

A graphic element on the left side of the slide features a stylized map of Thailand. The map is composed of several overlapping triangles in shades of red, blue, and grey, creating a layered effect. The word "THAILAND" is overlaid on this graphic in large, white, sans-serif capital letters.

THAILAND

Cyber
Security



 Microsoft Security

Cloud SECURITY Intensive

Do Pre-test first:
[forms.office.com
/r/nAVERFASdE](https://forms.office.com/r/nAVERFASdE)



[github.com
/SarahAHA121
/MSCloudSeclntensive](https://github.com/SarahAHA121/MSCloudSeclntensive)





ZERO LO

Basic On Tour

 M365 Admin

 Azure Resource Creation

 Defender XDR Admin





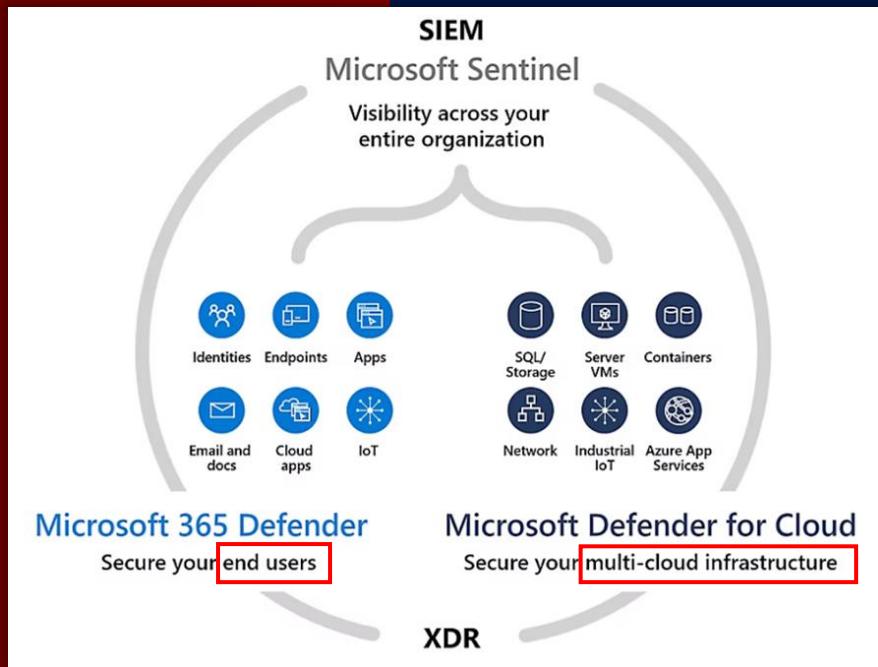
Why MS Cloud Sec needs:



M365



365 Defender





Why MS Cloud Sec needs:

M365 → 365 Defender





Copilot for **Security**

securitycopilot.
microsoft.com

Why MS Cloud Sec needs:



M365

Tend to be
centralize more



365 Defender

Improved to be for
“multi” Cloud/Platforms

Old Name

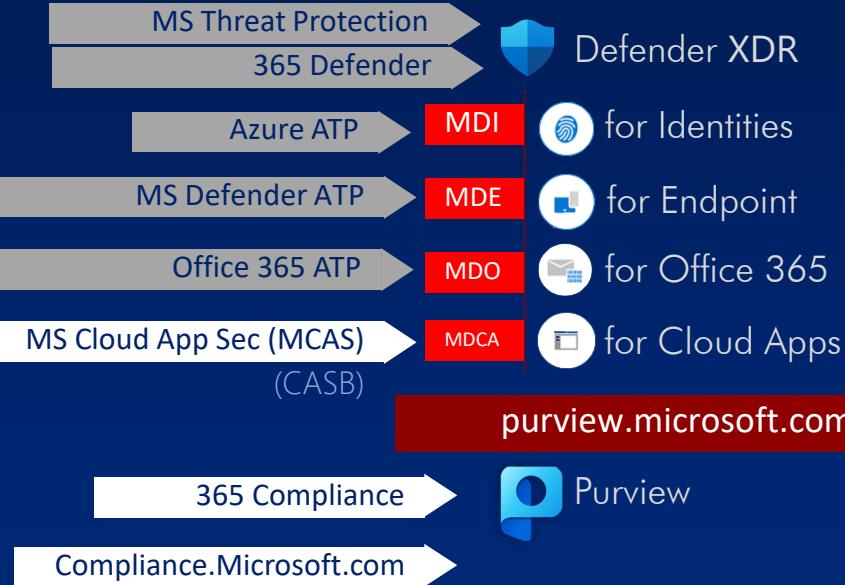
New Name



M365



AZURE



portal.azure.com



Azure AD

entra.microsoft.com



Network Security



Defender for Cloud

Azure Defender



Cloud Security Posture
Management (CSPM)

Azure Security Center



(CWP) Defender for
Server/Storage/SQL/etc.



Sentinel

intune.microsoft.com

Intune
(Endpoint Manager)





-  Portal.Azure.com
-  Admin.Microsoft.com
-  Defender.Microsoft.com
-  Entra.Microsoft.com
-  Intune.Microsoft.com
-  Purview.Microsoft.com
-  SecurityCopilot.
Microsoft.com



Portal.Azure.com

https://portal.azure.com/#home

Microsoft Azure

Search for resources you want to create / config.

Or click+ “Create resource” to browse

Azure services

- All Services
- Services
 - Network security groups
 - Network security groups (classic)
 - Application security groups
 - Groups
- Marketplace
 - Network security group
 - Application security group
 - Azure Network Security Groups solution for Sentinel
- Documentation
 - Azure network security groups overview
 - Introduction to Azure security
 - Network security group - how it works
 - Azure application security groups overview
- Continue searching in Microsoft Entra ID
- Resource groups

Give feedback

Subscriptions

Open Copilot

Open Cloud “Shell”

sarah@thaiysec.com THAIYSEC (THAIYSEC.COM)

Copilot Preview

Network Security Group (Classic) ต่างจาก Network Security Group ใหม่อย่างไรบ้างค่ะ

The main difference between the classic Network Security Group (NSG) and the new NSG in Azure is the deployment model. The classic NSG is used in the classic deployment model, while the new NSG is used in the Resource Manager deployment model. The classic NSG is limited to controlling traffic at the virtual network level, while the new NSG can control traffic at the subnet and network interface level. Additionally, the new NSG allows for more granular control over traffic by allowing the use of service tags and application security groups.

References:

- [Network security groups overview](#)
- [Azure for network engineers - Security](#)
- [How network security groups filter network traffic](#)

AI-generated content may be incorrect

1 of 15 requests

What are the benefits of using the Resource Manager deployment model for NSGs?

Can you explain how to create a new NSG in Azure?

What are service tags and application security groups in the context of NSGs?

I want to ...

0 / 500

Ask Copilot for free: technical details, our resources info, etc.

THCS



Portal.Azure.com

https://portal.azure.com/#settings/directory

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

Portal settings | Directories + subscriptions

Search menu

Directories + subscriptions

Appearance + startup views

Language + region

My information

Signing out + notifications

Useful links

- Learn more about settings ↗
- Safelist URLs ↗
- Microsoft partner network
- Privacy Statement ↗
- More Azure resources
- Provide feedback

Subscription - Groups of “Resources” contract (billing) w/ Azure

All services and resources across the Azure portal will inherit the selection from basic filtering. Your selection will also be saved and reloaded the next time you sign in or reload the Azure portal.

Default subscription filter ⓘ

Azure subscription 1 - Don't see a subscription? Switch to another directory.

