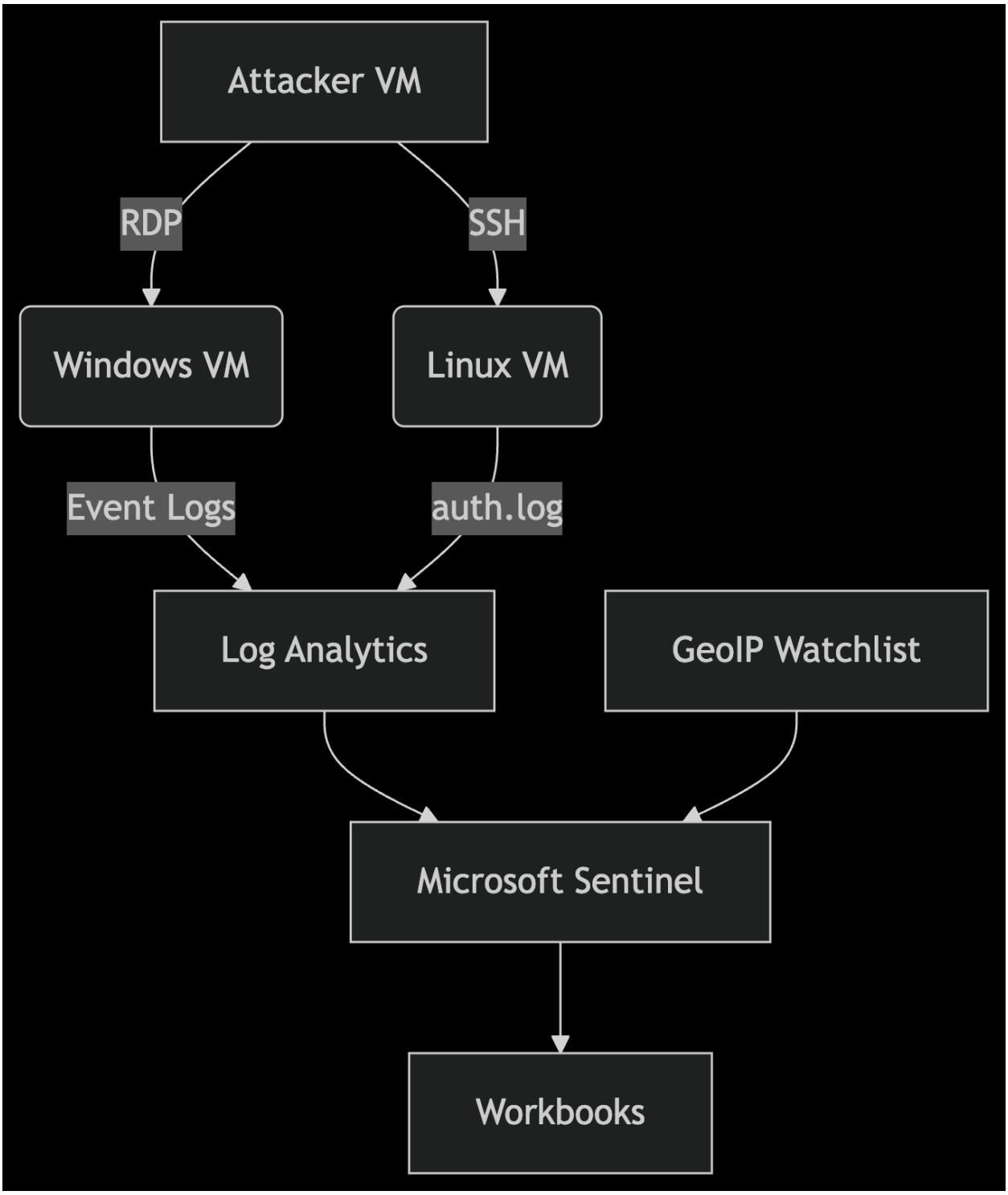
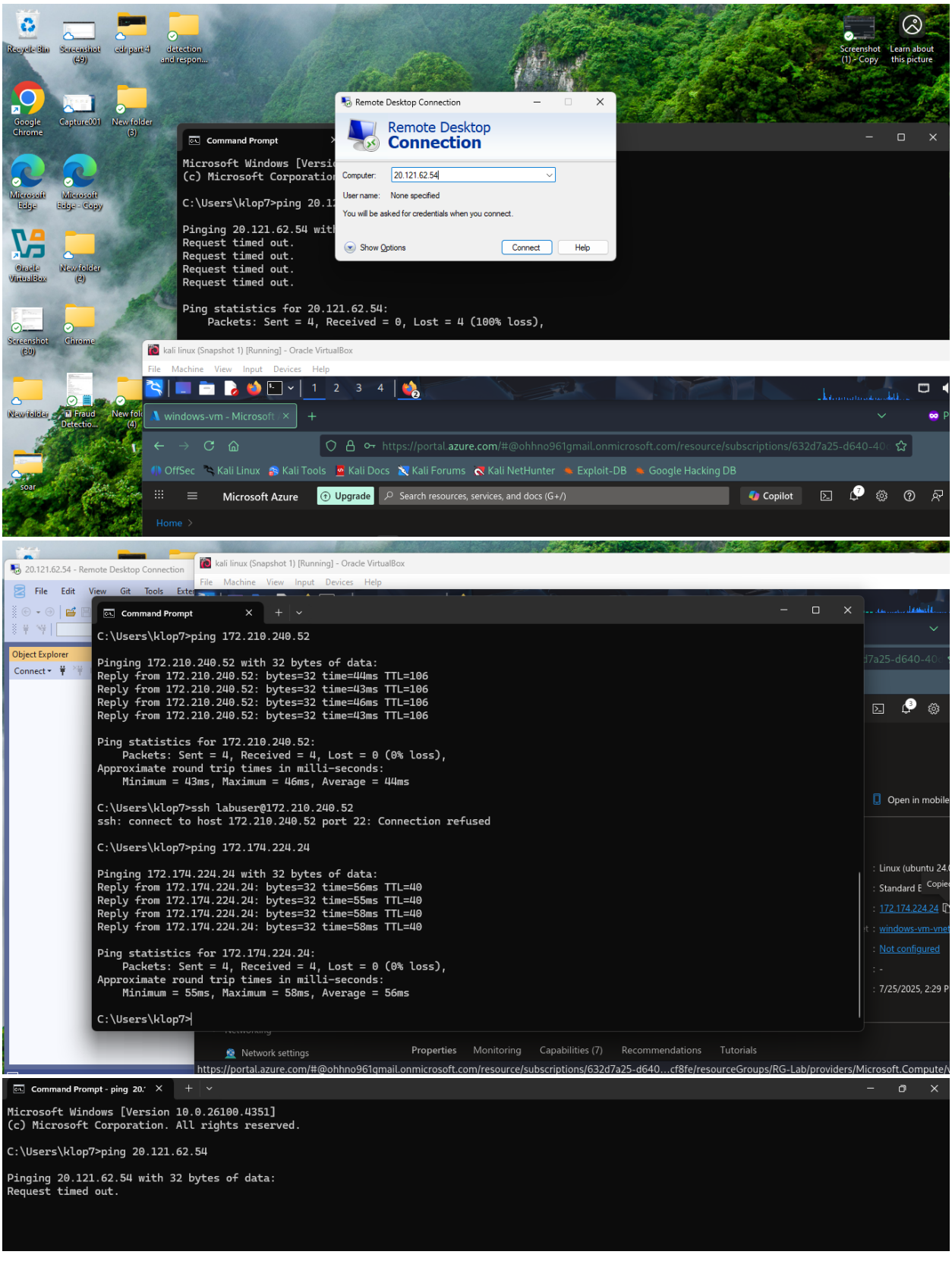
Azure Honeypot Project (In Progress): Attempted Threat Simulation & Microsoft Sentinel Integration

Goal: Deploy and simulate a honeypot environment in Azure using three virtual machines (Windows, Linux, Kali), then ingest and analyze attack data via Microsoft Sentinel.



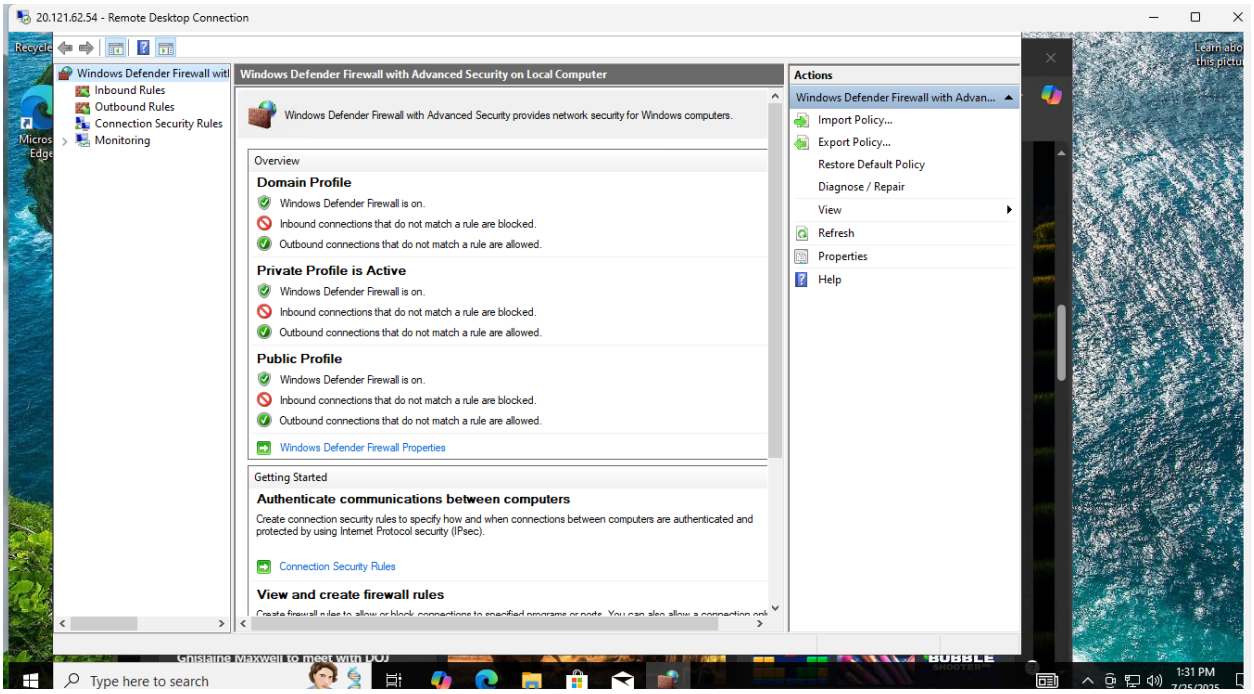
1. Initial VM Deployment and Network Configuration

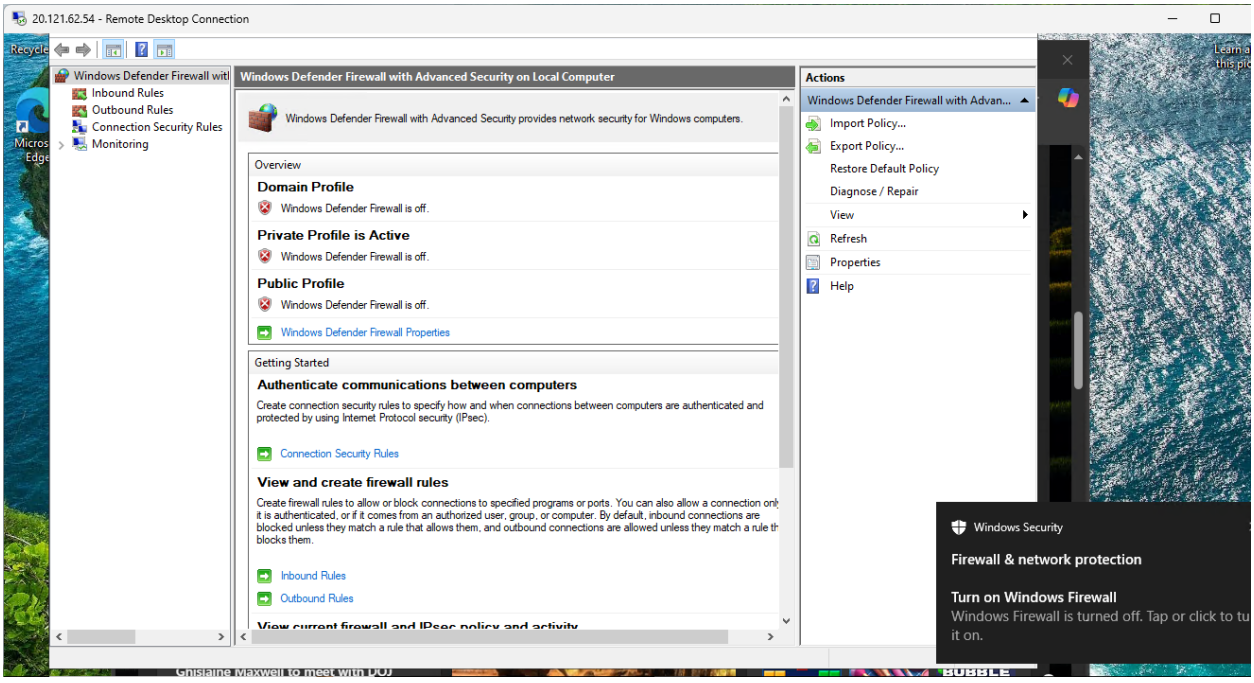
- **Created VMs on Microsoft Azure**:
  - **Windows VM** (IP: `20.121.62.54`)
  - **Linux VM (Ubuntu)** (IP: `172.174.224.24`)
  - **Attacker VM**: Initially `Kali-Lab-001` (IP: `172.210.240.52`), later recreated as `attacker-vm` (IP: `48.217.80.146`)
- Used **Remote Desktop Connection** (RDP) and SSH to connect to each VM from my host machine.
- Tested connectivity using `ping` but initially received timeouts. Fixed the issue by **disabling Windows Defender Firewall** (Domain, Private, and Public profiles) across all VMs.



2. Simulating Vulnerabilities

- **Disabled all firewall protections** to intentionally expose the VMs to the internet.
- Set **Network Security Group (NSG)** inbound rules to `Allow Any` for source/destination/port for all VMs.

