

We will first create our windows 10 VM that will be used in our honeynet

HOME > VIRTUAL MACHINES >

Create a virtual machine ...

This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

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 * ⓘ (New) RG-Cyber-Lab

[Create new](#)

Instance details

Virtual machine name * ⓘ windows-vm

Region * ⓘ (US) East US 2

Availability options ⓘ Availability zone

Availability zone * ⓘ Zones 1

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

Security type ⓘ Trusted launch virtual machines

[Configure security features](#)

Image * ⓘ Windows 10 Pro, version 22H2 - x64 Gen2 (free services eligible)

[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ Arm64 x64

ⓘ Actual memory and vCPU values available after deployment. Standard_B2s has 2 vcpus and 4 GiB memory.

We ended up choosing a bit of a beefier RIG because otherwise we would get DDOS'd and our logs would stop feeding into our SIEM. Here is what I choose:

Standard_B2s - 2 vcpus, 4 GiB memory (30,37 US\$/month)

[See all sizes](#)

We pretty much left everything else as stock but made a new VNET as you can see here

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) Lab-Vnet

Subnet * ⓘ (new) default (10.0.0.0/24)

Public IP ⓘ (new) windows-vm-ip

NIC network security group ⓘ None Basic Advanced

Public inbound ports * ⓘ None Allow selected ports

Select inbound ports * RDP (3389)

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is deleted

linux-vm

(US) East US 2

Availability zone

Zones 1

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

Trusted launch virtual machines

Configure security features

 Ubuntu Server 20.04 LTS - x64 Gen2 (free services eligible)

[See all images](#) | [Configure VM generation](#)

We will now create another VM but this time a linux machine in the same resource group as the other.

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 *	<input type="text" value="Lab-Vnet"/> 
	Create new
Subnet *	<input type="text" value="default (10.0.0.0/24)"/> 
	Manage subnet configuration
Public IP	<input type="text" value="(new) linux-vm-ip"/> 
	Create new
NIC network security group	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports *	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports

We will put it in the same VNET and the other machine as well so they can communicate with one another!

 Add inbound security rule X

linux-vm-nsg

Source * (i)

Source port ranges * (i)

Destination * (i)

Service * (i)

Destination port ranges * (i)

Protocol

Any

TCP

UDP

ICMP

Action

Allow

Deny

Priority * (i)

Name *

Description

We will now also add an inbound rule to both of the VMs that allow any traffic to reach to them from the internet!

What we will do now is install the SQL Database onto the windows VM.

RG-Cyber-Lab

Operating system : Windows (Windows 10 Pro)

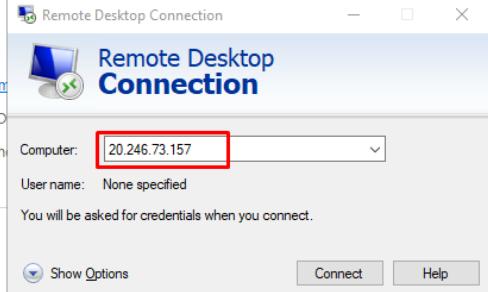
Size : Standard Copied 4 GiB memory.

Public IP address : 20.246.73.157

Virtual network/subnet : Lab-Vnet/default

DNS name : Not configured

Health state : -



Remote Desktop Connection

Computer: 20.246.73.157

User name: None specified

You will be asked for credentials when you connect.

Show Options Connect Help

Virtual machine

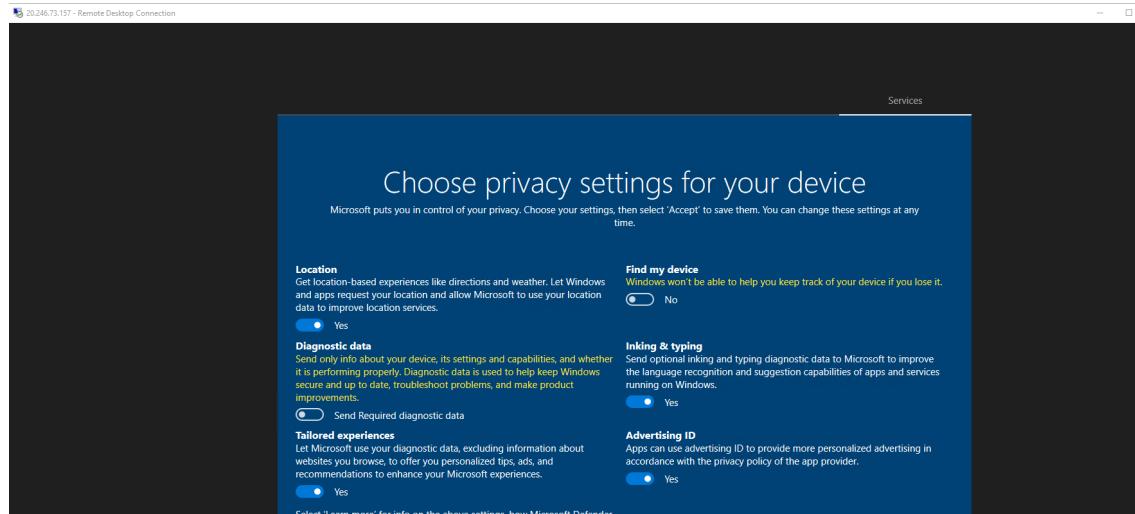
Computer name windows-vm

Networking

Public IP address 20.246.73.157 (Network interface)

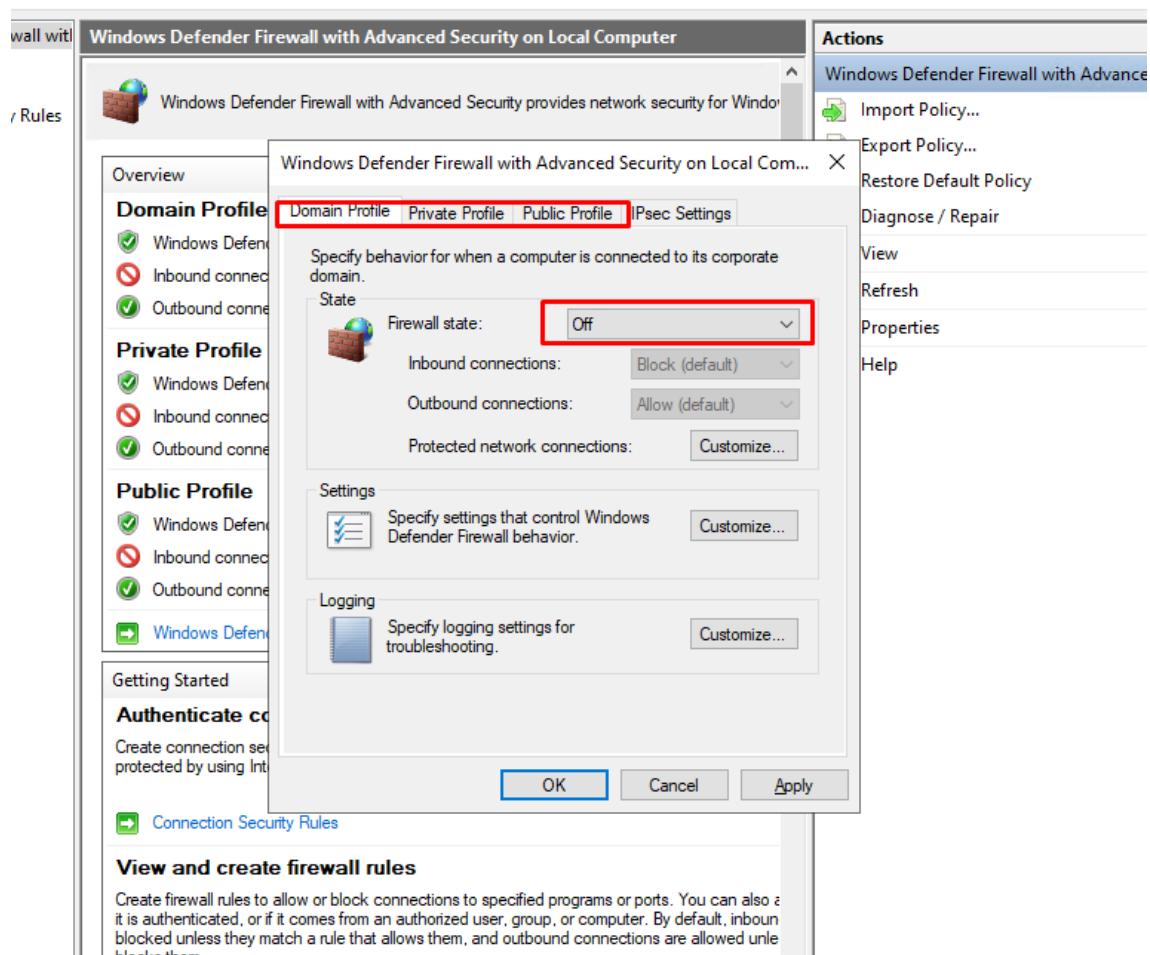
We will first RDP into the Windows VM like this.

We will use the User and Password we set before and we should be right here:



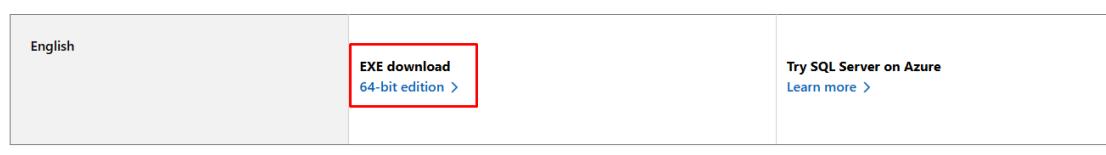
We will now proceed to Turn off the windows Firewall. (So, it can be easier to find online)

For example, with ping requests.



We will now proceed to install SQL Server Evaluation

Please select your SQL Server 2019 download



SQL Server 2019



-

X

Evaluation Edition

Specify SQL Server installer download

SELECT LANGUAGE

English

WHICH PACKAGE WOULD YOU LIKE TO DOWNLOAD?

- ISO (1367 MB)
Uncompressed, mountable disk image media
- CAB (1416 MB)
Compressed media, .exe and .box files

Or, go to the Microsoft Azure portal to provision SQL Server in the cloud

SELECT DOWNLOAD LOCATION *:

C:\Users\labuser\Downloads

Browse

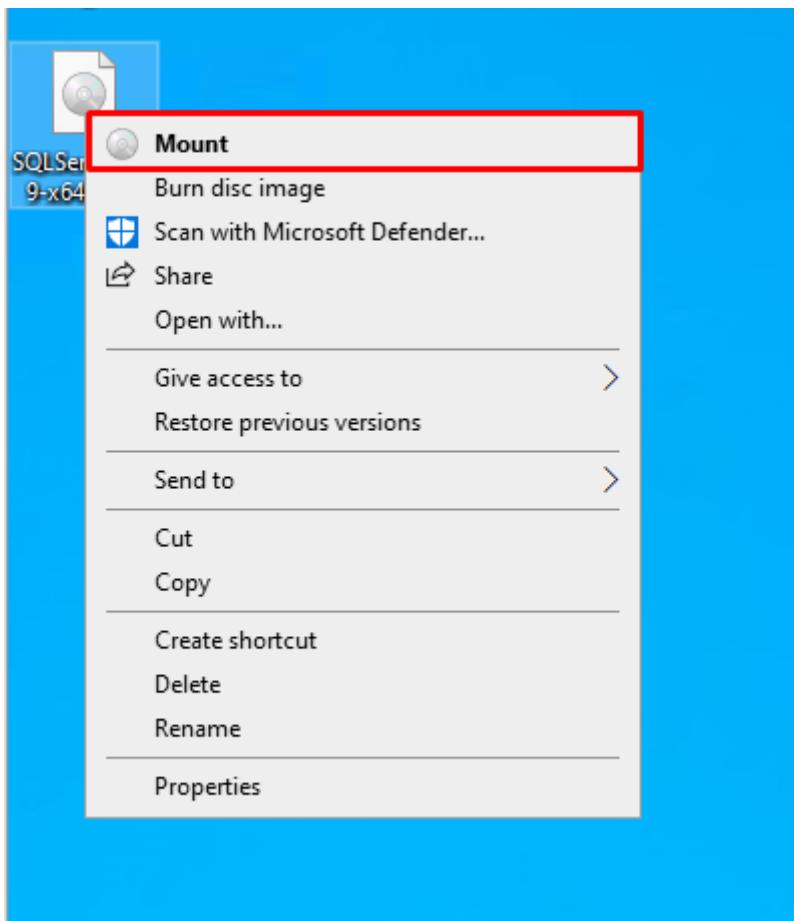
Close

< Previous

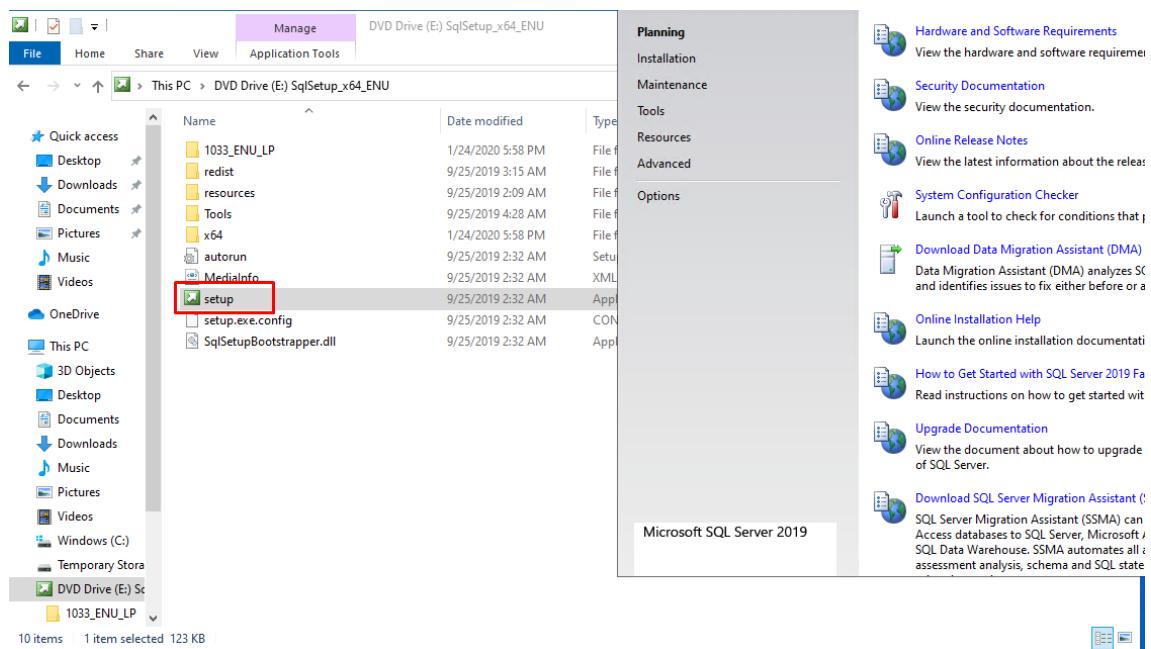
Download

15.2204.5490

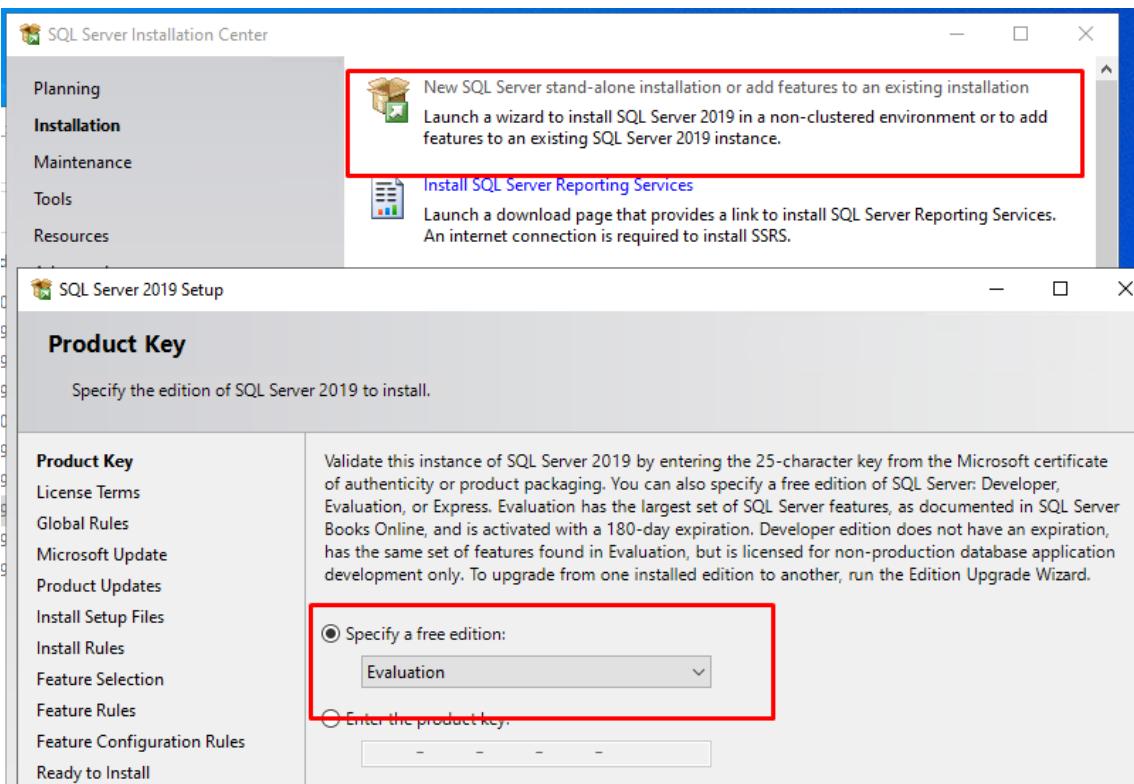
We will keep going with the installation.



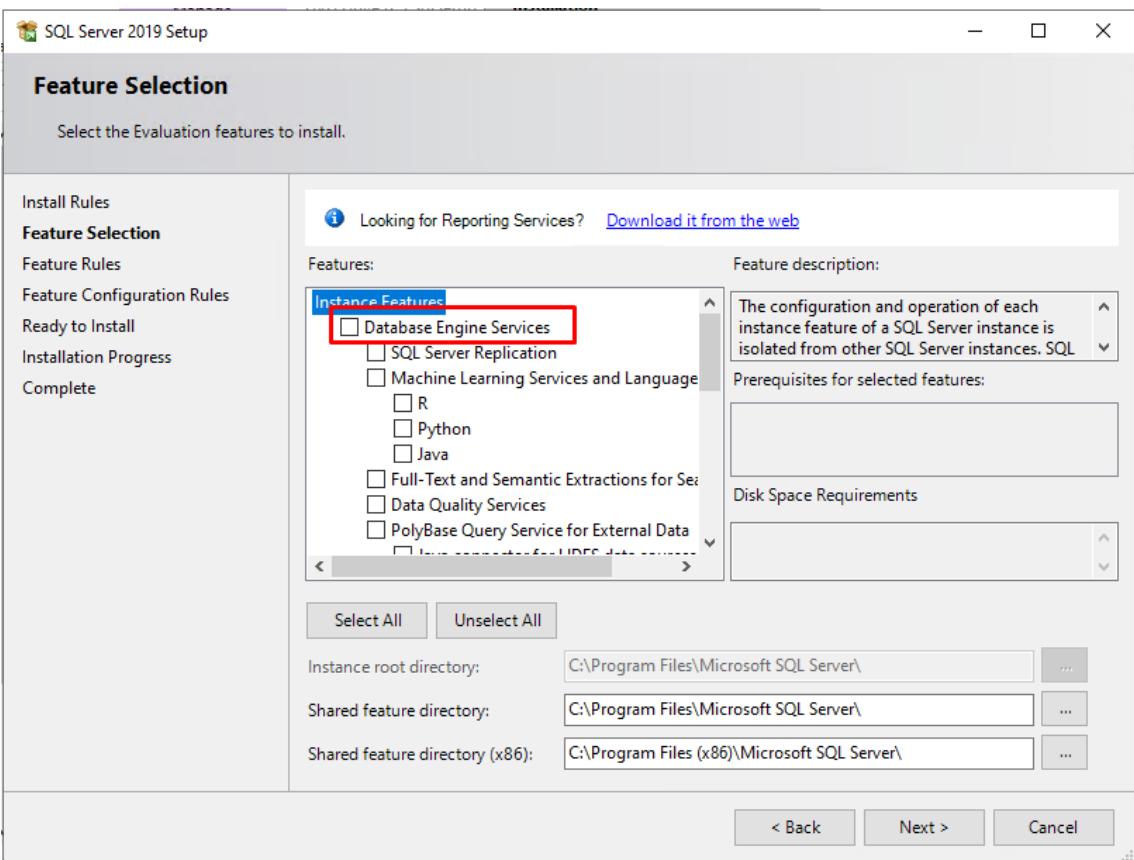
Since this is a ISO file we need to right click it and MOUNT!