Advanced filters ⓘ

Directories ⓘ

Switching directories will reload the portal. The directory you choose will impact the subscription, resource group, and region filters that are available in the portal. [Learn more about directories.](#) ↗

Current directory ⓘ : ThaiCySec (thaicysec.com)

Startup directory ⓘ : Last visited

Favorites All Directories

Search

Directory name ↑↓ Domain ↑↓ Directory ID ↑↓

Directory name ↑↓	Domain ↑↓	Directory ID ↑↓
ThaiCySec	thaicysec.com	e694a5e9-d890-472c

Tenant - top security boundary
Directory - Entra ID (Biggest Group of Directory Objects)

ThaiCySec

sarah@thaicysec.com THAICYSEC (THAICYSEC.COM)

Sign out

sarah@thaicysec.com

sarah@thaicysec.com

[View account](#)

[Switch directory](#)

kmtnb.ac.th s6607031857086@kmtnb.ac.th

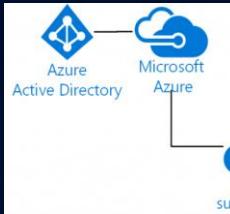
akeake sarah.h@akeake.com

Sign in with a different account

In Azure?

- Can you explain how to transfer a subscription to a different directory? ↗
- What are the best practices for managing Azure subscriptions? ↗
- I want to ... ↗

0 / 500



Can switch between users, or directory (Tenant) under same user.





Portal.Azure.com

Management groups ThaiCySec

+ Create + Add subscription

Search Overview Get started Settings

Human Resources IT Marketing

Dev/Test subscription Apps Production Free trial subscription Free trial subscription

Geo Region 1 Geo Region 2 EA subscription EA subscription EA subscription EA subscription EA subscription

Tenant root group Management groups Subscriptions Resource groups Resources

Showing 1 subscriptions in 1 group

Search by name or ID

Name Type ID Total subscriptions

Tenant Root Group Management group 1

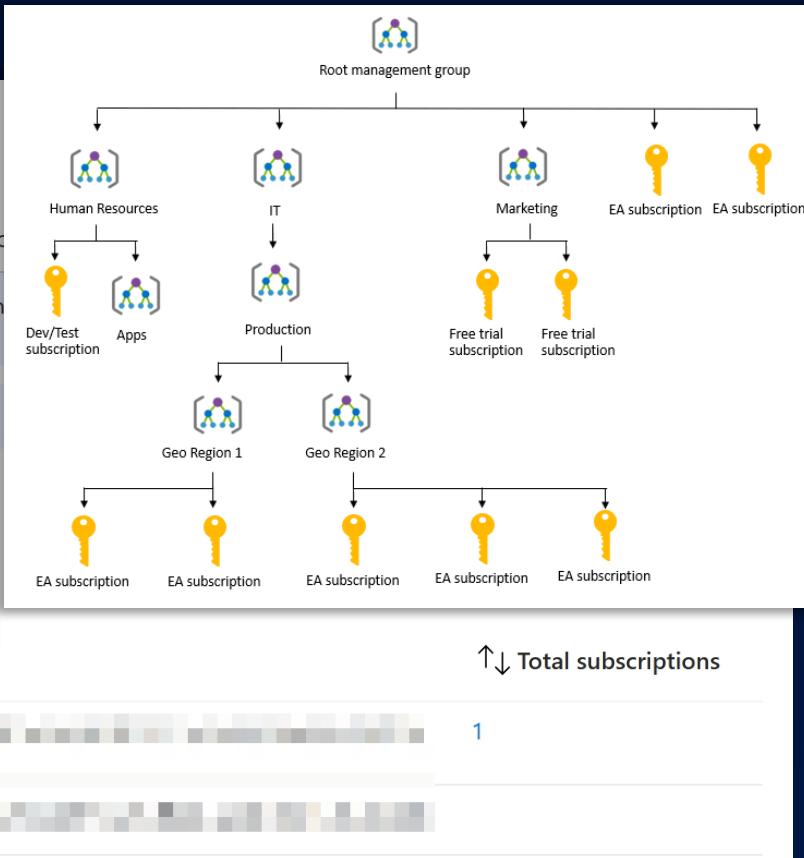
Azure subscription 1 Subscription

If you want to manage multiple subs, including root tenant, must get "User Access Admin" RBAC roles in every subs scope

Tenant as top container. But Directory is about identities.

One user can create multiple tenants via Entra ID

Name	Type	ID	Total subscriptions
Tenant Root Group	Management group	[Redacted]	1
Azure subscription 1	Subscription	[Redacted]	





Entra is family.
Entra ID (Identity) is
one of them,
configure directory
(tenants)



Entra.Microsoft.com

https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView

Microsoft Entra admin center Search resources, services, and docs (G+/-)

Identity Add Manage tenants What's new Preview features Got feedback?

Azure Active Directory is now Microsoft Entra ID. [Learn more](#)

Overview Monitoring Properties Recommendations Tutorials

Search your tenant

Basic information

Name	Tenant ID	Primary domain	Users	Groups	Applications	Devices
ThaiCySec	e694a5e9-d890-472c-9fa1-8be5b87b823d	thaicysec.com	14	22	10	15

License Microsoft Entra ID Free

Alerts

Azure AD is now Microsoft Entra ID

Check for Entra ID license, which is Tenant-wide (Honor System)

Honor system

License that applicable throughout "tenant", even specs defined "per user/device"

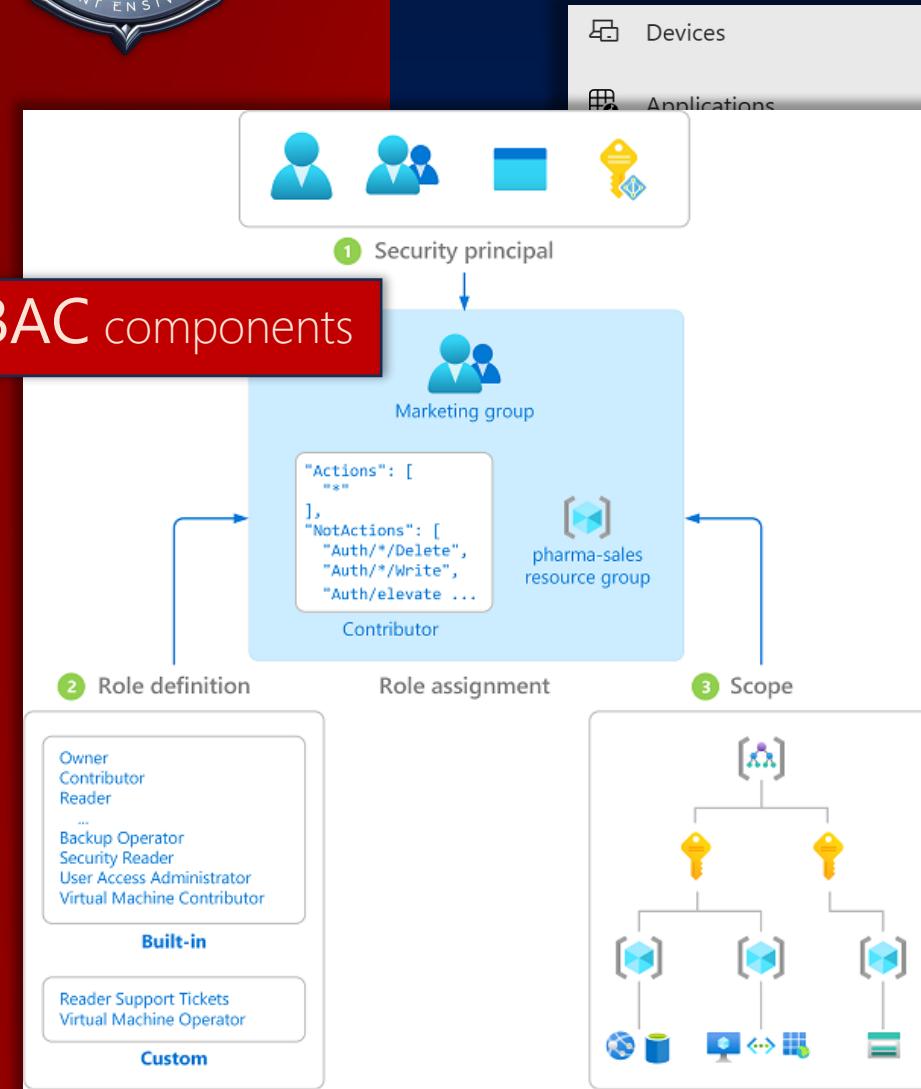
Such as Entra ID P1/P2, MDE P1/P2, etc.

