

Virtual network name * Services_Hub

Region (US) East US

Deploy to an edge zone

Previous Next Review + create Give feedback

Microsoft Azure portal (PWA) - Create a resource group - Microsoft Azure

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

Home > Resource groups >

Create a resource group

Validation passed.

Basics Tags Review + create

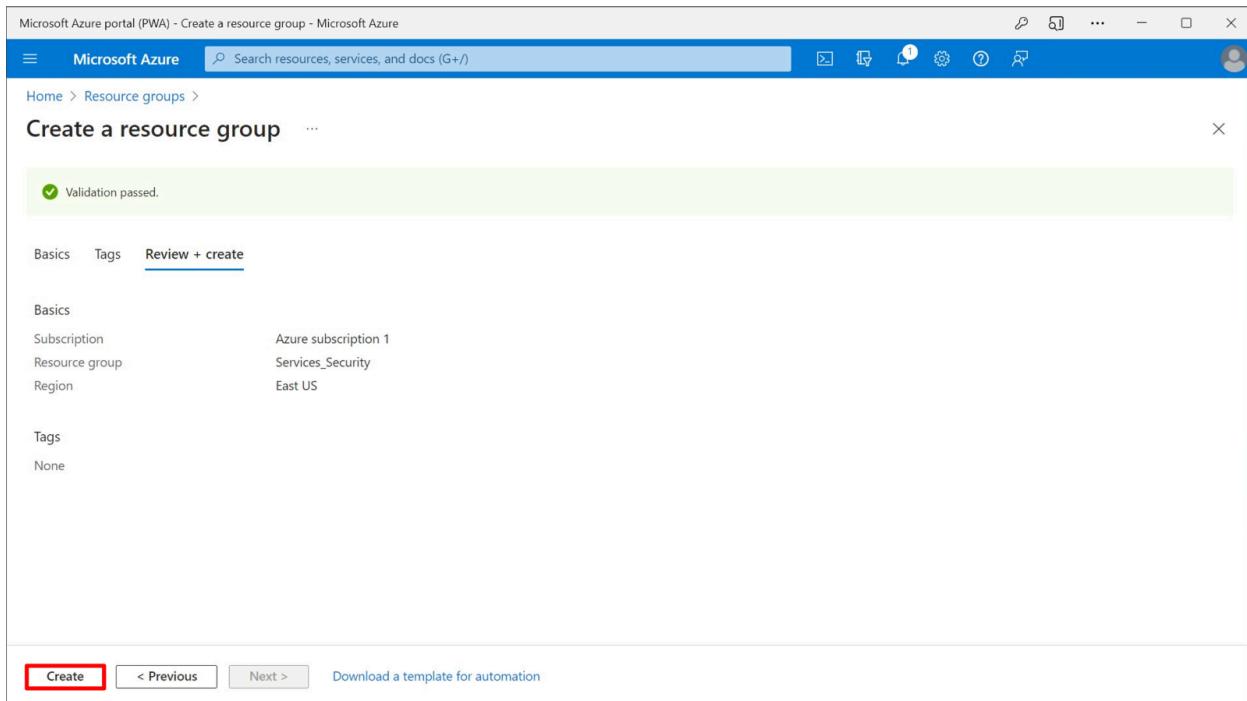
Basics

Subscription	Azure subscription 1
Resource group	Services_Security
Region	East US

Tags

None

Create < Previous Next > Download a template for automation



5. Go back to the Azure home page by selecting **Home** in the top left-hand corner.

Microsoft Azure portal (PWA) - Resource groups - Microsoft Azure

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

Home >

Resource groups

SamsScoops (SamsScoops.onmicrosoft.com)

+ Create Manage view Refresh Export to CSV Open query Assign tags

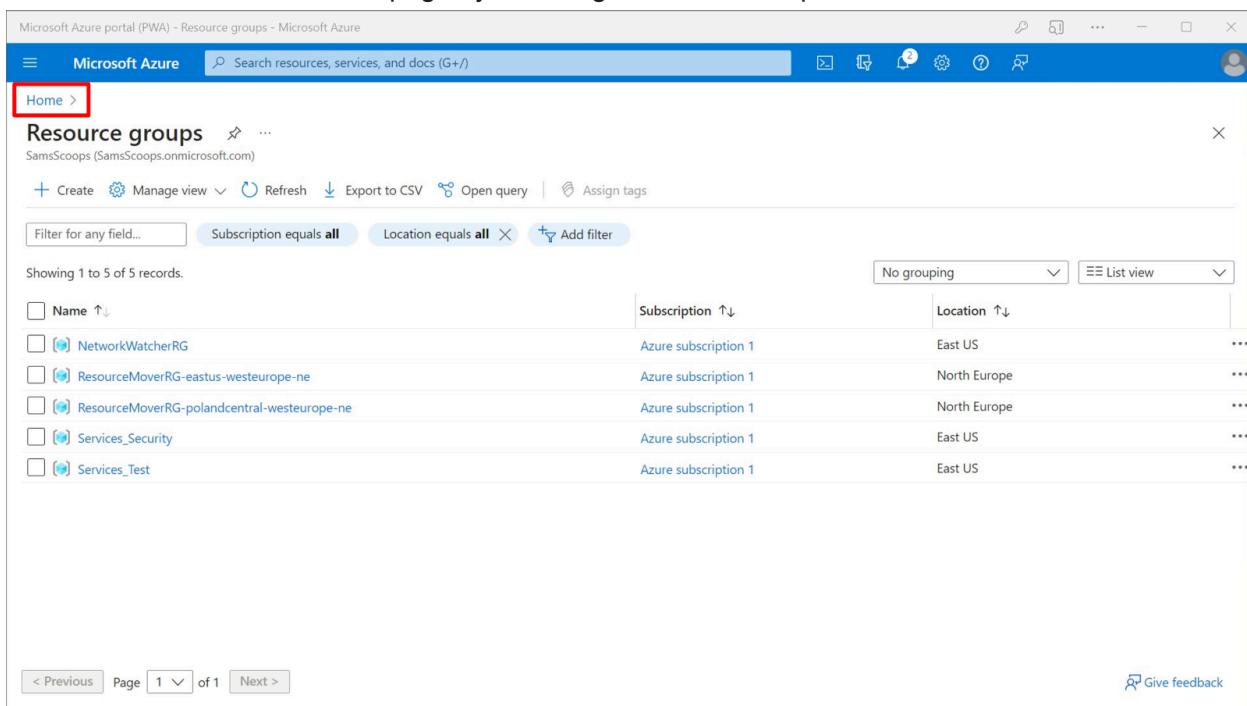
Filter for any field... Subscription equals all Location equals all Add filter

Showing 1 to 5 of 5 records.