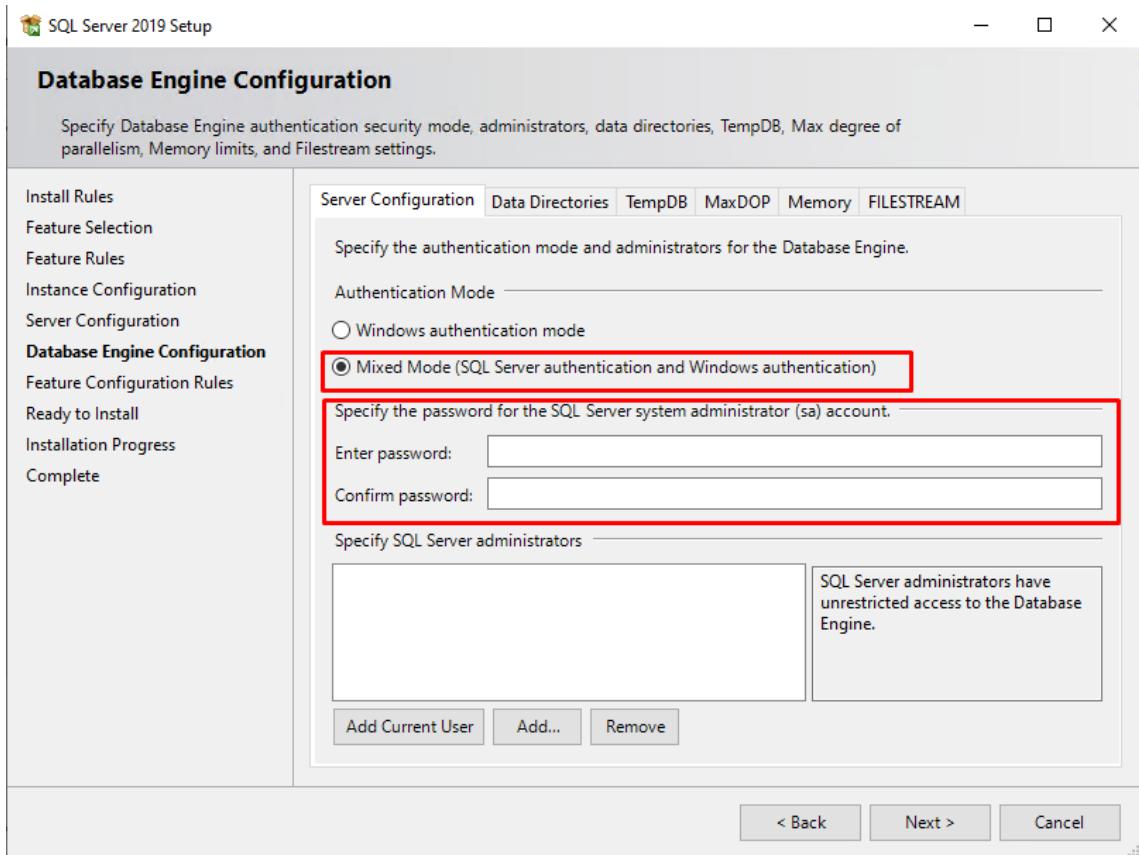
Now we run the setup.



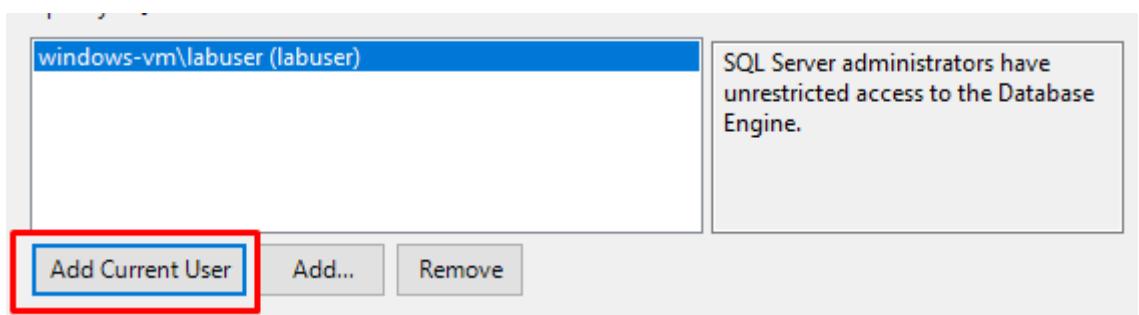
We will pick the first option and just leave it as evaluation.



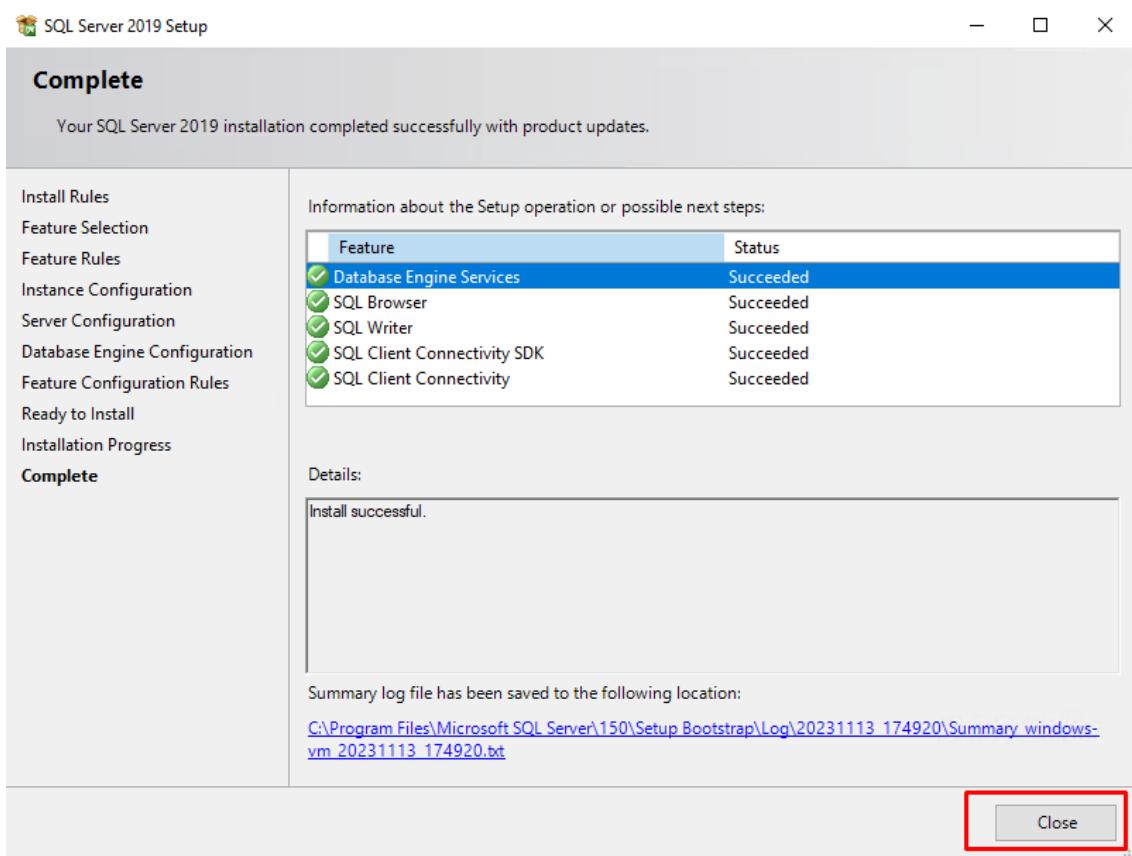
When we get to here we check the first option.



When we get to here, we will pick the second option and I will now input the admin password I want.



We will also add ourselves as an admin.

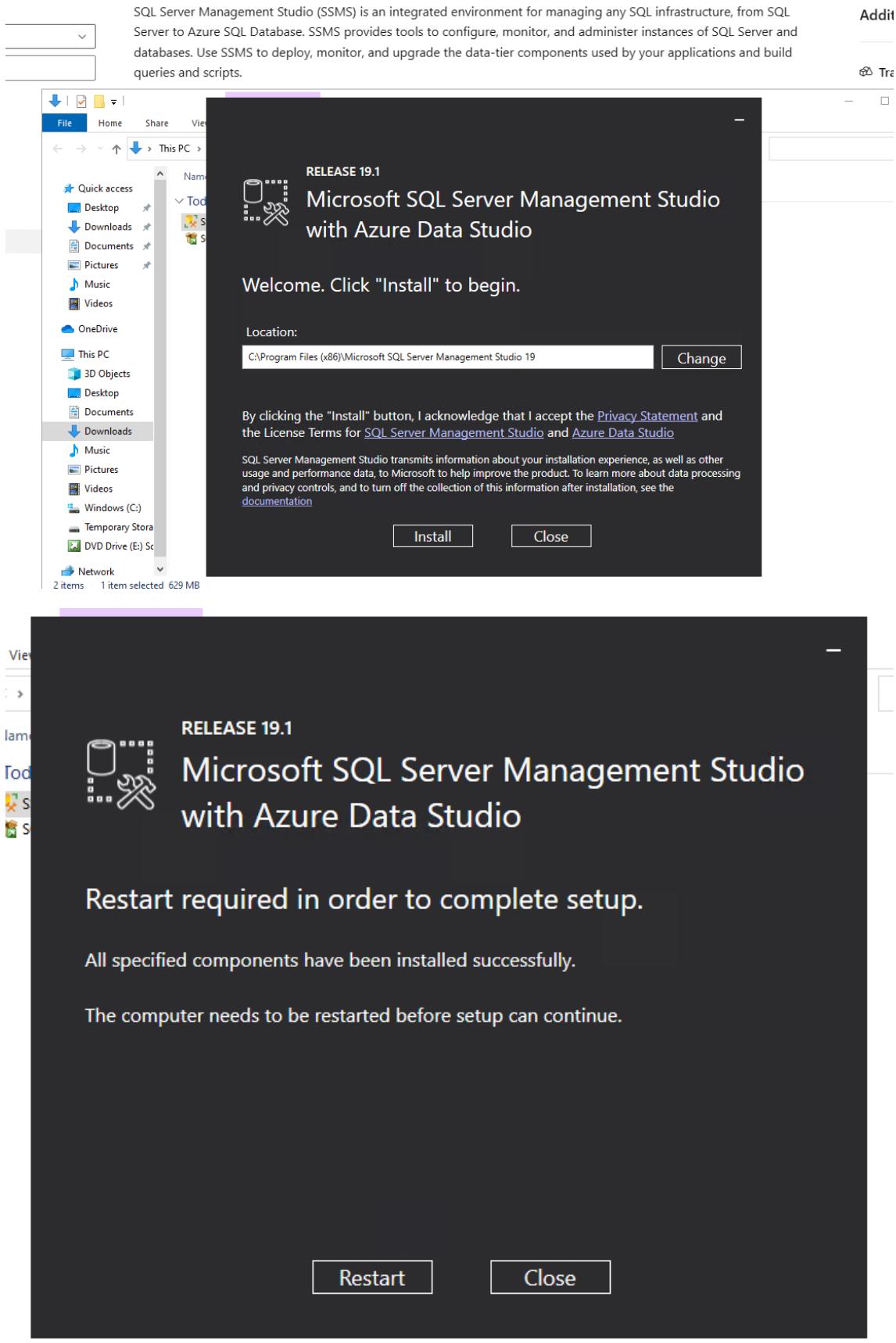


We keep going and when we get here, we just close out.

We will now install:

- SSMS (SQL Server Management Studio): <https://learn.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms>

Which we will use to login and generate logs for our SQL database.



We will now restart the VM to complete the install.

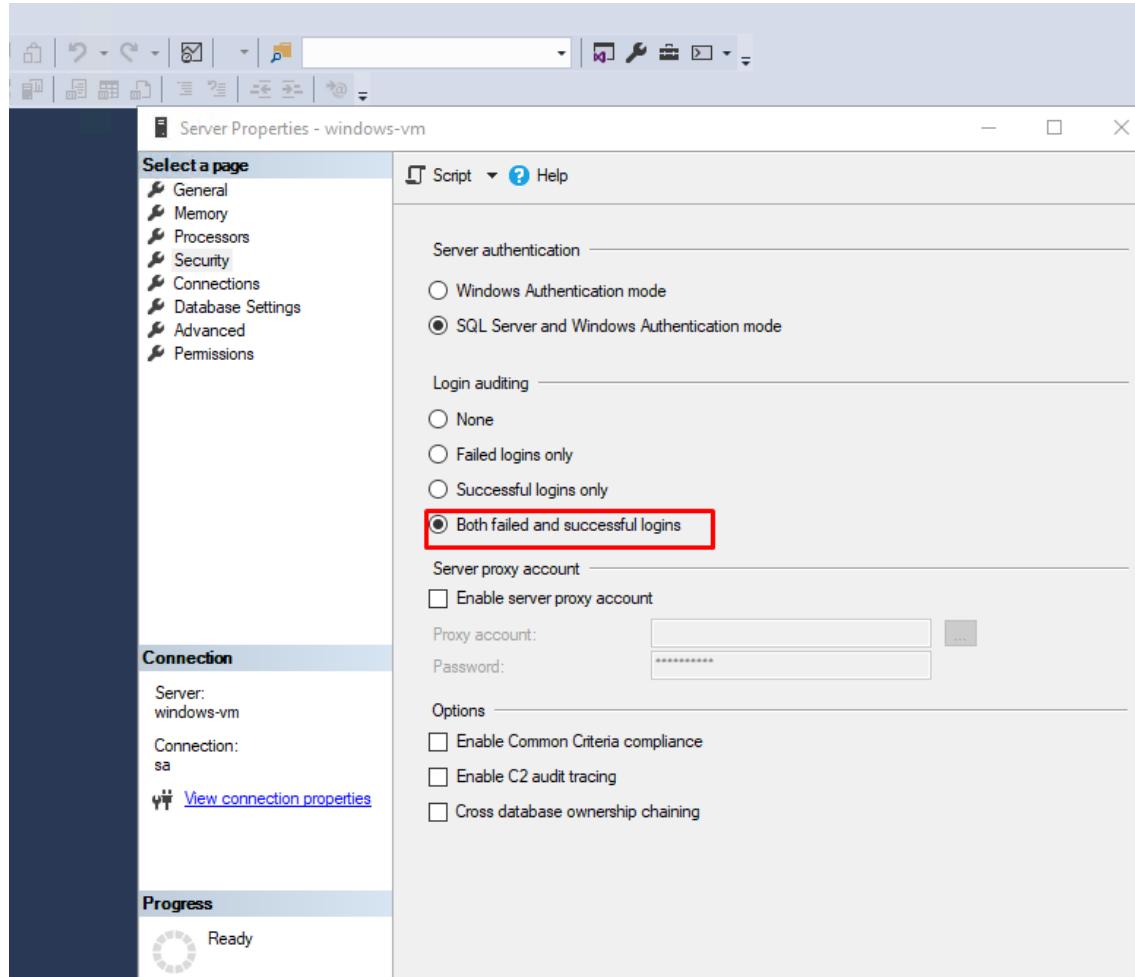
Next what we want is to

Enable logging for SQL Server to be ported into Windows Event Viewer

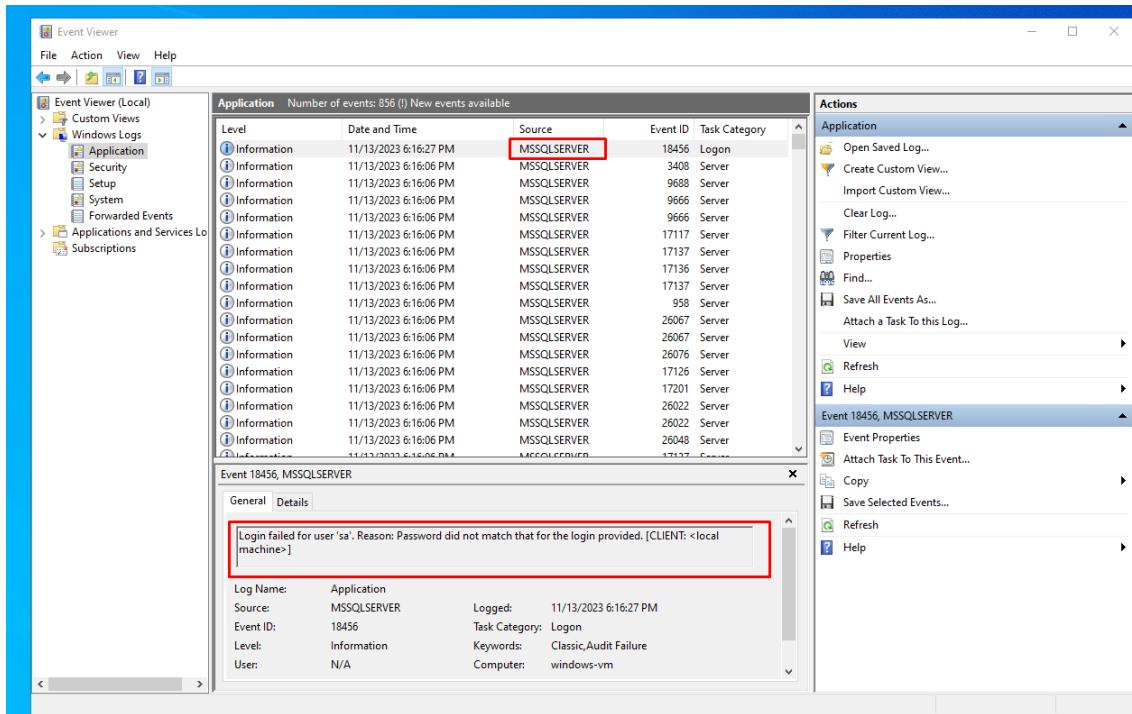
So that we can keep track of who is trying to login, etc.... Just so that we can use our SIEM later to practice incident response.

I will follow these steps:

<https://learn.microsoft.com/en-us/sql/relational-databases/security/auditing/write-sql-server-audit-events-to-the-security-log?view=sql-server-ver16>



After doing all that we want to make sure as well that we want to log both failed and successful login attempts.



After trying a wrong password, we can indeed see that it works and out events are now being logged into the event viewer!

I will also test the Linux vm by logging into it and pinging it from the windows VM!

We will now proceed to create a third VM, this will be our ATTACK vm where we will try to connect to the SQL database over the internet as well as the SSH login on the linux machine.

And after the fact we will observe the logs.