MS **honors** customer to be honest, but keep auditing randomly





Entra.Microsoft.com



Devices Applications

Overview Monitoring Properties Recommendations Tutorials

Access management for Azure resources

Sarah ThaiCySec (sarah@thaicysec.com) can manage access to all Azure subscriptions and management groups in this tenant.

Learn more ↗

Yes

Turn on to add “User Access Admin” RBAC role (definition) to Principal: Sarah, Scope: whole tenant (every subs)

Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity-related attacks.

Learn more ↗

i Your organization is currently using Conditional Access policies which prevents you from enabling security defaults. You can use Conditional Access to configure custom policies that enable the same behavior provided by security defaults.

Manage Conditional Access

Save Discard

Do not forget to click “Save” when change / turn setting on/off



Portal.Azure.com

Microsoft Azure sarah@thaiysec.com THAIYSEC (THAIYSEC.COM)

Search resources, services, and docs (G+)

Copilot

Home > Management groups

ThaiCySec

Search

+ Create + Add subscription Refresh Expand / Collapse all Export to CSV Feedback

Use management groups to group subscriptions. Click on an existing group to drill in, view details and govern resources. Right-click on any subscription or management group to launch quick actions. Click the "Get Started" tab to learn more.

Search by name or ID

Showing 3 subscriptions in 2 groups

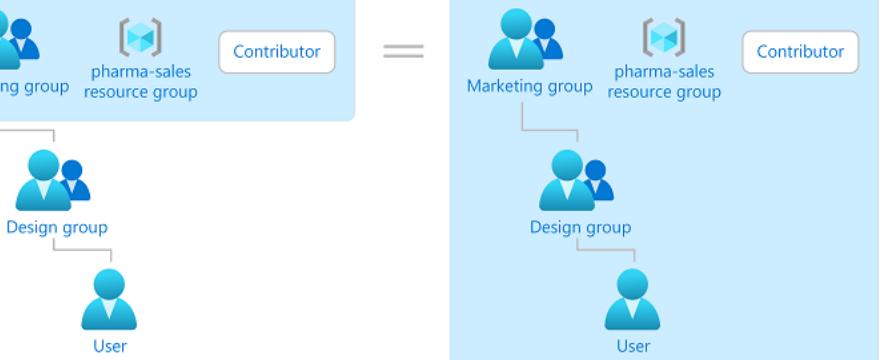
Name	Type	ID	Total subscriptions
Tenant Root Group	Management group	[REDACTED]	3
Azure subscription 1	Subscription	[REDACTED]	
Azure subscription 1	Subscription	[REDACTED]	
Infrastructure Team	Management group	[REDACTED]	1
AZ-500	Subscription	[REDACTED]	

With “User Access Admin” role, now we can configure every subs in top tenant.





When click IAM in each Resource /RG/subs/MG, it means "Scope"



A Portal.Azure.com

Role Assignment: 3 components: Scope, Role (Def), Principal

Click "Role" to see Role (Def) list applicable with this scope.

Number of role assignments for this subscription: 8

Privileged: 4

Built-in Roles:
Owner – assign
Contributor – create/edit
Reader – Read only

Name	Type	Role	Scope	Condition
Admin ThaiCySec	User	Owner	This resource	Add
Admin ThaiCySec	User	Owner	Management group (Inherited)	None
Admin ThaiCySec	User	User Access Administrator	Root (Inherited)	None
Sarah ThaiCySec	User	User Access Administrator	Root (Inherited)	None

Sec Principal (User)

Role(Def)

Scope

(inherited) means original scope is bigger container (Root Tenant)



Azure

Spending Limit

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

Home > Upgrade > Get started with your upgraded account > Cost Management + Billing | Billing scopes > Saran Hansakul

Saran Hansakul | Budgets

Billing profile

+ Add Refresh Help

Scope : Saran Hansakul

Search by name All periods

Name	Scope	Reset period	Creation date	Expiration date
10USD-mth	5OUA-QSOH-BG7-P...	Monthly	6/1/2024	5/31/2026

Search Overview Access control (IAM) Billing scopes Diagnose and solve problems Cost management Cost analysis Cost alerts Budgets Advisor recommendations



Azure

Spending Limit

Home > Upgrade > Get started with your upgraded account > Cost Management + Billing | Billing

Create budget

Budget

✓ Create a budget ✓ Set alerts

Configure alert conditions and send email notifications based on your spend.

* Alert conditions

Type	% of budget	Amount
Forecasted	80	8
Actual	100	10
Select type	Enter %	-

Alert type:
Forecasted and
Actual usages

https://portal.azure.com/#view/Microsoft_Azure_CostManagement/BudgetCreateBlade/id/%2Fproviders%2FMicrosoft.Billing

Microsoft Azure

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

Home > Upgrade > Get started with your upgraded account > Cost Management + Billing | Billing scopes > Saran Hansakul | Budgets >

Create budget

Budget

✓ Create a budget ② Set alerts

Create a budget and set alerts to help you monitor your costs.

Budget scoping

The budget you create will be assigned to the selected scope. Use additional filters like resource groups to have your budget monitor with more granularity as needed.

Scope Saran Hansakul

Filters + Add filter

Budget Details

Give your budget a unique name. Select the time window it analyzes during each evaluation period, its expiration date and the amount.

* Name 10USD-mth

* Reset period Monthly

* Creation date 2024 June 1

* Expiration date 2026 May 31

Budget Amount

Give your budget amount threshold

Amount * 10

Reach limit, services stop / de-allocated Storage > Read-only

Previous Next >



Azure

Resource Creation

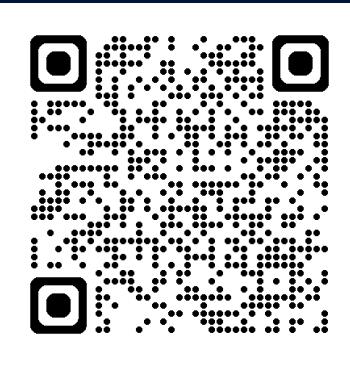
A screenshot of the Azure portal's Resource Groups page. The URL is https://portal.azure.com/#browse/resourcegroups. The page shows a list of resource groups under the 'ThaiCySec' subscription. A red arrow points to the 'Create' button in the top-left corner of the list area.