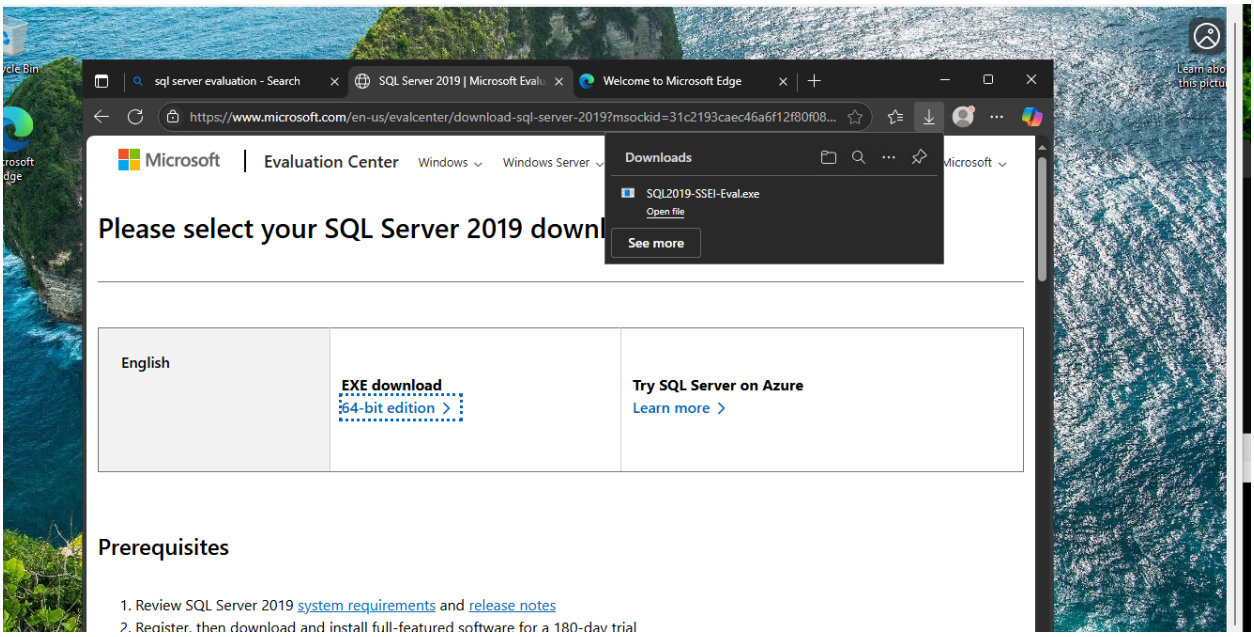


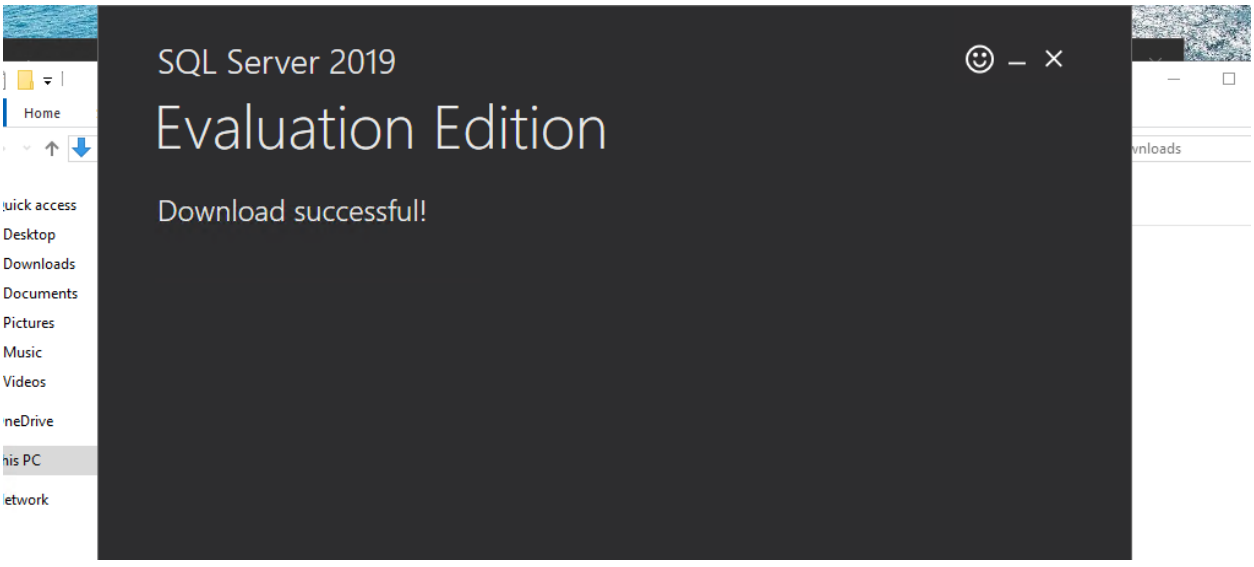


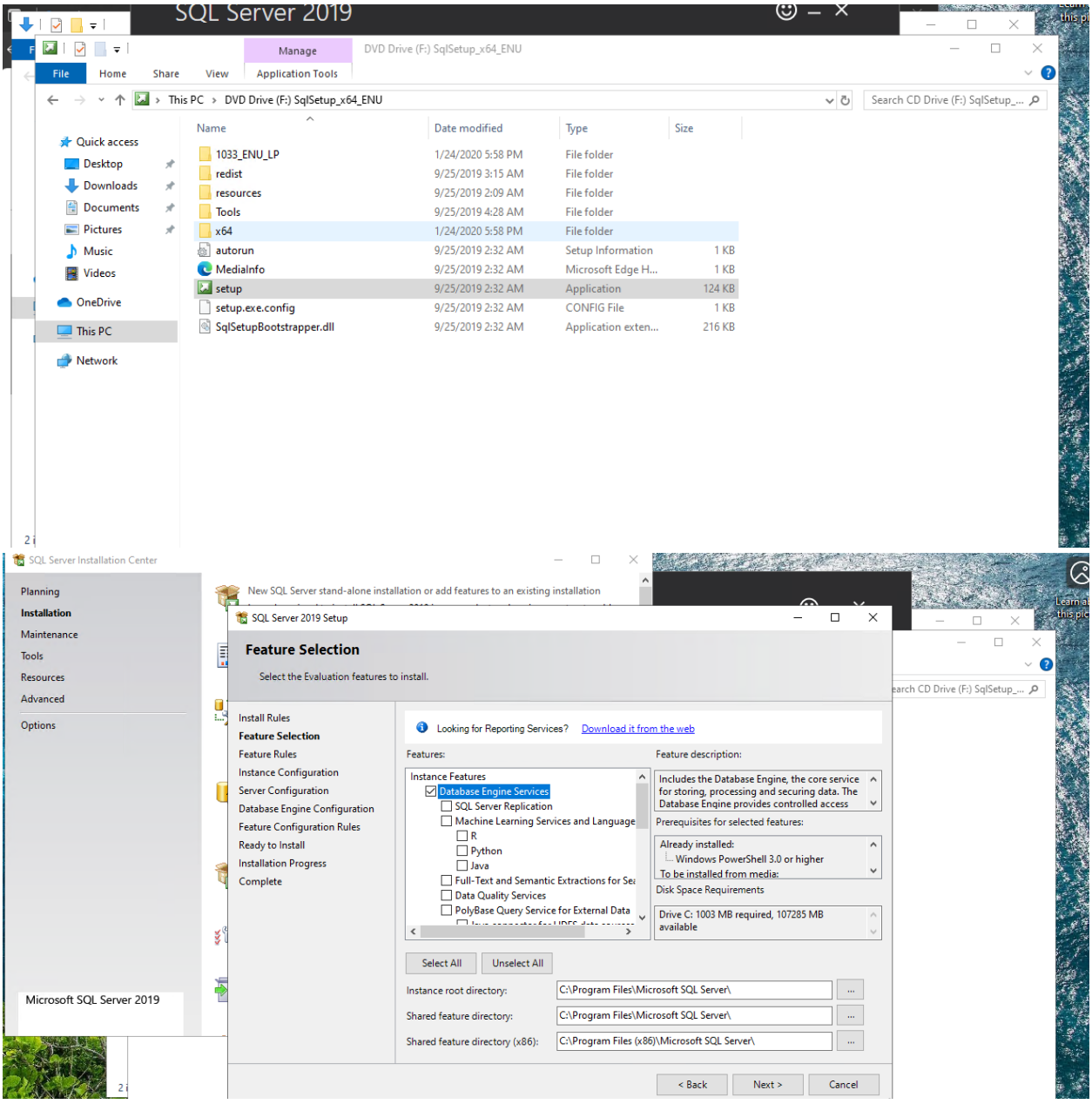
3. SQL Server Installation and Auditing on Windows VM

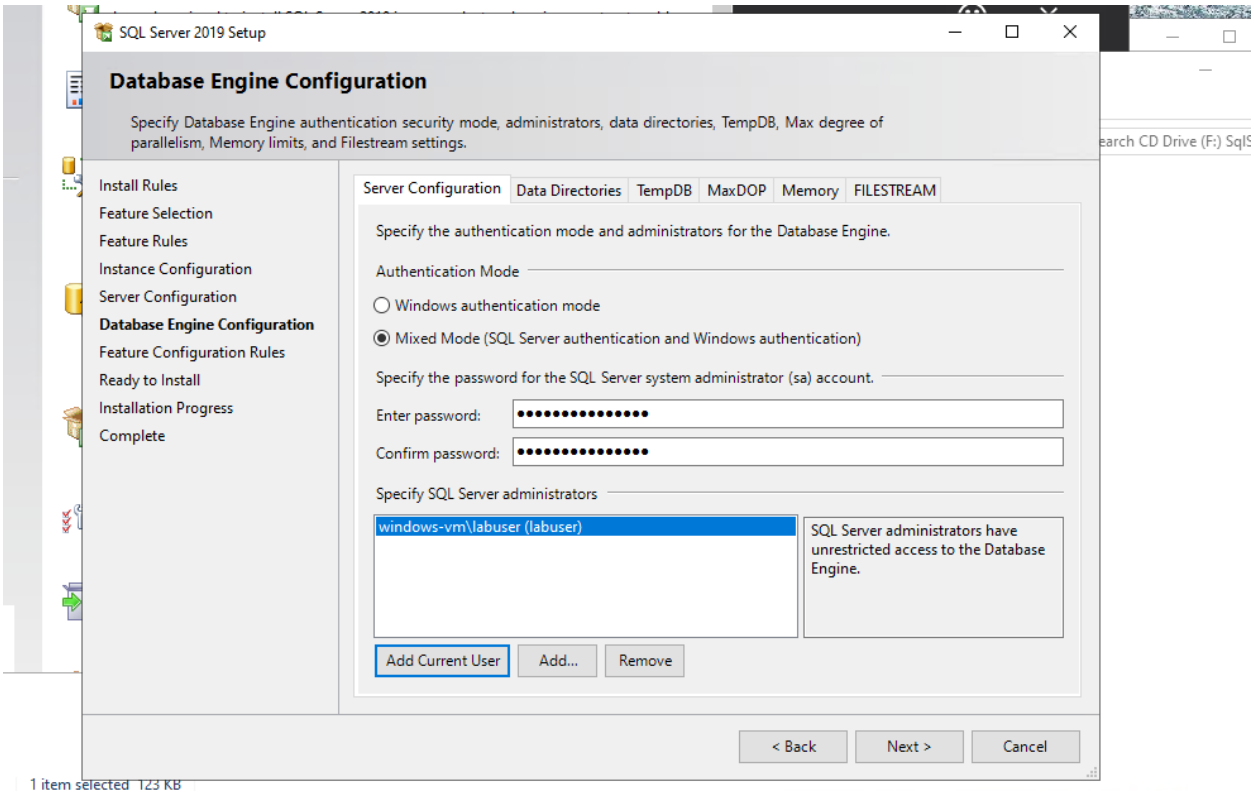
- Installed **SQL Server 2019 (64-bit)** and configured it in **Mixed Mode Authentication**.
- Enabled **Database Engine Services** and set up an `sa` password.

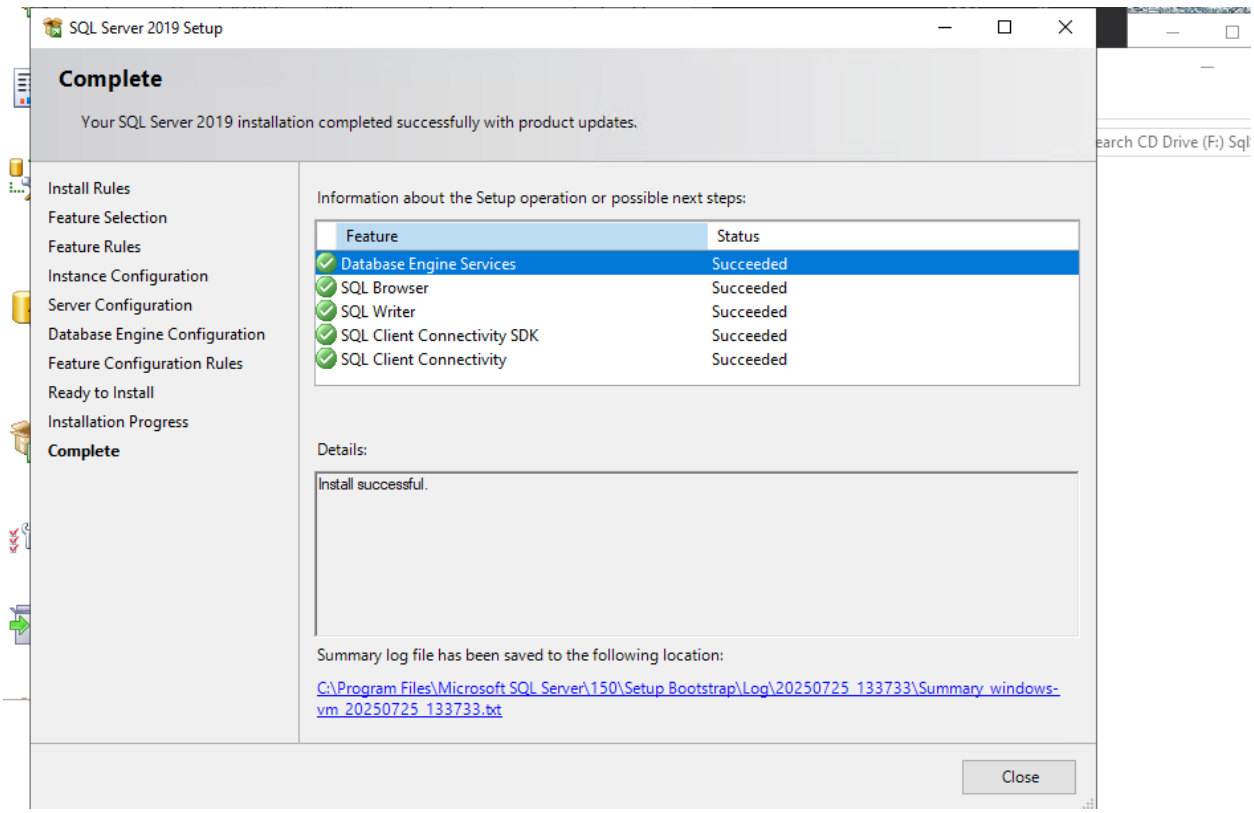
- Installed **SQL Server Management Studio (SSMS v21)**.
- Followed Microsoft Learn guides to:
  - Grant full registry permissions to `NETWORK SERVICE` under `HKEY_LOCAL_MACHINE\SECURITY`.
  - Enable **audit object access** via command:
  - `auditpol /set /subcategory:"Audit Object Access" /success:enable /failure:enable`
- Verified failed login events by intentionally inputting incorrect SQL credentials; logs appeared in Event Viewer under `Windows Logs > Application`.

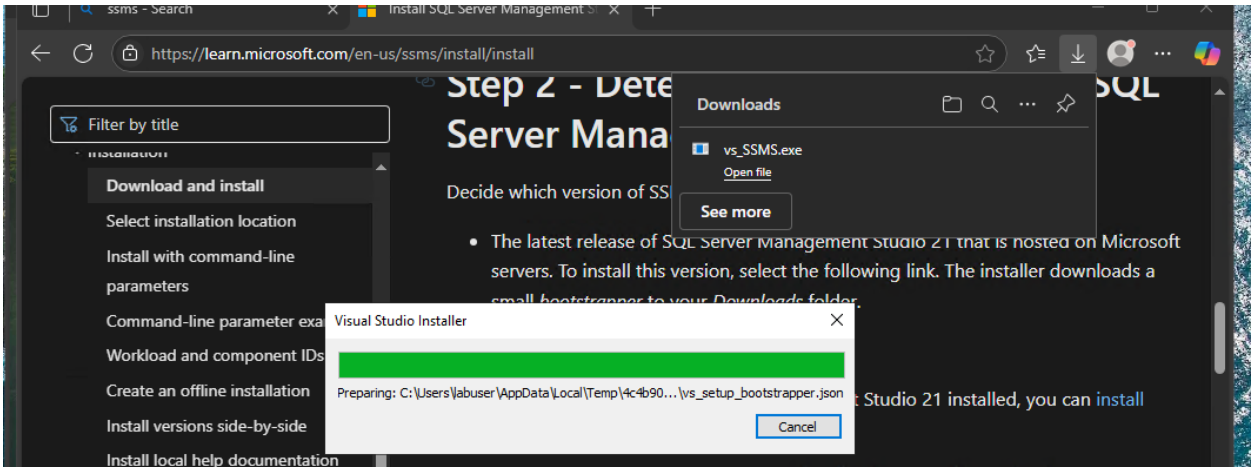





SQL Server 2019
Manage
DVD Drive (F:) SqlSetup_x64_ENU
File
Home
Share
View
Application Tools
This PC › DVD Drive (F:) SqlSetup_x64_ENU
Search CD Drive (F:) SqlSetup_...
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
1033_ENU_LP 1/24/2020 5:58 PM File folder
redist 9/25/2019 3:15 AM File folder
resources 9/25/2019 2:09 AM File folder
Tools 9/25/2019 4:28 AM File folder
x64 1/24/2020 5:58 PM File folder
autorun 9/25/2019 2:32 AM Setup Information 1 KB
MediaInfo 9/25/2019 2:32 AM Microsoft Edge H... 1 KB
setup 9/25/2019 2:32 AM Application 124 KB
setup.exe.config 9/25/2019 2:32 AM CONFIG File 1 KB
SqlSetupBootstrapper.dll 9/25/2019 2:32 AM Application exten... 216 KB
SQL Server Installation Center
Planning
Installation
Maintenance
Tools
Resources
Advanced
Options
New SQL Server stand-alone installation or add features to an existing installation
Microsoft SQL Server 2019
SQL Server 2019 Setup
Feature Selection
Select the Evaluation features to install.
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Looking for Reporting Services?
Download it from the web
Features:
Feature description:
Instance Features
Database Engine Services
SQL Server Replication
Machine Learning Services and Language
R
Python
Java
Full-Text and Semantic Extractions for Sea
Data Quality Services
PolyBase Query Service for External Data
Includes the Database Engine, the core service for storing, processing and securing data. The Database Engine provides controlled access
Prerequisites for selected features:
Already installed:
Windows PowerShell 3.0 or higher
To be installed from media:
Disk Space Requirements
Drive C: 1003 MB required, 107285 MB available
Select All
Unselect All
Instance root directory:
C:\Program Files\Microsoft SQL Server\
Shared feature directory:
C:\Program Files\Microsoft SQL Server\
Shared feature directory (x86):
C:\Program Files (x86)\Microsoft SQL Server\
< Back
Next >
Cancel


SQL Server 2019 Setup
Database Engine Configuration
Specify Database Engine authentication security mode, administrators, data directories, TempDB, Max degree of parallelism, Memory limits, and Filestream settings.
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Server Configuration
Data Directories
TempDB
MaxDOP
Memory
FILESTREAM
Specify the authentication mode and administrators for the Database Engine.
Authentication Mode
Windows authentication mode
Mixed Mode (SQL Server authentication and Windows authentication)
Specify the password for the SQL Server system administrator (sa) account.
Enter password:
Confirm password:
Specify SQL Server administrators
windows-vm\labuser (labuser)
SQL Server administrators have unrestricted access to the Database Engine.
Add Current User
Add...
Remove
< Back
Next >
Cancel


SQL Server 2019 Setup
Complete
Your SQL Server 2019 installation completed successfully with product updates.
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Information about the Setup operation or possible next steps:
Feature
Status
Database Engine Services
Succeeded
SQL Browser
Succeeded
SQL Writer
Succeeded
SQL Client Connectivity SDK
Succeeded
SQL Client Connectivity
Succeeded
Details:
Install successful.
Summary log file has been saved to the following location:
C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20250725_133733\Summary_windows-vm_20250725_133733.txt
Close



Visual Studio Installer

Installed Available

All installations are up to date.

SQL Server Management Studio 21

21.4.8

An integrated environment for managing any SQL infrastructure, from SQL Server to Azure SQL

Release notes

Modify

Launch

Done installing

The installation has completed successfully. We recommend restarting Windows to clean up any remaining files.