Basics Disks Networking Management Monitoring Advanced Tags Review + create

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

i This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

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 * ⓘ

(New) RG-Cyber-Lab-Attacker

[Create new](#)

Instance details

Virtual machine name * ⓘ

attack-vm

Region * ⓘ

(Asia Pacific) Australia East

Availability options ⓘ

Availability zone

Availability zone * ⓘ

Zones 1

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

Security type ⓘ

Trusted launch virtual machines

[Configure security features](#)

Image * ⓘ

Windows 10 Pro, version 22H2 - x64 Gen2 (free services eligible)

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) Lab-VNet-Attacker

[Create new](#)

Subnet * ⓘ

(new) default (10.0.0.0/24)

Public IP ⓘ

(new) attack-vm-ip

[Create new](#)

NIC network security group ⓘ

None

[Create new](#)

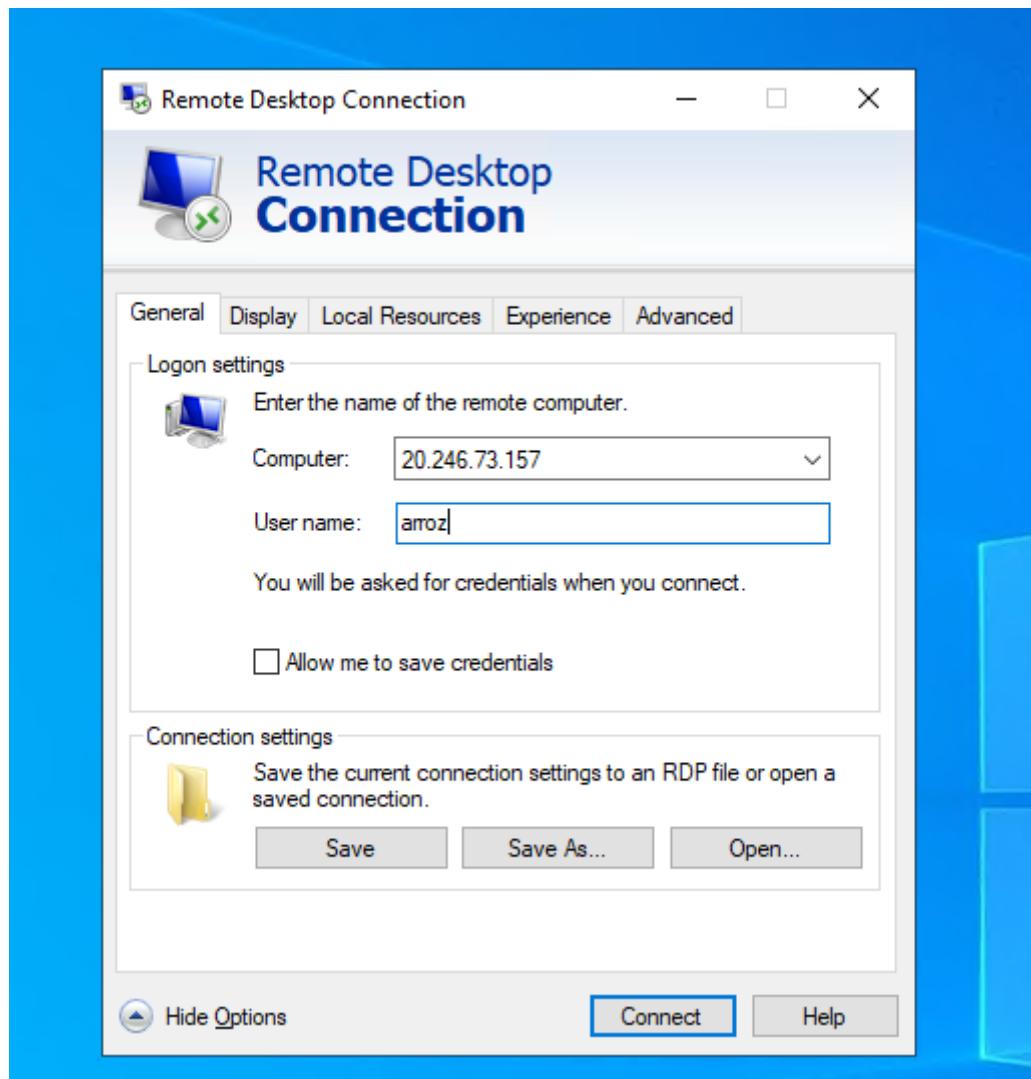
We will create another vnet so we can make sure they are segmented.

<input type="checkbox"/>	Name ↑↓	Type ↑↓	Subscription ↑↓
<input type="checkbox"/>	attack-vm	Virtual machine	Azure subscription 1
<input type="checkbox"/>	linux-vm	Virtual machine	Azure subscription 1
<input type="checkbox"/>	windows-vm	Virtual machine	Azure subscription 1

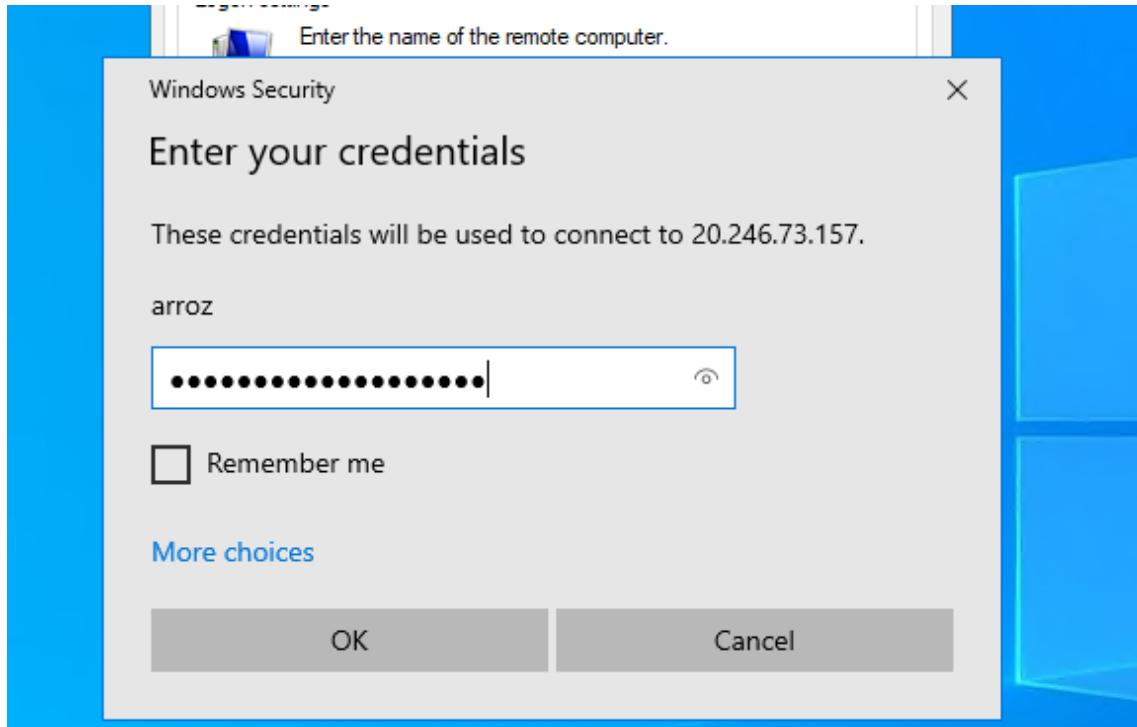
Here is what we have so far.

We will now login to the attack VM using RDP.

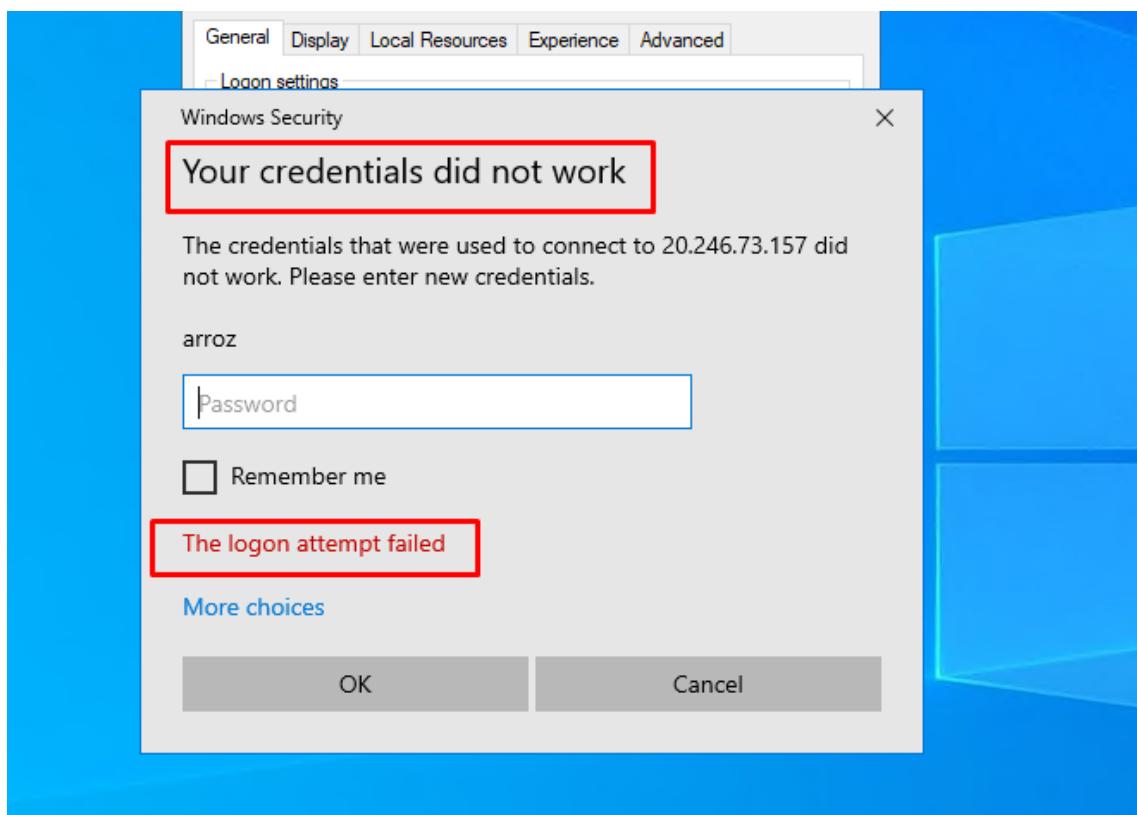
What will we do now is FROM WITHIN the ATTACK vm we will try and RDP into the windows VM (sql database) and input the wrong info on purpose to generate some logs.



So we will put a random username for example



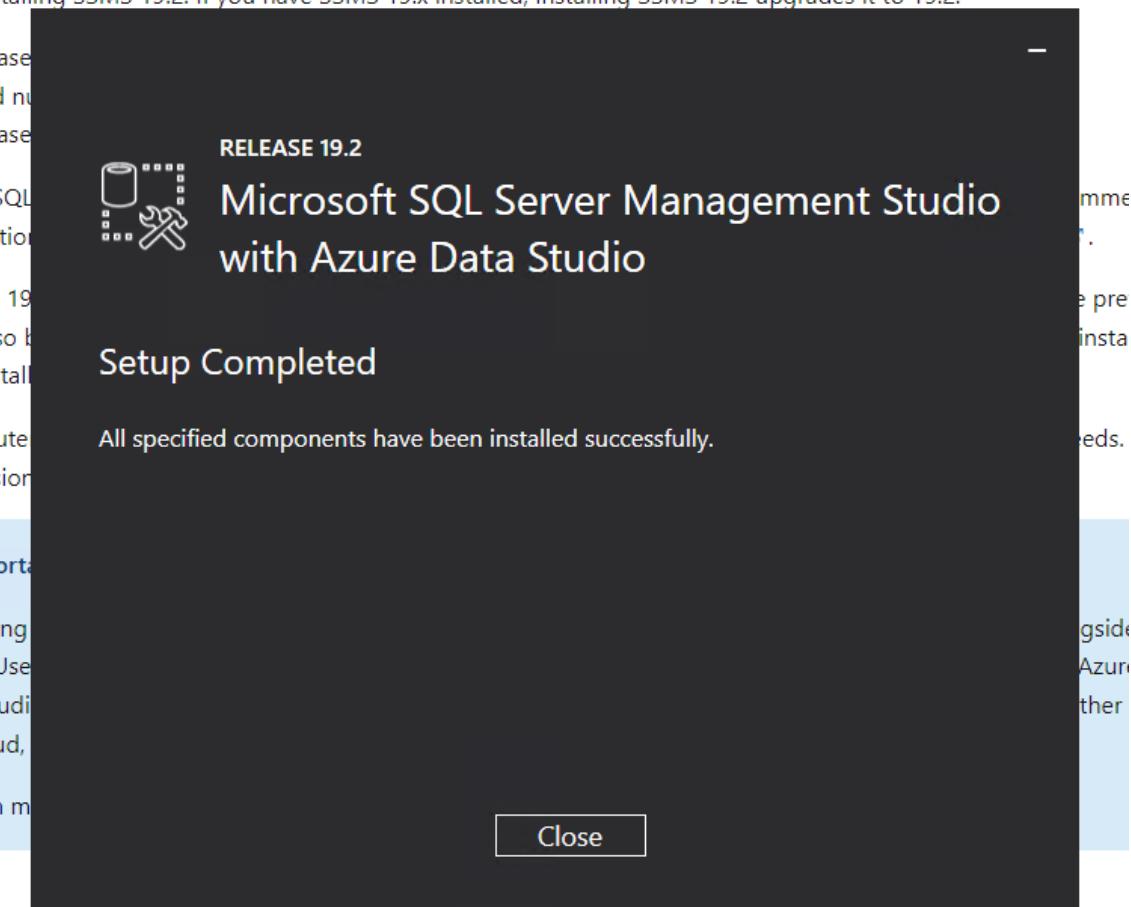
And random pass



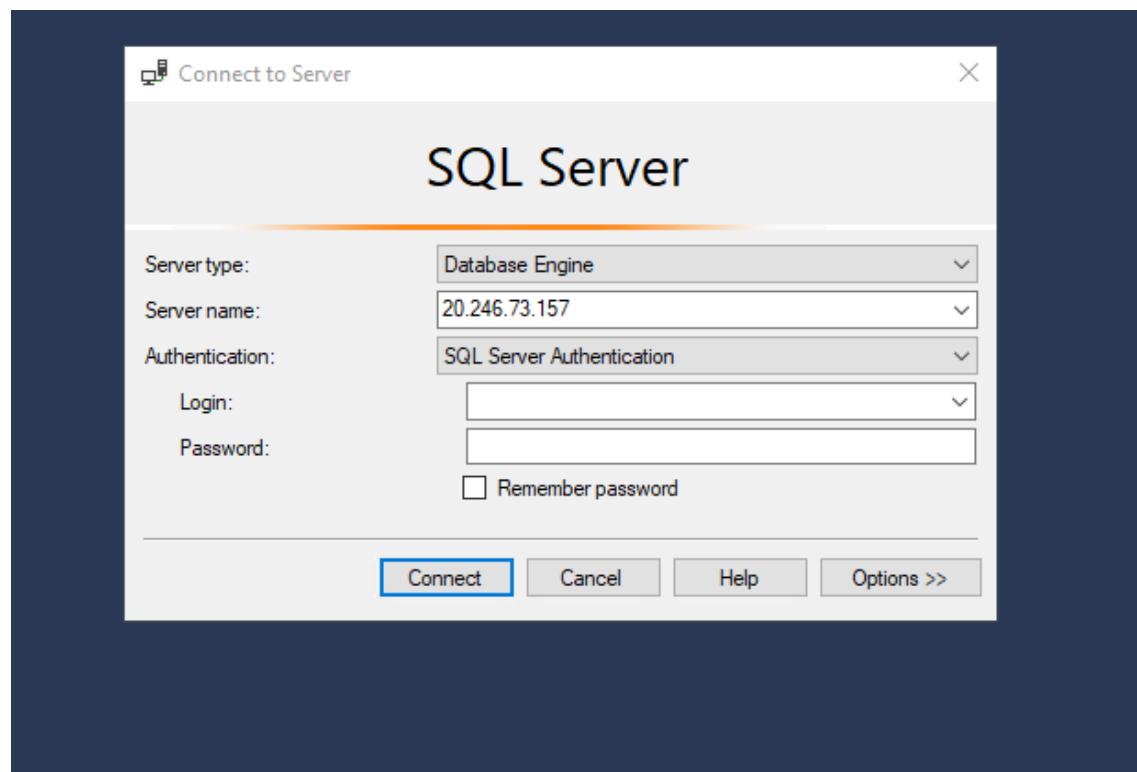
And this is what we want.

What we will do now is install SSMS and we will generate some SQL logs instead of the windows Logs. Let's generate some logs for that.

2 is the latest general availability (GA) version. If you have a *preview* version of SSMS 19 installed, [uninstall it](#) and install SSMS 19.2. If you have SSMS 19.x installed, [installing SSMS 19.2](#) upgrades it to 19.2.



Installable languages



For server name we input the machine IP and we will now generate some failed logs.

Now we will try and SSH into the linux VM still using the ATTACK VM.

```
PS C:\Users\labuser> ssh josh@20.246.73.205
The authenticity of host '20.246.73.205 (20.246.73.205)' can't be established.
ECDSA key fingerprint is SHA256:oTvAzKVJoByZegATQcQUi8WD86LreR72HM8SCu+9aQc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.246.73.205' (ECDSA) to the list of known hosts.
josh@20.246.73.205's password:
Permission denied, please try again.
josh@20.246.73.205's password: ■
```

Just like this.

We will now take the perspective of an admin and login to the windows Vm to check the logs as well as the linux VM.

The screenshot shows the Windows Event Viewer interface. The main pane displays a list of events, with one event selected. The details pane shows the following information:

Event 4625, Microsoft Windows security auditing.

General tab selected.

Event Details:

- An account failed to log on.
- Subject:**
 - Security ID: NULL SID
 - Account Name: -
 - Account Domain: -
 - Logon ID: 0x0
- Logon Type:** 3
- Account For Which Logon Failed:**
 - Security ID: NULL SID
 - Account Name: ADMIN
 - Account Domain: -

Log Properties:

- Log Name: Security
- Source: Microsoft Windows security
- Event ID: 4625
- Level: Information
- User: N/A
- OpCode: Info
- Logged: 11/17/2023 8:19:25 PM
- Task Category: Logon
- Keywords: Audit Failure
- Computer: windows-vm

More Information: [Event Log Online Help](#)

Let's just take a note of these.

Application Number of events: 1,133					
Level	Date and Time	Source	Event ID	Task Category	
i Information	11/17/2023 8:54:04 PM	MSSQLSERVER	18453	Logon	
i Information	11/17/2023 8:44:04 PM	MSSQLSERVER	18453	Logon	
i Information	11/17/2023 8:41:04 PM	Security-SPP	16384	None	
i Information	11/17/2023 8:40:34 PM	Security-SPP	16394	None	
i Information	11/17/2023 8:34:04 PM	MSSQLSERVER	18453	Logon	
i Information	11/17/2023 8:31:04 PM	MSSQLSERVER	17890	Server	
i Information	11/17/2023 8:25:32 PM	MSSQLSERVER	17890	Server	
i Information	11/17/2023 8:24:03 PM	MSSQLSERVER	18453	Logon	
i Information	11/17/2023 8:21:08 PM	MSSQLSERVER	17890	Server	
i Information	11/17/2023 8:15:37 PM	MSSQLSERVER	17890	Server	
i Information	11/17/2023 8:14:03 PM	MSSQLSERVER	18453	Logon	
i Information	11/17/2023 8:10:10 PM	MSSQLSERVER	17890	Server	
i Information	11/17/2023 8:05:40 PM	MSSQLSERVER	17890	Server	
i Information	11/17/2023 8:04:03 PM	MSSQLSERVER	18453	Logon	
i Information	11/17/2023 8:00:10 PM	MSSQLSERVER	17890	Server	
i Information	11/17/2023 7:58:56 PM	SecurityCenter	15	None	

Here are the SQL logs.