Name	Subscription	Location
NetworkWatcherRG	Azure subscription 1	East US
ResourceMoverRG-eastus-westeuropene	Azure subscription 1	North Europe
ResourceMoverRG-polandcentral-westeuropene	Azure subscription 1	North Europe
Services_Security	Azure subscription 1	East US
Services_Test	Azure subscription 1	East US

No grouping List view

< Previous Page 1 of 1 Next > Give feedback



6. On the Azure home page search for **Virtual networks** and select the **Virtual networks** service.

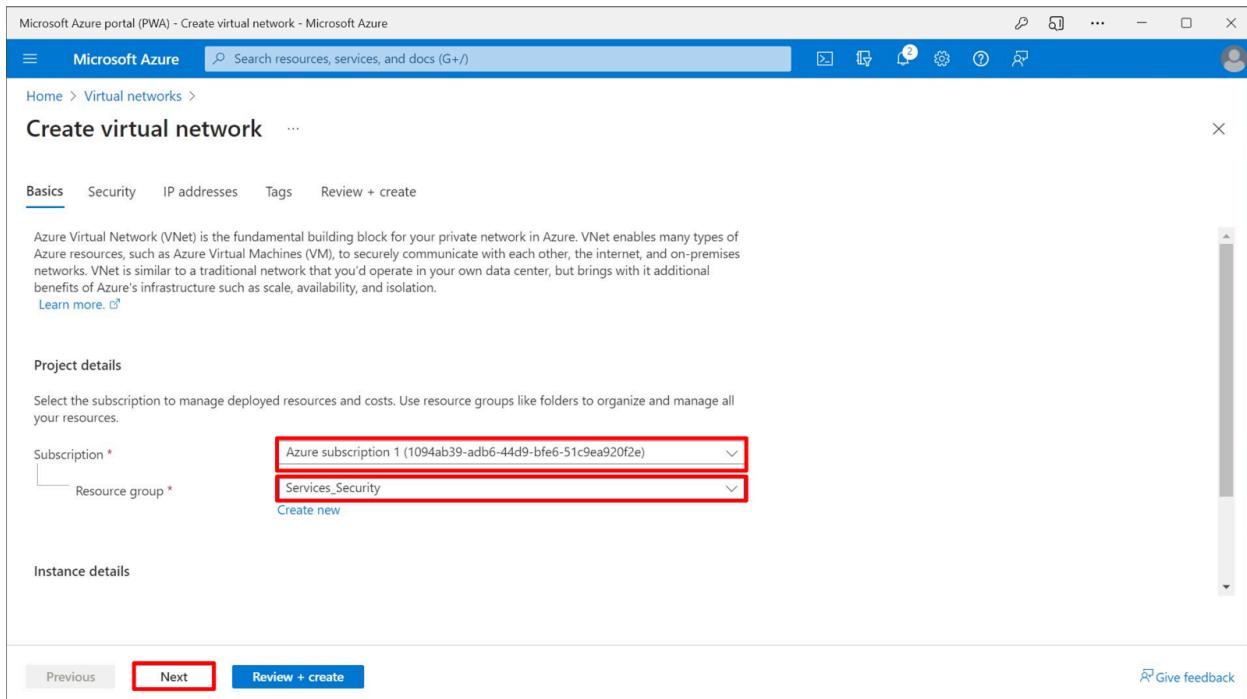
The screenshot shows the Microsoft Azure portal interface. The search bar at the top contains the text 'virtual'. Below the search bar, the 'Services' section is visible, with 'Virtual networks' highlighted and surrounded by a red box. Other services listed include Virtual machines, Virtual WANs, Virtual network gateways, Virtual Network Managers, and Virtual Network Verifiers.

7. Select Create.

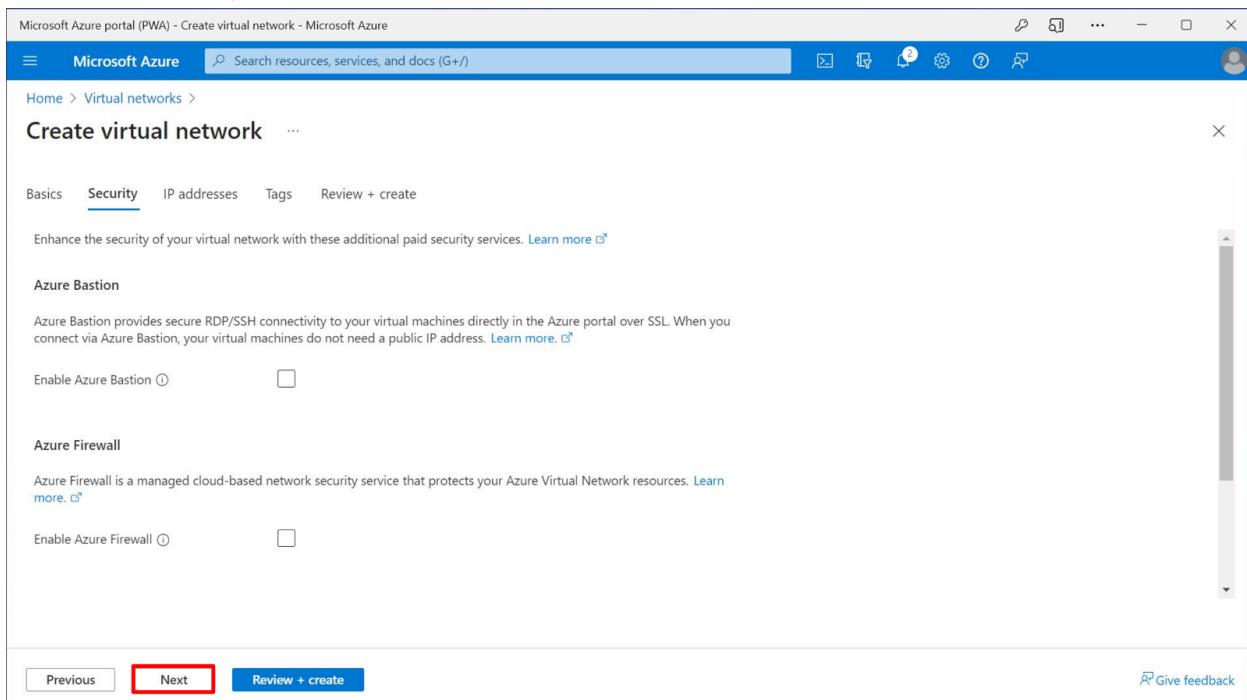
The screenshot shows the 'Virtual networks' list page in the Microsoft Azure portal. The 'Create' button is highlighted with a red box. The page displays one record: 'Services_Test_Network' with Resource group 'Services_Test', Location 'East US', and Subscription 'Azure subscription 1'. Navigation controls at the bottom include '< Previous', 'Page 1 of 1', and 'Next >'.

8. Select your subscription and resource group **Services_Security**.

9. Select **Next**.



10. Select Next again.



11. Edit the IP address space with the following enter **192.168.1.0** and for the address space size, enter **/24**.

12. Select **default** under Subnets.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal, specifically the 'IP addresses' step. A subnet named 'default' is selected. The 'Subnet template' dropdown is set to 'Azure Firewall'. The 'Starting address' field contains '192.168.1.0'. The 'NAT gateway' dropdown is set to 'None'.

13. Fill in the subnet template: **Azure Firewall**.

14. Fill in a new starting address: **192.168.1.0**.

15. Select **Save**.

The screenshot shows the 'Edit subnet' configuration page. The 'Subnet template' dropdown is set to 'Azure Firewall'. The 'Starting address' field is highlighted with a red box and contains '192.168.1.0'. The 'NAT gateway' dropdown is set to 'None'.

16. Select **Review + Create**.

Microsoft Azure portal (PWA) - Create virtual network - Microsoft Azure

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

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Add IPv4 address space

192.168.1.0/24

192.168.1.0 /24 (256 addresses) Delete address space

192.168.1.0 - 192.168.1.255 (256 addresses)

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
AzureFirewallSubnet	192.168.1.0 - 192.168.1.63	/26 (64 addresses)	-

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#)

Previous Next Review + create Give feedback

17. Select Create.

Microsoft Azure portal (PWA) - Create virtual network - Microsoft Azure

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

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

[View automation template](#)

Basics

Subscription	Azure subscription 1
Resource Group	Services_Security
Name	Services_Hub
Region	East US

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Add address space 192.168.1.0/24 (256 addresses)

Previous Next Create Give feedback

18. Select Go to resource.

Microsoft Azure portal (PWA) - Services_Hub - Microsoft Azure

Home > Services_Hub | Overview

Your deployment is complete

Deployment name : Services_Hub Start time : 7/6/2023, 12:13:23 PM

Subscription : Azure subscription 1 (1094ab3...) Correlation ID : 52354a2f-fdbe-411a-8ebe-060...