OK

Develo

Fresh Lear for VS Sub

We've bee

Tuesday, J

Better Mo GPT-4.1, a

We're excit

Wednesda

Inside Acc Week of D

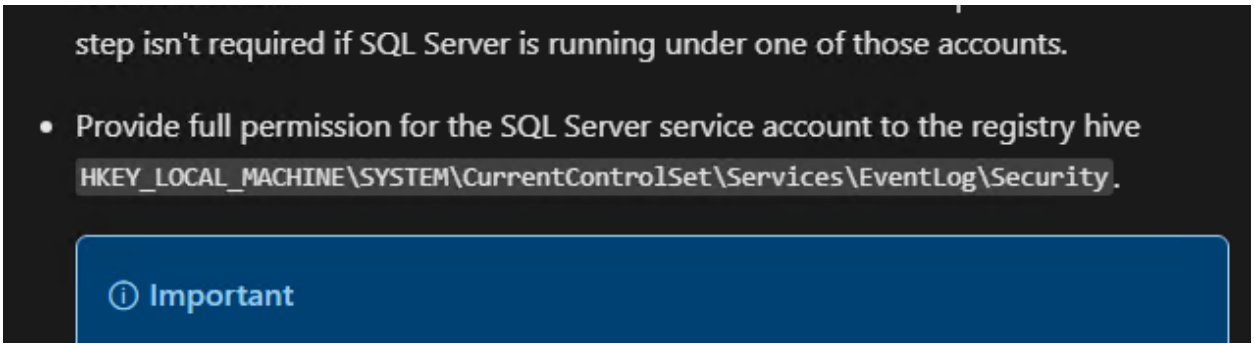
A long tim

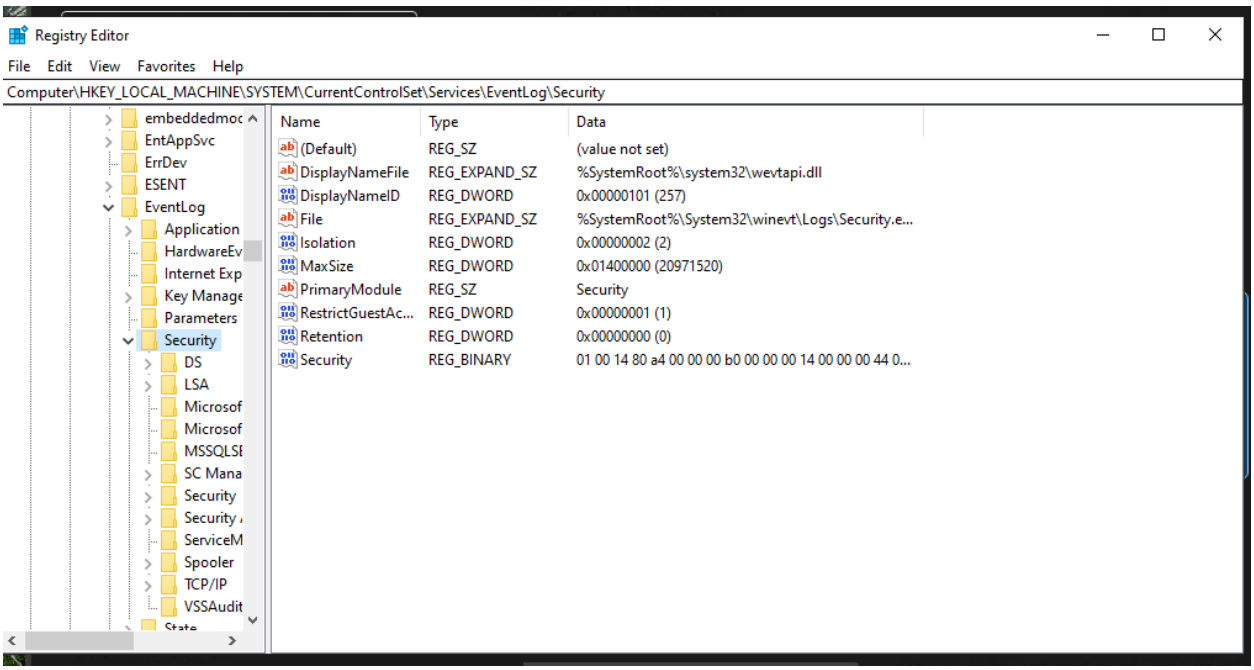
Monday, J

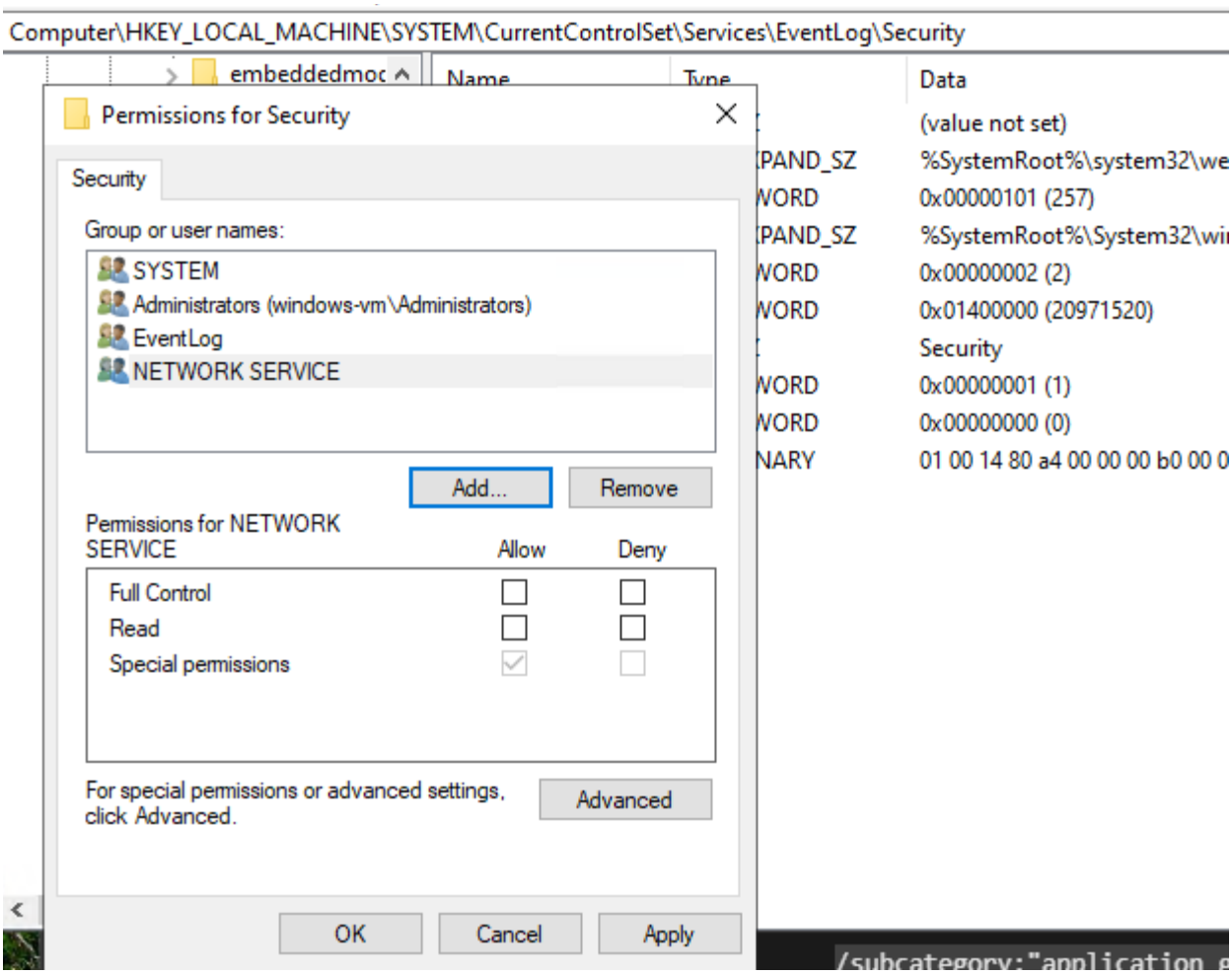
View more

Need hel Commun Support.


Microsoft Ignite
November 17–21, 2025
Register now
Learn
Discover
Product documentation
Development languages
Topics
Sign in
SQL
Overview
Install
Secure
Develop
Administer
Analyze
More
Azure Portal
Download SQL Server
Version
SQL Server 2025 Preview
Filter by title
Write audit events to Windows log
Ledger
Networking
Concepts
Download PDF
Learn / SQL / SQL Server /
Ask Learn
Write SQL Server Audit events to the Security log
03/24/2023
In this article
Limitations and restrictions
Permissions


step isn't required if SQL Server is running under one of those accounts.
• Provide full permission for the SQL Server service account to the registry hive HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security.
Important


Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security
embeddedmoc
EntAppSvc
ErrDev
ESENT
EventLog
Application
HardwareEv
Internet Exp
Key Manage
Parameters
Security
DS
LSA
Microsof
Microsof
MSSQLSE
SC Mana
Security
Security
ServiceM
Spooler
TCP/IP
VSSAudit
Name
Type
Data
(Default) REG_SZ (value not set)
DisplayNameFile REG_EXPAND_SZ %SystemRoot%\system32\wevtapi.dll
DisplayNameID REG_DWORD 0x00000101 (257)
File REG_EXPAND_SZ %SystemRoot%\System32\winevt\Logs\Security.e...
Isolation REG_DWORD 0x00000002 (2)
MaxSize REG_DWORD 0x01400000 (20971520)
PrimaryModule REG_SZ Security
RestrictGuestAc... REG_DWORD 0x00000001 (1)
Retention REG_DWORD 0x00000000 (0)
Security REG_BINARY 01 00 14 80 a4 00 00 00 b0 00 00 00 14 00 00 00 44 0...


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security
embeddedmod
Name
Type
Data
(value not set)
%SystemRoot%\system32\we
0x00000101 (257)
%SystemRoot%\System32\wi
0x00000002 (2)
0x01400000 (20971520)
Security
0x00000001 (1)
0x00000000 (0)
01 00 14 80 a4 00 00 00 b0 00 0
Permissions for Security
Security
Group or user names:
SYSTEM
Administrators (windows-vm\Administrators)
EventLog
NETWORK SERVICE
Add...
Remove
Permissions for NETWORK SERVICE
Allow
Deny
Full Control
Read
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

Configure the audit object access setting in Windows using `auditpol`

1. Open a command prompt with administrative permissions.

   a. From the **Start** menu, navigate to **Command Prompt**, and then select **Run as administrator**.

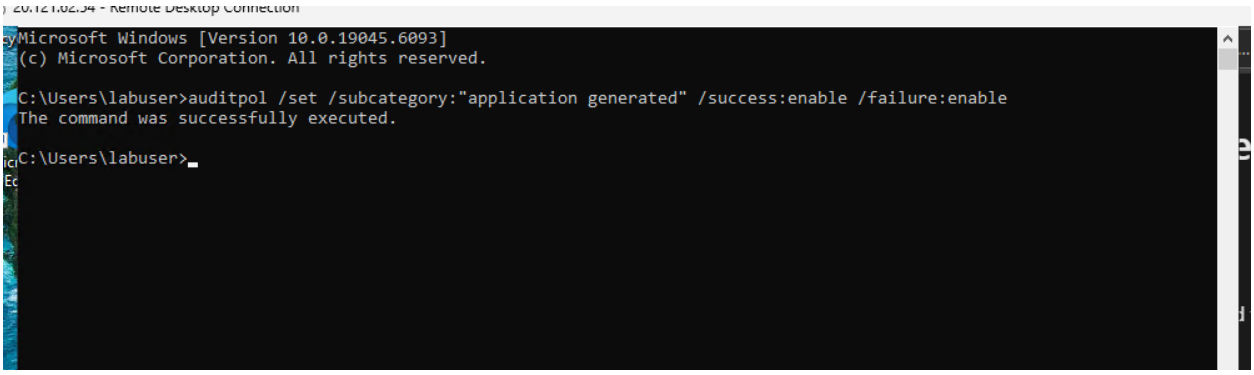
   b. If the **User Account Control** dialog box opens, select **Continue**.

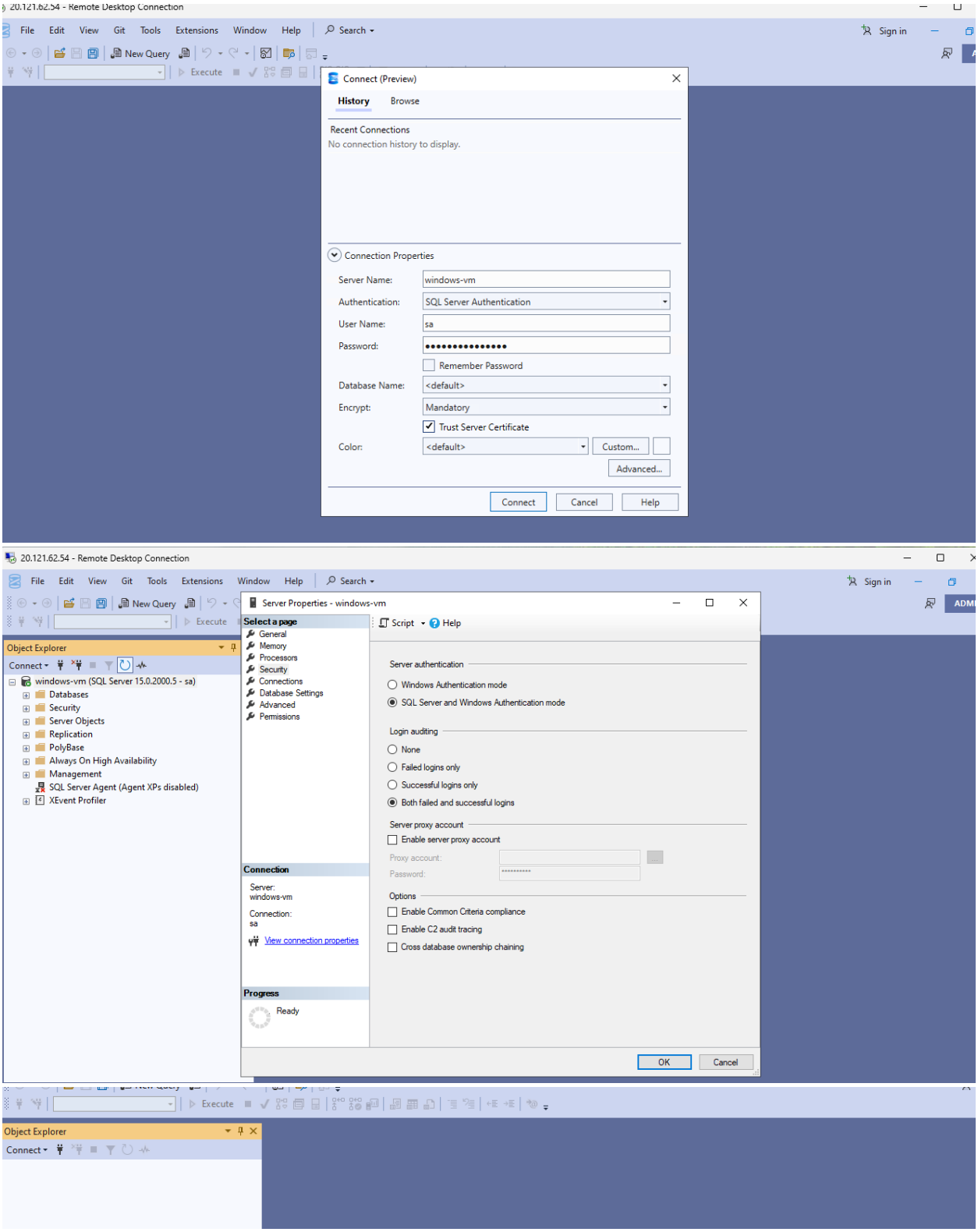
2. Execute the following statement to enable auditing from SQL Server.