Let's take notes of a couple of things like Ips, event IDs and more.

```

labuser@linux-vm:~$ cd /var/log
labuser@linux-vm:/var/log$ ls
auth.log      chrony          dmesg      journal    private          ubuntu-advantage.log
auth.log      cloud-init-output.log  dmesg.0    kern.log   syslog          unattended-upgrades
chrony        cloud-init.log     dmesg.1.gz  landscape  syslog.1       waagent.log
dmesg        dist-upgrade      dmesg.1.gz  lastlog   ubuntu-advantage-daemon.log  wtmp
labuser@linux-vm:/var/log$ ls -lasht
total 1.8M
drwxr----- 1 syslog  adm  139K Nov 17 21:50 auth.log
-rw-rw---- 1 root   utmp 189K Nov 17 21:50 btmp
drwxr----- 1 root   utmp 286K Nov 17 21:47 lastlog
drwxr----- 1 root   utmp 8.7K Nov 17 21:47 wtmp
drwxr----- 1 syslog  adm  78K Nov 17 21:47 syslog
drwxr----- 1 root   root  78K Nov 17 21:45 waagent.log
drwxr----- 1 root   root 19K Nov 17 13:24 dpkg.log
drwxr-xr-x  2 root   root 4.0K Nov 17 13:24 apt
drwxr----- 1 syslog  adm 150K Nov 17 13:23 kern.log
drwxrwxr-x 10 root  syslog 4.0K Nov 17 13:23 .
drwxr----- 1 root   adm  41K Nov 17 12:38 dmesg
drwxr----- 1 root   adm 11K Nov 17 12:38 cloud-init-output.log
drwxr----- 1 syslog  adm 388K Nov 17 12:38 cloud-init.log
drwxr----- 1 root   root 1.4K Nov 17 12:38 ubuntu-advantage-daemon.log
drwxr----- 1 syslog  adm 549K Nov 17 12:38 syslog.1
drwxr-xr-x  2 landscape  landscape 4.0K Nov 13 18:21 landscape
drwxr----- 1 root   root 11K Nov 13 18:20 ubuntu-advantage.log
drwxr----- 2 root   adm  4.0K Nov 13 16:53 unattended-upgrades
drwxr----- 1 root   adm 41K Nov 13 16:26 dmesg.0
drwxr----- 1 root   adm 14K Nov  9 16:44 dmesg.1.gz
drwxr----- 2 root   root 4.0K Nov  9 16:44 chrony
drwxr----- 2 root   root 4.0K Nov  9 16:43 private
drwxr----- 3 root   systemd-journal 4.0K Nov  9 16:43 journal
drwxr----- 13 root  root 4.0K Oct 25 21:51 ..
drwxr----- 2 root   root 4.0K Mar 14  2023 dist-upgrade
drwxr----- 2 _chrony _chrony 4.0K Aug 25  2020 chrony
labuser@linux-vm:/var/log$
```

And finally, here is the linux logs.

```

Nov 17 21:56:54 linux-vm sshd[10143]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:56:55 linux-vm sshd[10143]: Failed password for invalid user test2 from 14.35.32.94 port 39144 ssh2
Nov 17 21:56:56 linux-vm sshd[10143]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:56:58 linux-vm sshd[10143]: Failed password for invalid user test2 from 14.35.32.94 port 39144 ssh2
Nov 17 21:56:59 linux-vm sshd[10143]: Received disconnect from 14.35.32.94 port 39144:11: disconnected by user [preauth]Nov 17 21:57:01: Disconnected from invalid user test2 14.35.32.94 port 39144 [preauth]
Nov 17 21:56:59 linux-vm sshd[10143]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=14.35.32.94
Nov 17 21:56:59 linux-vm sshd[10143]: PAM service(sshd) ignoring max retries; 4 > 3
Nov 17 21:57:00 linux-vm sshd[10145]: Invalid user contador from 14.35.32.94 port 41184
Nov 17 21:57:00 linux-vm sshd[10145]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:57:00 linux-vm sshd[10145]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=14.35.32.94
Nov 17 21:57:02 linux-vm sshd[10145]: Failed password for invalid user contador from 14.35.32.94 port 41184 ssh2
Nov 17 21:57:02 linux-vm sshd[10145]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:57:04 linux-vm sshd[10145]: Failed password for invalid user contador from 14.35.32.94 port 41184 ssh2
Nov 17 21:57:06 linux-vm sshd[10145]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:57:08 linux-vm sshd[10145]: Failed password for invalid user contador from 14.35.32.94 port 41184 ssh2
Nov 17 21:57:08 linux-vm sshd[10145]: Received disconnect from 14.35.32.94 port 41184:11: disconnected by user [preauth]Nov 17 21:57:09: Disconnected from invalid user contador 14.35.32.94 port 41184 [preauth]
Nov 17 21:57:08 linux-vm sshd[10145]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=14.35.32.94
Nov 17 21:57:09 linux-vm sshd[10147]: Invalid user ubuntu from 14.35.32.94 port 42904
Nov 17 21:57:09 linux-vm sshd[10147]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:57:09 linux-vm sshd[10147]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=14.35.32.94
Nov 17 21:57:11 linux-vm sshd[10147]: Failed password for invalid user ubuntu from 14.35.32.94 port 42904 ssh2
Nov 17 21:57:12 linux-vm sshd[10147]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:57:13 linux-vm sshd[10147]: Failed password for invalid user ubuntu from 14.35.32.94 port 42904 ssh2
Nov 17 21:57:14 linux-vm sshd[10147]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:57:16 linux-vm sshd[10147]: Failed password for invalid user ubuntu from 14.35.32.94 port 42904 ssh2
Nov 17 21:57:18 linux-vm sshd[10147]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:57:20 linux-vm sshd[10147]: Failed password for invalid user ubuntu from 14.35.32.94 port 42904 ssh2
Nov 17 21:57:21 linux-vm sshd[10147]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:57:22 linux-vm sshd[10147]: Failed password for invalid user ubuntu from 14.35.32.94 port 42904 ssh2
Nov 17 21:57:23 linux-vm sshd[10147]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:57:24 linux-vm sshd[10147]: Failed password for invalid user ubuntu from 14.35.32.94 port 42904 ssh2
Nov 17 21:57:25 linux-vm sshd[10147]: error: maximum authentication attempts exceeded for invalid user ubuntu from 14.35.32.94 port 42904
Nov 17 21:57:25 linux-vm sshd[10147]: Disconnecting invalid user ubuntu 14.35.32.94 port 42904: Too many authentication failures [PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=14.35.32.94]
Nov 17 21:57:25 linux-vm sshd[10147]: PAM service(sshd) ignoring max retries; 6 > 3
Nov 17 21:57:27 linux-vm sshd[10149]: Invalid user ubuntu from 14.35.32.94 port 46120
Nov 17 21:57:27 linux-vm sshd[10149]: pam_unix(sshd:auth): check pass; user unknown
Nov 17 21:57:27 linux-vm sshd[10149]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=14.35.32.94
Nov 17 21:57:28 linux-vm sshd[10149]: Failed password for invalid user ubuntu from 14.35.32.94 port 46120 ssh2
Nov 17 21:57:30 linux-vm sshd[10149]: pam_unix(sshd:auth): check pass; user unknown
```

If we CAT the auth.logs we get the authorization logs from the machine.

Log	Layer	Description
AAD logs	Azure Tenant	Contain the history of sign-in activity and audit trail of changes made in Azure AD for a particular tenant.
Activity log	Azure Subscription	Provides insight into the operations on each Azure resource in the subscription from the outside (the management plane) in addition to updates on Service Health events. Use the Activity log to determine the <i>what</i> , <i>who</i> , and <i>when</i> for any write operations (PUT, POST, DELETE) taken on the resources in your subscription. There's a single activity log for each Azure subscription.
Resource logs	Azure Resources	Provide insight into operations that were performed within an Azure resource (the data plane). Examples might be getting a secret from a key vault or making a request to a database. The content of resource logs varies by the Azure service and resource type. <i>Resource logs were previously referred to as diagnostic logs.</i>

Here is an overview on how logs work in azure, I am showing this because we will work mostly on logging for right now.

We will start by downloading a file to our pc, this is a list with IPs and locations that we can use to map our attackers later on a map. Here is what I used:

	A	B	C	D	E	F	G	H
1	network	latitude	longitude	cityname	countryname			
2	1.0.0.0/16	-33.494	143.2104		Australia			
3	1.1.0.0/16	17.8148	103.3386	Ban Chan	Thailand			
4	1.2.0.0/16	13.8667	100.1917	Nakhon P.	Thailand			
5	1.3.0.0/16	13.8679	100.1891	Nakhon P.	Thailand			
6	1.4.0.0/16	13.6687	100.579	Bangkok	Thailand			
7	1.5.0.0/16	13.6659	100.5882	Bangkok	Thailand			
8	1.6.0.0/16	12.9634	77.5855	Bengaluru	India			
9	1.7.0.0/16	12.9691	77.5902	Bengaluru	India			
10	1.8.0.0/16	12.9557	77.5843	Bengaluru	India			
11	1.9.0.0/16	3.1539	101.7448	Ampang	Malaysia			
12	1.10.0.0/1	17.8842	102.7394	Nong Khai	Thailand			
13	1.11.0.0/1	37.5841	127.0616	Dongdaen	South Korea			
14	1.12.0.0/1	37.5917	127.069	Dongdaen	South Korea			
15	1.13.0.0/1	37.5814	127.0663	Dongdaen	South Korea			
16	1.14.0.0/1	37.58	127.0609	Dongdaen	South Korea			
17	1.15.0.0/1	37.5786	127.0678	Dongdaen	South Korea			
18	1.16.0.0/1	37.5802	127.0644	Dongdaen	South Korea			
19	1.17.0.0/1	37.5838	127.0617	Dongdaen	South Korea			
20	1.18.0.0/1	37.5872	127.0651	Dongdaen	South Korea			
21	1.19.0.0/1	37.5757	127.0658	Dongdaen	South Korea			
22	1.20.0.0/1	13.5052	102.1872	Wang Nan	Thailand			
23	1.21.0.0/1	35.6384	139.6288	Kamiogi	Japan			
24	1.22.0.0/1	12.9634	77.5855	Bengaluru	India			
25	1.23.0.0/1	19.1963	72.9675	Thane	India			
26	1.24.0.0/1	19.1954	72.9646	Thane	India			
27	1.25.0.0/1	19.195	72.969	Thane	India			
28	1.26.0.0/1	19.1874	72.965	Thane	India			
29	1.27.0.0/1	19.2048	72.9588	Thane	India			
30	1.28.0.0/1	19.1879	72.9592	Thane	India			
31	1.29.0.0/1	19.2007	72.963	Thane	India			
32	1.30.0.0/1	19.2026	72.9631	Thane	India			
33	1.31.0.0/1	19.1989	72.9773	Thane	India			
34	1.32.0.0/1	3.0995	101.6054	Petaling J.	Malaysia			
35	1.33.0.0/1	35.6887	139.745	Chiyoda-k	Japan			
36	1.34.0.0/1	24.9466	121.586	New Taipei	Taiwan			
37	1.35.0.0/1	24	121		Taiwan			

We will now create a Log analytics workspace (log aggregator)

Create Log Analytics workspace

Validation passed

Basics Tags Review + Create

 **Log Analytics workspace**
by Microsoft

Basics

Subscription	Azure subscription 1
Resource group	RG-Cyber-Lab
Name	LAW-Cyber-Lab-01
Region	East US 2

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.

Tags

None

Here it is created.

We will now setup Microsoft Sentinel (SIEM) and we will connect it to our analytics workspace.



No Microsoft Sentinel to display

before they cause harm, with SIEM reinvented for a modern world. Micro
birds-eye view across the enterprise.

[Create Microsoft Sentinel](#)

[Learn more](#) 

After sentinel is created, we will create the geoip watchlist.

Watchlist wizard

General **Source** **Review + create**

Name *

Description

Alias *

Source type * Local file

File type * CSV file with a header (.csv)

Number of lines before row with headings * 0

Upload file * geoip-summarized.csv

SearchKey * network

Reset

network	latitude	longitude	cityname	countryname
1.0.0/16	-33.494	143.2104		Australia
1.1.0/16	17.8148	103.3386	Ban Chan	Thailand
1.2.0/16	13.8667	100.1917	Nakhon Pathom	Thailand
1.3.0/16	13.8679	100.1891	Nakhon Pathom	Thailand
1.4.0/16	13.6687	100.579	Bangkok	Thailand
1.5.0/16	13.6659	100.5882	Bangkok	Thailand
1.6.0/16	12.9634	77.5855	Bengaluru	India
1.7.0/16	12.9691	77.5902	Bengaluru	India
1.8.0/16	12.9557	77.5843	Bengaluru	India
1.9.0/16	3.1539	101.7448	Ampang	Malaysia

And here it is.

Watchlists Watchlist Items

My Watchlists Templates (Preview)

Search by name, alias and description Add filter

Name	Alias	Source	Created time	Last u...
geoip	geoip	geoip-summarized.csv	11/20/2023, 3:17:24 PM	11/20/2023, 3:17:24 PM

geoip
Name

Microsoft Provider 0 Rows 11/20/2023, 3:17:24 PM Created time

Description

Source geoip-summarized.csv

Created by antoniofilipearroz@hotmail.com

Last updated 11/20/2023, 3:17:24 PM

SearchKey network

Status (Preview) Uploading (9.12%)

We now must wait for the csv to upload!

Next, we will go to our log analytics, and we will make sure something comes out when we query _GetWatchlist("geoip")

Something like this:

The screenshot shows a Microsoft Log Analytics workspace interface. At the top, there are buttons for 'Run' (with a play icon), 'Save' (with a floppy disk icon), 'Share' (with a share icon), 'New alert rule' (with a plus icon), 'Export' (with an arrow icon), 'Pin to' (with a pin icon), and 'Format query' (with a gear icon). The time range is set to 'Last 24 hours'. Below the toolbar, a code editor window displays the following PowerShell-like query:

```

1 _GetWatchlist("geoip")
2

```

Below the code editor is a table titled 'Results' with columns: LastUpdatedTimeUTC [U...], _DTItemId, SearchKey, cityname, countryname, latitude, longitude, and net. The table contains 14 rows of data, each representing a location entry with its timestamp, ID, search key, city name, country name, latitude, longitude, and network information.

Next, we will enable Microsoft defender for cloud, it allows us to take logs from virtual machines and setwork security groups and ingest them in our log analytics workspace!

The screenshot shows the Microsoft Defender for Cloud portal. On the left, there is a navigation sidebar with sections: Security alerts, Inventory, Cloud Security Explorer, Workbooks, Community, Diagnose and solve problems, Cloud Security (Security posture, Regulatory compliance, Workload protection, Data security, Firewall Manager, DevOps security), Management (Environment settings, Security solutions), and a bottom section for Environment settings. The main area displays connectivity status for various cloud providers: Azure subscriptions (1), AWS accounts (0), GCP projects (0), GitHub connectors (0), AzureDevOps connectors (0), and GitHub connectors (0). Below this, there is a table for GCP Projects (0), AWS Accounts (0), and AzureDevOps Connectors (0). A red box highlights the 'Edit settings' button in the 'Environment settings' section of the sidebar.

We will go here after getting to the azure page.

The screenshot shows the Microsoft Defender for Cloud portal under the 'Environment settings' section. It lists three plans: Foundational CSPM (Free), Servers (\$15/Server/Month), and SQL servers on machines (\$15/Server/Month \$0.015/Core/Hour). Each plan has an 'On/Off' toggle switch. The 'Servers' and 'SQL servers on machines' toggles are highlighted with a red box.

Plan	Pricing*	Resource quantity	Plan
Foundational CSPM	Free		<input type="button" value="Off"/> <input checked="" type="button" value="On"/>
Servers	\$15/Server/Month	0 servers	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>
SQL servers on machines	\$15/Server/Month \$0.015/Core/Hour	0 servers	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>

We need these 2 on!

Settings

Defender plans

Data collection

Store additional raw data - Windows security events

To help audit, investigate, and analyze threats, you can collect raw events, logs, and additional security data and save it to your Log Analytics workspace for analysis.

Select the level of data to store for this workspace. Charges will apply for all settings other than "None".

[Learn more](#)

All Events

All Windows security and AppLocker events.

Common

A standard set of events for auditing purposes.

Minimal

A small set of events that might indicate potential threats. By enabling this option, you won't be able to have a full audit trail.

None

No security or AppLocker events.

We also want to click on All events on this TAB.

Azure

Azure subscription 1

LAW-Cyber-Lab-01

6

0/12 plans

2/2 plans

We also want to make sure it is set for the subscription as well!

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (\$15/Server/Month) Change plan >	3 servers	<input checked="" type="radio"/> Full Settings >	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>
App Service	\$15/instance/Month Details >	0 instances	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>	
Databases	Selected: 0/4 Select types >	Protected: 0/0 instances	<input checked="" type="radio"/> Full Settings >	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>
Storage	\$10/Storage account/month \$0.15/GB scanned for On-Upload Malware Scanning (configurable)	0 storage accounts	<input checked="" type="radio"/> Full Settings >	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>
Containers	\$7/VM core/Month Details >	0 container registries; 0 kubernetes cores	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>	
Key Vault	\$0.25/Vault/Month Details >	0 key vaults	<input checked="" type="radio"/> Full	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>
Resource Manager	\$5/Subscription/Month Details >	0 Azure API Management services	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>	
APIs	Plan 1 (free until February 2024) Details >	0 Azure API Management services	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>	

We want to make sure all of these are turned on because we will be creating some more resources like a key vault in the future.

Home > Microsoft Defender for Cloud | Environment settings > Settings | Defender plans >

Settings & monitoring ...

Azure subscription 1

Continue

When you enable an extension, it will be installed on any new or existing resource, by assigning a security policy.

Defender plans : Servers

Component	Description	Defender plans
Log Analytics agent ⚠ Agent is in deprecation path. Learn more >	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. Learn more	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Vulnerability assessment for machines	Enables vulnerability assessment on your Azure and hybrid machines. Learn more	<input type="checkbox"/>

Auto-provisioning configuration

Log analytics agent

Workspace selection * Custom workspace [LAW-Cyber-Lab-01](#)

When selecting a custom workspace, make sure the relevant solutions are enabled on it. [Learn more >](#)

Security events storage* [All Events](#)

We also want to click settings under the servers and select for the logs to be sent to our custom log aggregation space and not a default one.

Settings | Continuous export

N/A

Search Save

Settings

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

Continuous export

Configure streaming export setting of Defender for Cloud data to multiple export targets.
Exporting Defender for Cloud's data also enables you to use experiences such as integration with 3rd-party SIEM and Azure Data Explorer.
[Learn More >](#)

Event hub Log Analytics workspace

Export enabled **On**

Exported data types

<input checked="" type="checkbox"/> Security recommendations	All recommendations selected
Recommendation severity *	Low,Medium,High
Include security findings	<input checked="" type="radio"/> Yes
<input checked="" type="checkbox"/> Secure score	Overall score,Control score
Controls	All controls selected
<input checked="" type="checkbox"/> Security alerts	Low,Medium,High,Informational
<input type="checkbox"/> Regulatory compliance	No selected standards

Export frequency

Export frequency

Streaming updates

Snapshots

Export configuration

Resource group * RG-Cyber-Lab

Export target

Subscription * Azure subscription 1

Select target workspace * LAW-Cyber-Lab-01

 Saving data to Log Analytics workspace incurs ingestion charges, as detailed [here](#)

Next, we will send the logs using continuous export like shown above.

We will now create an azure storage account, it must be in the same region as the VMs, this will be used to store the NSG flow logs which we will create shortly!

sacyberlab088_1700667470055 | Overview

Deployment

Deployment is in progress

Deployment name: sacyberlab088_1700667470055
Subscription: Azure subscription 1
Resource group: RG-Cyber-Lab

Start time: 11/22/2023, 3:37:55 PM
Correlation ID: 35c51e45-600f-4b97-ecd7-8a17bb0df2c0

Deployment details

Resource	Type	Status	Operation details
sacyberlab088	Microsoft.Storage/storageAccounts	Accepted	Operation details

Give feedback
[Tell us about your experience with deployment](#)

Created, next we will enable flow logs for both NSGs.

Network security g...

windows-vm-nsg | NSG flow logs

Showing 0 to 0 of 0 records.

No flow logs match your filters.
Try changing or clearing your filters.

[Create flow log](#) [Clear filters](#)

This is how we create the flow logs (:

Basics Analytics Tags Review + create

Flow logs allow you to view information about ingress and egress IP traffic through a Network Security Group. [Learn more](#)

Project details

Subscription * [Azure subscription 1](#)

[Select resource](#)

Flow Log Name	Resource	Resource Group
linux-vm-nsg-rg-cyber-lab-flowlog	linux-vm-nsg	rg-cyber-lab
windows-vm-nsg-rg-cyber-lab-flo...	windows-vm-nsg	rg-cyber-lab

Instance details

Select storage account

Info You'll be charged normal data rates for storage and transactions when you send data to a storage account.

Location	eastus2
Subscription	Azure subscription 1
Storage Accounts *	sacyberlab088

[Create a new storage account](#)

Retention (days) * [\(1\)](#)

We will now configure the data collection rules within our log analytics workspace.

LAW-Cyber-Lab-01 | Agents [...](#)

Log Analytics workspace

Search Tags Diagnose and solve problems Logs Settings Tables **Agents** Usage and estimated costs Data export Network isolation Linked storage accounts Properties Locks Classic Legacy agents management Legacy activity log connector

Windows servers [Linux servers](#)

0 Windows computers connected via Azure Monitor Windows agent [See them in Logs](#)

0 Windows computers connected via Log Analytics Windows agent (legacy) [See them in Logs](#)

Want to setup the new Azure Monitor agent? Go to 'Data Collection Rules' **Data Collection Rules**

Log Analytics agent instructions

Basics Resources Collect and deliver Tags Review + create

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. [Learn more](#)

Rule details

Rule Name *	dcr-all-vms
Subscription *	Azure subscription 1
Resource Group *	RG-Cyber-Lab
Region *	East US 2
Platform Type *	<input type="radio"/> Windows <input type="radio"/> Linux <input checked="" type="radio"/> All
Data Collection Endpoint	<none>

this will be the data collection rule for all our VMs so here is what we input.