Resource group : Services_Security

Deployment details

Next steps

Go to resource

Give feedback

Tell us about your experience with deployment

Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill.

Set up cost alerts >

Microsoft Defender for Cloud

Secure your apps and infrastructure

Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

Start learning today >

Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

19. Select Peering either on the left or right-hand side of the page.

Microsoft Azure portal (PWA) - Services_Hub - Microsoft Azure

Home > Services_Hub | Overview

Services_Hub

Virtual network

Move Delete Refresh Give feedback

Address space

Connected devices

Subnets

Bastion

DDoS protection

Firewall

Microsoft Defender for Cloud

Network manager

DNS servers

Peerings

Service endpoints

Private endpoints

Properties

Locks

Essentials

Resource group (move) : Services_Security

Location (move) : East US

Subscription (move) : Azure subscription 1

Subscription ID : 1094ab39-adb6-44d9-bfe6-51c9ea920f2e

Address space : 192.168.1.0/24

DNS servers : Azure provided DNS service

Flow timeout : Configure

BGP community string : Configure

Virtual network ID : d45e5716-14d6-4530-aba4-35b6febb16f8

Tags (edit) : Click here to add tags

Topology Properties Capabilities (5) Recommendations Tutorials

DDoS protection

Configure additional protection from distributed denial of service attacks.

Not configured

Azure Firewall

Protect your network with a stateful L3-L7 firewall.

Not configured

Peerings

Seamlessly connect two or more virtual networks.

Not configured

Microsoft Defender for Cloud

Strengthen the security posture

Private endpoints

Privately access Azure services

20. Select Add to add a new peering.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons. Below the navigation is a breadcrumb trail: Home > Services_Hub | Overview > Services_Hub. The main content area is titled "Services_Hub | Peerings" and "Virtual network". On the left, a sidebar lists several options: Address space, Connected devices, Subnets, Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, Network manager, DNS servers, Peerings (which is selected and highlighted in grey), Service endpoints, Private endpoints, Properties, and Locks. At the top of the main content area, there is a search bar, a "Peering status == all" filter, and sorting columns for Name, Peering status, Peer, and Gateway transit. A large message says "Add a peering to get started". At the bottom right of the main area is a "Give feedback" link. The "Add" button, located at the top left of the main content area, is highlighted with a red box.

21. Name the peering "Hub_Test".

The screenshot shows the Microsoft Azure portal interface for adding a peering. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons. Below the navigation is a breadcrumb trail: Home > Services_Hub | Overview > Services_Hub | Peerings > Add peering. The main content area is titled "Add peering". It displays a note: "For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links." Under "This virtual network", the "Peering link name" field is filled with "Hub_Test" and is highlighted with a red box. Below this, there are sections for "Traffic to remote virtual network" (with "Allow (default)" selected) and "Traffic forwarded from remote virtual network" (with "Allow (default)" selected). At the bottom, there is a section for "Virtual network gateway or Route Server" (with "None (default)" selected). At the very bottom is a blue "Add" button.

22. Scroll down, leave the default settings and under **Peering link name** type "Test_Hub".

23. Under the **Virtual network** dropdown, select **Services_Test_Network**.

24. Select **Add** and the network peering will be set up.

Microsoft Azure portal (PWA) - Add peering - Microsoft Azure

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

Home > Services_Hub | Overview > Services_Hub | Peerings >

Add peering

Peering link name *

Virtual network deployment model

 Resource manager
 Classic

I know my resource ID

Subscription *

Virtual network *

Traffic to remote virtual network

 Allow (default)
 Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network

 Allow (default)
 Block traffic that originates from outside the remote virtual network

Add

Microsoft Azure portal (PWA) - Services_Hub - Microsoft Azure

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

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

Home > Services_Hub | Overview > Services_Hub

Services_Hub | Peerings

Virtual network

Peering status == all			
Name	Peer	Gateway transit	...
Hub_Test	Updating	Services_Test_Network	Disabled

Give feedback

Step 3: Azure Standard Firewall deployment

Deploy an Azure Standard Firewall within the hub network. Refer back to the video [Azure Firewall deployment](#) to remind you of all the necessary steps that need to be performed when deploying a firewall.

1. Search for **firewalls** and select **Firewalls**.

The screenshot shows the Microsoft Azure portal interface. The search bar at the top contains the text "Firewall". Below the search bar, the "Services" section is expanded, and the "Firewalls" option is highlighted with a red box. Other options like "Overview", "Activity log", and "Tags" are also listed. To the right, there are marketplace and documentation sections.

2. Select Create Firewall.

The screenshot shows the "Firewalls" blade in the Microsoft Azure portal. At the top, there are filter options: "Subscription equals all", "Resource group equals all", "Location equals all", and "Add filter". Below this, it says "Showing 0 to 0 of 0 records." There are columns for "Name", "Type", "Resource group", "Location", and "Subscription". A large "Create" button is prominently displayed in the center, highlighted with a red box. Below the button, there is a message about cloud-native network security and a link to "Learn more about Azure Firewall".

3. Fill in the following details:

- Subscription: **Select your subscription**
- Resource group: **Services_Security**
- Give the firewall instance the name "ServicesFirewall".
- Region: Select the same location that you have used previously.

Microsoft Azure portal (PWA) - Create a firewall - Microsoft Azure

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

Home > Firewalls >

Create a firewall

Basics Tags Review + create

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. [Learn more](#)

Project details

Subscription * Azure subscription 1 (1094ab39-adb6-44d9-bfe6-51c9ea920f2e)

Resource group * Services_Security

Instance details

Name * ServicesFirewall

Region * East US

Availability zone None

Review + create Previous Next : Tags > Download a template for automation

- Firewall SKU: Select **Standard**.
- Firewall management: Use **Firewall rules (classic)** to manage this firewall.
- Virtual network: select **Use existing** and select **Services_Security_Network**.
- For the public IP address select Add new and give it the name "Services".

4. Click **Review + create** then **Create** and the firewall will be deployed.

Microsoft Azure portal (PWA) - Create a firewall - Microsoft Azure

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

Home > Firewalls >

Create a firewall

Premium firewalls support additional capabilities, such as SSL termination and IDPS. Additional costs may apply. [Learn more](#)

Firewall SKU

Basic
 Standard
 Premium

Firewall management

Use a Firewall Policy to manage this firewall
 Use Firewall rules (classic) to manage this firewall

Choose a virtual network

Create new
 Use existing

Virtual network

Services_Hub (Services_Security)

Public IP address *

(New) Services

Forced tunneling Disabled

Review + create Previous Next : Tags > Download a template for automation

Validation passed

Basics Tags Review + create

Summary

Basics

Subscription	Azure subscription 1
Resource group	Services_Security
Region	East US
Azure Firewall Sku	Standard
Virtual network	Services_Hub
Address space	192.168.1.0/24
Firewall public IP address	Services
Availability zone	None

Tags

Resource type	Name	Value
No results		

Create Previous Next Download a template for automation

Deployment in progress... Deployment to resource group 'Services_Security' is in progress.