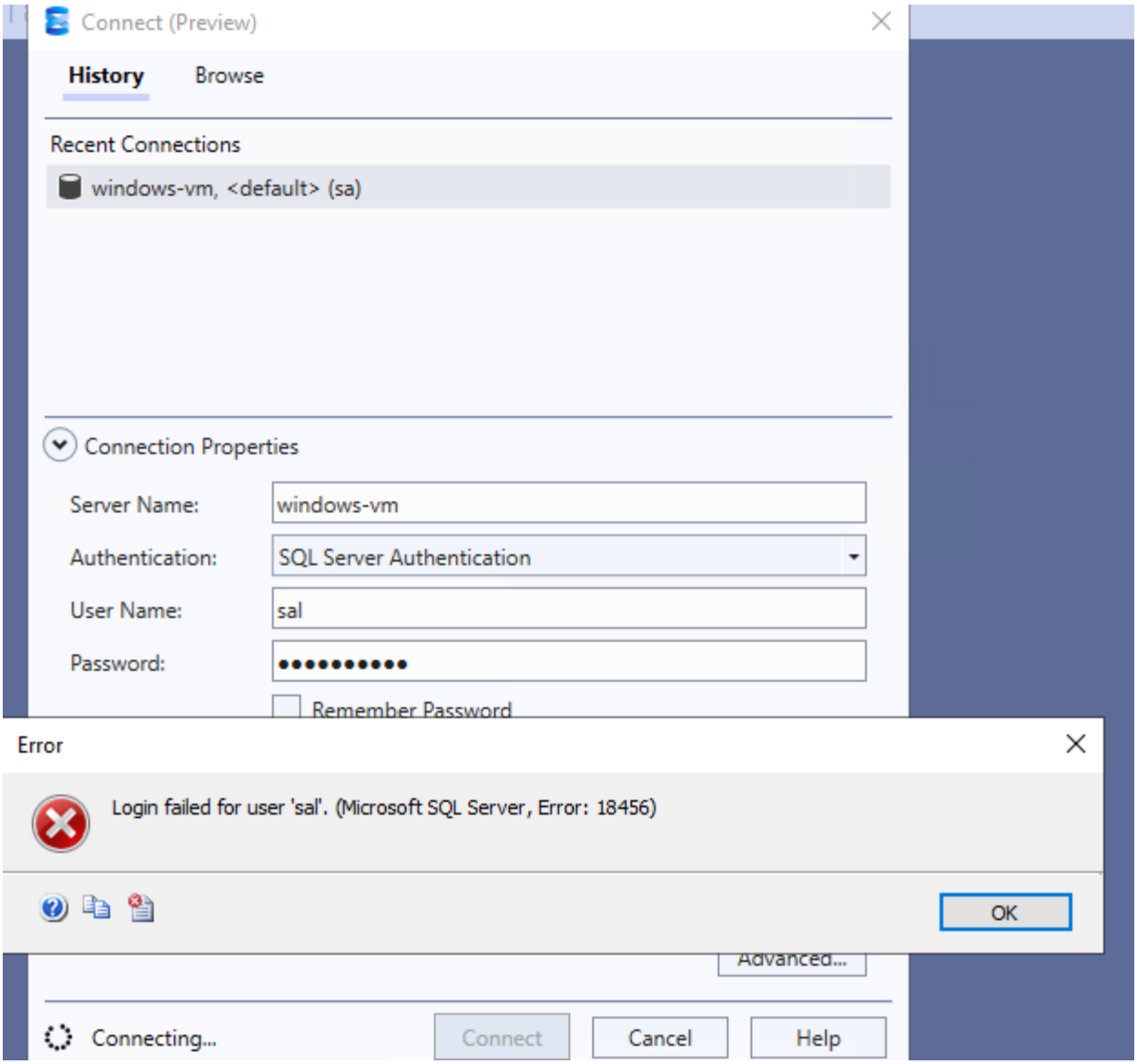
```
Windows Command Prompt                                    Copy

auditpol /set /subcategory:"application generated" /success:enable /failur
```

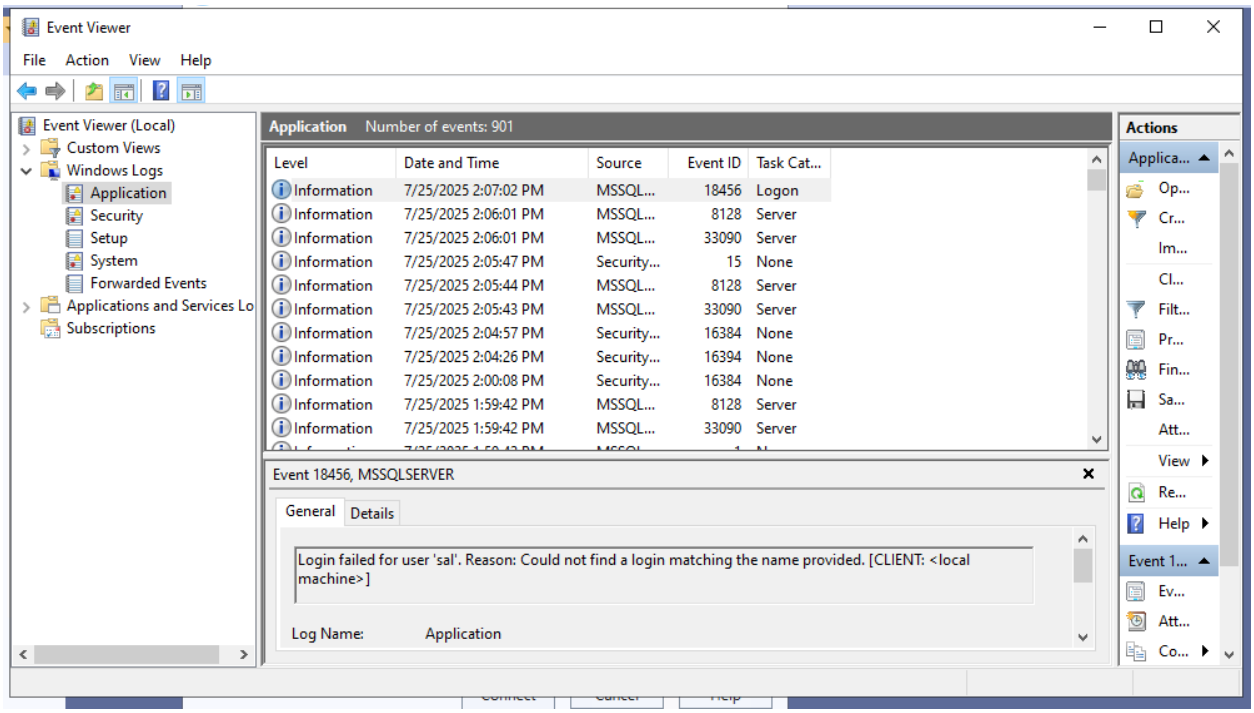
3. Close the command prompt window.

Grant the generate security audits




20.121.62.54 - Remote Desktop Connection
File Edit View Git Tools Extensions Window Help
Search
Sign in
New Query
Execute
Connect (Preview)
History
Browse
Recent Connections
No connection history to display.
Connection Properties
Server Name: windows-vm
Authentication: SQL Server Authentication
User Name: sa
Password:
Remember Password
Database Name: <default>
Encrypt: Mandatory
Trust Server Certificate
Color: <default>
Custom...
Advanced...
Connect
Cancel
Help
20.121.62.54 - Remote Desktop Connection
File Edit View Git Tools Extensions Window Help
Search
Sign in
New Query
Execute
Server Properties - windows-vm
Select a page
General
Memory
Processors
Security
Connections
Database Settings
Advanced
Permissions
Script
Help
Server authentication
Windows Authentication mode
SQL Server and Windows Authentication mode
Login auditing
None
Failed logins only
Successful logins only
Both failed and successful logins
Server proxy account
Enable server proxy account
Proxy account:
Password:
Options
Enable Common Criteria compliance
Enable C2 audit tracing
Cross database ownership chaining
Connection
Server:
windows-vm
Connection:
sa
View connection properties
Progress
Ready
OK
Cancel
Object Explorer
Connect
windows-vm (SQL Server 15.0.2000.5 - sa)
Databases
Security
Server Objects
Replication
PolyBase
Always On High Availability
Management
SQL Server Agent (Agent XPs disabled)
XEvent Profiler
Execute
Object Explorer
Connect


Connect (Preview)
History
Browse
Recent Connections
windows-vm, <default> (sa)
Connection Properties
Server Name:
windows-vm
Authentication:
SQL Server Authentication
User Name:
sal
Password:
Remember Password
Error
Login failed for user 'sal'. (Microsoft SQL Server, Error: 18456)
OK
Advanced...
Connecting...
Connect
Cancel
Help




```
C:\Users\klop7>ping 172.210.240.52

Pinging 172.210.240.52 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.210.240.52:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\klop7>
```

```
C:\Users\klop7>ping 172.210.240.52

Pinging 172.210.240.52 with 32 bytes of data:
Reply from 172.210.240.52: bytes=32 time=44ms TTL=106
Reply from 172.210.240.52: bytes=32 time=43ms TTL=106
Reply from 172.210.240.52: bytes=32 time=46ms TTL=106
Reply from 172.210.240.52: bytes=32 time=43ms TTL=106

Ping statistics for 172.210.240.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 43ms, Maximum = 46ms, Average = 44ms

C:\Users\klop7>
```

```
C:\Users\klop7>ssh labuser@172.210.240.52
ssh: connect to host 172.210.240.52 port 22: Connection refused

C:\Users\klop7>
```

```
Ping statistics for 172.174.224.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 55ms, Maximum = 58ms, Average = 56ms

C:\Users\klop7>
```

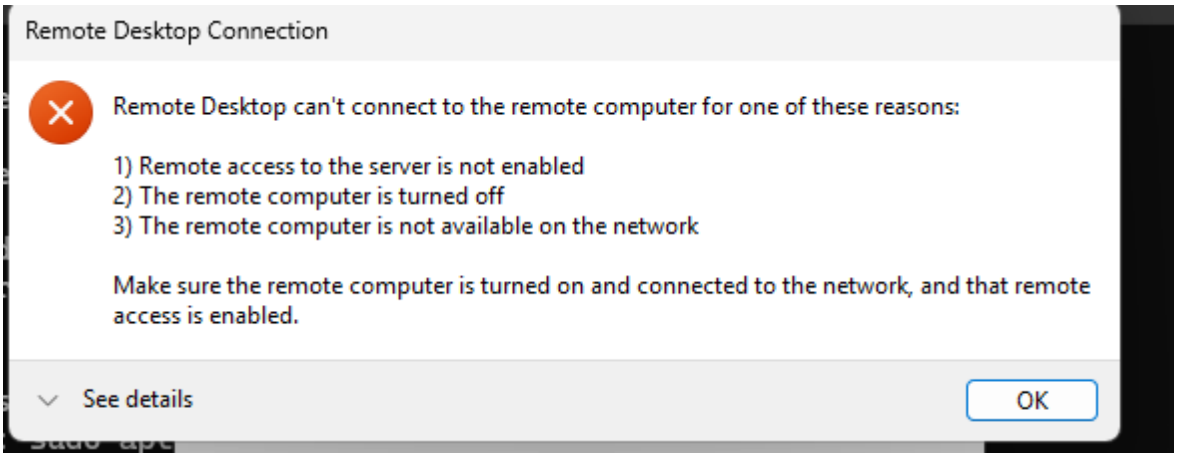
```
C:\Users\klop7>ssh labuser@172.174.224.24
The authenticity of host '172.174.224.24 (172.174.224.24)' can't be established.
ED25519 key fingerprint is SHA256:5rtxeHbb3qs715KHm8aJ2PmrUSOiG4Xpegxufe6PNnQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.174.224.24' (ED25519) to the list of known hosts.
labuser@172.174.224.24's password:
```

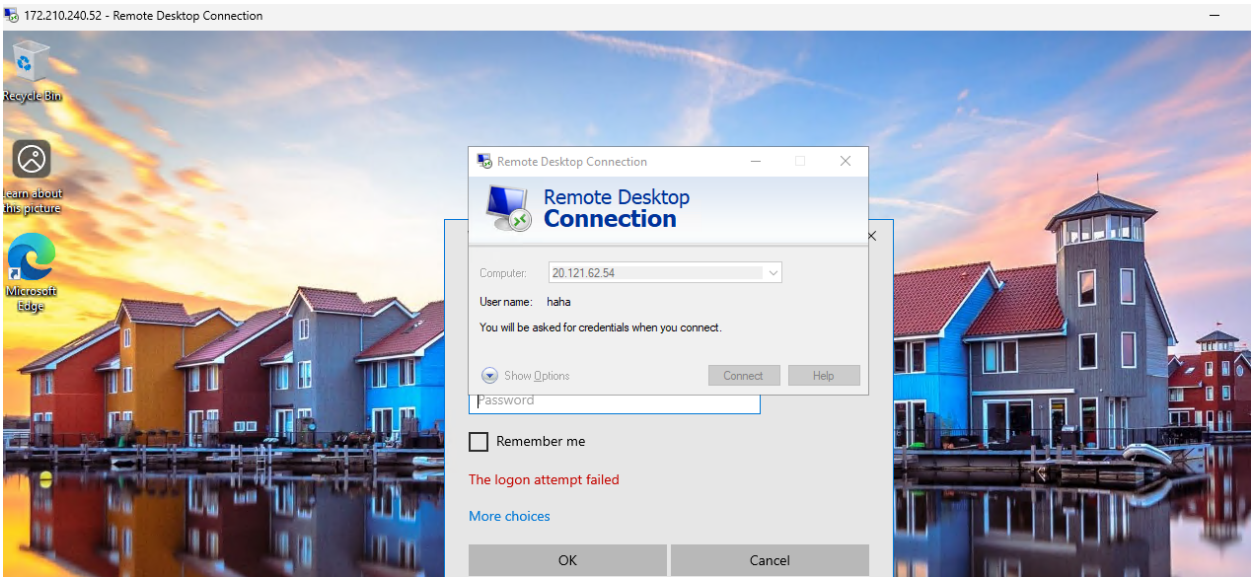
```
System information as of Fri Jul 25 14:36:21 UTC 2025

 System load:  0.11              Processes:             111
 Usage of /:   5.5% of 28.02GB   Users logged in:       0
 Memory usage: 29%               IPv4 address for eth0: 10.0.0.5
 Swap usage:   0%

xpanded Security Maintenance for Applications is not enabled.

 updates can be applied immediately.

nable ESM Apps to receive additional future security updates.
ee https://ubuntu.com/esm or run: sudo pro status


he list of available updates is more than a week old.
o check for new updates run: sudo apt update


he programs included with the Ubuntu system are free software;
he exact distribution terms for each program are described in the
ndividual files in /usr/share/doc/*/copyright.

buntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
pplicable law.

o run a command as administrator (user "root"), use "sudo <command>".
ee "man sudo_root" for details.
```

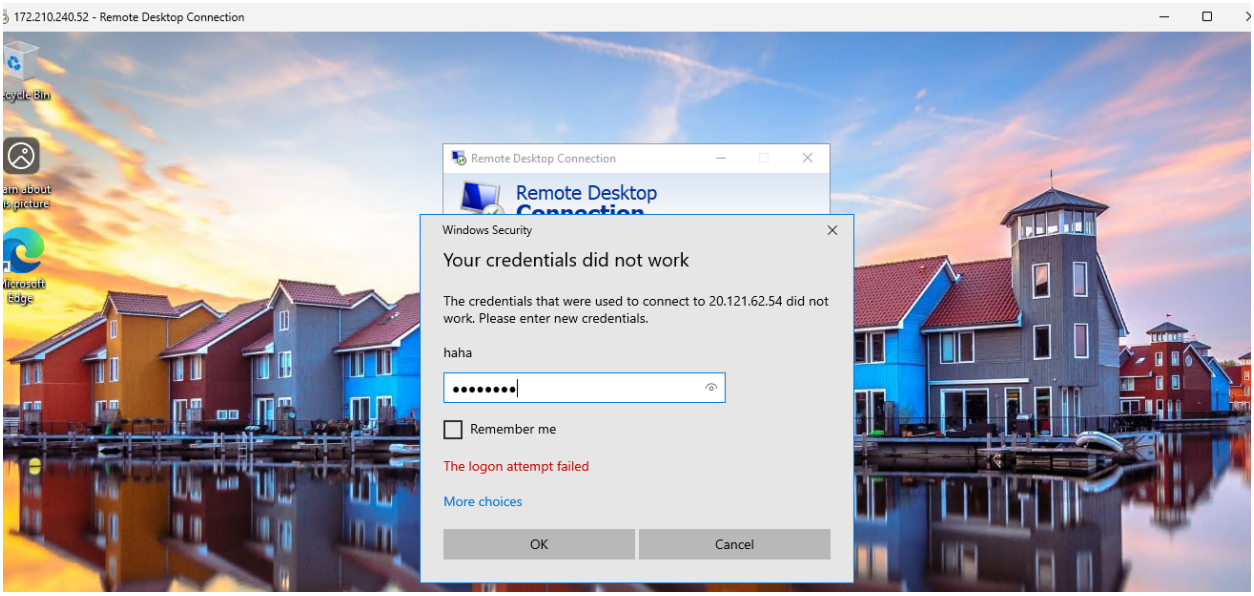
```
labuser@linux-vm:~$ id
uid=1000(labuser) gid=1000(labuser) groups=1000(labuser),4(adm),24(cdrom),27(sudo),30(dip),105(lxd)
```