Data collection endpoints					
Name	Type	Location	Resource group	Subscription	
linux-vm	Virtual machine	East US 2	RG-Cyber-Lab	Azure subscription 1	
windows-vm	Virtual machine	East US 2	RG-Cyber-Lab	Azure subscription 1	

We will add both vms here.

Facility	Minimum log level
LOG_ALERT	none
LOG_AUDIT	none
LOG_AUTH	LOG_DEBUG
LOG_AUTHPRIV	none
LOG_CLOCK	none
LOG_CRON	none
LOG_DAEMON	none
LOG_FTP	none
LOG_KERN	none
LOG_LOCAL0	none

For this lab we will only collect AUTH logs so rest should be set to none.

Data source type *

Windows Event Logs

i If using Sentinel, use [the connector configuration](#) for collecting Windows Secu
[Learn More](#)

Choose Basic to enable collection of event logs. Choose Custom if you want more control.

None Basic Custom

Configure the event logs and levels to collect:

Application

- Critical
- Error
- Warning
- Information **SQL**
- Verbose

Security

- Audit success
- Audit failure **WINDOWS LOGON**

System

- Critical
- Error
- Warning
- Information
- Verbose

For windows we only need these.

Choose Basic to enable collection of event logs. Choose Custom if you want more control over which event logs are collected.

None Basic Custom

Use XPath queries to filter event logs and limit data collection. [Learn more about event logs and XPath syntax](#)

<input type="text"/> Application!*[System[(Level=4 or Level=0)]]	<input type="button" value=""/>	<input type="button" value="Add"/>
<input type="text"/> Security!*[System[(band(Keywords,13510798882111488))]]	<input type="button" value=""/>	<input type="button" value=""/>

We will actually set this to custom after creating and changing it to custom since we also want to record logs of people messing with the windows defender and more and we need to input 2 more lines here, here they are:

One of these is for malware and the other it for tempering detection!

// Windows Defender Malware Detection XPath Query

Microsoft-Windows-Windows Defender/Operational!*[System[(EventID=1116 or EventID=1117)]]

// Windows Firewall Tampering Detection XPath Query

Microsoft-Windows-Windows Firewall With Advanced Security/Firewall!*[System[(EventID=2003)]]

The screenshot shows two main sections. The top section is titled 'Windows computers connected' and includes a checkmark icon, the count '1', the category 'Windows computers', the connection method 'via Azure Monitor Windows agent', and a link 'See them in Logs'. The bottom section is titled 'Linux servers' and includes a checkmark icon, the count '1', the category 'Linux servers', the connection method 'via Log Analytics Linux agent (legacy)', and a link 'See them in Logs'.

1 Windows computers connected
via Azure Monitor Windows agent
[See them in Logs](#)

1 Windows computers connected
via Log Analytics Windows agent (legacy)
[See them in Logs](#)

Windows servers [Linux servers](#)

1 Linux computers connected
via Azure Monitor Linux agent
[See them in Logs](#)

1 Linux computers connected
via Log Analytics Linux agent (legacy)
[See them in Logs](#)

And now both machines should be sending logs!

The screenshot shows the Azure Log Analytics search interface. At the top, there are various navigation and configuration buttons. Below that is a search bar with the query 'SecurityEvent'. The results table has columns for TimeGenerated [UTC], Account, AccountType, Computer, and EventSourceName. The data shows multiple log entries from a single machine ('windows-vm') over a 24-hour period, with event types like Microsoft-Windows-AppLoc, Microsoft-Windows-Security, and Microsoft-Windows-AppLoc.

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName
11/22/2023, 4:39:23.013 PM	NT AUTHORITY\SYSTEM	User	windows-vm	Microsoft-Windows-AppLoc
11/22/2023, 4:39:23.011 PM	WORKGROUP\windows-vm\$	Machine	windows-vm	Microsoft-Windows-Security
11/22/2023, 4:38:23.002 PM	NT AUTHORITY\SYSTEM	User	windows-vm	Microsoft-Windows-AppLoc
11/22/2023, 4:38:23.000 PM	WORKGROUP\windows-vm\$	Machine	windows-vm	Microsoft-Windows-Security
11/22/2023, 4:37:23.005 PM	NT AUTHORITY\SYSTEM	User	windows-vm	Microsoft-Windows-AppLoc
11/22/2023, 4:37:23.003 PM	WORKGROUP\windows-vm\$	Machine	windows-vm	Microsoft-Windows-Security
11/22/2023, 4:36:23.011 PM	NT AUTHORITY\SYSTEM	User	windows-vm	Microsoft-Windows-AppLoc
11/22/2023, 4:36:23.010 PM	WORKGROUP\windows-vm\$	Machine	windows-vm	Microsoft-Windows-Security
11/22/2023, 4:35:31.103 PM	NT AUTHORITY\SYSTEM	User	windows-vm	Microsoft-Windows-AppLoc
11/22/2023, 4:35:31.094 PM	WORKGROUP\windows-vm\$	Machine	windows-vm	Microsoft-Windows-Security
11/22/2023, 4:35:23.016 PM	NT AUTHORITY\SYSTEM	User	windows-vm	Microsoft-Windows-AppLoc

And just to make sure we can query some logs and we can see that they are actually being forwarded!

Now that we have logs from our 2 VMs we will start ingesting logs from our Microsoft active directory as well!

Let's start by:

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

Home > Default Directory | Diagnostic settings >

Diagnostic settings | General

Default Directory

Diagnostic settings

- General
- Custom security attributes

Diagnostic settings

Name	Storage account	Event hub
No diagnostic settings defined		

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- AuditLogs
- SignInLogs
- NoninteractiveUserSignInLogs
- ServicePrincipalSignInLogs
- ManagedIdentitySignInLogs
- ProvisioningLogs
- ADFSgnInLogs
- RiskyUsers
- UserRiskEvents
- NetworkAccessTrafficLogs
- RiskyServicePrincipals
- ServicePrincipalRiskEvents
- EnrichedOffice365AuditLogs
- MicrosoftGraphActivityLogs

Save Discard Delete Feedback

Diagnostic setting

ds-audit-sgnin

Logs

Categories

- AuditLogs
- SignInLogs
- NoninteractiveUserSignInLogs
- ServicePrincipalSignInLogs
- ManagedIdentitySignInLogs
- ProvisioningLogs
- ADFSSgnInLogs
- RiskyUsers

Destination details

Send to Log Analytics workspace

Subscription: Azure subscription 1

Log Analytics workspace: LAW-Cyber-Lab-01 (eastus2)

Archive to a storage account

Stream to an event hub

Send to partner solution

And this is all we need.

We will now create a dummy user in active directory and see if we can generate some logs!

Basics Properties Assignments Review + create

Create a new user in your organization. This user will have a user name like alice@contoso.com. [Learn more](#)

Identity

User principal name	<input type="text" value="dummy_user"/> @ <input type="text" value="antoniofilipearrozhotm..."/>
	<small>Domain not listed</small>
Mail nickname *	<input type="text" value="dummy_user"/>
	<input checked="" type="checkbox"/> Derive from user principal name
Display name*	<input type="text" value="dummy_user"/>
Password *	<input type="password" value="*****"/>
	<input checked="" type="checkbox"/> Auto-generate password
Account enabled	<input checked="" type="checkbox"/>

We logged it to this user using a private tab and this should already generate a log, we will now assign the role of global admin to this user and this should generate another log as well.

Directory roles

X

To assign custom roles to a user, your organization needs Microsoft Entra ID Premium P1 or P2.

Choose admin roles that you want to assign to this user. [Learn more](#)

Role	Description
<input checked="" type="checkbox"/> Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.
<input type="checkbox"/> Global Reader	Can read everything that a Global Administrator can, but not update anything.
<input type="checkbox"/> Global Secure Access Administrator	Create and manage all aspects of Microsoft Entra Internet Access and Microsoft Entra Private Access, including managing access to public and private endpoints.

We will now delete the dummy user and this should generate one more log.

And Boom,

1 AuditLogs

2

Results Chart

TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion	Category
> 11/23/2023, 2:36:00.706 PM	/tenants/e50924e0-82a7-4a71-93cd-6d6af0c55bc8/providers...	Change password (self-service)	1.0	User
> 11/23/2023, 2:36:00.688 PM	/tenants/e50924e0-82a7-4a71-93cd-6d6af0c55bc8/providers...	Update SsRefreshTokenValidFrom Timestamp	1.0	User
> 11/23/2023, 2:36:00.687 PM	/tenants/e50924e0-82a7-4a71-93cd-6d6af0c55bc8/providers...	Change user password	1.0	User
> 11/23/2023, 2:34:59.282 PM	/tenants/e50924e0-82a7-4a71-93cd-6d6af0c55bc8/providers...	Add user	1.0	User
> 11/23/2023, 2:33:53.194 PM	/tenants/e50924e0-82a7-4a71-93cd-6d6af0c55bc8/providers...	Delete user	1.0	User
> 11/23/2023, 2:33:53.193 PM	/tenants/e50924e0-82a7-4a71-93cd-6d6af0c55bc8/providers...	Delete user	1.0	User
> 11/23/2023, 2:33:53.185 PM	/tenants/e50924e0-82a7-4a71-93cd-6d6af0c55bc8/providers...	Delete user	1.0	User

Many logs!

Adding user, deleting user, everything is in there and more should come in the next few minutes.

Run Time range : Last 48 hours Save Share New alert rule Export Pin to Format query

```

1 AuditLogs
2 | where OperationName == "Add member to role" and Result == "success"
3 | where TargetResources[0].modifiedProperties[1].newValue == "Global Administrator" or TargetResources[0].modifiedProperties[1].newValue == "Company Administrator"
4 | order by TimeGenerated desc
5 | project TimeGenerated, OperationName, AssignedRole = TargetResources[0].modifiedProperties[1].newValue, Status = Result, TargetResources
6

```

Results Chart

TimeGenerated [UTC]	OperationName	AssignedRole	Status	TargetResources
> 11/23/2023, 2:38:06.143 PM	Add member to role	"Global Administrator"	success	[{"id": "25163d24-79c5-44bf-b722-1f3a2a2a2a2a"}]

This query searches for adding someone as a global admin and like we expected we get a result!

All we need now for logging is subscription level logging, let's start with activity logs!

Like creating resources, deleting resources, etc....

Activity log

Alerts Metrics Logs Change Analysis Service health Workbooks Insights Applications Virtual Machines Storage accounts Containers Networks SQL (preview) Azure Cosmos DB Key Vaults Azure Cache for Redis

Activity Edit columns Refresh Export Activity Logs Download as CSV Insights Feedback Pin current filters Reset filters

Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. Visit Log Analytics

Subscription: Azure subscription 1 Event severity: All Timespan: Last 6 hours Add filter

10 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
> Returns Storage Service SAS Token	Succeeded	2 hours ago	Sun Nov 26 ...	Azure subscription 1	NetworkTrafficAnalyticsSe...
> Registers EventGrid Resource Provider	Succeeded	3 hours ago	Sun Nov 26 ...	Azure subscription 1	StorageAccounts/securit...
> Create role assignment	Succeeded	3 hours ago	Sun Nov 26 ...	Azure subscription 1	StorageAccounts/securit...
> Update data scanners	Succeeded	3 hours ago	Sun Nov 26 ...	Azure subscription 1	Windows Azure Security R...
> Returns Storage Service SAS Token	Succeeded	3 hours ago	Sun Nov 26 ...	Azure subscription 1	NetworkTrafficAnalyticsSe...
> Returns Storage Service SAS Token	Succeeded	3 hours ago	Sun Nov 26 ...	Azure subscription 1	NetworkTrafficAnalyticsSe...
> Returns Storage Service SAS Token	Succeeded	4 hours ago	Sun Nov 26 ...	Azure subscription 1	NetworkTrafficAnalyticsSe...
> Returns Storage Service SAS Token	Succeeded	5 hours ago	Sun Nov 26 ...	Azure subscription 1	NetworkTrafficAnalyticsSe...
> Returns Storage Service SAS Token	Succeeded	6 hours ago	Sun Nov 26 ...	Azure subscription 1	NetworkTrafficAnalyticsSe...
> Returns Storage Service SAS Token	Succeeded	6 hours ago	Sun Nov 26 ...	Azure subscription 1	NetworkTrafficAnalyticsSe...

We first went to azure monitor, after that we need to click activity log and we will export those logs.

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a subscription, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name * ds-azure-activity

Logs

Categories

- Administrative
- Security
- ServiceHealth
- Alert
- Recommendation
- Policy
- Autoscale
- ResourceHealth

Destination details

Send to Log Analytics workspace

Subscription: Azure subscription 1

Log Analytics workspace: LAW-Cyber-Lab-01 (eastus2)

Archive to a storage account

Stream to an event hub

Send to partner solution

We will send everything to our log analytics workspace!

Time range : Last 24 hours

1 AzureActivity

2

Results

TimeGenerated [UTC]	OperationNameValue	Level	ActivityStatusValue	ActivitySubstatusValue	Subscription
> 11/26/2023, 2:13:04.648 PM	MICROSOFT.INSIGHTS/DIAGNOSTICSETTINGS/WRITE	Information	Success	OK	842840fc-2c
> 11/26/2023, 2:13:01.695 PM	MICROSOFT.INSIGHTS/DIAGNOSTICSETTINGS/WRITE	Information	Start		842840fc-2c

If we test, we have some logs already!

Lastly, we will setup resource logging, we will create a key vault and a blob storage!

The screenshot shows the Azure Storage accounts interface. On the left, there's a sidebar with various monitoring and diagnostic options like Configuration, Data Lake Gen2 upgrade, Resource sharing (CORS), Advisor recommendations, Endpoints, Locks, Insights, Alerts, Metrics, Workbooks, Diagnostic settings, and Logs. The 'Logs' section is currently selected. In the main pane, it says 'sacyberlab088 | Diagnostic settings'. It shows a table with five rows: 'sacyberlab088' (Storage account, RG-Cyber-Lab, Disabled), 'blob' (Storage account, RG-Cyber-Lab, Disabled), 'queue' (Storage account, RG-Cyber-Lab, Disabled), 'table' (Storage account, RG-Cyber-Lab, Disabled), and 'file' (Storage account, RG-Cyber-Lab, Disabled). The 'blob' row is highlighted with a red box.

We now have to go to our storage account, we scroll down to diagnostic settings and next we will enable logging for the blob portion of the storage account.

Diagnostic setting ...

This screenshot shows the 'Diagnostic setting' configuration page. At the top, there are buttons for Save, Discard, Delete, and Feedback. Below that, a note explains what a diagnostic setting is: 'A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur.' A link to 'Learn more about the different log categories and contents of those logs' is provided. The 'Diagnostic setting name' is 'ds-storage-account'. The 'Logs' section has 'Category groups' with 'audit' and 'allLogs' checked. The 'Categories' section has 'Storage Read', 'Storage Write', and 'Storage Delete' checked. The 'Metrics' section has 'Transaction' checked. The 'Destination details' section has 'Send to Log Analytics workspace' checked, with 'Subscription' set to 'Azure subscription 1' and 'Log Analytics workspace' set to 'LAW-Cyber-Lab-01 (eastus2)'. There are also options for 'Archive to a storage account', 'Stream to an event hub', and 'Send to partner solution'.

Same things as the others, we will send all logs including audit logs to our analytics workspace!

Let's create our key vault now!

Create a key vault

A key vault is a cloud service used to manage keys, secrets, and certificates. It allows you to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.

Project details

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

Subscription *
└ Resource group *

Azure subscription 1
RG-Cyber-Lab
Create new

Instance details

Key vault name * ⓘ

akv-cyber-lab-995

Region *

East US 2

Pricing tier * ⓘ

Standard

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

Configure data plane access for this key vault

To access a key vault in data plane, all callers (users or applications) must have proper authentication and authorization. Authentication establishes the identity of the caller. Authorization determines which operations the caller can execute. [Learn more](#)

Permission mode

Grant data plane access by using a [Azure RBAC](#) or [Key Vault access policy](#).

Azure role-based access control (recommended) ⓘ
 Vault access policy ⓘ

Resource access

Azure Virtual Machines for deployment ⓘ
 Azure Resource Manager for template deployment ⓘ
 Azure Disk Encryption for volume encryption ⓘ

Access policies

Access policies enable you to have fine grained control over access to vault items. [Learn more](#)

+ Create	Edit	Delete	Name ↗	Email ↗	Key Permissions	Secret Permissions	Certificate Permissions
			antonio.filipearaz@hotmail.com#EXT#@antonio.filipearaz...	antonio.filipearaz@hotmail.com#EXT#@antonio.filipearaz...	Get, List, Update, Create, Import, Delete, Recover, Backup, R...	Get, List, Set, Delete, Recover, Backup, Restore	Get, List, Update, Create, Import, Delete, Recover, Backup, R...

We want to change our vault policy to the one above!

akv-cyber-lab-995 | Secrets

Key vault

Search + Generate/Import Refresh Restore Backup View sample code Manage deleted secrets

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

Objects

Keys Secrets Certificates

Settings

Access configuration Networking Microsoft Defender for Cloud

The screenshot shows the Azure Key Vault interface for the 'akv-cyber-lab-995' vault. The 'Secrets' tab is highlighted with a red box. The left sidebar lists various vault management sections: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Access policies, Events, Objects (with 'Secrets' selected), Settings, Access configuration, Networking, and Microsoft Defender for Cloud. The main pane displays a message stating 'There are no secrets available.'

After creating the key vault, we will create a “secret” which is like a password we want to store.

Upload options	Manual
Name *	Tenant-global-admin-password
Secret value *	*****
Content type (optional)	
Set activation date	<input type="checkbox"/>
Set expiration date	<input type="checkbox"/>
Enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No
Tags	0 tags

Just create a random secret.

The screenshot shows the 'Diagnostic settings' page for a Key Vault named 'akv-cyber-lab-995'. The left sidebar lists various monitoring and automation options. The 'Metrics' and 'Diagnostic settings' items are highlighted with a red box. The main content area displays diagnostic settings configuration, showing a table for adding new settings and a list of available data types.

Name	Storage account	Event hub
No diagnostic settings defined		

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- Audit Logs
- Azure Policy Evaluation Details
- AllMetrics

And like always, let's create Diagnostic settings so we can start generating some logs.

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name *

Logs

Category groups audit allLogs

Categories Audit Logs Azure Policy Evaluation Details

Destination details

Send to Log Analytics workspace

Subscription

Log Analytics workspace

Metrics

AllMetrics

Archive to a storage account

Stream to an event hub

Send to partner solution

Like this.

1 StorageBlobLogs

Results					
TimeGenerated [Local Time]	AccountName	Location	Protocol	OperationName	Authentication
> 9/8/2023, 12:30:42.911 PM	sacyberlab999	eastus2	HTTPS	PutBlob	SAS
> 9/8/2023, 12:29:43.820 PM	sacyberlab999	eastus2	HTTPS	GetContainerServiceMetadata	AccountKey
> 9/8/2023, 12:29:24.468 PM	sacyberlab999	eastus2	HTTPS	GetContainerServiceMetadata	AccountKey

And everything is being logged, the blob storage as well as the key vault.

We will finally start working on our SIEM, creating incidents, creating a threat map, harden our environment, work on incidents,etc...

We will start by creating 4 MAPS, one for windows VMs: RDP, SMB / GENERAL AUTHENTICATION FAILURES

LINUX VMs: SSH authentication FAILURES.

AZURE SQL SERVER: authentication FAILURES.

NETWORK SECURITY GROUP: MALICIOUS FLOWS

The screenshot shows the Microsoft Sentinel Workbooks interface. On the left, there's a navigation sidebar with various sections like General, Logs, Threat management, Incidents, Workbooks (which is highlighted with a red box), Notebooks, Entity behavior, Threat intelligence, and MITRE ATT&CK (Preview). The main area is titled 'Microsoft Sentinel | Workbooks' and shows 'My workbooks' with 0 items. It also includes sections for Templates, Logs, News & guides, and Search. At the top right, there are buttons for Refresh, Add Workbook (highlighted with a red box), Guides & Feedback, and a link to Content hub.