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service provider partners
who can help manage your assets on Azure
and be your first line of support.
Find an Azure expert >

Step 4: Just-in-time access (JIT) setup

Enable JIT access on the **Services_VM**. RDP access is enabled by default. To remind you of the steps for enabling JIT access refer back to the video [Implementing just-in-time access](#).

1. Search for and select **Virtual machines**.

The screenshot shows the Microsoft Azure portal interface. The search bar at the top contains the text "Virtual". Below the search bar, there are several navigation tabs: All, Services (34), Marketplace (31), Documentation (99+), Azure Active Directory (5), and Resources (0). The "Services" tab is selected. Under the "Services" heading, the "Virtual machines" option is highlighted and enclosed in a red box. Other listed services include Virtual WANs, Virtual network gateways, Virtual Network Managers, and Virtual Network Verifiers. Below the services, there are sections for Marketplace (Virtual machine, Azure SQL, Free account virtual machine, Container Instances) and Documentation (Virtual networks and virtual machines in Azure, Azure Virtual WAN Overview). A sidebar on the right provides links for Cloud and Infrastructure, and a feedback button.

2. Select the Services_VM virtual machine.

The screenshot shows the "Virtual machines" list page in the Microsoft Azure portal. The search bar at the top contains "Search resources, services, and docs (G+)". The main title is "Virtual machines". There are filter options: Subscription equals all, Type equals all, Resource group equals all, Location equals all, and a "No grouping" dropdown. The table lists one record: "ServicesVM" (Type: Virtual machine, Subscription: Azure subscription 1, Resource group: Services_Test, Location: East US, Status: Running, Operating system: Windows, Size: Standard_DS1_v2). The row for "ServicesVM" is highlighted with a red box. At the bottom, there are navigation buttons for < Previous, Page 1 of 1, Next >, and a feedback link.

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

The screenshot shows the Microsoft Azure portal interface for a virtual machine named 'ServicesVM'. The left sidebar contains navigation links like Home, Virtual machines, and Configuration (which is highlighted with a red box). The main content area displays the VM's details under the 'Essentials' tab, including its operating system (Windows Server 2022 Datacenter Azure Edition), status (Running), location (East US), and subscription information. Below the essentials, there are sections for Tags, Properties, and Networking.

4. Select Enable just-in-time.

The screenshot shows the 'ServicesVM | Configuration' page. The left sidebar includes 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Networking', 'Connect', 'Windows Admin Center', 'Disks', 'Size', 'Microsoft Defender for Cloud', 'Advisor recommendations', 'Extensions + applications', 'Availability + scaling', and 'Configuration' (which is highlighted with a red box). The main content area has a 'Just-in-time VM access' section with a prominent 'Enable just-in-time' button, which is also highlighted with a red box. Below this, there are sections for Licensing, Proximity placement group, and a note about updating the placement group.

Step 5: Azure Bastion configuration

Configure Azure Bastion for the **ServicesVM**. Refer back to the video [Bastion and virtual machines](#) for a reminder of the steps.

1. Use the search bar and search for **Virtual networks** and select **Virtual networks**.

The screenshot shows the Microsoft Azure portal interface. The search bar at the top has the letter 'v' typed into it, which is highlighted with a red box. Below the search bar, the main content area displays a list of services under the 'Services' category. One item, 'Virtual networks', is also highlighted with a red box. The list includes other items like 'Virtual machines', 'Virtual clusters', 'Virtual WANS', etc. To the right, there's a detailed view of specific resources: 'ServicesVM' (Virtual machine), 'ServicesVM-nsg' (Network security group), 'servicesvm926' (Network interface), and 'ServicesVM_disk1_449442436f974d29bf032081590f6826' (Disk). The left sidebar contains navigation links for Home, Virtual machines, Services, Resources, Resource Groups, Marketplace, Documentation, and Settings.

2. Select the Services_Test_Network network.

The screenshot shows the 'Virtual networks' page in the Microsoft Azure portal. The search bar at the top has 'Virtual networks' typed into it. The main table lists two virtual networks: 'Services_Hub' and 'Services_Test_Network'. The 'Services_Test_Network' row is highlighted with a red box. The table columns include Name, Resource group, Location, and Subscription. Both networks belong to the 'Services_Security' resource group, are located in 'East US', and are part of 'Azure subscription 1'. At the bottom of the page, there are navigation buttons for '< Previous', 'Page 1 of 1', and 'Next >'.

3. On the page for the virtual network, in the left pane, select Bastion to open the Bastion page.

The screenshot shows the Microsoft Azure portal interface for a virtual network named 'Services_Test_Network'. The left sidebar contains navigation links like Overview, Activity log, Access control (IAM), Tags, and several others under Settings. The main content area has tabs for Overview, Essentials, and Capabilities (5). The 'Bastion' section is highlighted with a red box. It includes options for DDoS protection, Firewall, Microsoft Defender for Cloud, Network manager, DNS servers, and Peerings. Below these are sections for DDoS protection, Azure Firewall, Microsoft Defender for Cloud, and Private endpoints.

4. On the **Bastion** page, select **Configure manually**.

The screenshot shows the 'Create Bastion' configuration page for the 'Services_Test_Network' virtual network. The left sidebar shows the 'Bastion' section selected. The main area displays fields for Name (Services_Test_Network-bastion), Resource group (Services_Test), Virtual network (Services_Test_Network), and Public IP address (Services_Test_Network-ip). A note indicates that Bastion pricing starts with an hourly base rate. At the bottom, there are two buttons: 'Deploy Bastion' and 'Configure manually', with 'Configure manually' highlighted by a red box.

5. On the **Create a Bastion** page, use the following settings:

- Instance Name: "Services_Bastion".
- Virtual network: "Services_Test_Network".

Microsoft Azure portal (PWA) - Create a Bastion - Microsoft Azure

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

Home > Virtual networks > Services_Test_Network | Bastion >

Create a Bastion

Bastion allows web based RDP access to your vnet VM. [Learn more](#)

Project details

Subscription * Azure subscription 1 (1094ab39-adb6-44d9-bfe6-51c9ea920f2e)

Resource group * Services_Test
Create new

Instance details

Name * Services_Bastion

Region * East US

Tier * Standard

Instance count * 2

Configure virtual networks

Virtual network * Services_Test_Network
Create new

To associate a virtual network with a Bastion, it must contain a subnet with name AzureBastionSubnet and a prefix of at least /26

Review + create Previous Next : Tags > Download a template for automation

6. Scroll down and to configure the AzureBastionSubnet select Manage subnet configuration.

Microsoft Azure portal (PWA) - Create a Bastion - Microsoft Azure

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

Home > Virtual networks > Services_Test_Network | Bastion >

Create a Bastion

Region * East US

Tier * Standard

Instance count * 2

Configure virtual networks

Virtual network * Services_Test_Network
Create new

To associate a virtual network with a Bastion, it must contain a subnet with name AzureBastionSubnet and a prefix of at least /26

Subnet * Manage subnet configuration

Public IP address

Public IP address * Create new Use existing

Public IP address name * Services_Test_Network-ip

Public IP address SKU Standard

Review + create Previous Next : Tags > Download a template for automation

7. On the subnets page select + Subnet.

The screenshot shows the Microsoft Azure portal interface. The left sidebar has a 'Subnets' section selected. The main content area displays a table of existing subnets, with one row for 'VMs' having an IP range of '172.16.1.0/24'. A red box highlights the '+ Subnet' button at the top left of the table.

8. Create the AzureBastionSubnet subnet using the following values.

- Subnet name: "AzureBastionSubnet".
- Subnet address range: **172.16.2.0/24**.
- Select **Save** at the bottom of the page to save your values.