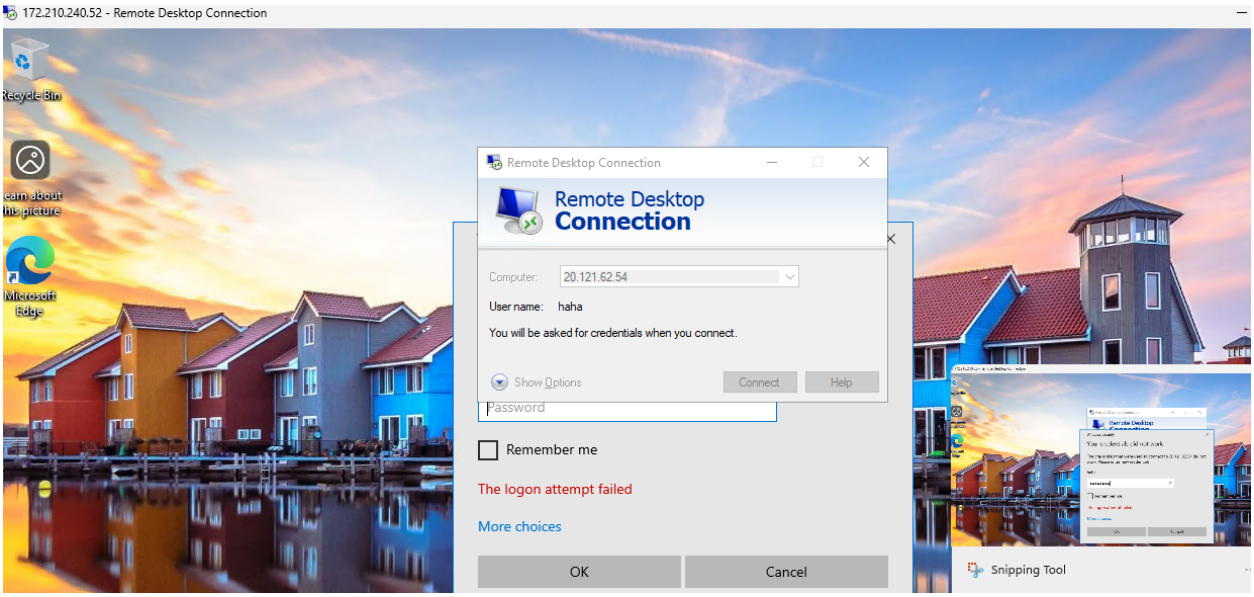
```
abuser@linux-vm:~$ exit
ogout
```

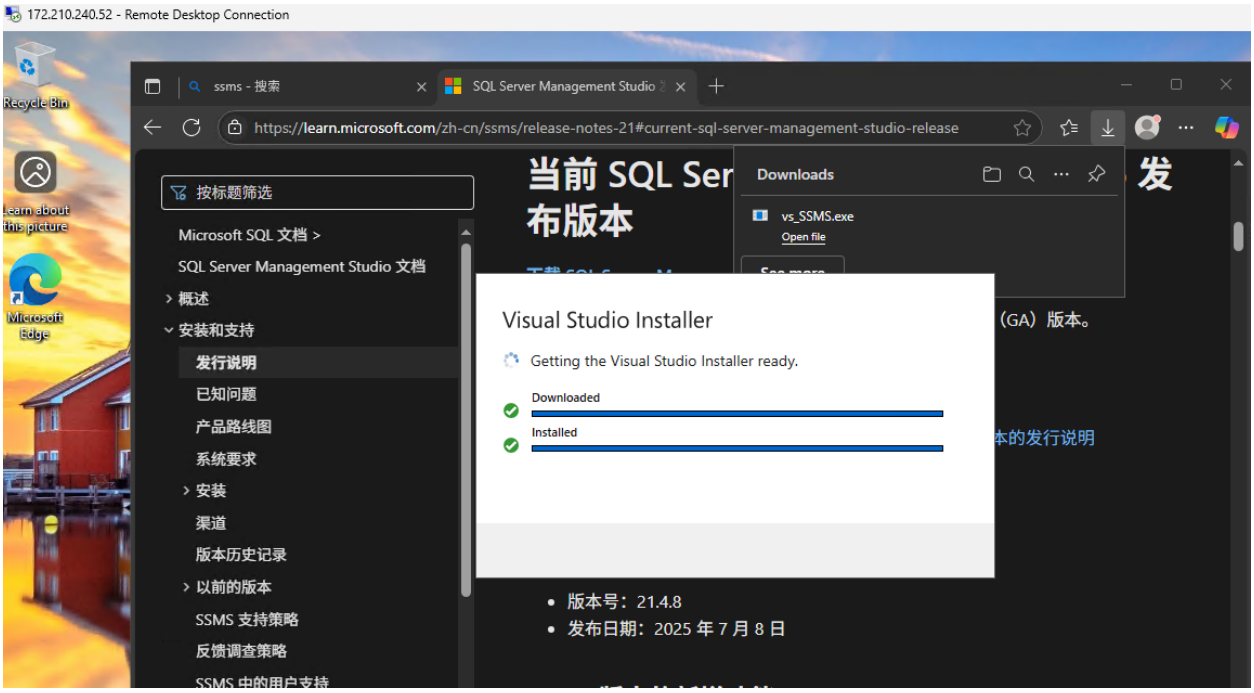
```
labuser@linux-vm:~$ exit
logout
Connection to 172.174.224.24 closed.

C:\Users\klop7>
```

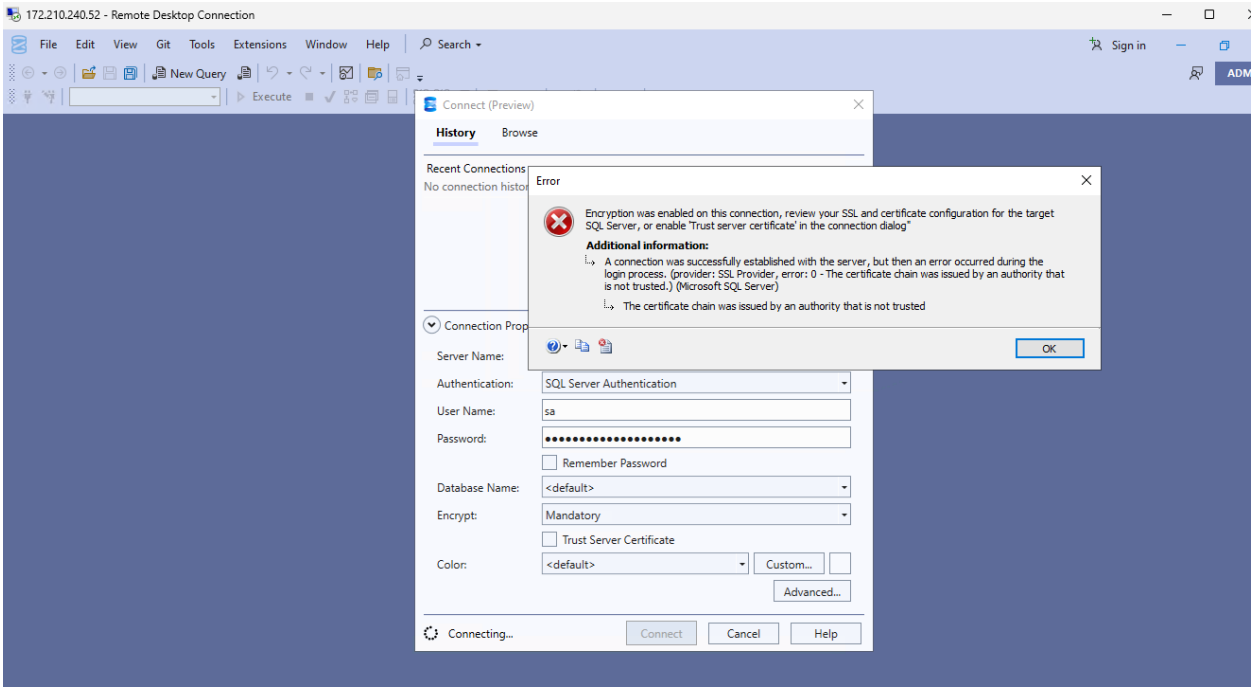

Remote Desktop Connection
Remote Desktop can't connect to the remote computer for one of these reasons:
1) Remote access to the server is not enabled
2) The remote computer is turned off
3) The remote computer is not available on the network
Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.
See details
OK

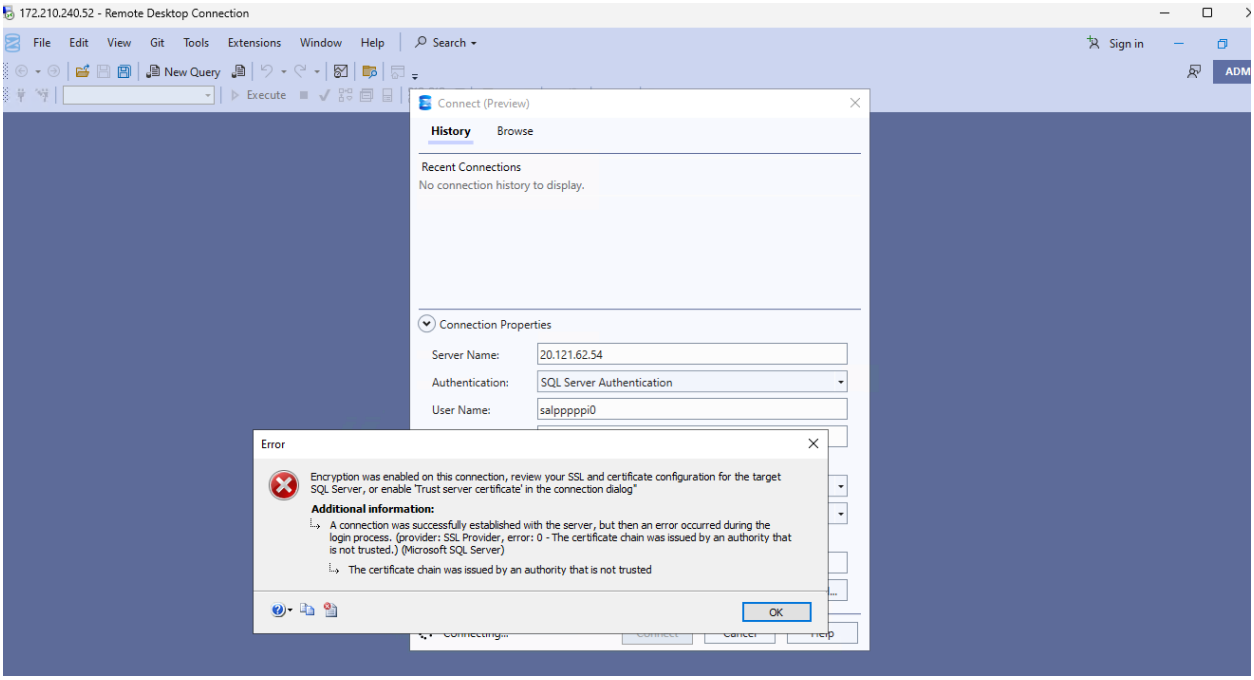

172.210.240.52 - Remote Desktop Connection
Recycle Bin
Microsoft Edge
Remote Desktop Connection
Remote Desktop Connection
Computer: 20.121.62.54
User name: haha
You will be asked for credentials when you connect.
Show Options
Connect
Help
Password
Remember me
The logon attempt failed
More choices
OK
Cancel

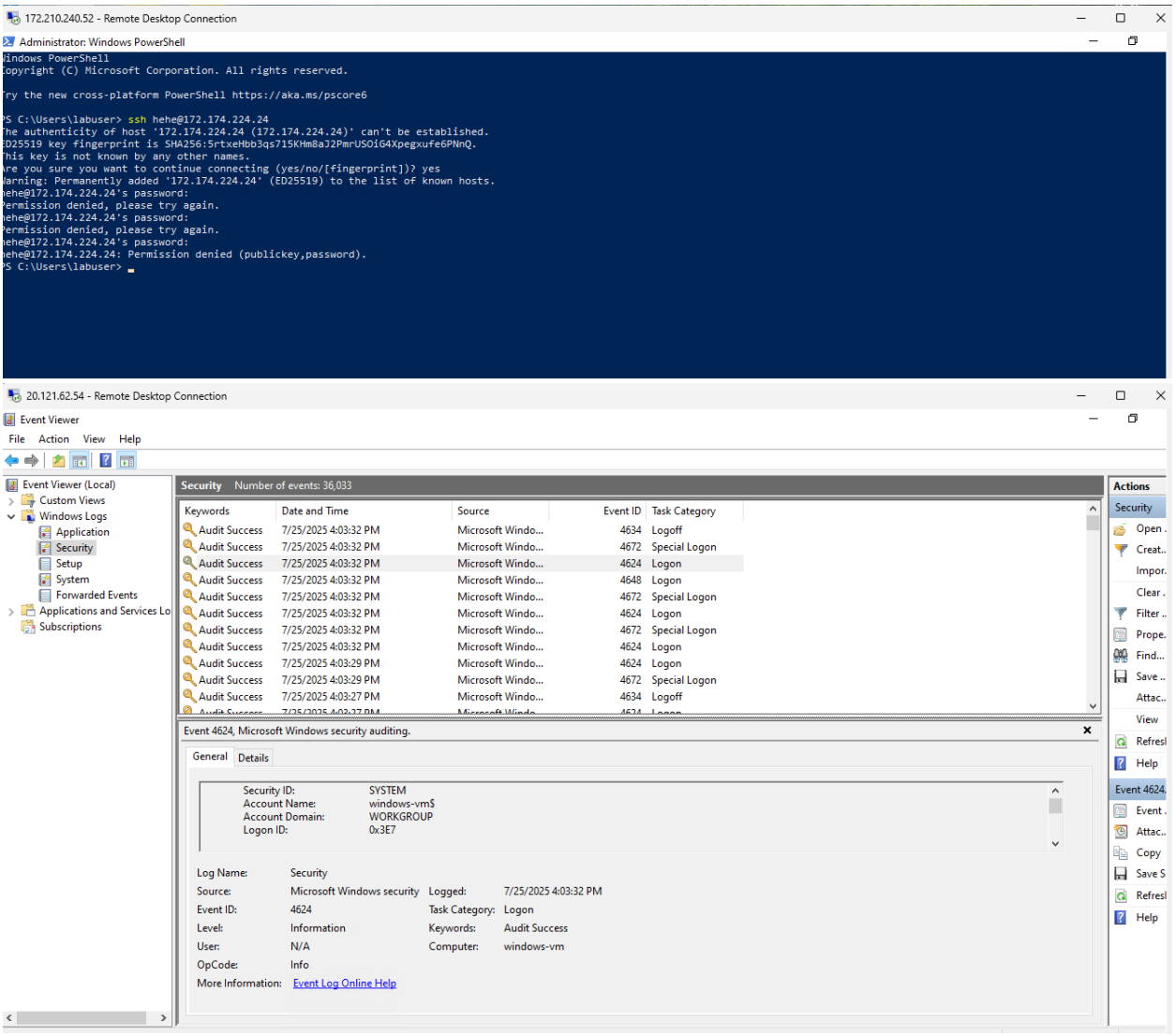

172.210.240.52 - Remote Desktop Connection
Remote Desktop Connection
Windows Security
Your credentials did not work
The credentials that were used to connect to 20.121.62.54 did not work. Please enter new credentials.
haha
Remember me
The logon attempt failed
More choices
OK
Cancel


172.210.240.52 - Remote Desktop Connection
Recycle Bin
Learn about this picture
Microsoft Edge
Remote Desktop Connection
Remote Desktop Connection
Computer: 20.121.62.54
User name: haha
You will be asked for credentials when you connect.
Show Options
Connect
Help
Password
Remember me
The logon attempt failed
More choices
OK
Cancel
Snipping Tool

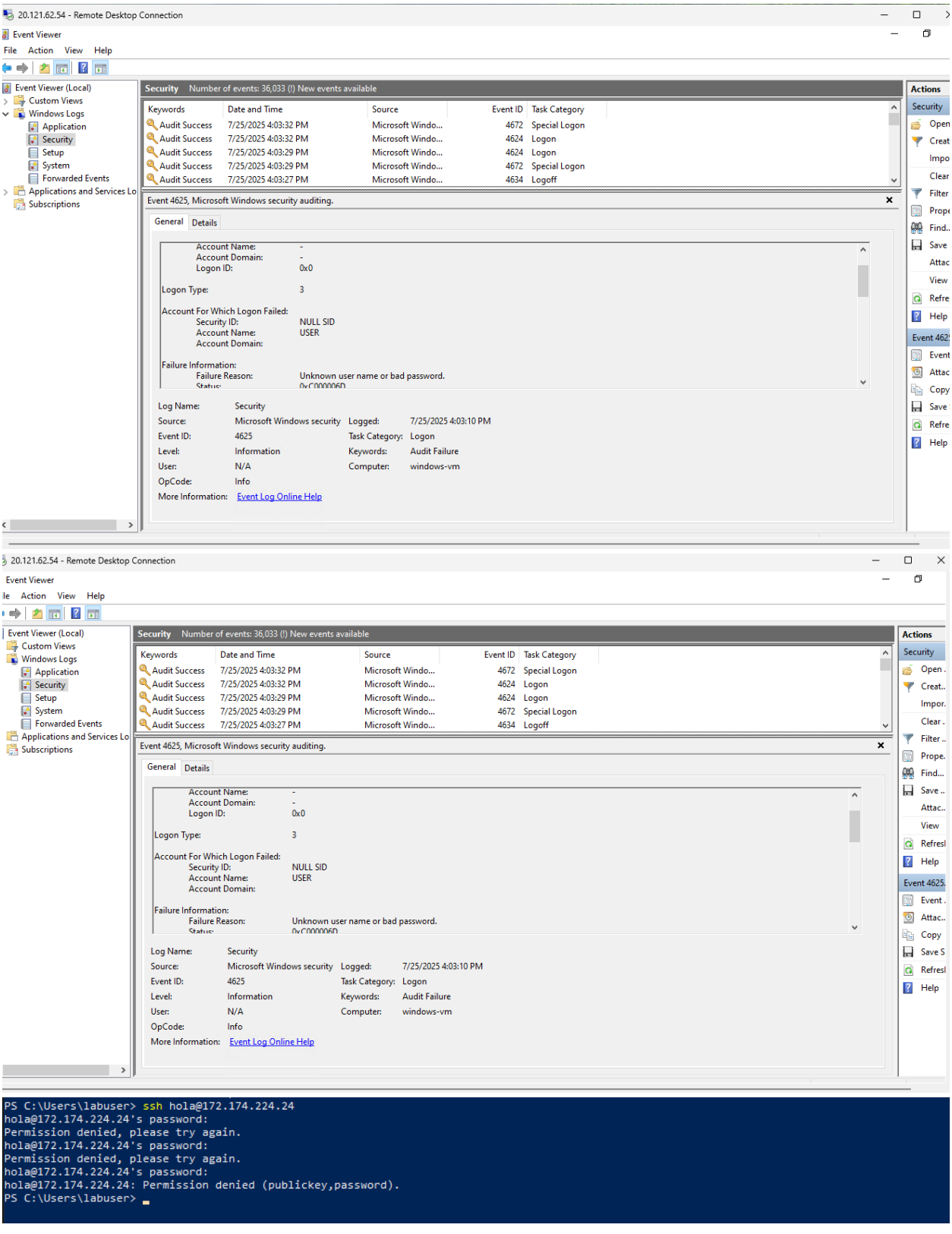

172.210.240.52 - Remote Desktop Connection
Recycle Bin
Learn about this picture
Microsoft Edge
ssms - 搜索
SQL Server Management Studio
https://learn.microsoft.com/zh-cn/ssms/release-notes-21#current-sql-server-management-studio-release
按标题筛选
Microsoft SQL 文档 >
SQL Server Management Studio 文档
概述
安装和支持
发行说明
已知问题
产品路线图
系统要求
安装
渠道
版本历史记录
以前的版本
SSMS 支持策略
反馈调查策略
当前 SQL Ser
布版本
Downloads
vs_SSMS.exe
Open file
Visual Studio Installer
Getting the Visual Studio Installer ready.
Downloaded
Installed
(GA) 版本。
本的发行说明
版本号：21.4.8
发布日期：2025 年 7 月 8 日