In sentinel, maps are workbooks, so let's create one.

The screenshot shows the Microsoft Sentinel Advanced Editor. The title bar says 'Editing query item: query - 0'. Below it, there are tabs for Settings, Advanced Settings, and Style, with 'Advanced Settings' selected. A red box highlights the 'Advanced Editor' tab. A note below it says: 'Shown below is a JSON representation of the current item. Any changes you make here will be reflected when you press 'Done Editing''. The main area contains the following JSON code:

```

1 {
2   "type": 3,
3   "content": {
4     "version": "KqlItem/1.0",
5     "query": "",
6     "size": 0,
7     "timeContext": {
8       "durationMs": 86400000
9     },
10    "queryType": 0,
11    "resourceType": "microsoft.operationalinsights/workspaces"
12  },
13  "name": "query - 0"
14 }

```

At the bottom, there are buttons for Done Editing (with a checkmark), Cancel, Add, Move, Clone, and Remove.

We will edit the default workbook that comes with sentinel and use the advanced feature to create our maps.

Here is a snippet of what we will be using for the SSH logs/MAP.

And boom! Here is the map, since my VM has been off most of the time, almost nobody has tried to break in yet.

Refresh + Add Workbook Guides & Feedback

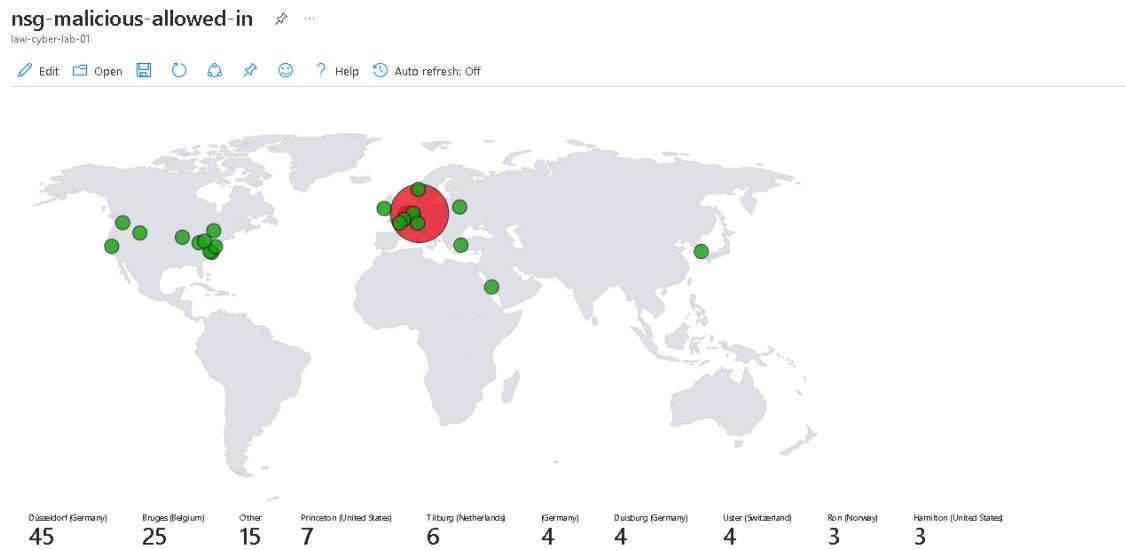
1 My workbooks 0 Templates 0 Updates More content at Content hub

My workbooks Templates

Search Add filter

Name	Content source	Source name
linux-ssh-auth-fail	Custom	--

Now that we have 1 created, I will go ahead and create the other 3 Maps.

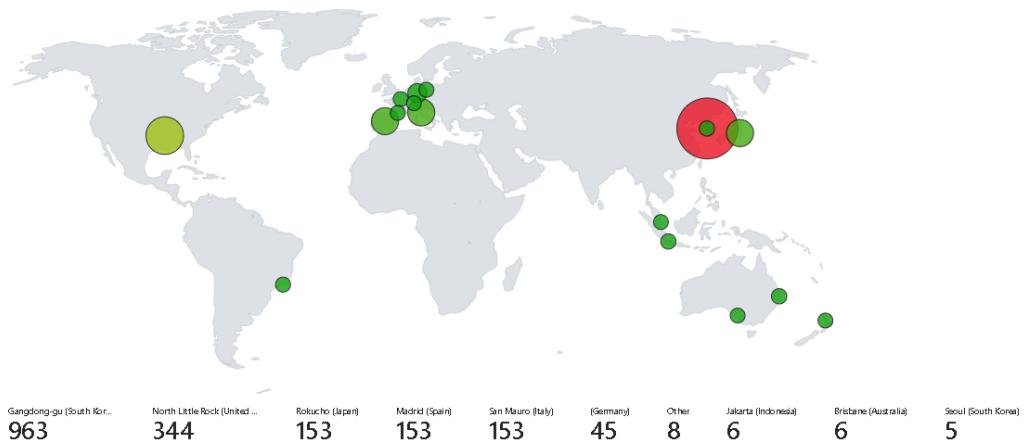


For example, there is a lot of malicious traffic from our NSG.

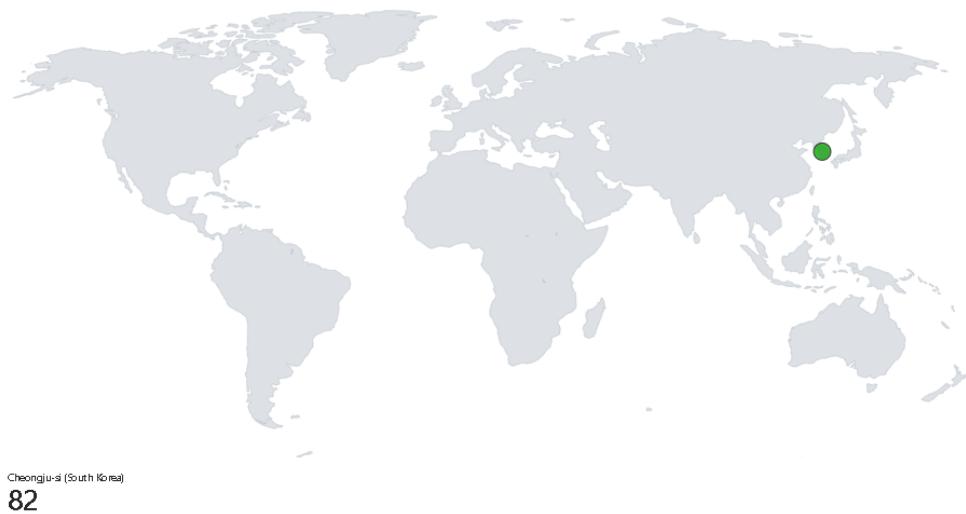
24 hours later and here is how the graphs are looking:

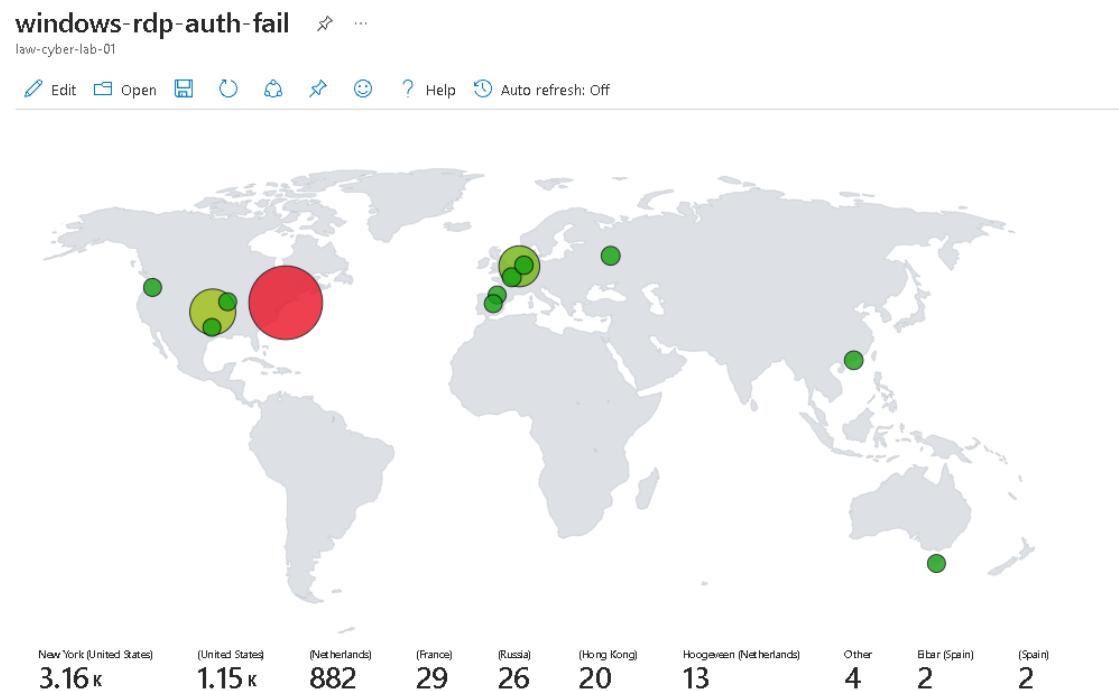
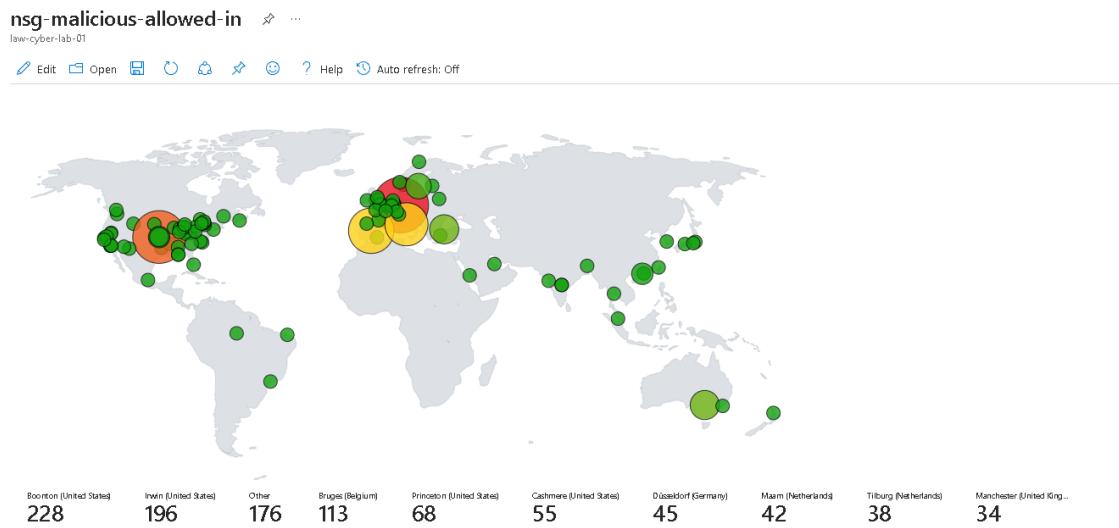
linux-ssh-auth-fail ⚡ ...

law-cyber-lab-01

[Edit](#) [Open](#) [Save](#) [Share](#) [Help](#) [Auto refresh: Off](#)**mssql-auth-fail** ⚡ ...

law-cyber-lab-01

[Edit](#) [Open](#) [Save](#) [Share](#) [Help](#) [Auto refresh: Off](#)



Definitely a lot of malicious traffic and a lot of attack attempts, let's go ahead and create some alerts in our SIEM!

- **SecurityEvent**

```

| where EventID == 4625
| where TimeGenerated > ago(60m)
| summarize FailureCount = count() by AttackerIP =
IpAddress, EventID, Activity, DestinationHostName =
Computer
| where FailureCount >= 10
    
```

THIS WILL BE OUR TEST ALERT!

And pretty much what this is checking is for a windows brute force attack, like CHATGPT puts it:

1. `| SecurityEvent`: This specifies the data source that the query will operate on, which in this case is a table or dataset containing security events.
2. `| where EventID == 4625`: This filters the events to include only those where the `EventID` is `4625`, which typically represents a failed login attempt in Windows security event logs.
3. `| where TimeGenerated > ago(60m)`: This further filters the events to only include those generated in the last 60 minutes.
4. `| summarize FailureCount = count() by AttackerIP = IPAddress, EventID, Activity, DestinationHostName = Computer`: This aggregates the data by counting the number of failed login attempts (`count()`) and groups them by the IP address of the attacker (`AttackerIP`), the `EventID`, the type of activity (`Activity`), and the host name of the target machine (`Computer`). The result is aliased to `FailureCount` for the count, `AttackerIP` for the `IPAddress`, and `DestinationHostName` for the `Computer`.
5. `| where FailureCount >= 10`: This final filter includes only the aggregated results where the count of failed login attempts is 10 or more.

The query is useful for identifying potential brute-force attack attempts by detecting multiple failed login attempts from the same IP address within the last hour. It helps in pinpointing which attackers (by IP address) are frequently trying to log in to which host machines, allowing for a targeted security response.

The screenshot shows the Microsoft Sentinel Analytics interface. On the left, there's a navigation sidebar with sections like Overview (Preview), Logs, News & guides, Search, Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview)), Content management (Content hub, Repositories (Preview), Community), Configuration (Workspace manager (Preview), Data connectors), and Analytics (selected). At the top, there's a search bar and a 'Create' button with a dropdown menu showing 'Scheduled query rule' (highlighted with a red box), 'NRT query rule', and 'Microsoft incident creation rule'. Below this is a table titled 'Active rules' with columns for Severity, Name, Rule t..., Status, Tactics, and Tech. A single row is shown: 'High' severity, 'Advanced Multi...' name, 'Enabled' status, and 'Fus' tactic. To the right, there's a 'Rules by severity' chart with three bars: High (1), Medium (0), and Low (0).

We will go to sentinel and create a scheduled query rule!

This screenshot shows the 'General' tab of the 'Create rule' wizard. The tabs at the top are General (selected), Set rule logic, Incident settings, Automated response, and Review + create. The main area is titled 'Analytics rule details' and contains fields for 'Name *' (with 'TEST: Brute Force ATTEMPT - Windows' entered) and 'Description' (with 'When the same person fails to logon the same VM at least 10 times in the last 60mins.' entered). There are also dropdowns for 'Severity' (Medium), 'Tactics and techniques', and a 'Status' toggle switch set to 'Enabled'.

We will enter a name of our choosing and a description.

The screenshot shows the 'Alert enhancement' section of the Microsoft Sentinel Analytics Rule configuration. It includes a KQL query editor at the top with the following code:

```

SecurityEvent
| where EventID == 4625
| where TimeGenerated > ago(60m)
| summarize FailureCount = count() by AttackerIP = IPAddress, EventID, Activity, DestinationHostName
| where FailureCount >= 10

```

Below the query is a 'View query results >' link. The main configuration area is highlighted with a red box. It contains an 'Entity mapping' section with two rows:

- Row 1: IP (dropdown) → Address (dropdown) → AttackerIP (dropdown) → Add identifier (+)
- Row 2: Host (dropdown) → HostName (dropdown) → DestinationHostName (dropdown) → Add identifier (+)

At the bottom of this section is a 'Add new entity' button.

We will put our KQL query on the top and here in entity mapping we will map an IP address as the attacker IP and the host, this pretty much let's sentinel correlate different alerts with one another (let's say the same IP is attacking another HOST, sentinel will know that and alert us as well that it's the same IP).

Query scheduling

Run query every *

 Minutes

Lookup data from the last *

 Hours

We will make sure this query is running every 5 mins.

Everything else is default!

Alert grouping

Set how the alerts that are triggered by this analytics rule, are grouped into incidents.
Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents
 Enabled

Up to 150 alerts can be grouped into a single incident. If more than 150 alerts are generated, a new incident will be created with the same incident details as the original, and the excess alerts will be grouped into the new incident.

Limit the group to alerts created within the selected time frame *

Hours

Group alerts triggered by this analytics rule into a single incident by

- Grouping alerts into a single incident if all the entities match (recommended)
- Grouping all alerts triggered by this rule into a single incident
- Grouping alerts into a single incident if the selected entity types and details match:

Select entities

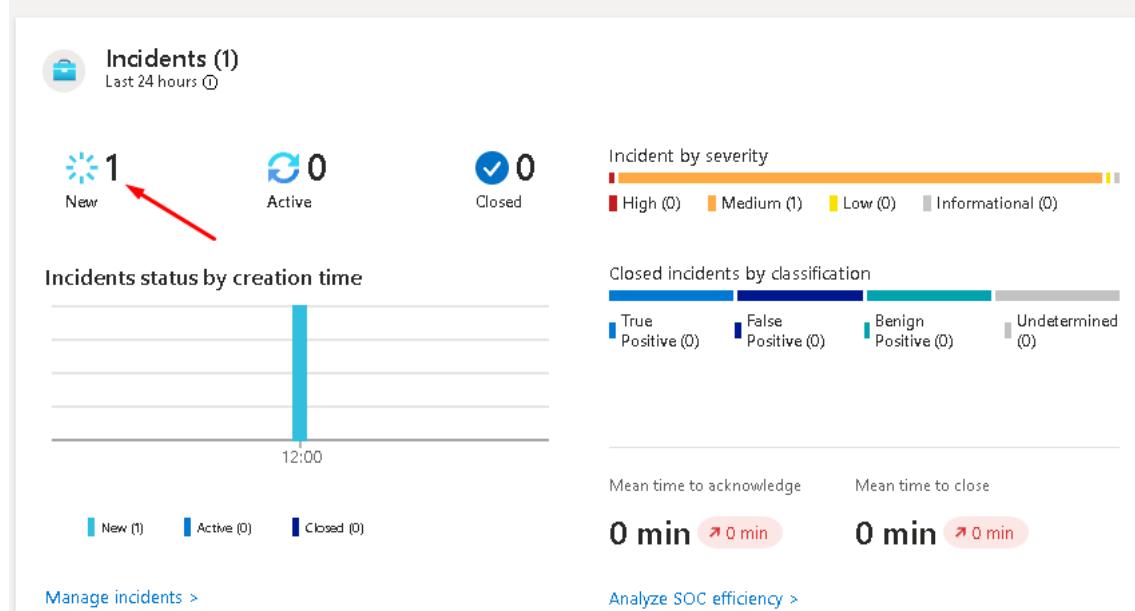
Select details

Re-open closed matching incidents

Disabled

We will enable alert grouping and leave the settings as default.

We don't want to automate anything because later we will respond to these incidents according to the NIST incident response framework.



We got “lucky” since the query came back positive without us having to do anything, if the query were to come back with no results, we would have needed to try and “attack” our own windows RDP login for us to get an alert.

Since this rule was mostly for testing, we will now import a whole bunch of detection queries for this project.

The screenshot shows a Notepad window titled 'Sentinel-Analytics-Rules(KQL Alert Queries).json - Notepad'. The content of the file is a JSON object representing an Azure Resource Manager template for an alert rule. The 'resources' array contains one item, which is a scheduled alert rule with the following properties:

```
{  
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.0",  
    "parameters": {  
        "workspace": {  
            "type": "String"  
        }  
    },  
    "resources": [  
        {  
            "id": "[concat(resourceId('Microsoft.OperationalInsights/workspaces/providers', parameters('workspace')), 'Microsoft.SecurityInsights/c220acf2-b8bb-436d-ad4f-7e3174bbf5a1')]",  
            "name": "[concat(parameters('workspace'), '/Microsoft.SecurityInsights/c220acf2-b8bb-436d-ad4f-7e3174bbf5a1')]",  
            "type": "Microsoft.OperationalInsights/workspaces/providers/alertRules",  
            "kind": "Scheduled",  
            "apiVersion": "2022-09-01-preview",  
            "properties": {  
                "displayName": "CUSTOM: Possible Privilege Escalation (Azure Key Vault Critical Credential Retrieval or Update)",  
                "description": "",  
                "severity": "High",  
                "enabled": true,  
                "query": "/// Updating a specific existing password Success\\nlet CRITICAL_PASSWORD_NAME = \"Tenant-Global-Admin-Passwor",  
                "queryFrequency": "PT10M",  
                "queryPeriod": "PT5H",  
                "triggerOperator": "GreaterThan",  
                "triggerThreshold": 0,  
                "suppressionDuration": "PT5H",  
                "suppressionEnabled": false,  
                "startTimeUtc": null,  
                "tactics": [  
                    "PrivilegeEscalation"  
                ],  
                "techniques": []  
            }  
        }  
    ]  
}
```

We will import this big file with a bunch of detection rules already setup.