A screenshot of the 'Create a resource group' wizard in the Azure portal. The URL is https://portal.azure.com/#create/Microsoft.ResourceGroup. The 'Basics' tab is selected. A red box highlights the 'Resource group' field, which contains 'SarahRG'. Another red box highlights the 'Region' field, which contains '(US) West US 2'. A red box also highlights the 'Review + create' button at the bottom. To the right, a blue box contains the text: 'Regions effect' followed by '1. Latency' and '2. Price rate'. Another blue box contains the text: 'Some resources need same region: VM+VNet, etc.'.



Azure

Pricing per Region



Azure pricing

Get the best value at every stage of your cloud journey with simple pricing and predictable, transparent costs.

[See pricing by product](#)[Pricing calculator](#)

OS/Software:	Category:	VM series:	Region:
Windows OS	All	All	East US 2
Currency:	Display pricing by:	Pricing model & comparison:	<input checked="" type="radio"/> Show Azure Hybrid Benefit pricing
United States – Dollar (\$) USD	Month	Savings plan (1 & 3 year)	

Showing 103 applicable virtual machine series.

Instance	vCPU(s)	RAM	Temporary storage	Pay as you go with AHB	1 year savings plan with AHB	3 year savings plan with AHB	Spot with AHB	Add to estimate
B2ts v2	2	1 GiB	0 GiB	\$7.5920/month	\$5.0881/month ~32% savings	\$3.4164/month ~54% savings	\$1.8980/month ~75% savings	+

Cheapest regions:
East US 1/2
West US 1/2

OS/Software:	Category:	VM series:	Region:
Windows OS	All	All	Southeast Asia
Currency:	Display pricing by:	Pricing model & comparison:	<input checked="" type="radio"/> Show Azure Hybrid Benefit pricing
United States – Dollar (\$) USD	Month	Savings plan (1 & 3 year)	

Showing 103 applicable virtual machine series.

Instance	vCPU(s)	RAM	Temporary storage	Pay as you go with AHB	1 year savings plan with AHB	3 year savings plan with AHB	Spot with AHB	Add to estimate
B2ts v2	2	1 GiB	0 GiB	\$9.6360/month	\$6.4532/month ~33% savings	\$4.2413/month ~55% savings	\$2.4090/month ~74% savings	+



Azure

Resource Creation

Home > Resource groups >

Create a resource group

Validation passed.

Basics Tags Review + create

Basics

Subscription Azure subscription 1

Resource group SarahRG

Region West US 2

Tags

None

Create

< Previous

Next >

Download a template

https://portal.azure.com/#view...

Microsoft Azure

Home >

Resource groups

ThaiCySec

+ Create Manage view Refresh Export to CSV

Filter for any field... Add filter More (2)

No grouping

Showing 1 to 1 of 1 records.

Name ↑	Subscription ↑	Location ↑
SarahRG	Azure subscription 1	West US 2





Azure

Delete Resource

Best practices:
Create RG first.
Create from bigger scope

Microsoft Azure Search resources, services, and docs (G+/-) Copilot | ... sarah@thaicysec.com THAICYSEC (THAICYSEC.COM)

Home > Resource groups >

SarahRG ... Resource group

Search Create Manage view Delete reso

Overview Essentials

Resources Recommendations

Filter for any field... Type equals all

Showing 0 to 0 of 0 records. Show hidden typ

Name ↑

The following resource group and all its dependent resources will be permanently deleted.

Delete a resource group

Resource group to be deleted

SarahRG Delete

Dependent resources to be deleted (0)

All dependent resources, including hidden types, are shown

Name	Resource type
------	---------------

Enter resource group name to confirm deletion *

SarahRG Delete Cancel

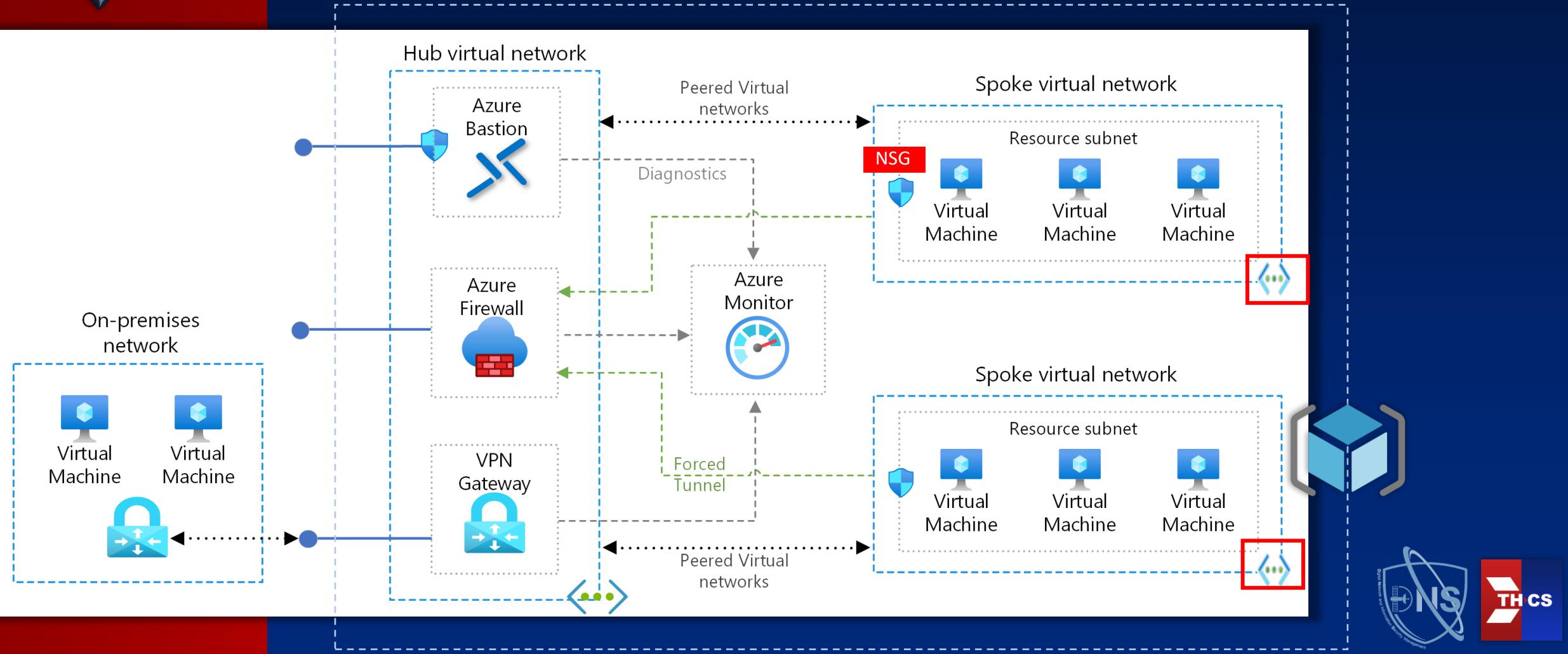
So you can be confident that you erase all resources in the same lab





Virtual Network

Then we should plan:
VNet > Subnet > Virtual
Appliances (VM/Bastion/FW,etc.)





Virtual Network

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
Resource group * SarahRG

Instance details

Virtual network name * SarahVNET
Region * (US) West US 2

Use same RG we created to group this lab altogether

Can be different region than RG in case of flexibility: DR, etc.

Home > Virtual networks > Create virtual network

Basics **Security** IP addresses Tags Review + create

Enable Virtual network encryption to encrypt traffic traveling within the virtual network. Virtual machines must have accelerated networking enabled. Traffic to public IP addresses is not encrypted. [Learn more](#).