The screenshot shows the 'Add subnet' dialog box overlaid on the Azure portal. The 'Name' field contains 'AzureBastionSubnet' and the 'Subnet address range' field contains '172.16.2.0/24'. The 'Save' button at the bottom right is highlighted with a red box.

9. At the top of the **Subnets** page, select **Create a Bastion** to return to the **Bastion configuration** page.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons. Below the navigation is a breadcrumb trail: Home > Virtual networks > Services_Test_Network | Bastion > Create a Bastion > Services_Test_Network. The main content area is titled "Services_Test_Network | Subnets" and shows a list of subnets. The left sidebar has a "Subnets" section selected, which contains links for Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, Network manager, DNS servers, and Peerings. At the bottom right of the main content area is a "Give feedback" link.

10. Select **Create new** under Public IP address. Leave the default naming suggestion. Select **Review + Create**.

The screenshot shows the "Create a Bastion" configuration page. It includes fields for Region (east US), Tier (Standard), and Instance count (2). Under "Configure virtual networks", it shows a Virtual network (Services_Test_Network) and a Subnet (AzureBastionSubnet (172.16.2.0/24)). In the "Public IP address" section, the "Create new" radio button is selected, and the "Public IP address name" field contains "Services_Test_Network-ip". The "Assignment" section shows "Static" selected. At the bottom, there are "Review + create", "Previous", "Next : Tags >", and "Download a template for automation" buttons.

11. Select **Create**.

Validation passed

Basics Tags Advanced Review + create

Summary

Basics

Name	Services_Bastion
Subscription	Azure subscription 1
Resource group	Services_Test
Region	East US
Virtual network	Services_Test_Network
Tier	Standard
Subnets	AzureBastionSubnet
Public IP address	Services_Test_Network-ip
Instance count	2
Copy and paste	Enabled
IP-based connection	Disabled
Kerberos authentication	Disabled
Shareable Link	Disabled
Native client support	Disabled

Create Previous Next Download a template for automation

Microsoft Azure portal (PWA) - Microsoft.BastionHost-20230706140539 - Microsoft Azure

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

Home > Microsoft.BastionHost-20230706140539 | Overview

Deployment

Overview Inputs Outputs Template

Deployment is in progress

Deployment name : Microsoft.BastionHost-20230706140539 Start time : 7/6/2023, 2:05:42 PM
Subscription : Azure subscription 1 (109ab3...) Correlation ID : 269c1939-c389-4269-951d-2ea...
Resource group : Services_Test

Deployment details

Resource	Type	Status	Operator
Services_Bastion	Bastion	Created	Operation
Services_Test_Netw	Public IP address	OK	Operation

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >

Step 6: Testing remote connectivity

Use Azure Bastion with JIT and connect to the Services VM using RDP, to confirm that the deployment is working. Refer back to the video [Bastion and virtual machines](#) for a reminder of the steps.

1. Search and select **Virtual machines**.

Microsoft Azure portal (PWA) - ServicesVM - Microsoft Azure

Microsoft Azure

Home > Virtual machines >

ServicesVM
Virtual machine

Search: v

All Services (99+) Resources (8) Resource Groups (2) Marketplace (31) Documentation (56)

Azure Active Directory (7)

Services

Virtual machines Virtual networks Virtual clusters Virtual WANs Virtual network gateways Virtual Network Managers

Virtual Appointments Builder Virtual Instances for SAP solutions

Resources

Services ServicesVM Public IP address Virtual machine

Networking Services_Hub Virtual network ServicesVM-nsg Network security group

Connect Services_Test_Network Virtual network servicesvm926 Network interface

Windows Admin Center ServicesFirewall Firewall ServicesVM_disk1_449442436f974d29bf032081590f6826 Disk

Disks

Size

Microsoft Defender for Cloud

Advisor recommendations

Extensions + applications

Availability + scaling

Configuration

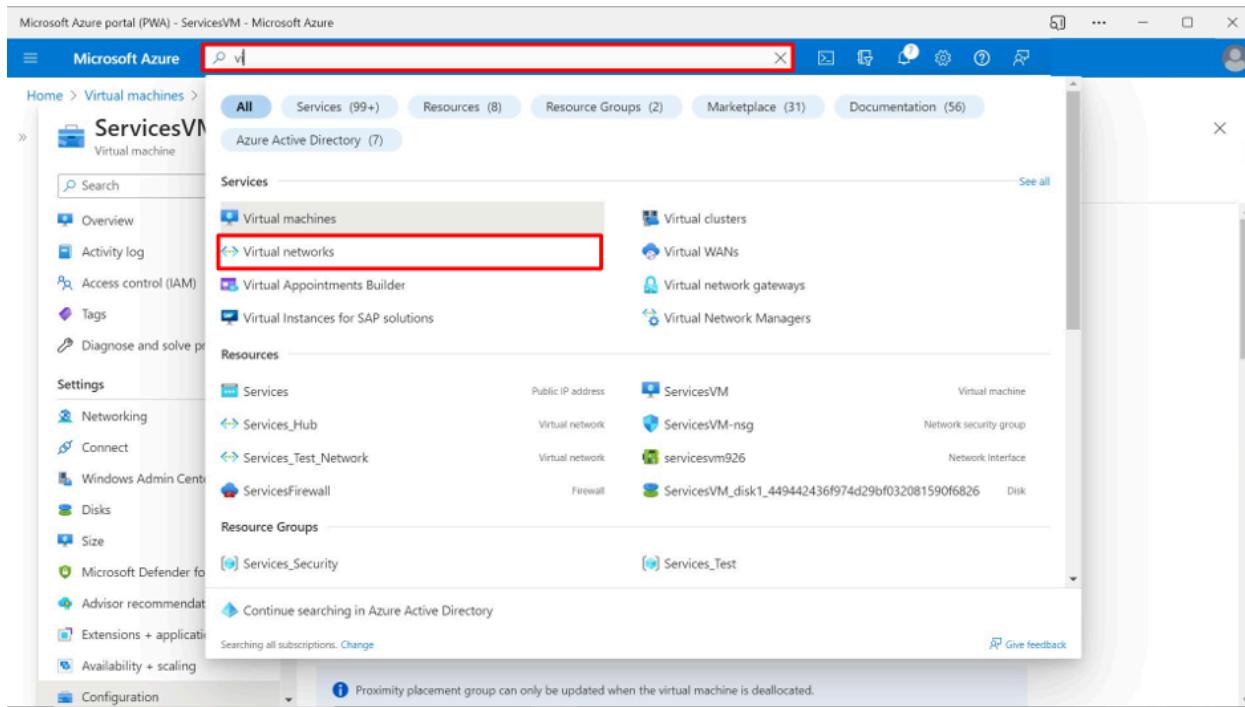
See all

Continue searching in Azure Active Directory

Searching all subscriptions. Change

Give feedback

Proximity placement group can only be updated when the virtual machine is deallocated.



2. Select the Services_VM.

Microsoft Azure portal (PWA) - Virtual machines - Microsoft Azure

Microsoft Azure

Search resources, services, and docs (G+/-)

Home >

Virtual machines

SemsScoops (SemsScoops.onmicrosoft.com)

+ Create Switch to classic Reservations Manage view Refresh Export to CSV Open query Assign tags Start Restart Stop ...