	Severity	Name	Rule t...	Status	Tactics	Techniques	Source name	Last Modified ↓	
	Medium	CUSTOM: Brute Force ATTEMPT - Linux S...	⌚ Scl	Enabled	🕒 Credential ...	T1110	Custom Content	30/11/2023, 10:...	...
	High	CUSTOM: Brute Force SUCCESS - Azure ...	⌚ Scl	Enabled			Custom Content	30/11/2023, 10:...	...
	High	CUSTOM: Malware Detected	⌚ Scl	Enabled			Custom Content	30/11/2023, 10:...	...
	Medium	CUSTOM: Brute Force ATTEMPT - MS SQ...	⌚ Scl	Enabled	🕒 Credential ...	T1110	Custom Content	30/11/2023, 10:...	...
	High	CUSTOM: Brute Force SUCCESS - Linux S...	⌚ Scl	Enabled	🕒 Credential ...	T1110	Custom Content	30/11/2023, 10:...	...
	Medium	CUSTOM: Brute Force ATTEMPT - Azure ...	⌚ Scl	Enabled	🕒 Credential ...	T1110	Custom Content	30/11/2023, 10:...	...
	High	CUSTOM: Possible Privilege Escalation (A...	⌚ Scl	Enabled	⚡ Privilege Es...		Custom Content	30/11/2023, 10:...	...
	High	CUSTOM: Possible Privilege Escalation (...	⌚ Scl	Enabled	⚡ Privilege Es...		Custom Content	30/11/2023, 10:...	...
	High	CUSTOM: Windows Host Firewall Tamper...	⌚ Scl	Enabled	🛡 Defense Ev...		Custom Content	30/11/2023, 10:...	...
	High	CUSTOM: Brute Force SUCCESS - Windo...	⌚ Scl	Enabled	🕒 Credential ...	T1110	Custom Content	30/11/2023, 10:...	...
	Medium	CUSTOM: Possible Lateral Movement (Ex...	⌚ Scl	Enabled	🕒 Cre... +1 ⓘ	T1555 +1 ⓘ	Custom Content	30/11/2023, 10:...	...
	Medium	CUSTOM: Brute Force ATTEMPT - Windo...	⌚ Scl	Enabled	🕒 Credential ...	T1110	Custom Content	30/11/2023, 10:...	...
	Medium	CUSTOM: Brute Force ATTEMPT - Azure ...	⌚ Scl	Enabled	🕒 Credential ...	T1110	Custom Content	30/11/2023, 10:...	...
	High	Advanced Multistage Attack Detection	⌚ Fus	Enabled	📅 Col... +11 ⓘ		Gallery Content	20/11/2023, 15:...	...

Everything worked like expected!

And we will have 13 custom detection rules and 1 default rule that comes already with sentinel.

```
// Brute Force Success Windows
let FailedLogons = SecurityEvent
| where EventID == 4625 and LogonType == 3
| where TimeGenerated > ago(1h)
| summarize FailureCount = count() by AttackerIP = IPAddress, EventID,
Activity, LogonType, DestinationHostName = Computer
| where FailureCount >= 5;
let SuccessfulLogons = SecurityEvent
| where EventID == 4624 and LogonType == 3
| where TimeGenerated > ago(1h)
| summarize SuccessfulCount = count() by AttackerIP = IPAddress,
LogonType, DestinationHostName = Computer, AuthenticationSuccessTime =
TimeGenerated;
SuccessfulLogons
| join kind = inner FailedLogons on DestinationHostName, AttackerIP,
LogonType
| project AuthenticationSuccessTime, AttackerIP, DestinationHostName,
FailureCount, SuccessfulCount
```

For example, this is one of our rules that detects brute force success on windows, let's break it down.

This KQL query is composed of two subqueries that interact with each other, and its primary function is to detect brute force login attempts that have eventually succeeded on Windows systems. Here is a breakdown of the query:

1. Define FailedLogons Subquery:

- `| SecurityEvent`: This selects the security events to be analyzed.
- `| where EventID == 4625 and LogonType == 3`: Filters for events with an ID of 4625, which indicates a failed logon attempt, and where the logon type is 3, which usually means a network logon (often used for remote access).
- `| where TimeGenerated > ago(1h)`: Limits the events to those generated in the last hour.
- `| summarize FailureCount = count() by AttackerIP = IPAddress, EventID, Activity, LogonType, DestinationHostName = Computer`: Aggregates the number of failed logon attempts, grouping them by IP address of the attacker, event ID, activity type, logon type, and the host name of the target machine.
- `| where FailureCount >= 5`: Filters the aggregated results to only include records where there have been five or more failed attempts.

2. Define SuccessfulLogons Subquery:

- `| SecurityEvent`: Again, selects the security events to be analyzed.
- `| where EventID == 4624 and LogonType == 3`: Filters for events with an ID of 4624, which indicates a successful logon, again where the logon type is 3.
- `| where TimeGenerated > ago(1h)`: Limits the events to those generated in the last hour.
- `| summarize SuccessfulCount = count() by AttackerIP = IPAddress, LogonType, DestinationHostName = Computer, AuthenticationSuccessTime = TimeGenerated`: Aggregates the number of successful logons, grouped by attacker IP, logon type, destination host name, and the time the authentication succeeded.

3. Combine FailedLogons and SuccessfulLogons:

- `| SuccessfulLogons`: This initiates the join operation with the results of the `SuccessfulLogons` subquery.
- `| join kind = inner FailedLogons on DestinationHostName, AttackerIP, LogonType`: Performs an inner join between the two subqueries on the destination host name, attacker IP, and logon type. This join will match records from `SuccessfulLogons` with records from `FailedLogons` where the logon type, attacker IP, and destination host name are the same.
- `| project AuthenticationSuccessTime, AttackerIP, DestinationHostName, FailureCount, SuccessfulCount`: Projects (selects) the final columns to display in the output, which includes the time of successful authentication, IP address of the attacker, the destination host name, the count of failed attempts, and the count of successful logons.

The resulting output from this query would give you the instances where an IP address had multiple failed logon attempts (suggesting a brute force attack) but eventually managed to successfully log in within the past hour. This could indicate that the brute force attack was successful and may warrant further investigation or immediate action.

BEFORE SECURING ENVIRONMENT	
Start Time	2023-03-10T21:03:08.1360519Z
Stop Time	2023-03-11T21:03:08.1360519Z
Security Events (Windows VMs)	4358
Syslog (Linux VMs)	2345
SecurityAlert (Microsoft Defender for Cloud)	6
SecurityIncident (Sentinel Incidents)	73
NSG Inbound Malicious Flows Allowed	103

AFTER SECURING ENVIRONMENT	
Start Time	2023-03-13T21:03:08.1360519Z
Stop Time	2023-03-14T21:03:08.1360519Z
Security Events (Windows VMs)	110
Syslog (Linux VMs)	344
SecurityAlert (Microsoft Defender for Cloud)	1
SecurityIncident (Sentinel Incidents)	2
NSG Inbound Malicious Flows Allowed	0

RESULTS (will auto update, do not edit formulas)	
	Change after security environment
Security Events (Windows VMs)	-97.48%
Syslog (Linux VMs)	-85.33%
SecurityAlert (Microsoft Defender for Cloud)	-83.33%
Security Incident (Sentinel Incidents)	-97.26%
NSG Inbound Malicious Flows Allowed	-100.00%

Before we keep on going, we will record our stats.

▷ Run

Time range : Set in query

Save

Share

New alert

```
1 SecurityEvent  
2 | where TimeGenerated >= ago(24h)  
3 | count
```

Results

Chart

Count

> 87394

We will record all the numbers in the spreadsheet.

mssql-auth-fail ⚙ ...

law-cyber-lab-01

Done Editing Open 📁 🗃 🚫 🖊️ 🔍 ⌂ ⌄ ? Help



Düsseldorf (Germany)

7.73 k

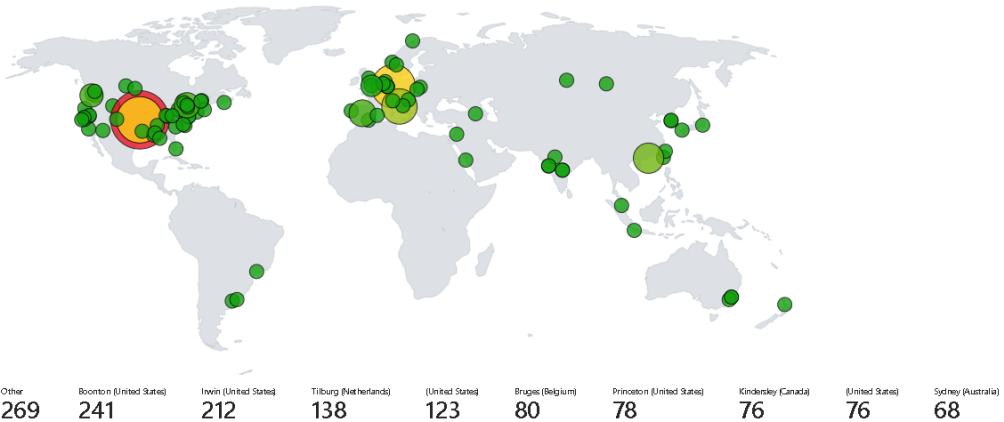
Eibar (Spain)

2.27 k

nsg-malicious-allowed-in ⚙ ...

law-cyber-lab-01

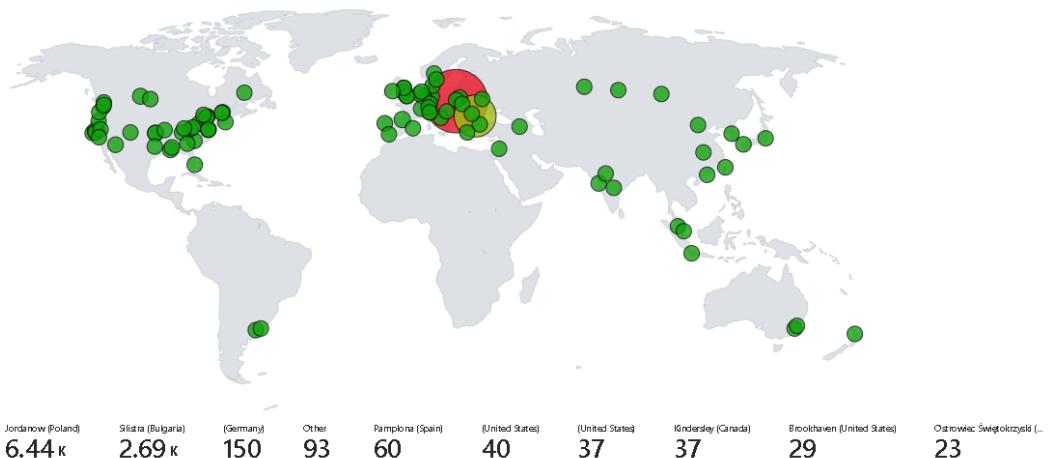
Edit Open 📁 🗃 🚫 🖊️ 🔍 ? Help ⏱ Auto refresh: Off



windows-rdp-auth-fail

law-cyber-lab-01

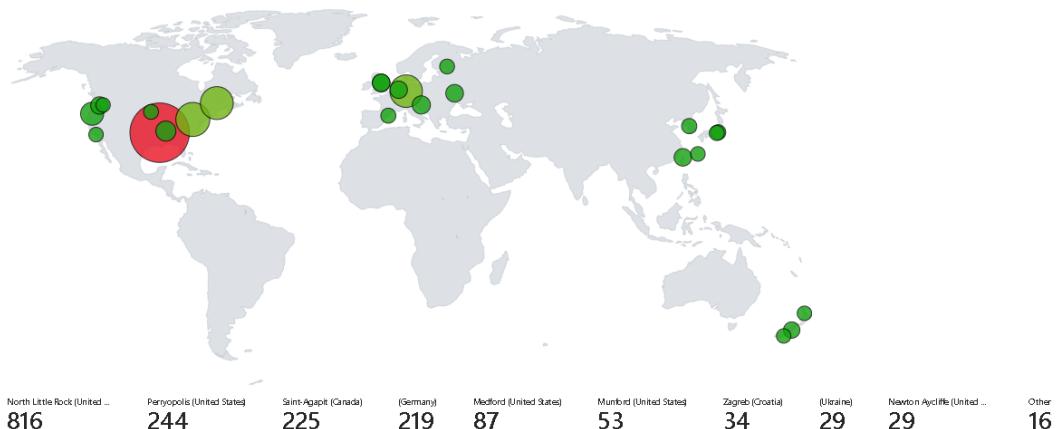
Edit Open ⌘ ⌘ ⌘ ⌘ ? Help ⌘ Auto refresh: Off



linux-ssh-auth-fail

law-cyber-lab-01

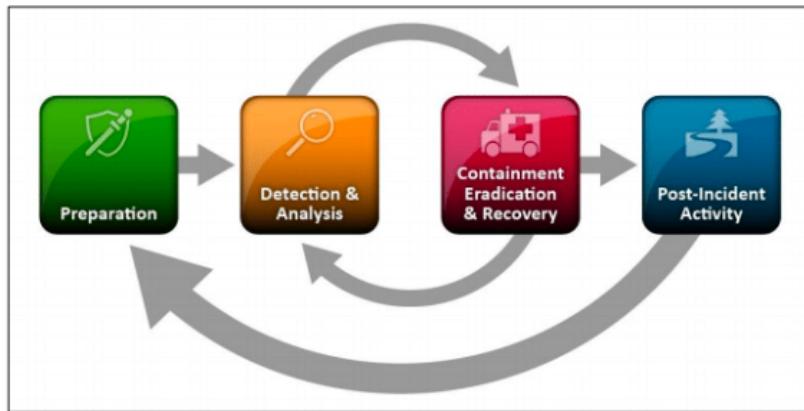
Done Editing Open ⌘ ⌘ ⌘ ⌘ ? Help



Here is all the malicious traffic in the last 24 hours.

We will now adhere to NIST 800-61 to practice incident response.

It goes something like this:



Step 1: Preparation

- (We initiated this already by ingesting all of the logs into Log Analytics Workspace and Sentinel and configuring alert rules)

Step 2: Detection & Analysis (You may have different alerts/incidents)

1. Set Severity, Status, Owner
2. View Full Details (New Experience)
3. Observe the Activity Log (for history of incident)
4. Observe Entities and Incident Timelines (are they doing anything else?)
5. "Investigate" the incident and continue trying to determine the scope
6. Inspect the entities and see if there are any related events
7. Determine legitimacy of the incident (True Positive, False Positive, etc.)
8. If True Positive, continue, if False positive, close it out

Step 3: Containment, Eradication, and Recovery

- Use the simple [Incident Response PlayBook](#)

CUSTOM: Brute Force SUCCESS - Windows
Incident ID: 24

Owner: Antonio Fi... ▾ | Status: Active ▾ | Severity: High ▾

Description: If you see a SUCCESS but the Account is "NT AUTHORITY\ANONYMOUS LOGON", check out this article: <https://www.inversecos.com/2020/04/successful-4624-anonymous-logons-to.html>

Alert product names:

- Microsoft Sentinel

Evidence:

1 Events 1 Alerts 0 Bookmarks

Last update time: 12/05/23, 06:20 PM Creation time: 11/30/23, 04:50 PM

Entities (2):

- windows-vm
- 123.25.255.29

Geolocation information

Organization: Vietnam Posts And Telecommunications Group Organization type: Telecommunications

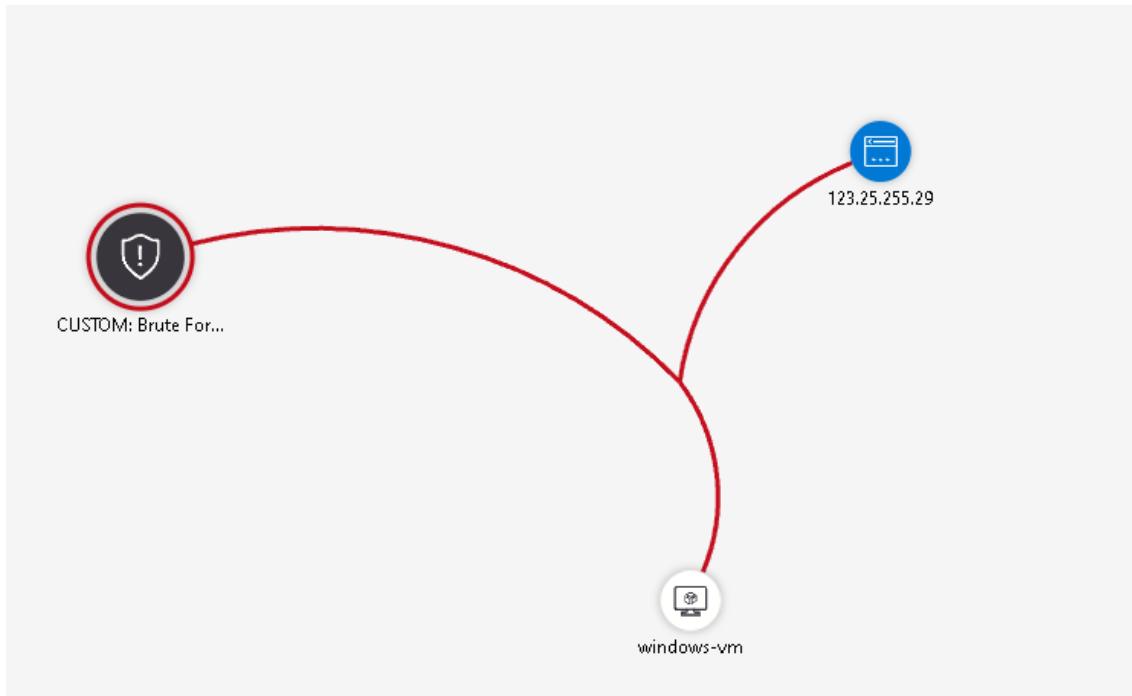
City: Dong Da Country: Vietnam

State: Ha Noi Continent: Asia

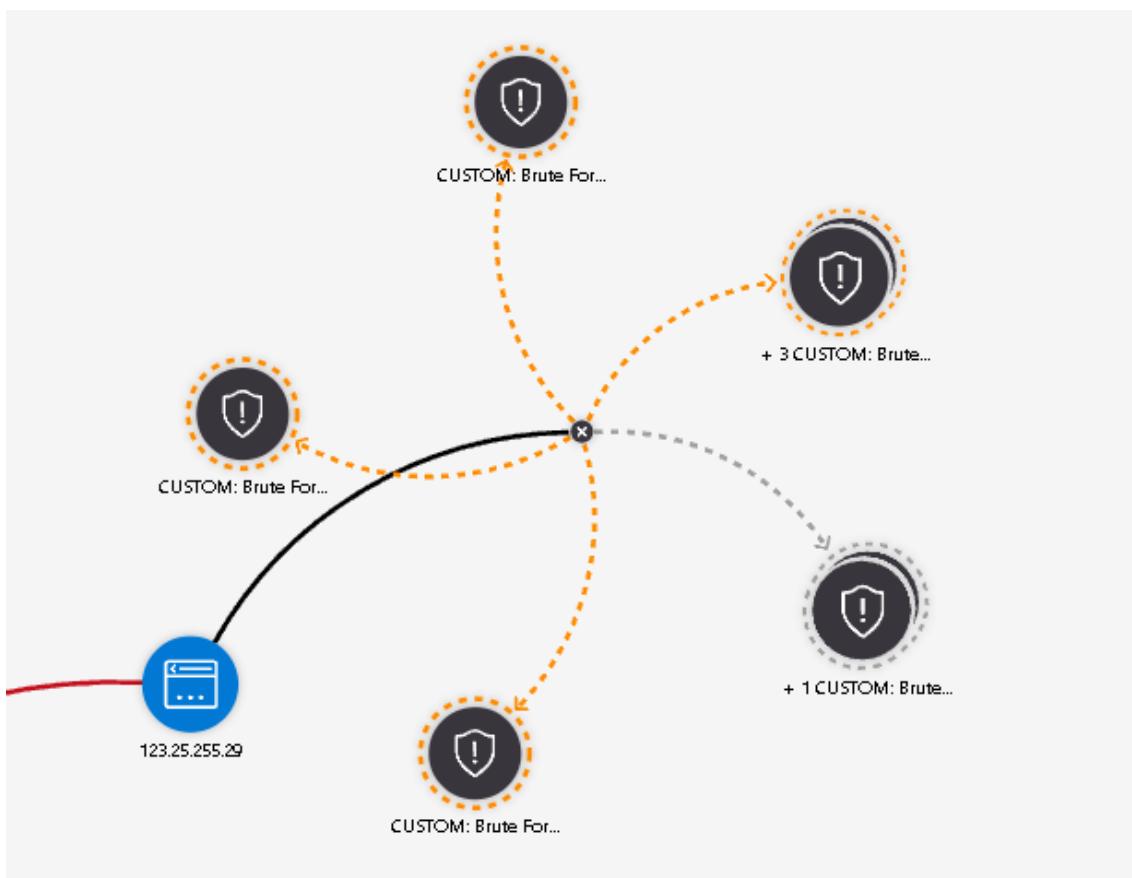
Log activity

First seen: 30/11/2023, 16:11:43 Last seen: 30/11/2023, 17:26:43

We have info that this person is from Vietnam.