Virtual network encryption

Azure Bastion

Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. [Learn more](#).

Enable Azure Bastion

Azure Bastion host name

Azure Bastion public IP address *





Virtual Network

Home > Virtual networks >

Create virtual network ...

Basics Security IP addresses Tags Review + create

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space | ▾

10.0.0.0/16

Delete address space

10.0.0.0

/16

10.0.0.0 - 10.0.255.255

65,536 addresses

+ Add a subnet

Subnets

IP address range

Size

NAT gateway

default

10.0.0.0 - 10.0.0.255

/24 (256 addresses)

-



AzureBastionSubnet

10.0.1.0 - 10.0.1.63

/26 (64 addresses)

-



Notice: there are subnets added auto from Sec components we choosed

Previous

Next

Review + create

Home > Virtual networks >

Create virtual network ...

Basics Security IP addresses Tags Review + create

[View automation template](#)

Basics

Subscription Azure subscription 1
Resource Group SarahRG
Name SarahVNET
Region West US 2

Security

Azure Bastion Enabled
- Name (New) SarahVNET-Bastion
- Public IP Address (New) sarahvnet-bastion

Azure Firewall Disabled

Azure DDoS Network Protection Disabled

IP addresses

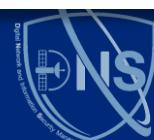
Address space 10.0.0.0/16 (65,536 addresses)
Subnet default (10.0.0.0/24) (256 addresses)
Subnet AzureBastionSubnet (10.0.1.0/26) (64 addresses)

Tags

Previous

Next

Create





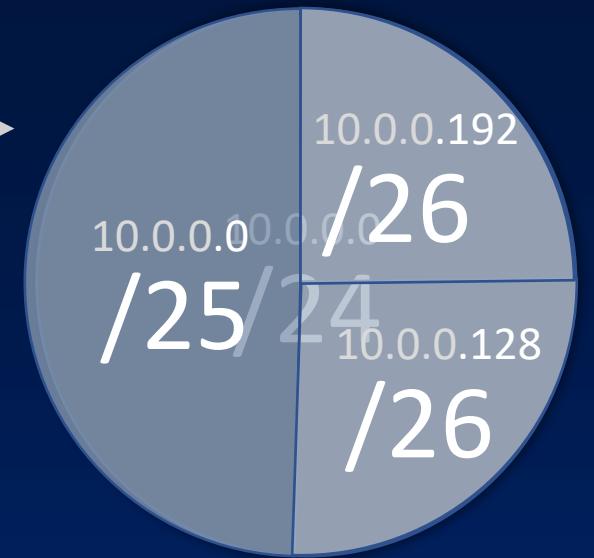
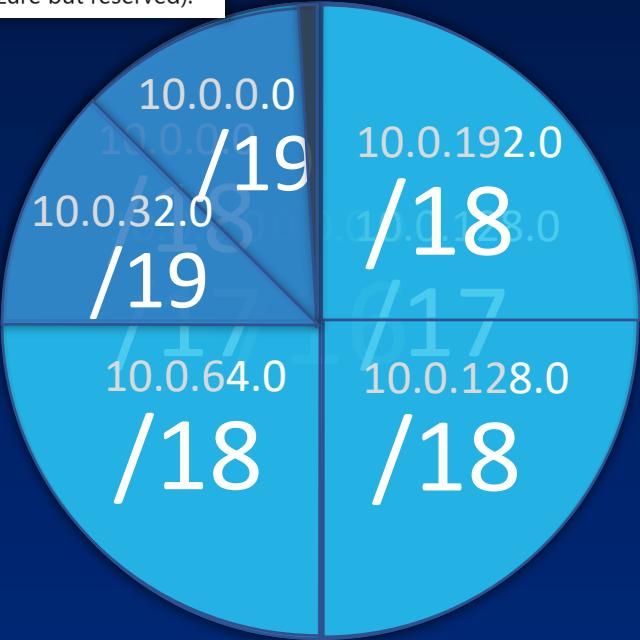
Reserved IP Addresses in Azure Subnets

For each subnet in Azure, the following IP addresses are reserved:

1. First IP address: Network address.
2. Second IP address: Reserved by Azure for the default gateway.
3. Third IP address: Reserved by Azure for DNS server.
4. Fourth IP address: Reserved by Azure for future use.
5. Last IP address: Broadcast address (not used in Azure but reserved).

Address Space
“Overlapped”

Cannot be peered
or connect via Vnet
(VPN) Gateway



Address Space
IP Subnetting



Virtual Machine

Microsoft Azure

Home >

Virtual machines

ThaiCySec

+ Create ▾ Switch to classic Reservations

- Azure virtual machine Create a virtual machine hosted by Azure
- Azure virtual machine with preset configuration Create a virtual machine with presets based on your workloads
- More VMs and related solutions Discover and deploy full workloads and Azure products for your business needs

https://portal.azure.com/#create/VM

Microsoft Azure

Home > Virtual machines > Create a virtual machine

Click here to try out the Azure Copilot for additional recommendations while creating a virtual machine →

Configure Azure Spot

Run with Azure Spot discount

Size * See all sizes

Request quota Refresh quota

Enable Hibernation

Administrator account

< Previous Next : Disks > Review + create Give feedback

Use Copilot to help setting options of your choices

Azure Spot is “sometimes” available, but “not” for Free VS (MCT) credit sub

Copilot Preview

Help me choose the right VM size for my workload

Help me create a low cost VM

I can help guide you through three options to lower the cost of your virtual machine.

1. Azure Spot
2. Low Cost Size
3. Auto-shutdown

AI-generated content may be incorrect

Enable Skip

AI-generated content may be incorrect

Cancel

I want to ...

0 / 500



Virtual Machine

https://learn.microsoft.com/en-us/azure/virtual-machines/sizes-b-series-burstable

B-series burstable virtual machine sizes

Article • 01/26/2024 • 16 contributors

In this article

Applies to: ✓ Linux VMs ✓ Windows VMs ✓ Flexible scale sets ✓ Uniform scale sets

The B-series VMs can be deployed on a variety of hardware types and processors, so competitive bandwidth allocation is provided. B-series run on the 3rd Generation Intel® Xeon® Platinum 8370C (Ice Lake), the Intel® Xeon® Platinum 8272CL (Cascade Lake), the Intel® Xeon® 8171M 2.1 GHz (Skylake), the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell), or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors. B-series VMs are ideal for workloads that do not need the full performance of the CPU continuously, like web servers, proof of concepts, small databases and development build environments. These workloads typically have burstable performance requirements. To determine the physical hardware on which this size is deployed, query the virtual hardware from within the virtual machine. The B-series provides you with the ability to purchase a VM size with baseline performance that can build up credits when it is using less than its baseline. When the VM has accumulated credits, the VM can burst above the baseline using up to 100% of the vCPU when your application requires higher CPU performance.

Configure size

Size * Stop / Deallocate Delete

See all sizes

< Previous Next : Disks > Review + create Give feedback

Copilot Preview

the cost of your virtual machine.

1. Azure Spot
2. Low Cost Size
3. Auto-shutdown

AI-generated content may be incorrect

Option 1: Use Azure Spot Virtual Machines to take advantage of our unused capacity at a significant cost savings. At any point in time when Azure needs the capacity back, the Azure infrastructure will evict Azure Spot Virtual Machine

Enable

AI-generated content may be incorrect

B = (Resource) Burstable
Burst only when use, such as Web Server.

Option 2: The B2s size from our B-series family is one of our lowest cost VM sizes.