172.210.240.52 - Remote Desktop Connection
File Edit View Git Tools Extensions Window Help
Search
Sign in
New Query
Execute
Connect (Preview)
History
Browse
Recent Connections
Error
Encryption was enabled on this connection, review your SSL and certificate configuration for the target SQL Server, or enable 'Trust server certificate' in the connection dialog"
Additional information:
A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority that is not trusted.) (Microsoft SQL Server)
The certificate chain was issued by an authority that is not trusted
OK
Server Name:
Authentication:
SQL Server Authentication
User Name:
sa
Password:
Remember Password
Database Name:
<default>
Encrypt:
Mandatory
Trust Server Certificate
Color:
<default>
Custom...
Advanced...
Connecting...
Connect
Cancel
Help

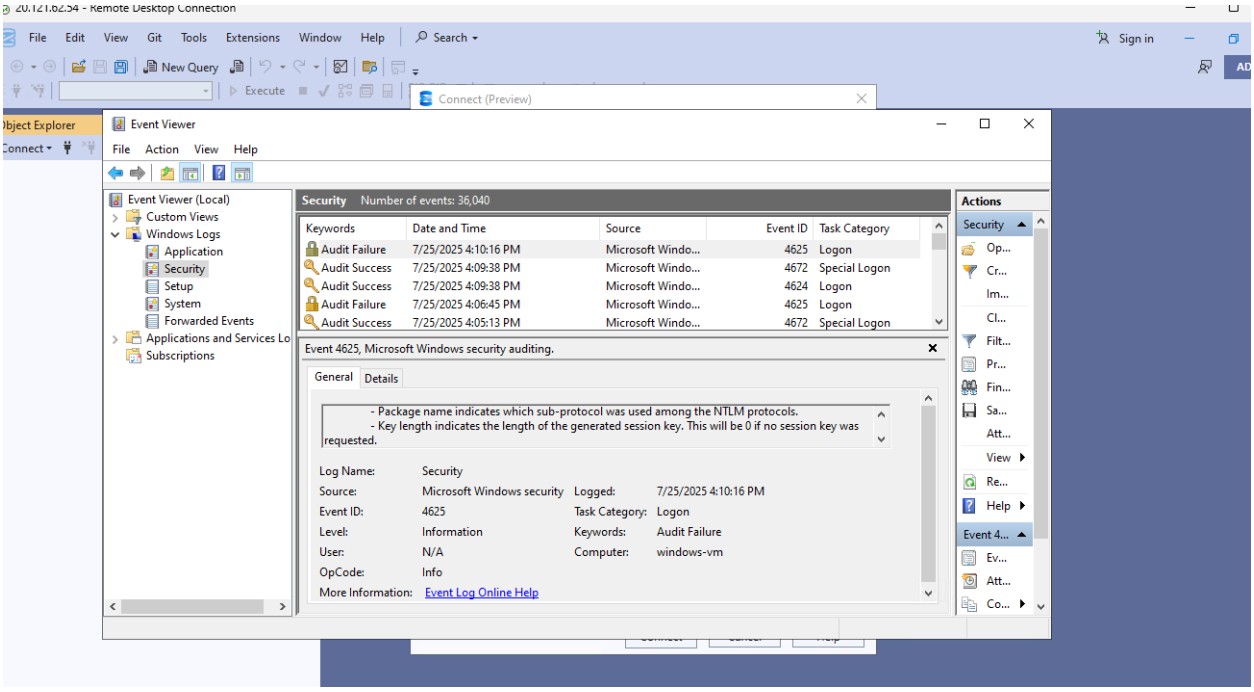

172.210.240.52 - Remote Desktop Connection
File Edit View Git Tools Extensions Window Help
Search
Sign in
New Query
Execute
Connect (Preview)
History
Browse
Recent Connections
No connection history to display.
Connection Properties
Server Name:
20.121.62.54
Authentication:
SQL Server Authentication
User Name:
salpppppi0
Error
Encryption was enabled on this connection, review your SSL and certificate configuration for the target SQL Server, or enable 'Trust server certificate' in the connection dialog"
Additional information:
A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority that is not trusted.) (Microsoft SQL Server)
The certificate chain was issued by an authority that is not trusted
OK

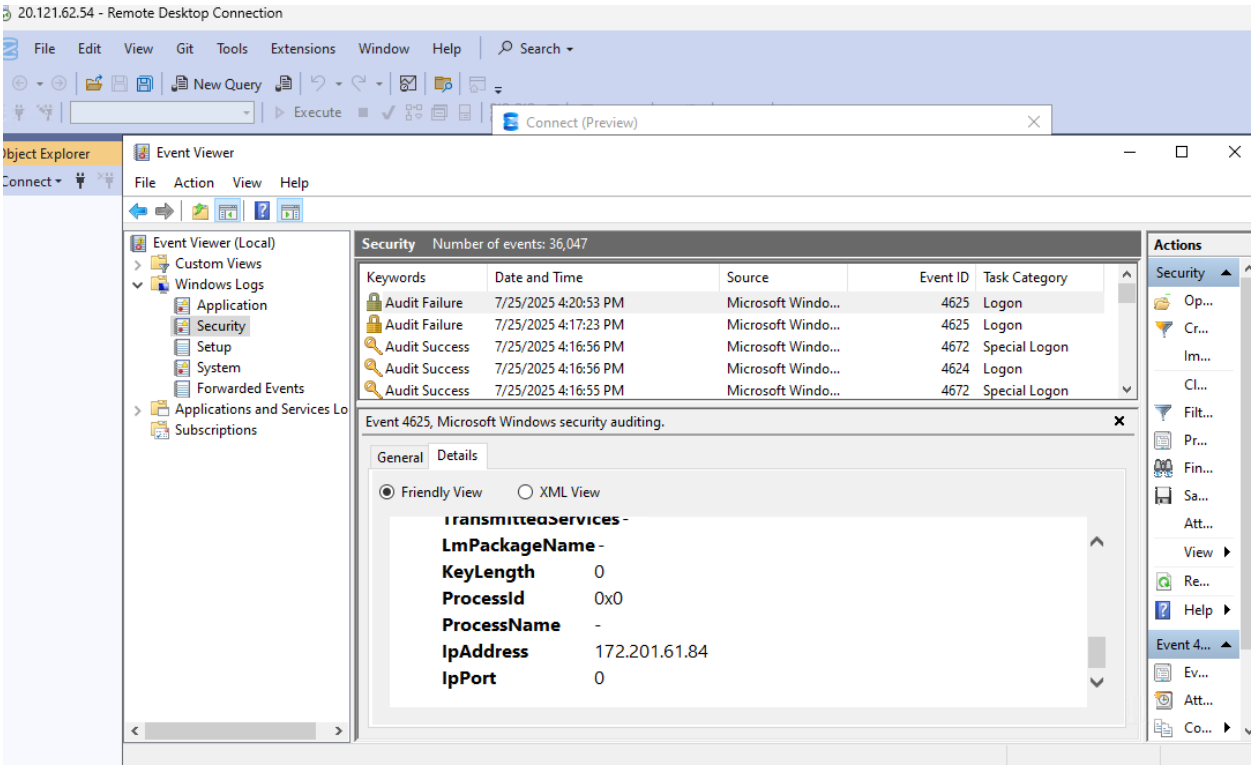

172.210.240.52 - Remote Desktop Connection
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\labuser> ssh hehe@172.174.224.24
The authenticity of host '172.174.224.24 (172.174.224.24)' can't be established.
ED25519 key fingerprint is SHA256:5rtxeHbb3qs715KHm8aJ2PmrUSOiG4Xpegxufe6PNnQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.174.224.24' (ED25519) to the list of known hosts.
hehe@172.174.224.24's password:
Permission denied, please try again.
hehe@172.174.224.24's password:
Permission denied, please try again.
hehe@172.174.224.24's password:
hehe@172.174.224.24: Permission denied (publickey,password).
PS C:\Users\labuser>

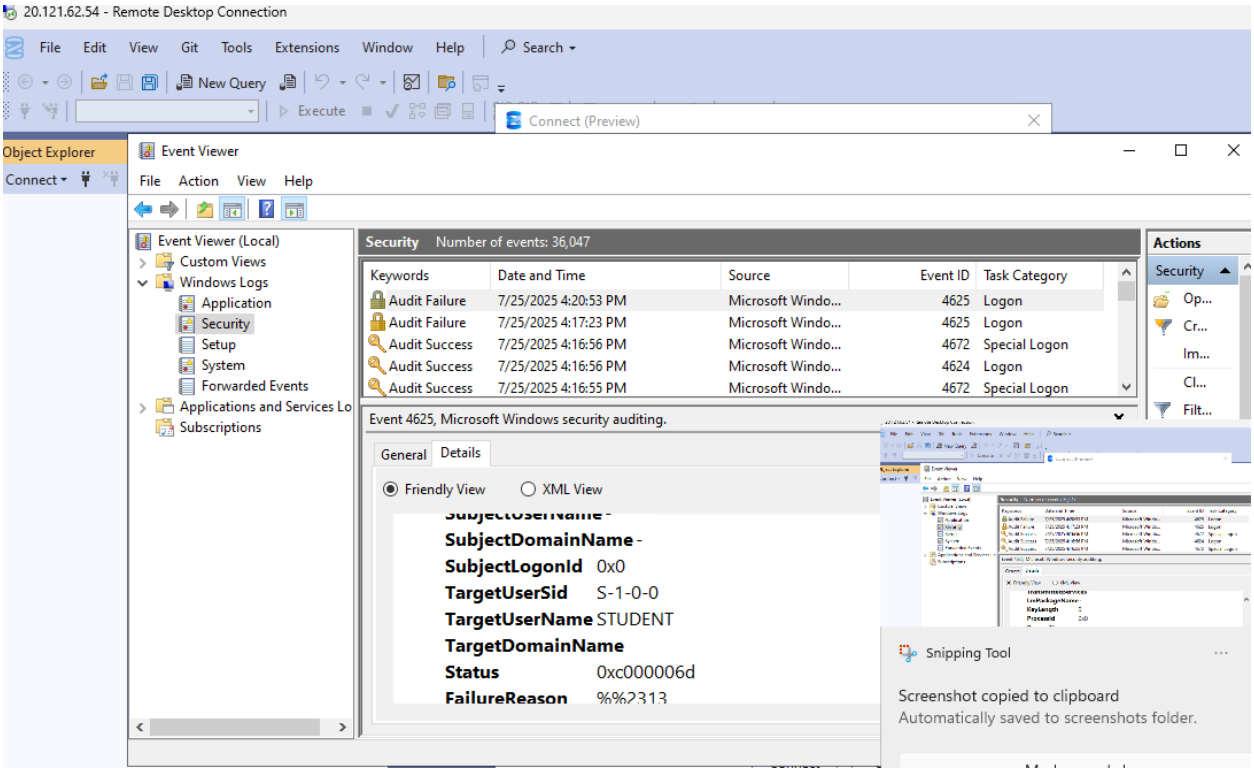
20.121.62.54 - Remote Desktop Connection
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
Security Number of events: 36,033
Keywords Date and Time Source Event ID Task Category
Audit Success 7/25/2025 4:03:32 PM Microsoft Windo... 4634 Logoff
Audit Success 7/25/2025 4:03:32 PM Microsoft Windo... 4672 Special Logon
Audit Success 7/25/2025 4:03:32 PM Microsoft Windo... 4624 Logon
Audit Success 7/25/2025 4:03:32 PM Microsoft Windo... 4648 Logon
Audit Success 7/25/2025 4:03:32 PM Microsoft Windo... 4672 Special Logon
Audit Success 7/25/2025 4:03:32 PM Microsoft Windo... 4624 Logon
Audit Success 7/25/2025 4:03:32 PM Microsoft Windo... 4672 Special Logon
Audit Success 7/25/2025 4:03:32 PM Microsoft Windo... 4624 Logon
Audit Success 7/25/2025 4:03:29 PM Microsoft Windo... 4624 Logon
Audit Success 7/25/2025 4:03:29 PM Microsoft Windo... 4672 Special Logon
Audit Success 7/25/2025 4:03:27 PM Microsoft Windo... 4634 Logoff
Event 4624, Microsoft Windows security auditing.
General Details
Security ID: SYSTEM
Account Name: windows-vm$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Log Name: Security
Source: Microsoft Windows security Logged: 7/25/2025 4:03:32 PM
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: windows-vm
OpCode: Info
More Information: Event Log Online Help
Actions
Security
Open .
Creat..
Impor.
Clear .
Filter ..
Prope.
Find...
Save ..
Attac..
View
Refresl
Help
Event 4624.
Event .
Attac..
Copy
Save S
Refresl
Help




```
PS C:\Users\labuser> ssh hola@172.174.224.24
hola@172.174.224.24's password:
Permission denied, please try again.
hola@172.174.224.24's password:
Permission denied, please try again.
hola@172.174.224.24's password:
hola@172.174.224.24: Permission denied (publickey,password).
PS C:\Users\labuser>
```

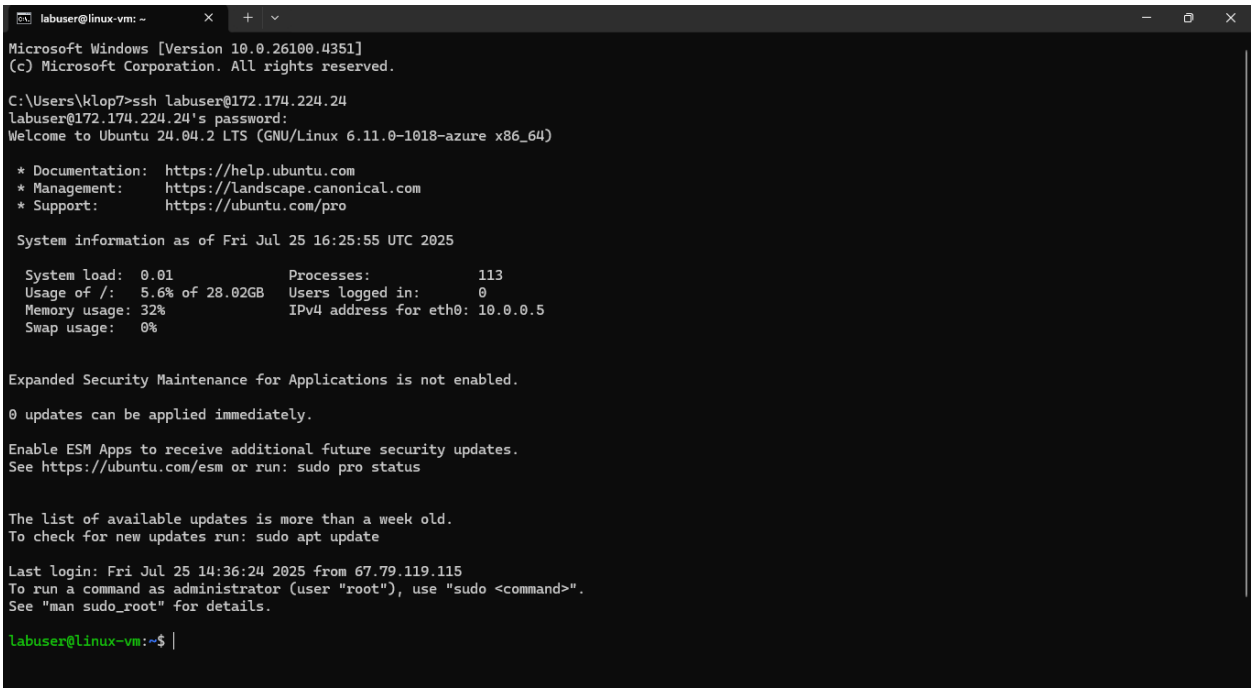

20.121.62.54 - Remote Desktop Connection
File Edit View Git Tools Extensions Window Help Search
New Query
Execute
Connect (Preview)
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
Security Number of events: 36,040
Keywords Date and Time Source Event ID Task Category
Audit Failure 7/25/2025 4:10:16 PM Microsoft Windo... 4625 Logon
Audit Success 7/25/2025 4:09:38 PM Microsoft Windo... 4672 Special Logon
Audit Success 7/25/2025 4:09:38 PM Microsoft Windo... 4624 Logon
Audit Failure 7/25/2025 4:06:45 PM Microsoft Windo... 4625 Logon
Audit Success 7/25/2025 4:05:13 PM Microsoft Windo... 4672 Special Logon
Event 4625, Microsoft Windows security auditing.
General Details
- Package name indicates which sub-protocol was used among the NTLM protocols.
- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Log Name: Security
Source: Microsoft Windows security Logged: 7/25/2025 4:10:16 PM
Event ID: 4625 Task Category: Logon
Level: Information Keywords: Audit Failure
User: N/A Computer: windows-vm
OpCode: Info
More Information: Event Log Online Help
Actions
Security
Event 4...