Filter for any field... Subscription equals all Type equals all Resource group equals all Location equals all Add filter

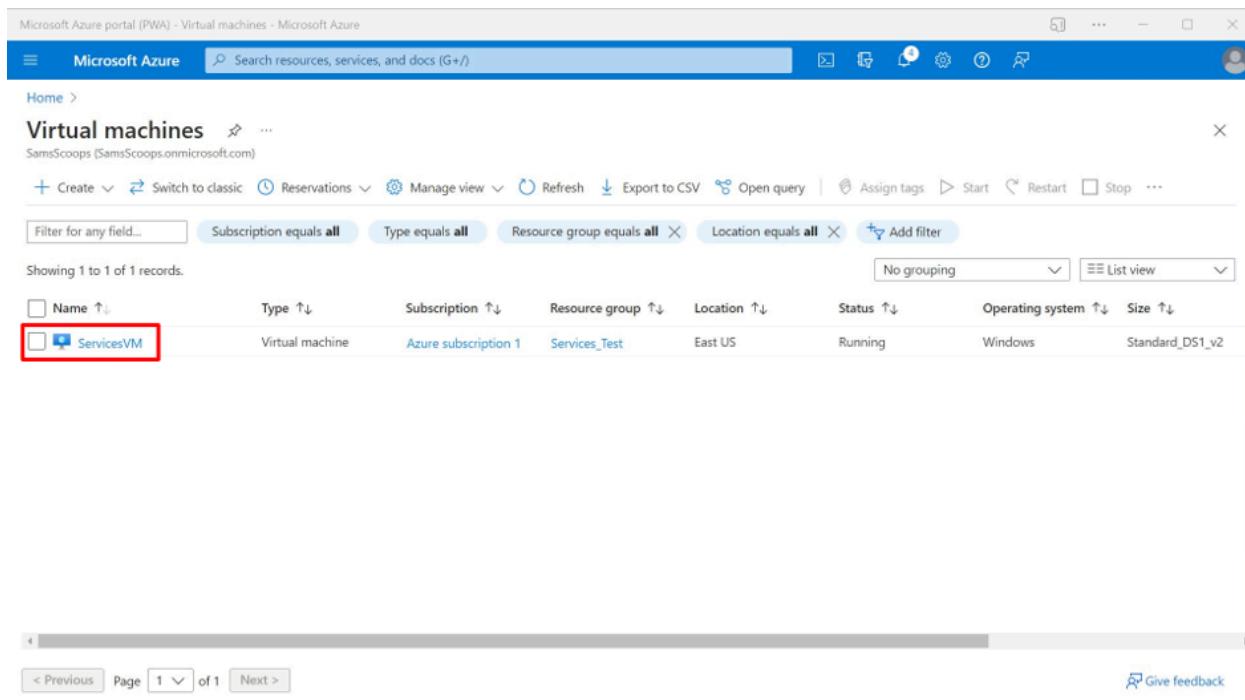
No grouping List view

Showing 1 to 1 of 1 records.

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size
ServicesVM	Virtual machine	Azure subscription 1	Services_Test	East US	Running	Windows	Standard_DS1_v2

< Previous Page 1 of 1 Next >

Give feedback



3. At the top of the page, select Connect.

The screenshot shows the Microsoft Azure portal interface for a virtual machine named 'ServicesVM'. The left sidebar contains navigation links like 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), and a search bar. The main content area displays the VM's details under the 'Essentials' tab, including its operating system (Windows Server 2022 Datacenter Azure Edition), status (Running), location (East US), subscription (Azure subscription 1), and a note about periodic system updates. A 'Tags (edit)' section allows adding tags. Below the essentials, there are tabs for Properties, Monitoring, Capabilities (8), Recommendations (9), and Tutorials. At the bottom, there are 'Virtual machine' and 'Networking' buttons. The 'Connect' button in the top navigation bar is highlighted with a red box.

4. Scroll down on the right scroll bar and select Request access.

The screenshot shows the 'ServicesVM | Connect' page. The left sidebar includes the same navigation as the previous screen. The main area has a note that the VM has a just-in-time access policy and requires selecting 'Request access' before connecting. It shows the VM is running. A form for connecting via RDP is present, with fields for IP address (Private IP address 172.16.1.4) and Port number (3389). Below the form, there are tabs for My IP, Other IP/ IPs, and All configured IPs. A prominent red box highlights the 'Request access' button. Below the button, there are links for 'Can't connect?' (Test network security groups, Run a comprehensive RDP connectivity test), 'Provide feedback' (Tell us about your RDP experience), and download options (Download RDP file anyway).

5. At the top of the page, select **Bastion** to go to the **Bastion** page.

Microsoft Azure portal (PWA) - ServicesVM - Microsoft Azure

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

Home > Virtual machines > ServicesVM

ServicesVM | Connect Virtual machine

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

RDP SSH Bastion

Access approved on port 3389 from the selected IPs. You can now connect.

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 ↗
- IP address prerequisite not met. Add a public IP address to the VM's network interface. 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 * Private IP address (172.16.1.4)

Port number 3389

Source IP ⓘ My IP Other IP/IPS All configured IPs

Download RDP File

6. Select Use Bastion.

Microsoft Azure portal (PWA) - ServicesVM - Microsoft Azure

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

Home > Virtual machines > ServicesVM

ServicesVM | Connect Virtual machine

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

RDP SSH Bastion

Access approved on port 3389 from the selected IPs. You can now connect.

Bastion is an Azure service that allows fast, secure connections to any VM within a VNet. Learn more ↗

Use Bastion

7. Complete the required authentication values, for the **Services_VM**:

- Username **AzAdmin**
- Password **P@\$\$@1234567**

8. Click **Connect** to connect to the VM.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons. Below the navigation bar, the breadcrumb trail shows 'Home > Virtual machines > ServicesVM'. The main content area is titled 'ServicesVM | Bastion' and 'Virtual machine'. On the left, there is a sidebar with a 'Search' field and several navigation links under 'Settings': Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Networking, Connect, Windows Admin Center, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, Extensions + applications, Availability + scaling, and Configuration. The 'Connect' link is highlighted. The main pane displays information about Azure Bastion, stating it protects virtual machines by providing lightweight, browser-based connectivity without exposing them through public IP addresses. It mentions that deploying will automatically create a Bastion host on a subnet in your virtual network. The provisioning state is listed as 'Succeeded'. A section for entering a username and password is shown, with 'Username' set to 'AzAdmin' and 'Authentication Type' set to 'Password'. The password field contains '*****'. A 'Show' button is available. A checked checkbox 'Open in new browser tab' is present. A large red box highlights the 'AzAdmin' username and the password field. At the bottom, a blue 'Connect' button is visible, and a feedback link 'Tell us what you think of the Bastion experience' is at the bottom right.