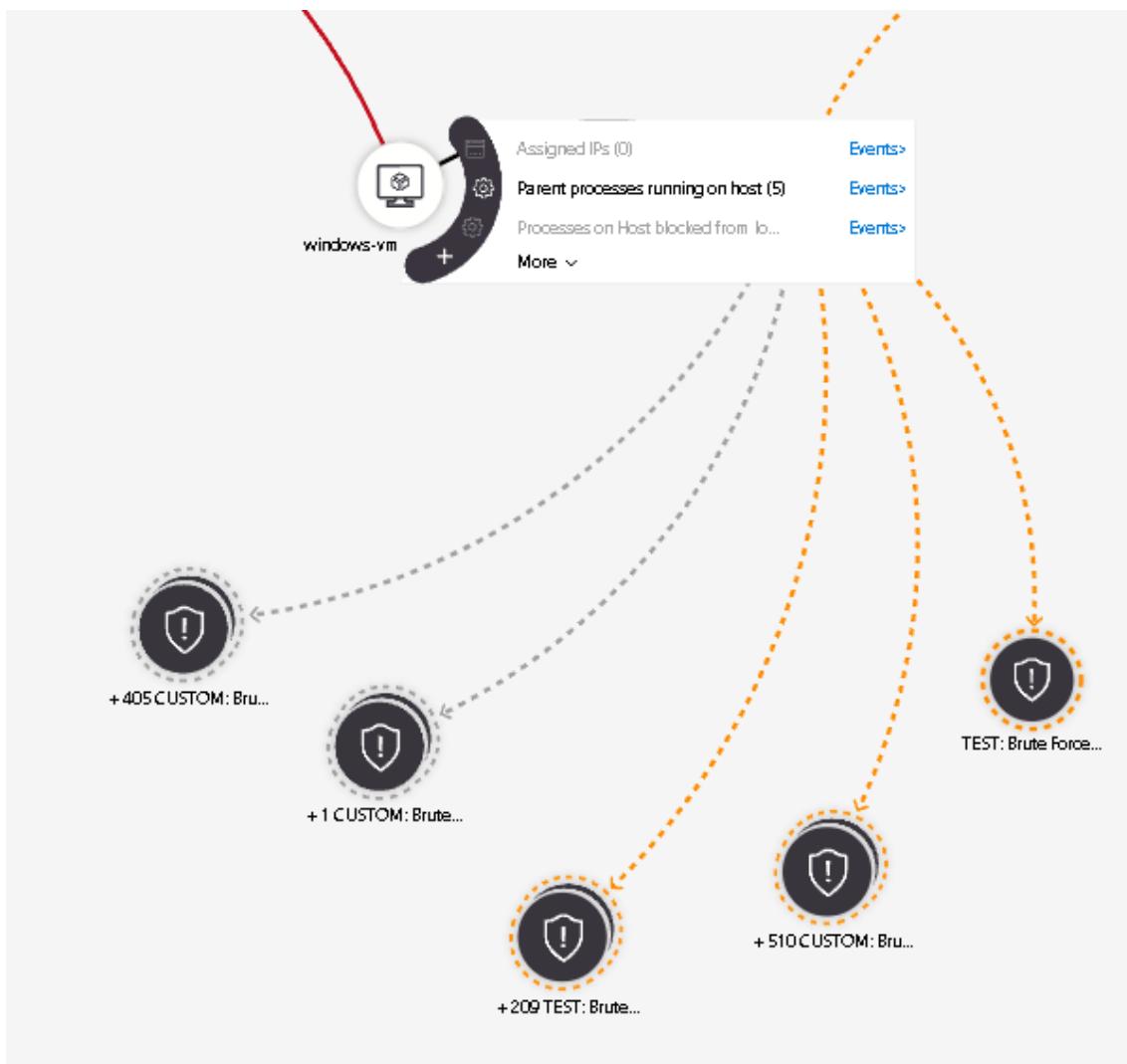


We can see that this attacker was not able to attack other hosts.



There are other events associated with this same attacker though, brute force attempts...

Potentially compromised system "windows-vm" involved in several other incidents/alerts.]



Seems like a true positive as the KQL query is very specific.

This KQL (Kusto Query Language) query is designed to identify potential brute force attack attempts on Windows systems, specifically by detecting multiple failed logon attempts followed by a successful logon within a certain time frame. The query is divided into several parts:

- Failed Logons**: This section of the query filters `SecurityEvent` logs for failed logon events (EventID 4625) with LogonType 3, which indicates network logon attempts. It only considers events generated in the last hour ('ago(1h)'). It then summarizes these events, counting the number of failures ('FailureCount') by the attacker's IP address ('AttackerIP'), along with other details like EventID, Activity, LogonType, and the destination host name ('DestinationHostName'). It filters for instances where there have been five or more failed attempts from the same IP.
- Successful Logons**: Similar to the first part, this section filters for successful logon events (EventID 4624) with LogonType 3, also within the last hour. It summarizes these events by counting the successful attempts ('SuccessfulCount') by the IP address, LogonType,

destination host name, and the time of successful authentication ('AuthenticationSuccessTime').

3. **Joining and Projecting Data**: The final part joins the two datasets ('SuccessfulLogons' and 'FailedLogons') using an inner join on shared columns ('DestinationHostName', 'AttackerIP', 'LogonType'). This means it only includes records that have matching values in both datasets for these columns. The 'project' statement then specifies which columns to include in the final output: the time of successful authentication, the attacker's IP address, the destination host name, the number of failed attempts, and the number of successful attempts.

The purpose of this query is to identify IP addresses that have had multiple failed logon attempts (suggesting a brute force attack) followed by a successful logon, which could indicate that the attacker eventually guessed the correct credentials. This can be a useful tool for security analysts monitoring for potential security breaches.

Though the alert was a true positive, this type of traffic should not be allowed to reach our VM in the first place, possible NSG configuration issue.

Will close out this incident but will look into NSG.

CUSTOM: Brute Force SUCCESS - Windows and Linux

Incident Description

- This incident involves observation of potential brute force attempts against a Windows VM.

Initial Response Actions

- Verify the authenticity of the alert or report.
- Immediately isolate the machine and change the password of the affected user
- Identify the origin of the attacks and determine if they are attacking or involved with anything else
- Determine how and when the attack occurred
 - Are the NSGs not being locked down? If so, check other NSGs
- Assess the potential impact of the incident.
 - What type of account was it? Permissions?

Containment and Recovery

- Lock down the NSG assigned to that VM/Subnet, either entirely, or to allow only necessary traffic
- Reset the affected user's password
- Enable MFA

Document Findings and Close out Incident

[\[Back to Top\]](#)

This is the playbook for this incident.

We will now lock down NSG.

<input type="checkbox"/> 100	DANGER_AllowAnyCustomA...	Any	Any	85.245.251.169	Any	<input checked="" type="checkbox"/> Allow	
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	<input checked="" type="checkbox"/> Allow	
<input type="checkbox"/> 65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	<input checked="" type="checkbox"/> Allow	
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any	Any	<input checked="" type="checkbox"/> Deny	

We just put so that only our IP address can access this VM.

So now this attack will not happen anymore as only we can access these VMs.

We will enable MFA later.

I will keep practicing incident response using the incident management playbook that states (reset password, enable mfa, lock down nsg, etc...)

After that I will now Enable NIST 800-53, we will lock down our environment more and more until it becomes complacent with NIST.

Microsoft Defender for Cloud | Regulatory compliance

No subscriptions are selected

Search Download report Manage compliance policies Open query Compliance over time workbook Audit reports

General

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

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Data security

Microsoft cloud security benchmark

16 of 19 passed controls

Lowest compliance regulatory standards

No additional standards are currently monitored

Open policy settings to manage additional compliance

Manage compliance policies >

Is the regulatory compliance experience clear to you? Yes No

Microsoft cloud security benchmark

Recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance

We will go to defender for cloud and enable nist 800-53 controls so we can have a checklist on how to harden out environment, security recommendations,etc...

Control Families

<u>AC</u>	ACCESS CONTROL
<u>AT</u>	AWARENESS AND TRAINING
<u>AU</u>	AUDIT AND ACCOUNTABILITY
<u>CA</u>	ASSESSMENT, AUTHORIZATION, AND MONITORING
<u>CM</u>	CONFIGURATION MANAGEMENT
<u>CP</u>	CONTINGENCY PLANNING
<u>IA</u>	IDENTIFICATION AND AUTHENTICATION
<u>IR</u>	INCIDENT RESPONSE
<u>MA</u>	MAINTENANCE
<u>MP</u>	MEDIA PROTECTION
<u>PE</u>	PHYSICAL AND ENVIRONMENTAL PROTECTION
<u>PL</u>	PLANNING
<u>PM</u>	PROGRAM MANAGEMENT
<u>PS</u>	PERSONNEL SECURITY
<u>PT</u>	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY
<u>RA</u>	RISK ASSESSMENT
<u>SA</u>	SYSTEM AND SERVICES ACQUISITION

Nist 800-53 family controls.



We just added revision 5!

Now that nist 800-53 family controls are enabled, we can go ahead and look at this:

Recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance. You must evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are subject to change and are provided "as is". See the [licensing terms](#).

[NIST SP 800 53 R5 is applied to the subscription Azure subscription 1](#)

Expand all compliance controls

✓ ✗ AC. Access Control

✓ ✓ AT. Awareness and Training

✗ ✗ AU. Audit and Accountability

✓ ✓ CA. Assessment, Authorization, and Monitoring

✓ ✓ CM. Configuration Management

✗ ✗ CP. Contingency Planning

✗ ✗ IA. Identification and Authentication

✗ ✗ IR. Incident Response

✓ ✓ MA. Maintenance

The screenshot shows the Microsoft Defender for Cloud dashboard with the NIST SP 800-53 R5 compliance report for 'Azure subscription 1'. The left sidebar lists 'Control Families' with red arrows pointing to their respective sections in the main content area. The main content area displays the 14 NIST categories with their status (e.g., ✗ for AT, ✗ for CA, ✗ for MA).

Control Family	NIST Category Status
AC	✗ ✗ AC. Access Control
AT	✓ ✓ AT. Awareness and Training
AU	✗ ✗ AU. Audit and Accountability
CA	✓ ✓ CA. Assessment, Authorization, and Monitoring
CM	✓ ✓ CM. Configuration Management
CP	✗ ✗ CP. Contingency Planning
IA	✗ ✗ IA. Identification and Authentication
IR	✗ ✗ IR. Incident Response
MA	✓ ✓ MA. Maintenance
MP	✗ ✗ MP. Media Protection
PE	✓ ✓ PE. Physical and Environmental Protection
PL	✓ ✓ PL. Planning
PM	✓ ✗ PS. Personnel Security

And we can see it does indeed match.

We will implement NIST 800-53: SC-7: BOUNDARY PROTECTION

Automated assessments			
	Resource type	Failed resources	Resource compliance status
Adaptive network hardening recommendations should be applied on internet facing virtual machines	Quick Virtual machines	2 of 2	<div style="width: 100%; background-color: red;"></div>
Subnets should be associated with a network security group	Subnets	2 of 2	<div style="width: 100%; background-color: red;"></div>
Azure Key Vaults should use private link	Key vaults	1 of 1	<div style="width: 100%; background-color: red;"></div>
Virtual networks should be protected by Azure Firewall	Virtual networks	1 of 1	<div style="width: 100%; background-color: red;"></div>
Storage account should use a private link connection	Storage accounts	1 of 1	<div style="width: 100%; background-color: red;"></div>

We will start first by configuring a private link and firewall for our key vault.

This is what we must do.

Next to that tab we will also create our private endpoint:

Create a private endpoint

Basics **Resource** **Virtual Network** **DNS** **Tags** **Review + create**

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription *	<input type="text" value="Azure subscription 1"/>
Resource group *	<input type="text" value="RG-Cyber-Lab"/> Create new

Instance details

Name *	<input type="text" value="PE-AKV"/> ✓
Network Interface Name *	<input type="text" value="PE-AKV-nic"/> ✓
Region *	<input type="text" value="East US 2"/> ✓

Basics **Resource** **Virtual Network** **DNS** **Tags** **Review + create**

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Connection method Connect to an Azure resource in my directory.
 Connect to an Azure resource by resource ID or alias.

Subscription *	<input type="text" value="Azure subscription 1"/>
Resource type *	<input type="text" value="Microsoft.KeyVault/vaults"/>
Resource *	<input type="text" value="akv-cyber-lab-995"/>
Target sub-resource *	<input type="text" value="vault"/>

Rest is left at default.

We will now do the same for our storage accounts.

The screenshot shows the 'Networking' settings for a storage account. The 'Public network access' section has a radio button labeled 'Disabled' selected, indicated by a red box. The 'Network Routing' section shows 'Microsoft network routing' selected. Other options like 'Internet routing' and 'Publish route-specific endpoints' are available but not selected.

Create a private endpoint ...

✓ Basics 2 Resource 3 Virtual Network 4 DNS 5 Tags 6 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription	Azure subscription 1 (842840fc-2cf5-4184-a918-39163fadddbc)
Resource type	Microsoft.Storage/storageAccounts
Resource	sacyberlab088
Target sub-resource *	<input type="text" value="blob"/>

The rest is just like the previous one, but we want to make sure blob is selected here since we are creating our private endpoint for a blob storage account.

Next, we will attach the network security group to the subnet.

Create network security group

Basics Tags Review + create

Project details

Subscription * Azure subscription 1

Resource group * RG-Cyber-Lab

Create new

Instance details

Name * NSG-SUBNET

Region * East US 2

Now that the nsg is created we will attach it to our subnet. This is mostly to satisfy the recommendation that defender for cloud gives us since we won't have any rules in this nsg. Our lab machines are already secure so there is really no point in adding the same rules again here. We are doing this to practice.

The screenshot shows the Azure portal interface for creating a Network Security Group (NSG). On the left, the navigation menu is visible with options like Overview, Activity log, Tags, Diagnose and solve problems, Settings, Address space, Connected devices, Subnets, Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, Network manager, DNS servers, Peering, Service endpoints, and Private endpoints. The 'Subnets' option under 'Settings' is selected. In the main pane, the 'Lab-Vnet | Subnets' section is shown. A table lists a single subnet named 'default' with the IP range 10.0.0.0/24. To the right, the 'default' subnet configuration page is displayed. The 'Network security group' field is highlighted with a red box and contains the value 'NSG-SUBNET'. Other fields include 'Name' (default), 'Subnet address range' (10.0.0.0/24), 'Available IPs' (247), 'Delegated to' (empty), 'Add IPv6 address space' (unchecked), 'NAT gateway' (None), 'Route table' (None), 'SERVICE ENDPOINTS' (Create service endpoint policies to allow traffic to specific Azure resources from your virtual machine over service endpoints. Learn more), 'Services' (0 selected), and 'SUBNET DELEGATION' (Delegate subnet to a service. None).

Now that these nist 800-53 controls are in place we will again run our environment for 24 hours and see if there is any difference in the number of attacks compared to before.

I am back after roughly 24 hours and now we will look at the results!

	B	C	D
BEFORE SECURING ENVIRONMENT			
Start Time		12/4/2023, 5:03:24 PM	
Stop Time		12/5/2023, 5:03:24 PM	
Security Events (Windows VMs)		87394	
Syslog (Linux VMs)		5221	
SecurityAlert (Microsoft Defender for Cloud)		5	
SecurityIncident (Sentinel Incidents)		384	
NSG Inbound Malicious Flows Allowed		3423	
AFTER SECURING ENVIRONMENT			
Start Time		12/21/2023, 5:21:59 PM	
Stop Time		12/22/2023, 5:21:59 PM	
Security Events (Windows VMs)			
Syslog (Linux VMs)			
SecurityAlert (Microsoft Defender for Cloud)			
SecurityIncident (Sentinel Incidents)			
NSG Inbound Malicious Flows Allowed			

These are the before numbers and now let's get the after.

We will use these queries to get the information we want:

Security Events (Windows VMs)	SecurityEvent where TimeGenerated >= ago(24h) count		
Syslog (Linux VMs)	Syslog where TimeGenerated >= ago(24h) count		
SecurityAlert (Microsoft Defender for Cloud)	SecurityAlert where DisplayName !startswith "CUSTOM" and DisplayName !startswith "TEST" where TimeGenerated >= ago(24h) count		
Security Incident (Sentinel Incidents)	SecurityIncident where TimeGenerated >= ago(24h) count		
NSG Inbound Malicious Flows Allowed	AzureNetworkAnalytics_CL where FlowType_s == "MaliciousFlow" and AllowedInFlows_d > 0 where TimeGenerated >= ago(24h) count		
NSG Inbound Malicious Flows Blocked	AzureNetworkAnalytics_CL where FlowType_s == "MaliciousFlow" and DeniedInFlows_d > 0 where TimeGenerated >= ago(24h) count		

```

1 Syslog
2 | where TimeGenerated >= ago(24h)
3 | count
4

```

Results Chart

Count

> 1

Let's keep going here is what we have so far:

BEFORE SECURING ENVIRONMENT

Start Time	12/4/2023, 5:03:24 PM
Stop Time	12/5/2023, 5:03:24 PM
Security Events (Windows VMs)	87394
Syslog (Linux VMs)	5221
SecurityAlert (Microsoft Defender for Cloud)	5
SecurityIncident (Sentinel Incidents)	384
NSG Inbound Malicious Flows Allowed	3423

AFTER SECURING ENVIRONMENT

Start Time	12/21/2023, 5:21:59 PM
Stop Time	12/22/2023, 5:21:59 PM
Security Events (Windows VMs)	11288
Syslog (Linux VMs)	1
SecurityAlert (Microsoft Defender for Cloud)	
SecurityIncident (Sentinel Incidents)	
NSG Inbound Malicious Flows Allowed	

RESULTS (will auto update, do not edit formulas)

	Change after security environment
Security Events (Windows VMs)	-87.08%
Syslog (Linux VMs)	-99.98%
SecurityAlert (Microsoft Defender for Cloud)	-100.00%
Security Incident (Sentinel Incidents)	-100.00%
NSG Inbound Malicious Flows Allowed	-100.00%

```

1 SecurityIncident
2 | where TimeGenerated >= ago(24h)
3 | count

```

Results Chart

Count

> 0

We can see a HUGE difference already...

And here is the result:

BEFORE SECURING ENVIRONMENT	
Start Time	12/4/2023, 5:03:24 PM
Stop Time	12/5/2023, 5:03:24 PM
Security Events (Windows VMs)	87394
Syslog (Linux VMs)	5221
SecurityAlert (Microsoft Defender for Cloud)	5
SecurityIncident (Sentinel Incidents)	384
NSG Inbound Malicious Flows Allowed	3423
AFTER SECURING ENVIRONMENT	
Start Time	12/21/2023, 5:21:59 PM
Stop Time	12/22/2023, 5:21:59 PM
Security Events (Windows VMs)	11288
Syslog (Linux VMs)	1
SecurityAlert (Microsoft Defender for Cloud)	0
SecurityIncident (Sentinel Incidents)	0
NSG Inbound Malicious Flows Allowed	0

RESULTS (will auto update, do not edit formulas)

	Change after security environment
Security Events (Windows VMs)	-87.08%
Syslog (Linux VMs)	-99.98%
SecurityAlert (Microsoft Defender for Cloud)	-100.00%
Security Incident (Sentinel Incidents)	-100.00%
NSG Inbound Malicious Flows Allowed	-100.00%

End.