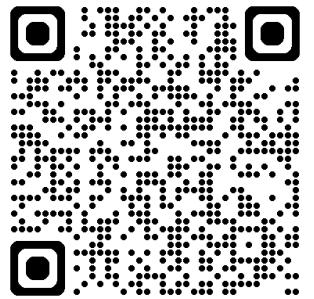
Use Standard_B2s_v2 size See more sizes

AI-generated content may be incorrect

Cancel



learn.microsoft.com
/azure/virtual-
machines/sizes-b-
series-burstable





Virtual Machine

Home > Virtual machines >

Create a virtual machine

Management

Configure management options for your VM.

Microsoft Defender for Cloud

Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

Enable basic plan for free (1)

This will apply to every VM in the selected subscription

Defender for Cloud: Free Basic Plan = CSPM

Enable system assigned managed identity

Microsoft Entra ID

Login with Microsoft Entra ID (1)

RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Microsoft Entra ID login. [Learn more](#)

Microsoft Entra ID login now uses SSH certificate-based authentication. You will need to use an SSH client that supports OpenSSH Cloud Shell from the Azure Portal. [Learn more](#)

Enable auto-shutdown

Enable auto-shutdown (1)

< Previous Next : Monitoring > Review + create

Give feedback

Copilot Preview

Option 2: The B2s size from our B-series family is one of our lowest cost VM sizes.

Use Standard B2s v2 size

A third option is to configure auto-shutdown on your VM. This will shut down your VM in the off-hours to save costs. This can be enabled in the management tab.

Continue to Management tab Skip

AI-generated content may be incorrect

Enabling and configuring auto-shutdown will lower costs by ensuring that your virtual machine is not inadvertently left running.

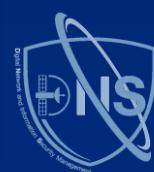
Enable auto-shutdown Skip

AI-generated content may be incorrect

Cancel

I want to ...

0 / 500





Virtual Machine

Image * ⓘ

Windows 11 Pro, version 22H2 - x64 Gen2

See all images | Configure VM generation

Home > Virtual machines >

Create a virtual machine

Great, you have configured a low cost VM. You can review and create the VM, or continue to configure.

[Continue to Review + Create](#) [Keep configuring](#)

AI-generated content may be incorrect

Basics Disks Networking Management Monitoring Advanced Tags Review +

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or for full customization. [Learn more](#)

Project details

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

Subscription * ⓘ Azure subscription 1

Resource group * ⓘ SarahRG [Create new](#)

Instance details

Virtual machine name * ⓘ SarahVM01

Region * ⓘ (US) West US 2

Availability options ⓘ Availability zone

Availability zone * ⓘ Zone 1

You can now select more zones for redundancy.

Licensing

I confirm I have an eligible Windows 10/11 license with multi-tenant hosting rights.

[Review multi-tenant hosting rights for Windows 10/11 compliance](#)

Must checked whenever choosing Windows as OS

Inbound port rules

Select which virtual machine network ports are accessible from the internet. You can change inbound port rules on the Networking tab.

Public inbound ports * ⓘ None Allow selected ports

Select one or more ports

Because we will use Bastion as Jumpbox

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

Image * ⓘ

Windows 11 Pro, version 22H2 - x64 Gen2

See all images | Configure VM generation

Username * ⓘ sarah

Password * ⓘ [Change](#)

Confirm password * ⓘ [Change](#)

Public inbound ports * ⓘ None Allow selected ports

Select one or more ports

Review + create

Give feedback

NS **THCS**



Virtual Machine

Home > Virtual machines >

Create a virtual machine

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 * ⓘ [Create new](#)

Subnet * ⓘ [Manage subnet configuration](#)

Public IP ⓘ [Create new](#)

NIC network security group ⓘ Basic None Advanced

Public inbound ports * ⓘ None Allow selected ports

Use same Vnet we created, then subnets will be auto listed for us

Because public IP, NIC, are separated resources

Delete public IP and NIC when VM is deleted

For more consistency,
easy to manage = same func VM should be in same subnet

A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, the virtual machine. To simplify management of security rules, it's recommended that you associate a network security group to individual subnets, rather than individual network interfaces within the subnet, whenever possible.

NIC network security group Basic None



Virtual Machine

Validation must be passed so we can create this VM

Review + create

Cost given below is an estimate and not the final price. For all your pricing needs, please use the pricing calculator.

Price
1 X Standard B2s v2 by Microsoft
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply
0.0208 USD/hr
[Pricing for other VM sizes](#)

Check estimated price before create

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

Deployment is in progress

Deployment name: CreateVm-microsoftwindowsdesktop.windows-...
Subscription: Azure subscription 1
Resource group: SarahRG
Start time: 6/29/2024, 7:03:32 AM
Correlation ID: abe7d572-c799-4f02

Deployment details

Resource	Type	Status
SarahVM01	Microsoft.Compute/virtualMachines	Created
sarahvm01809_z1	Microsoft.Network/networkInterfaces	Created
SarahVM01-ip	Microsoft.Network/publicIpAddresses	OK
SarahVM01-nsg	Microsoft.Network/networkSecurityGroups	OK

Your deployment is complete

Deployment name: CreateVm-microsoftwindowsdesktop.windows-...
Subscription: Azure subscription 1
Resource group: SarahRG
Start time: 6/29/2024, 7:03:32 AM
Correlation ID: abe7d572-c799-4f02-bad5-d1e160827fe8

Deployment details

Next steps

- Setup auto-shutdown Recommended
- Monitor VM health, performance and network dependencies Recommended
- Run a script inside the virtual machine Recommended

Go to resource

Create another VM





Virtual Machine

Home > CreateVm-microsoftwindowsdesktop.windows-11-win11-20240629064516 | Overview >

SarahVM01

Virtual machine

Search

Connect ▾ Start ▾ Restart ▾ Stop ▾ Hibernate ▾ ...

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

> Connect

> Networking

> Settings

> Availability + scale

> Security

> Backup + disaster recovery

> Operations

> Monitoring

> Automation

⚠ SarahVM01 virtual machine agent status is not ready. Troubleshoot the issue →

Essentials

Resource group

Status

Location

Subscription ([move](#))

Subscription ID

Availability zone

Operating system

Size

Public IP address

Virtual network/subnet

DNS name

Health state

Got issue? You can copy
to paste in Copilot for
solving.

Copilot

Preview

• [Prerequisites for Azure Virtual Desktop](#)

AI-generated content may be incorrect

5 of 15 requests

Processing ended abruptly since the blade closed.

3 of 3 requests

SarahVM01 virtual machine agent status is not ready.
Troubleshoot the issue

Is this the correct resource?

Name	Type
<input checked="" type="checkbox"/> SarahVM01 Azure subscription 1 / ...	Virtual machine

[Yes](#) [No, select a different resource](#)

AI-generated content may be incorrect

Cancel

There is currently 1 active service health event:

1. [Started by user](#)

- Status: Active
- Impacted Service(s):
- Last Updated:
- Impact Level: Critical
- Summary: The Virtual Machine is starting as requested by an authorized user or process. No other action is required at this time.

2. [Virtual Machine allocated](#)

- Status: Active
- Impacted Service(s):
- Last Updated:
- Impact Level: Critical
- Summary: The Virtual Machine is in the process of being set up, as requested by an authorized user or process. No other action is required at this time.

Please note that the status of these events can change, and it's recommended to check the Azure Portal's Notifications pane for the most up-to-date information.