20.121.62.54 - Remote Desktop Connection
File Edit View Git Tools Extensions Window Help Search
New Query
Execute
Connect (Preview)
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
Security Number of events: 36,047
Keywords Date and Time Source Event ID Task Category
Audit Failure 7/25/2025 4:20:53 PM Microsoft Windo... 4625 Logon
Audit Failure 7/25/2025 4:17:23 PM Microsoft Windo... 4625 Logon
Audit Success 7/25/2025 4:16:56 PM Microsoft Windo... 4672 Special Logon
Audit Success 7/25/2025 4:16:56 PM Microsoft Windo... 4624 Logon
Audit Success 7/25/2025 4:16:55 PM Microsoft Windo... 4672 Special Logon
Event 4625, Microsoft Windows security auditing.
General Details
Friendly View
XML View
TransmittedServices -
LmPackageName -
KeyLength 0
ProcessId 0x0
ProcessName -
IpAddress 172.201.61.84
IpPort 0
Actions
Security
Event 4...

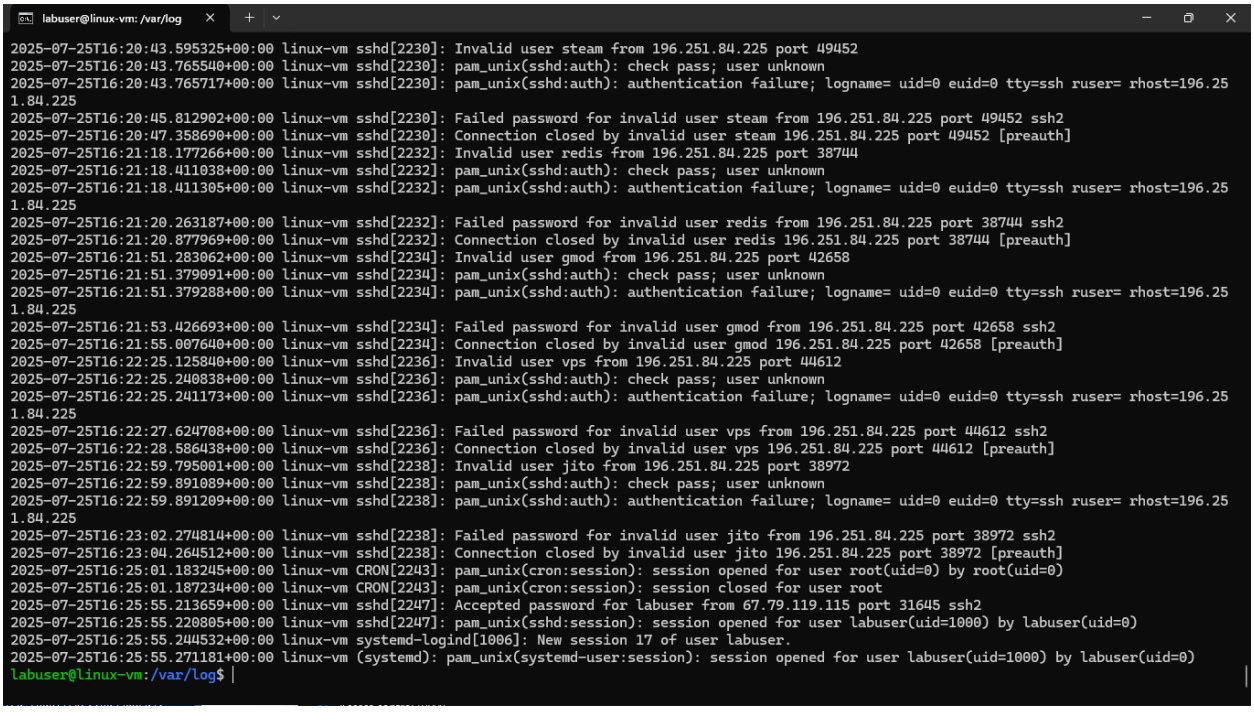


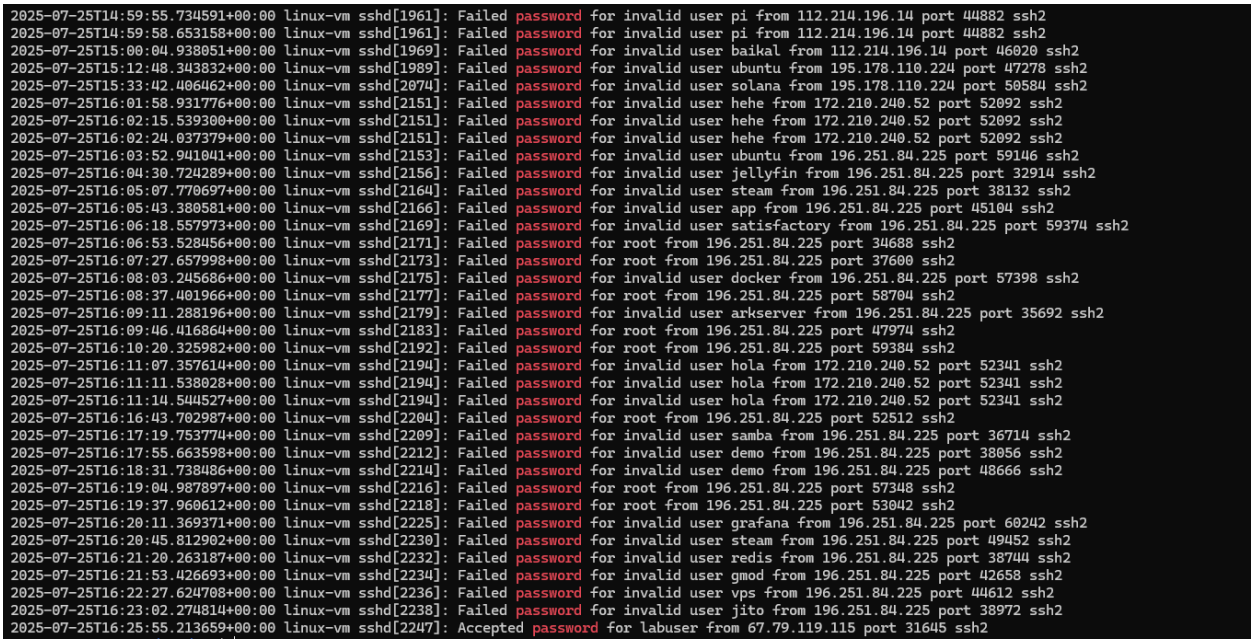
4. Linux VM Attack Monitoring

- Used SSH to access the Linux VM from Kali and the host.
- Commands used:
- `cd /var/log`
- `cat auth.log | grep "Failed password"`
- Successfully detected global SSH brute-force attempts within minutes of exposing the Linux VM.


labuser@linux-vm: ~
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.
C:\Users\klop7>ssh labuser@172.174.224.24
labuser@172.174.224.24's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-1018-azure x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Fri Jul 25 16:25:55 UTC 2025
System load: 0.01
Usage of /: 5.6% of 28.02GB
Memory usage: 32%
Swap usage: 0%
Processes: 113
Users logged in: 0
IPv4 address for eth0: 10.0.0.5
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Fri Jul 25 14:36:24 2025 from 67.79.119.115
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
labuser@linux-vm:~$


labuser@linux-vm:~$ cd /var/log/
labuser@linux-vm:/var/log$ ls
README apt azure chrony cloud-init.log dmesg kern.log lastlog syslog unattended-upgrades wtmp
apport.log auth.log btmp cloud-init-output.log dist-upgrade journal landscape private sysstat waagent.log
labuser@linux-vm:/var/log$ cat auth.log


labuser@linux-vm: /var/log
2025-07-25T16:20:43.595325+00:00 linux-vm sshd[2230]: Invalid user steam from 196.251.84.225 port 49452
2025-07-25T16:20:43.765540+00:00 linux-vm sshd[2230]: pam_unix(sshd:auth): check pass; user unknown
2025-07-25T16:20:43.765717+00:00 linux-vm sshd[2230]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=196.25
1.84.225
2025-07-25T16:20:45.812902+00:00 linux-vm sshd[2230]: Failed password for invalid user steam from 196.251.84.225 port 49452 ssh2
2025-07-25T16:20:47.358690+00:00 linux-vm sshd[2230]: Connection closed by invalid user steam 196.251.84.225 port 49452 [preauth]
2025-07-25T16:21:18.177266+00:00 linux-vm sshd[2232]: Invalid user redis from 196.251.84.225 port 38744
2025-07-25T16:21:18.411038+00:00 linux-vm sshd[2232]: pam_unix(sshd:auth): check pass; user unknown
2025-07-25T16:21:18.411305+00:00 linux-vm sshd[2232]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=196.25
1.84.225
2025-07-25T16:21:20.263187+00:00 linux-vm sshd[2232]: Failed password for invalid user redis from 196.251.84.225 port 38744 ssh2
2025-07-25T16:21:20.877969+00:00 linux-vm sshd[2232]: Connection closed by invalid user redis 196.251.84.225 port 38744 [preauth]
2025-07-25T16:21:51.283062+00:00 linux-vm sshd[2234]: Invalid user gmod from 196.251.84.225 port 42658
2025-07-25T16:21:51.379091+00:00 linux-vm sshd[2234]: pam_unix(sshd:auth): check pass; user unknown
2025-07-25T16:21:51.379288+00:00 linux-vm sshd[2234]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=196.25
1.84.225
2025-07-25T16:21:53.426693+00:00 linux-vm sshd[2234]: Failed password for invalid user gmod from 196.251.84.225 port 42658 ssh2
2025-07-25T16:21:55.007640+00:00 linux-vm sshd[2234]: Connection closed by invalid user gmod 196.251.84.225 port 42658 [preauth]
2025-07-25T16:22:25.125840+00:00 linux-vm sshd[2236]: Invalid user vps from 196.251.84.225 port 44612
2025-07-25T16:22:25.240838+00:00 linux-vm sshd[2236]: pam_unix(sshd:auth): check pass; user unknown
2025-07-25T16:22:25.241173+00:00 linux-vm sshd[2236]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=196.25
1.84.225
2025-07-25T16:22:27.624708+00:00 linux-vm sshd[2236]: Failed password for invalid user vps from 196.251.84.225 port 44612 ssh2
2025-07-25T16:22:28.586438+00:00 linux-vm sshd[2236]: Connection closed by invalid user vps 196.251.84.225 port 44612 [preauth]
2025-07-25T16:22:59.795001+00:00 linux-vm sshd[2238]: Invalid user jito from 196.251.84.225 port 38972
2025-07-25T16:22:59.891089+00:00 linux-vm sshd[2238]: pam_unix(sshd:auth): check pass; user unknown
2025-07-25T16:22:59.891209+00:00 linux-vm sshd[2238]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=196.25
1.84.225
2025-07-25T16:23:02.274814+00:00 linux-vm sshd[2238]: Failed password for invalid user jito from 196.251.84.225 port 38972 ssh2
2025-07-25T16:23:04.264512+00:00 linux-vm sshd[2238]: Connection closed by invalid user jito 196.251.84.225 port 38972 [preauth]
2025-07-25T16:25:01.183245+00:00 linux-vm CRON[2243]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-07-25T16:25:01.187234+00:00 linux-vm CRON[2243]: pam_unix(cron:session): session closed for user root
2025-07-25T16:25:55.213659+00:00 linux-vm sshd[2247]: Accepted password for labuser from 67.79.119.115 port 31645 ssh2
2025-07-25T16:25:55.220805+00:00 linux-vm sshd[2247]: pam_unix(sshd:session): session opened for user labuser(uid=1000) by labuser(uid=0)
2025-07-25T16:25:55.244532+00:00 linux-vm systemd-logind[1006]: New session 17 of user labuser.
2025-07-25T16:25:55.271181+00:00 linux-vm (systemd): pam_unix(systemd-user:session): session opened for user labuser(uid=1000) by labuser(uid=0)
labuser@linux-vm:/var/log$



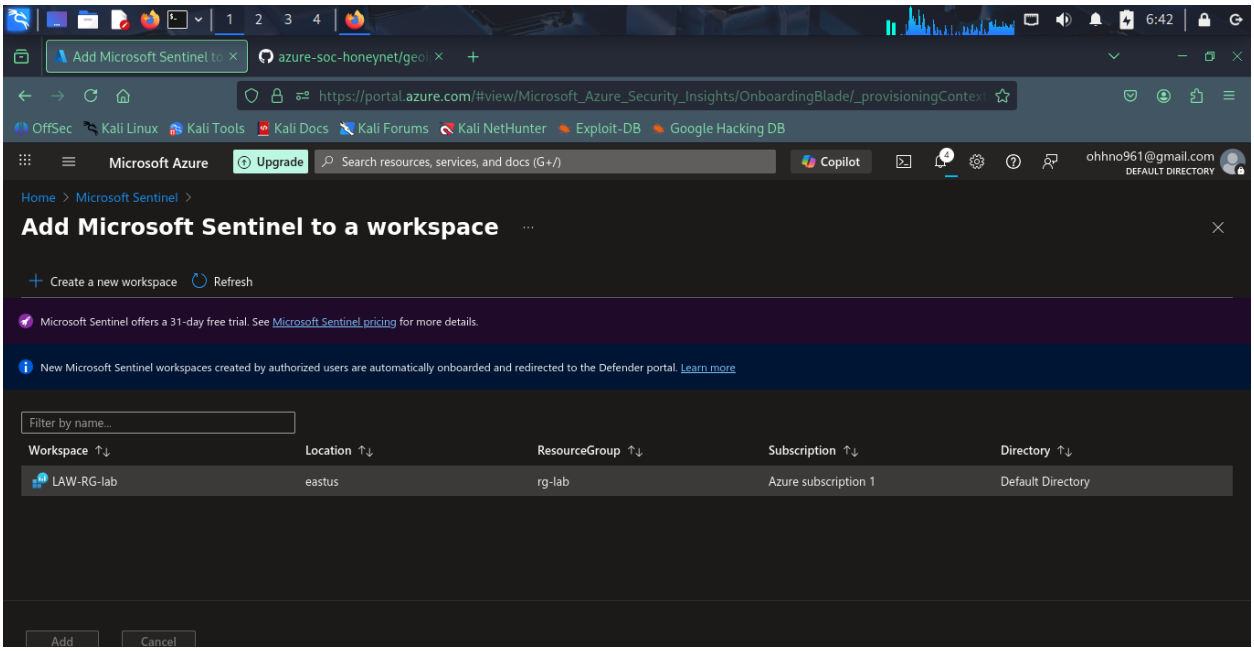
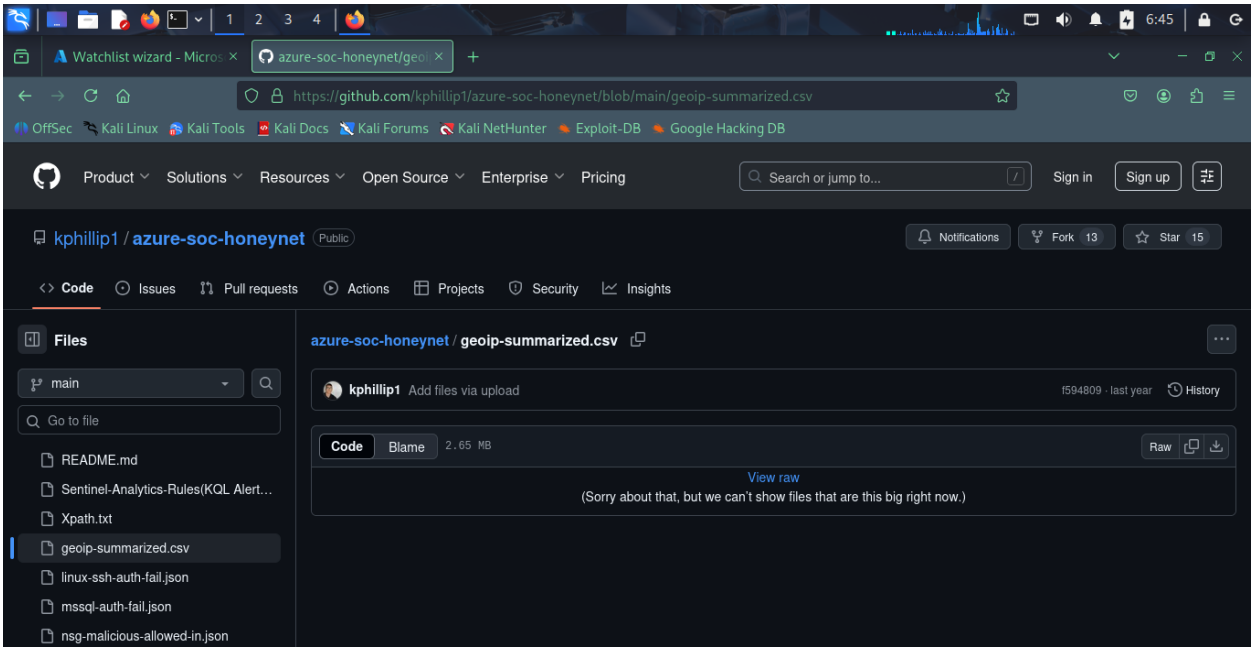
5. Attack Simulation from Kali (Attacker VM)

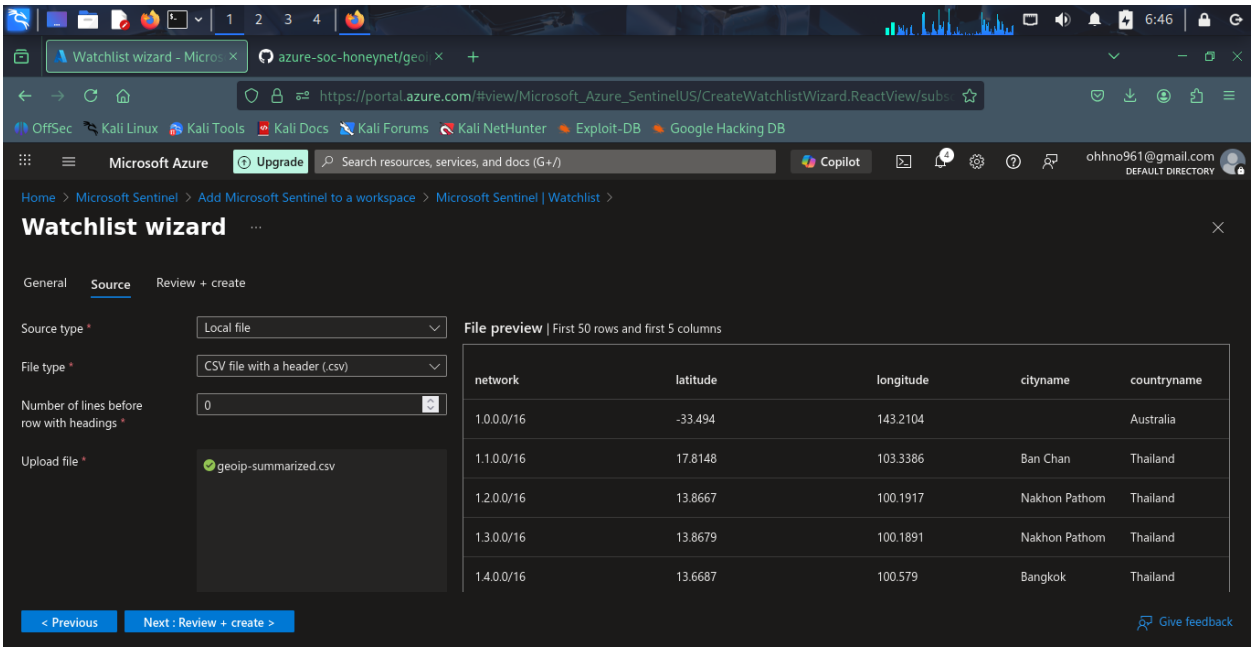
- Simulated RDP and SQL brute-force attacks on the Windows VM.
- Repeated incorrect login attempts via SSMS and RDP to generate events.
- SSH attempted into Linux VM using fake users to trigger logs like `Permission denied`.
- Verified the activity via:
    - **Event Viewer** on Windows.
    - **auth.log** on Linux.