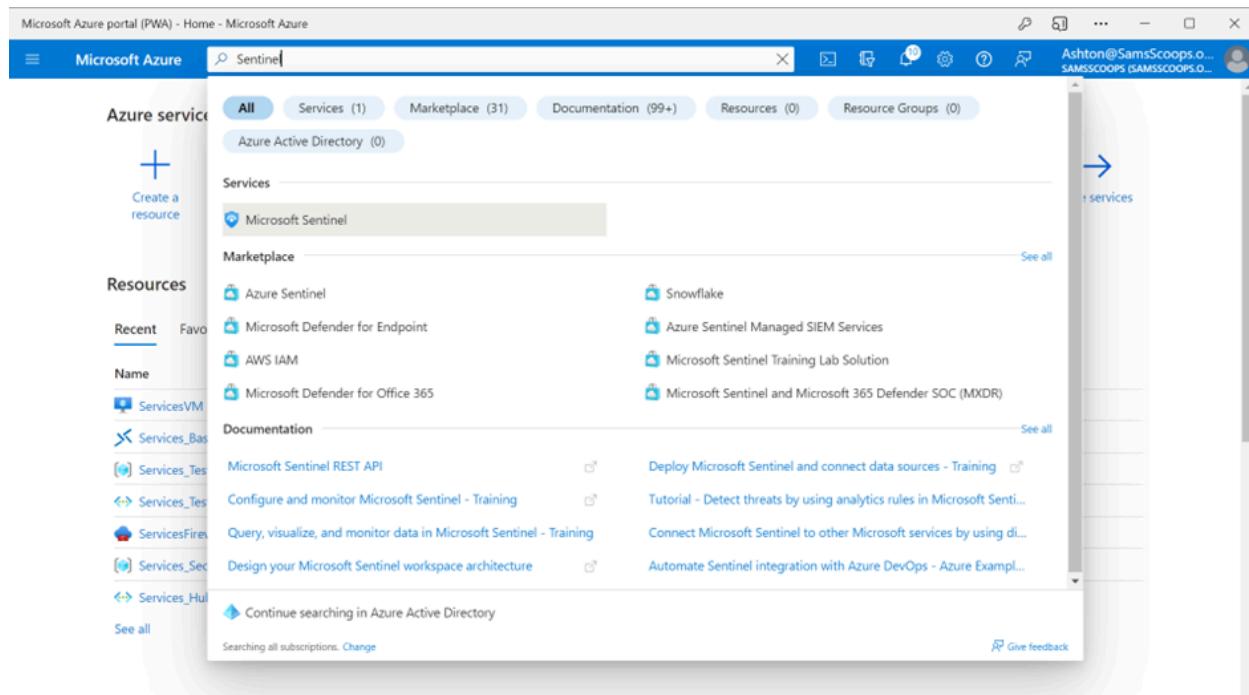
The connection to this virtual machine, via Bastion, will open directly in the Azure portal (over HTML5) using port 443 and the Bastion service.

The screenshot shows the Microsoft Server Manager interface. The title bar reads 'Server Manager > Dashboard'. The left sidebar has a 'Dashboard' section with 'Local Server' and 'All Servers' options. The main content area is titled 'WELCOME TO SERVER MANAGER'. It features a 'QUICK START' section with numbered steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Step 1 is highlighted with a red circle. Below this is a 'WHAT'S NEW' section and a 'LEARN MORE' button. The 'ROLES AND SERVER GROUPS' section shows 'Roles: 0 | Server groups: 1 | Servers total: 1'. It lists 'Local Server' (1 item, Manageability) and 'All Servers' (1 item, Manageability). A 'Hide' button is located in the top right corner of the main content area.

Step 7: Implement Microsoft Sentinel

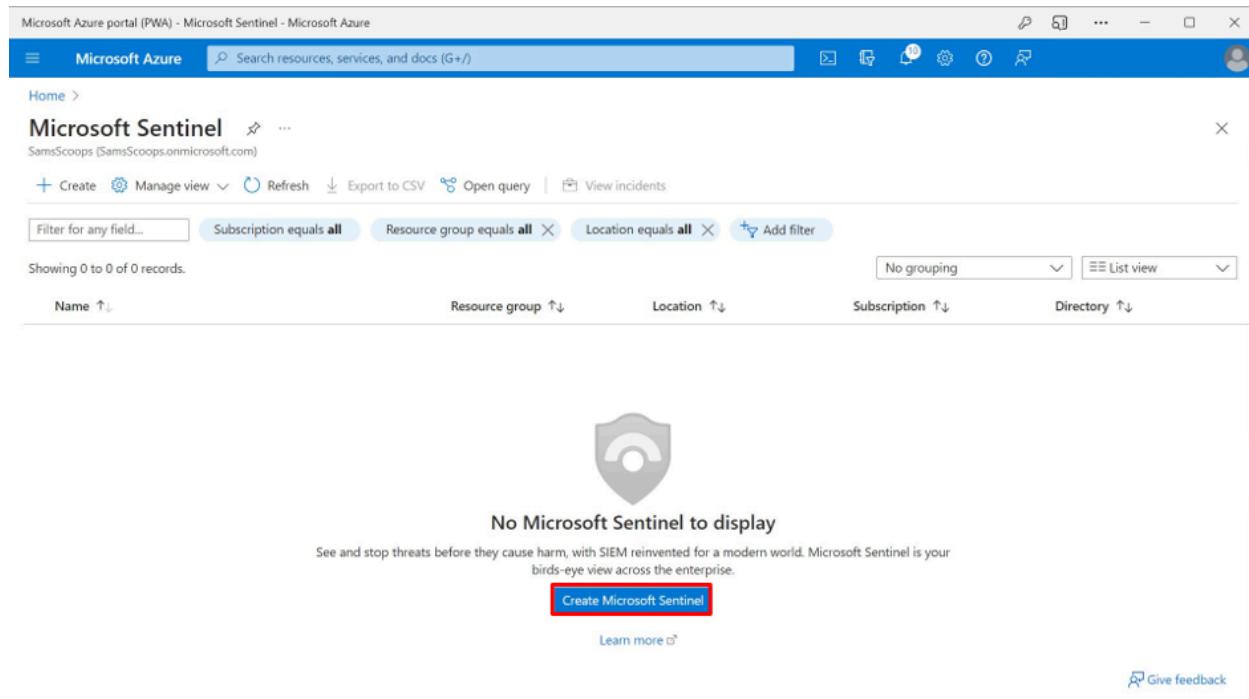
Implement Microsoft Sentinel ready for testing and training. If you need a reminder of the steps please refer back to the video [Microsoft Sentinel](#). If you need a reminder of the steps to do so please refer back to the video [Microsoft Sentinel](#).

1. From the Azure portal home page, search for and select **Microsoft Sentinel**.



The screenshot shows the Microsoft Azure portal's search interface. The search bar at the top contains the text "Sentinel". Below the search bar, there are several tabs: "All", "Services (1)", "Marketplace (31)", "Documentation (99+)", "Resources (0)", and "Resource Groups (0)". The "Services" tab is selected. In the main search results area, under the "Services" heading, "Microsoft Sentinel" is listed with a small icon and the text "Microsoft Sentinel". To the right of the search results, there is a sidebar with sections for "Marketplace" and "Documentation". The "Marketplace" section lists "Azure Sentinel", "Microsoft Defender for Endpoint", "AWS IAM", "Microsoft Defender for Office 365", "Snowflake", "Azure Sentinel Managed SIEM Services", "Microsoft Sentinel Training Lab Solution", and "Microsoft Sentinel and Microsoft 365 Defender SOC (MXDR)". The "Documentation" section lists several training articles: "Microsoft Sentinel REST API", "Configure and monitor Microsoft Sentinel - Training", "Query, visualize, and monitor data in Microsoft Sentinel - Training", "Design your Microsoft Sentinel workspace architecture", "Deploy Microsoft Sentinel and connect data sources - Training", "Tutorial - Detect threats by using analytics rules in Microsoft Senti...", "Connect Microsoft Sentinel to other Microsoft services by using di...", and "Automate Sentinel integration with Azure DevOps - Azure Exempl...". At the bottom of the search results, there is a link to "Continue searching in Azure Active Directory" and a "Give feedback" button.