[Continue troubleshooting](#) [Done](#)

AI-generated content may be incorrect





Virtual Machine

SarahVM01

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Got issue? You can copy to paste in Copilot for solving.

Connect

Bastion

Windows Admin Center

Networking

Settings

Availability + scale

Security

Backup + disaster recovery

Operations

Home > SarahVM01

SarahVM01 | Bastion

Virtual machine

Search

Overview

Activity log

Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. [Learn more](#)

Using Bastion: [SarahVNET-Bastion](#)

Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

Connection Settings

Keyboard Language: English (US)

Authentication Type: VM Password

Username: sarah

VM Password: [Show](#)

Open in new browser tab

Connect

Normally password will be pasted auto, just type your configured user



Virtual Machine

← ⏪ 🔒 https://portal.azure.com/#@thacysec.com/resource/subscriptions/e3d7bd45-7bc9-452b-a2c8-80d1e8ee004b... 

Microsoft Azure SarahVM01

Home > SarahVM01

SarahVM01 | Bastion Virtual machine

Search Overview Activity log Access control (IAM) Tags Diagnose and solve problems Connect Connect Bastion Windows Admin Center Networking Settings Availability + scale Security Backup + disaster recovery Operations Monitoring

Using Bastion: **SarahVNET-Bastion**

Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

Connection Settings

Keyboard Language ⓘ English (US)

Authentication Type ⓘ VM Password

Username ⓘ sarah

VM Password ⓘ Show

Open in new browser tab

Connect

Pop-ups blocked:

- https://bst-d0713c4b-0...ting.portal.azure.net

Always allow pop-ups and redirects from https://portal.azure.com
 Continue blocking

Manage **Done**

Set browser to allow
Pop-up from Azure Portal



Virtual Machine

A screenshot of a web browser window displaying a Bastion connection dialog. The dialog shows the URL <https://bst-d0...bastion.azure.com>. The message reads: "bst-d0...bastion.azure.com wants to [] See text and images copied to the clipboard". Below are two buttons: "Allow" and "Block". A hand cursor is hovering over the "Allow" button. A red arrow points from the text "Even no public connection open, you can still connect via Bastion" to this dialog.

Even no public connection open, you can still connect via Bastion

A screenshot of a Windows desktop environment. On the left, a user profile icon for "sarah" is shown. In the center, a "Clipboard" window is open, displaying the text "Sarah is beautiful!". On the right, a command prompt window titled "Administrator: Command Prompt" is open, showing the output of the command "ping 8.8.8.8".

Clipboard

Text copied/cut within Bastion will appear here. Changes to the text below will affect the remote clipboard.

Sarah is beautiful!

Administrator: Command Prompt

Microsoft Windows [Version 10.0.22621.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sarah>ping 8.8.8.8

```
Pinging 8.8.8.8 with 32 bytes of data:  
Reply from 8.8.8.8: bytes=32 time=5ms TTL=115  
Reply from 8.8.8.8: bytes=32 time=5ms TTL=115  
Reply from 8.8.8.8: bytes=32 time=4ms TTL=115  
Reply from 8.8.8.8: bytes=32 time=11ms TTL=115  
  
Ping statistics for 8.8.8.8:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 4ms, Maximum = 11ms, Average = 6ms
```

Welcome



Defender For Endpoint

Microsoft Defender

Settings

- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules
- Reports
- Audit
- Health
- Permissions
- Endpoints**
- More resources
- Customize navigation

Endpoints

Asset rule management

Configuration management

Enforcement scope

Intune Permissions

Device management

Onboarding

Offboarding

Network assessments

Assessment jobs

We will “Onboard” this new endpoint (VM) to our MDE

Select operating system to start onboarding process:
Windows 10 and 11

1. Onboard a device

First device onboarded: Completed ✓

Connectivity type

Streamlined

This package allows devices to onboard using [streamlined connectivity method](#). Check devices you onboard meet specific prerequisites. Onboard devices to Microsoft Defender using the onboarding configuration package that matches your [preferred deployment method](#). For other device preparation instructions, read [Onboard and set up](#).



Defender For Endpoint

Deployment method

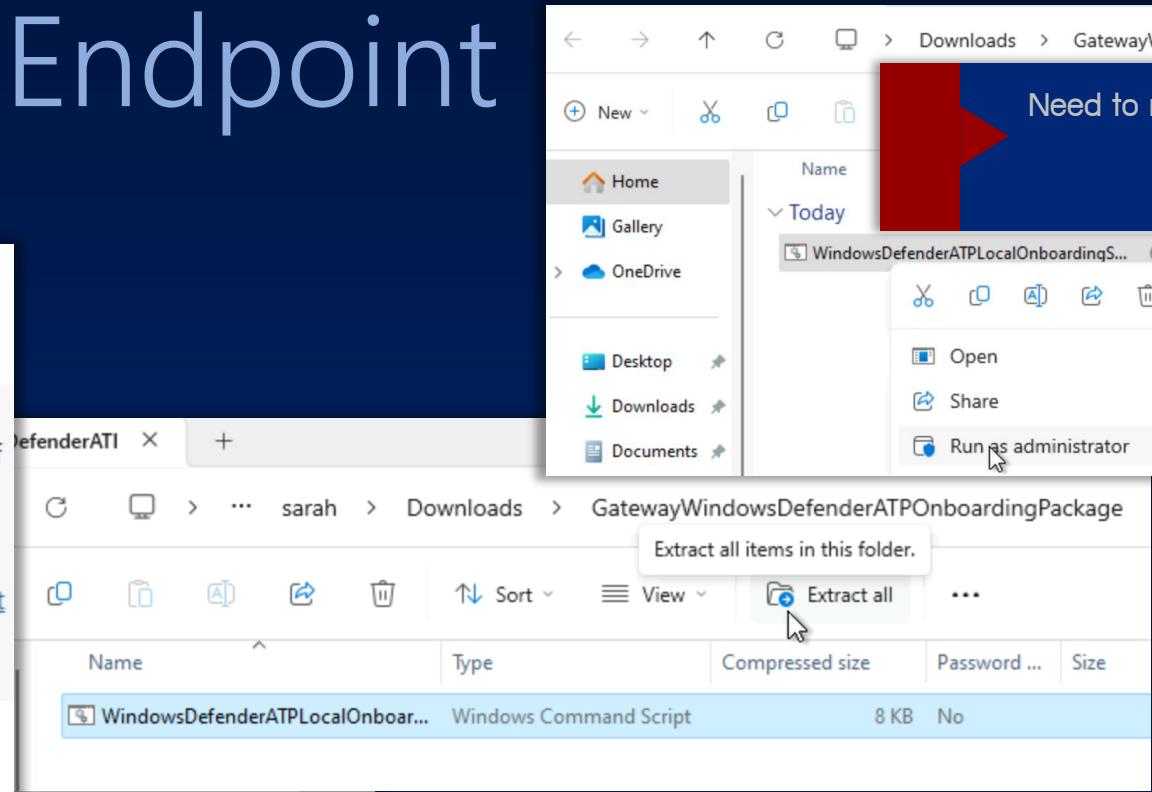
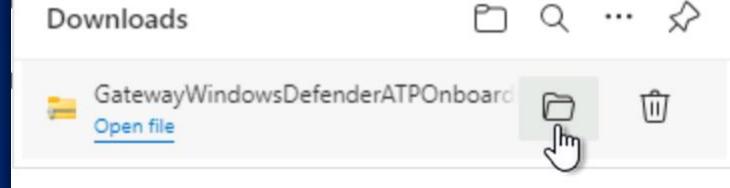
Local Script (for up to 10 devices)

You can configure a single device by running a script locally.