2. Select **Create Microsoft Sentinel**.



The screenshot shows the Microsoft Sentinel blade within the Azure portal. At the top, there is a navigation bar with "Microsoft Azure" and a search bar containing "Search resources, services, and docs (G+/)". Below the navigation bar, the title "Microsoft Sentinel" is displayed with a "Home >" link. Underneath the title, it says "SamsScoops (SamsScoops.onmicrosoft.com)". There are several action buttons: "+ Create", "Manage view", "Refresh", "Export to CSV", "Open query", and "View incidents". Below these buttons are filter options: "Filter for any field...", "Subscription equals all", "Resource group equals all", "Location equals all", and "Add filter". A message "Showing 0 to 0 of 0 records." is displayed. The main content area has five columns: "Name ↑", "Resource group ↑", "Location ↑", "Subscription ↑", and "Directory ↑". In the center of the page, there is a large shield icon. Below the icon, the text "No Microsoft Sentinel to display" is centered. A descriptive paragraph follows: "See and stop threats before they cause harm, with SIEM reinvented for a modern world. Microsoft Sentinel is your birds-eye view across the enterprise." Below this text is a prominent red rectangular button with the white text "Create Microsoft Sentinel". At the bottom of the page, there is a "Learn more" link and a "Give feedback" button.

3. Select **Create a new workspace**.

Microsoft Azure portal (PWA) - Add Microsoft Sentinel to a workspace - Microsoft Azure

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

Home > Microsoft Sentinel >

Add Microsoft Sentinel to a workspace ...

+ Create a new workspace ⏪ Refresh

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...

No workspaces found

Create a new workspace

Add Cancel

4. Fill in the following deployment details for a log analytics workspace. Your current subscription will be already selected.

- Resource group: "Services_Test"
- Instance name: "ServiceSentinel"

5. Select **Review + Create**.

Microsoft Azure portal (PWA) - Create Log Analytics workspace - Microsoft Azure

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

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace >

Create Log Analytics workspace ...

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

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

Subscription * ○ Azure subscription 1 (1094ab39-adb6-44d9-bfe6-51c9ea920f2e) ▾

Resource group * ○ Services_Test ▾

Create new

Instance details

Name * ○ ServiceSentinel ▾

Region * ○ East US ▾

Review + Create ⏪ Previous Next : Tags >

6. Select **Create**.

Microsoft Azure portal (PWA) - Create Log Analytics workspace - Microsoft Azure

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

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace >

Create Log Analytics workspace ...

Validation passed

Basics Tags Review + Create

Log Analytics workspace by Microsoft

Basics

Subscription	Azure subscription 1
Resource group	Services_Test
Name	ServiceSentinel
Region	East US

Pricing

Pricing tier Pay-as-you-go (Per GB 2018)

The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the [Azure Monitor pricing page](#). You can change to a different pricing tier after the workspace is created. [Learn more](#) about Log Analytics pricing models.

Create « Previous Download a template for automation

This screenshot shows the 'Create Log Analytics workspace' wizard. It has completed validation. The 'Review + Create' tab is selected. The workspace is named 'ServiceSentinel'. The 'Pricing tier' is set to 'Pay-as-you-go (Per GB 2018)'. A note about regional pricing is present. At the bottom, there are 'Create' and 'Download a template for automation' buttons.

7. After a few seconds a new workspace is created. Select **Service_Sentinel**.
8. Select **Add**.

Microsoft Azure portal (PWA) - Add Microsoft Sentinel to a workspace - Microsoft Azure

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

Home > Microsoft Sentinel >

Add Microsoft Sentinel to a workspace ...

+ Create a new workspace ⏪ Refresh

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

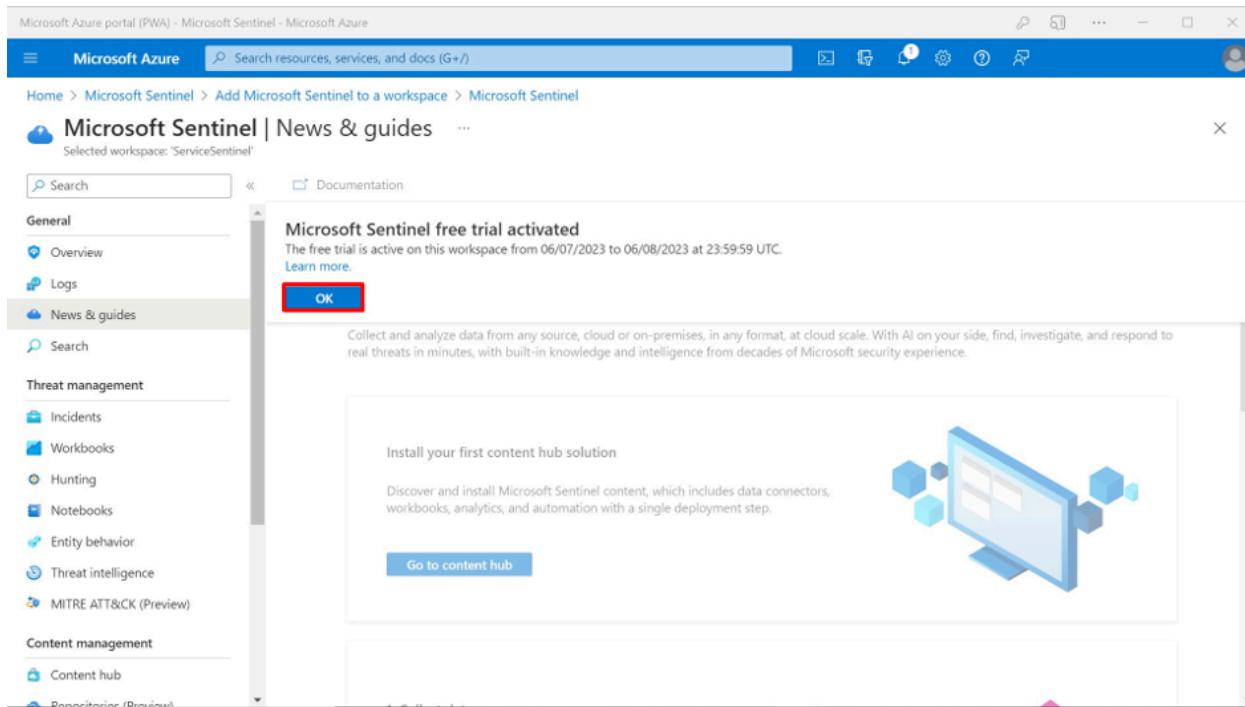
Filter by name...

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
ServiceSentinel	eastus	services_test	Azure subscription 1	SamsScoops

Add Cancel

This screenshot shows the 'Add Microsoft Sentinel to a workspace' screen. It lists a workspace named 'ServiceSentinel' with location 'eastus', resource group 'services_test', subscription 'Azure subscription 1', and directory 'SamsScoops'. The 'Add' button is highlighted with a red box.

9. Select **OK** to the Microsoft Sentinel free trail.



Clean-up

If you are using your own Azure subscription, it is recommended that you follow the clean-up instructions to stop compute resources after completing each lesson. When you're working in your own subscription, it's also a good idea at the end of a project to identify whether you still need the resources you created. Resources left running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

Please refer to the reading, [Clean up resources](#) for instructions on how to delete resources after you've completed the exercise.

Remember to also delete the Standard Firewall as it cannot be powered off and you will continue being charged if it stays active.

Conclusion

Completing this final course project allowed you to put into practice what you have learned about securing virtual machines. By setting up a testing environment for a small business you demonstrated your understanding of how to configure and deploy key Microsoft services. You first demonstrated how to deploy a virtual machine, before moving on to protecting the network by deploying an Azure firewall. Next, you demonstrated how to protect management ports on that VM by using JIT and Azure Bastion combined. And finally, you demonstrated how to deploy Microsoft Sentinel ready for different data connectors to be added in the future.