Note: This script has been optimized for usage with a limited number of devices (1-10). To deploy at scale, please see other deployment options above.

For more information on how to configure and monitor Microsoft Defender for Endpoint devices, see [Configure devices using a local script](#) section in the [Microsoft Defender for Endpoint guide](#).

 Download onboarding package





Defender For Endpoint

Windows protected your PC

Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

[More info](#)



Windows protected your PC

Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

App: WindowsDefenderATPLocalOnboardingScript.c
md

Publisher: Unknown publisher

[Run anyway](#)

[Don't run](#)

```
C:\Windows\System32\cmd.exe
This script is for onboarding machines to the Microsoft Defender for Endpoint services, including security and compliance products.
Once completed, the machine should light up in the portal within 5-30 minutes, depending on this machine's Internet connectivity availability and machine power state (plugged in vs. battery powered).
IMPORTANT: This script is optimized for onboarding a single machine and should not be used for large scale deployment.
For more information on large scale deployment, please consult the MDE documentation (links available in the MDE portal under the endpoint onboarding section).

Press (Y) to confirm and continue or (N) to cancel and exit: Y
Press (Y) to confirm and continue or (N) to cancel and exit: Y

Starting Microsoft Defender for Endpoint onboarding process...
Testing administrator privileges
Script is running with sufficient privileges

Performing onboarding operations

Starting the service, if not already running

Finished performing onboarding operations

Waiting for the service to start

Successfully onboarded machine to Microsoft Defender for Endpoint

Press any key to continue . . .
```





Defender For Endpoint

Endpoints

Asset rule management

Configuration management

Enforcement scope

Intune Permissions

Device management

Onboarding

Offboarding

Network assessments

Assessment jobs

Administrator: Command Prompt

```
C:\Users\sarah>powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference= 'silentlycontinue';(New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\\\test-WDATP-test\\\\invoice.exe');Start-Process 'C:\\\\test-WDATP-test\\\\invoice.exe'
```

Run test command from MDE
to show in the MDE incident

To verify that the device is properly onboarded and reporting to the service, run the detection script on the newly onboarded device:

- Open a Command Prompt window
- At the prompt, copy and run the command below. The Command Prompt window will close automatically.

```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden  
$ErrorActionPreference= 'silentlycontinue';(New-Object  
System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe',  
'C:\\\\test-WDATP-test\\\\invoice.exe');Start-Process 'C:\\\\test-WDATP-  
test\\\\invoice.exe'
```

Copy



Defender For Endpoint

Device - Microsoft Defender Welcome to Microsoft Edge

https://security.microsoft.com/machines?tid=...

Microsoft Defender

Search

Exposure management

Overview

Attack surface

Exposure insights

Secure score

Data connectors

Assets

Devices

Endpoints

Vulnerability management

Partners and APIs

Configuration management

Computers & Mobile

Network devices

IoT de

Total 7 Critical assets 2 High risk 0

Export

Transient device: No

Name	Domain
mercury.redteam.lab	redteam.lab
apollo11.redteam.lab	redteam.lab
yellow	Workgroup
thanos.redteam.lab	redteam.lab
thanos	Workgroup
sarahvm01	Workgroup

sarahvm01

No known risks ▲ No data available

Open device page View in map Device value ...

Workgroup: Windows 11 64-bit (Release 22H2 Build 22621.3737)

SAM name: Asset group: -

Health state: Active Data sensitivity: None

IP addresses: First seen: 10.0.0.4 Jun 29, 2024 12:40:01 AM See IP addresses info

Last seen: Jun 29, 2024 12:40:01 AM Onboarding status: Onboarded





Defender For Endpoint

Wait for about 5 mins to get this incident

Microsoft Defender

Incidents

Most recent incidents and alerts

Export Manage incidents

Filter set: Save Add filter

Incident name: [Test Alert] Suspicious Powershell commandline on one endpoint

[Test Alert] Suspicious Powershell commandline on one endpoint

Informational Active

Open incident page Manage incident Activity log ...

First activity: Jun 29, 2024 12:43:16 AM Last activity: Jun 29, 2024 12:43:16 AM

Impacted assets

Devices (1)	Risk Level	Exposure Level
sarahvm01	None	Low

Users (1)

S-1-5-21-3930159704-1967891269-2340024595-500

The screenshot shows the Microsoft Defender for Endpoint web interface. On the left, a sidebar menu includes 'Incidents & alerts' (with 'Incidents' selected) and a search bar. The main area displays an 'Incidents' list with a single item: '[Test Alert] Suspicious Powershell commandline on one endpoint'. This item is highlighted with a red box. A large red arrow points from the top right towards this incident. A message at the top right says 'Wait for about 5 mins to get this incident'. The incident details show it's informational and active, with first and last activity times of Jun 29, 2024 12:43:16 AM. The 'Impacted assets' section shows one device, 'sarahvm01', with low exposure level. The 'Users' section lists one user with the S-1-5-21-3930159704-1967891269-2340024595-500 identifier.





Intune.Microsoft.com

https://intune.microsoft.com/#view/Microsoft_Intune_Workflows/SecurityManagementMenu/~/overview

Microsoft Intune admin center

Home > Endpoint security | Overview

Search

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall

Summary

Refresh Report generated 06/29/2024, 12:54 AM

Defender for Endpoint Connector Status

Defender for Endpoint connector unavailable

Windows devices onboarded to Defender for Endpoint

0 / 0

Onboarded 0 Not Onboarded 0 Total 0

Deploy preconfigured policy

Onboard devices to Defender for Endpoint



Intune.Microsoft.com

- ≡
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules
- Reports
- Audit
- Health
- Permissions
- Settings**
- More resources

Settings > Endpoints

Endpoints

Asset rule management

Configuration management

Enforcement scope

Intune Permissions

Device management

Onboarding

Offboarding

Network assessments

Intune Permissions

This selection enables Microsoft 365 Defender administrators to grant Endpoint Security permissions in Intune.

If [Intune scope tags](#) are in use, global permissions for the Endpoint Security Manager role may be limited.

+ Add Azure AD Group

Azure AD Group Name

General

Advanced features

Licenses

Email notifications

Auto remediation

On

Microsoft Intune connection

Connects to [Microsoft Intune](#) to enable sharing of device information and enhanced policy enforcement.

Intune provides additional information about managed devices for secure score. It can use risk information to enforce [conditional access](#) and other security policies.



Intune.Microsoft.com

Microsoft Intune admin center Home > Endpoint security

Endpoint security | Microsoft Defender for Endpoint

Search Save Refresh Discard Delete

Some toggles are disabled and acting as "off" because Microsoft Defender for Endpoint is not actively communicating with Intune for this account. Please check the state of the connection in the Microsoft Defender for Endpoint admin console.

When the connection has returned to a healthy status (Active or Provisioned), the toggles will be re-enabled and any pre-existing setting state will be restored.

Endpoint Security Profile Settings

Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations On

Compliance policy evaluation

Connect Android devices version 6.0.0 and above to Microsoft Defender for Endpoint Off

Connect iOS/iPadOS devices version 13.0 and above to Microsoft Defender for Endpoint Off

Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint Off

Endpoint security settings menu:

- Endpoint Privilege Management
- Endpoint detection and response
- App Control for Business (Preview)
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access
- Monitor
- Assignment failures
- Setup
- Microsoft Defender for Endpoint





ພາກປະເມີນໃນຮະບຸ Metrics That
Matter ໃຫ້ຫຼວຍບະຄະ ❤️ 🧸