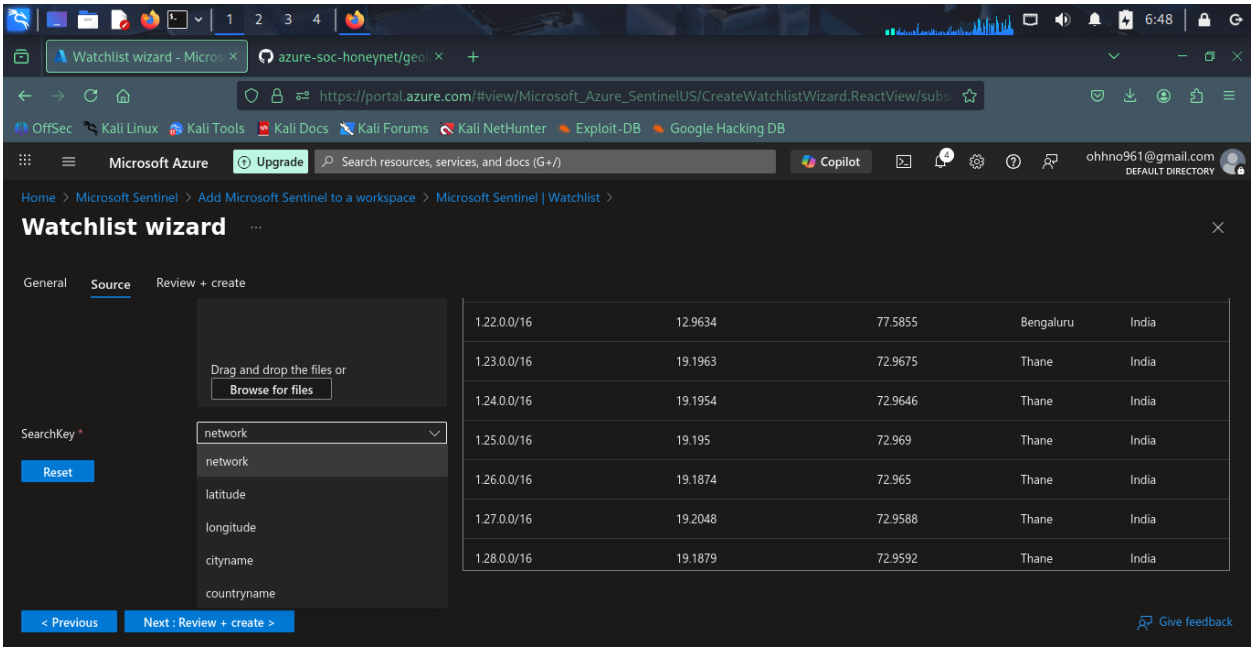
6. Attempted Integration with Microsoft Sentinel

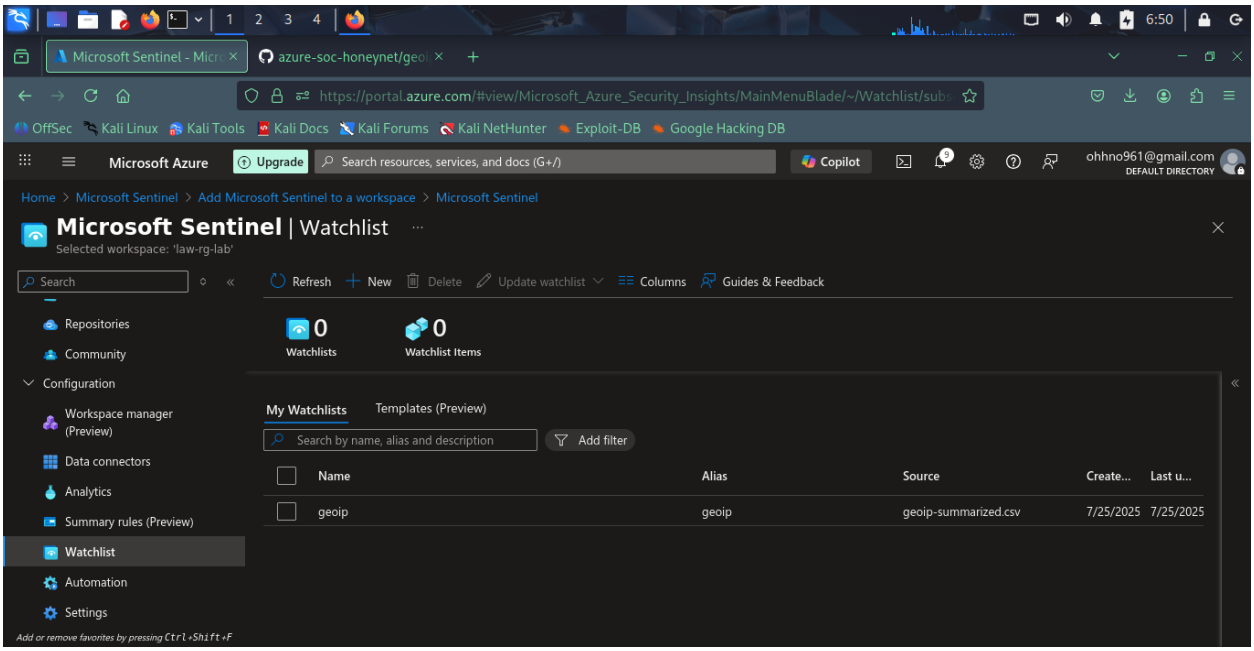
- Created a **Log Analytics Workspace** (`law-rg-lab`) under resource group `rg-lab`.

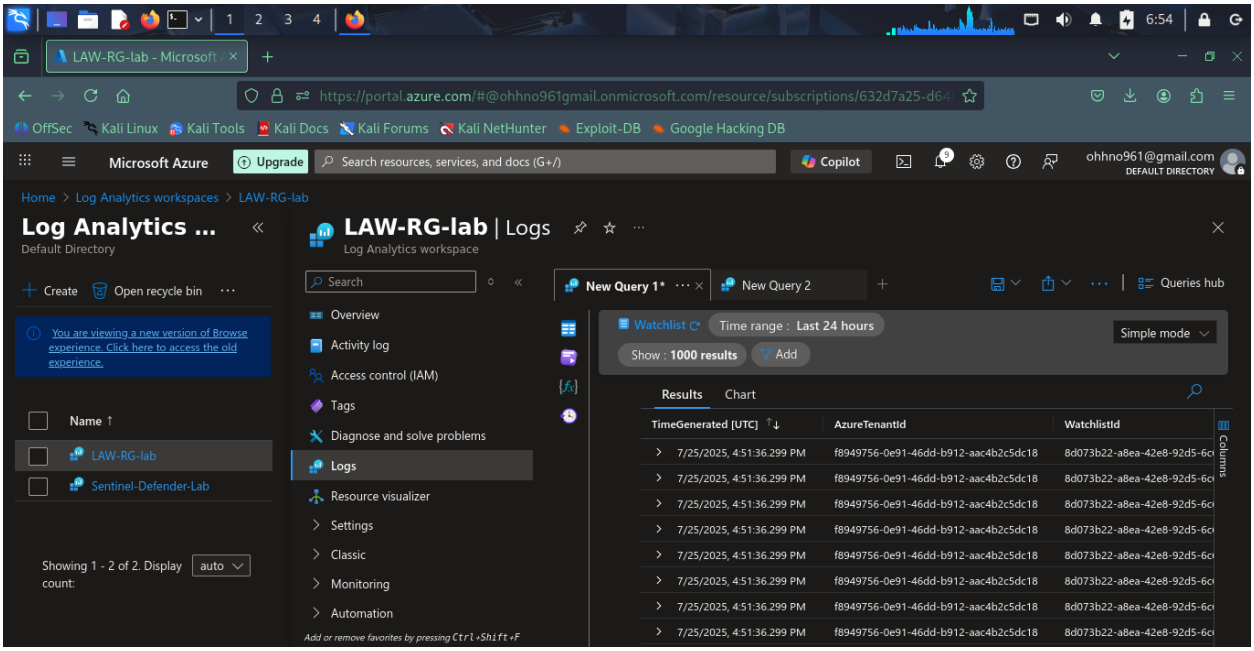
- Tried to connect Microsoft Sentinel and import **GeoIP watchlist** (`goip-summarize.csv`) from GitHub.
    - Successfully previewed 54,803 GeoIP records using:
    - `_GetWatchlist('GeoIP') | count`
- **Microsoft Defender for Cloud**:
    - Enabled plans for **Servers, SQL, Storage, Key Vault**.
    - Set **Data Collection** to *All Events*.
    - Configured **Continuous Export** (security score, alerts, compliance, etc.) to Log Analytics.

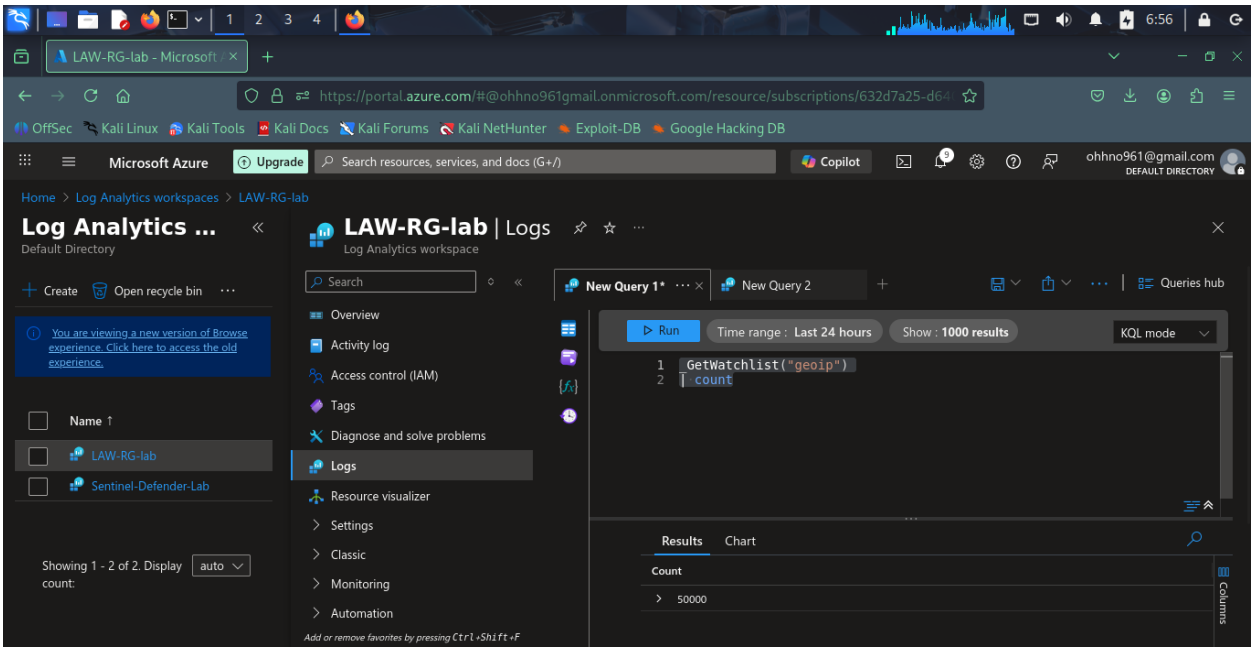
- 
Add Microsoft Sentinel to a workspace
Create a new workspace
Refresh
Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.
New Microsoft Sentinel workspaces created by authorized users are automatically onboarded and redirected to the Defender portal. Learn more
Filter by name...
Workspace
Location
ResourceGroup
Subscription
Directory
LAW-RG-lab
eastus
rg-lab
Azure subscription 1
Default Directory
Add
Cancel

azure-soc-honeynet / geoip-summarized.csv
kphillip1 Add files via upload
Code
Blame
2.65 MB
View raw
(Sorry about that, but we can't show files that are this big right now.)
README.md
Sentinel-Analytics-Rules(KQL Alert...
Xpath.txt
geoip-summarized.csv
linux-ssh-auth-fail.json
mssql-auth-fail.json
nsg-malicious-allowed-in.json

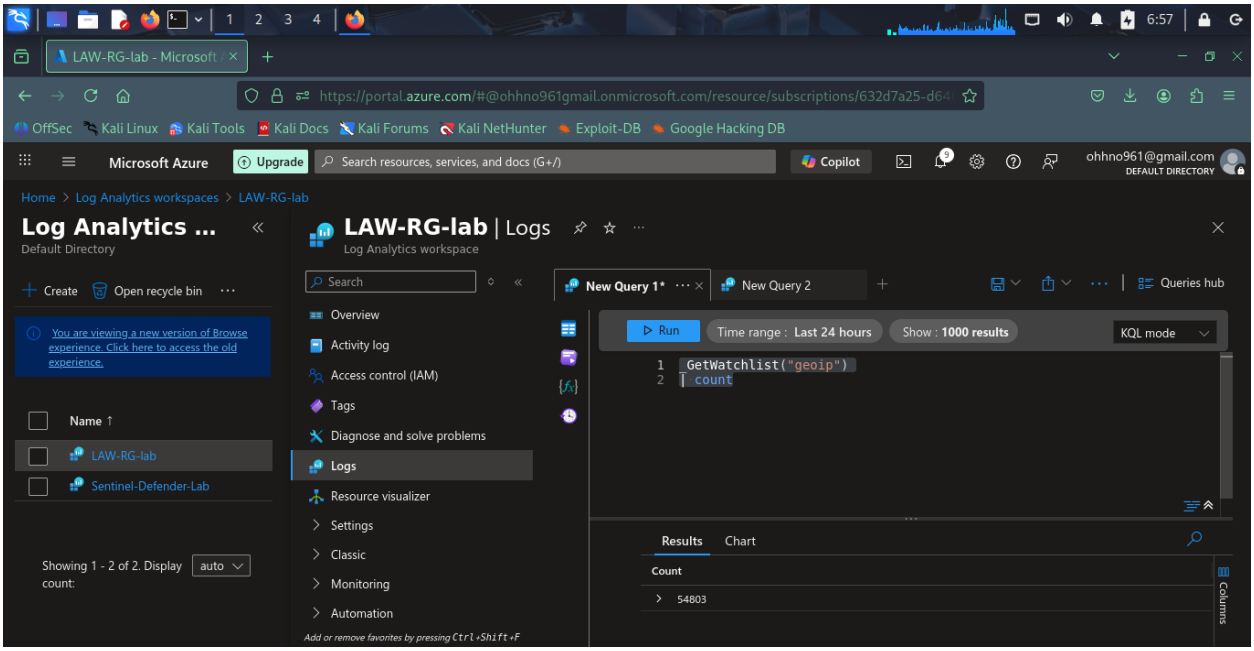

Watchlist wizard - Micros
azure-soc-honeynet/geoi
https://portal.azure.com/#view/Microsoft_Azure_SentinelUS/CreateWatchlistWizard.ReactView/subs
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Watchlist >
Watchlist wizard
General
Source
Review + create
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
File preview | First 50 rows and first 5 columns
network
latitude
longitude
cityname
countryname
1.0.0.0/16
-33.494
143.2104
Australia
1.1.0.0/16
17.8148
103.3386
Ban Chan
Thailand
1.2.0.0/16
13.8667
100.1917
Nakhon Pathom
Thailand
1.3.0.0/16
13.8679
100.1891
Nakhon Pathom
Thailand
1.4.0.0/16
13.6687
100.579
Bangkok
Thailand
< Previous
Next : Review + create >
Give feedback

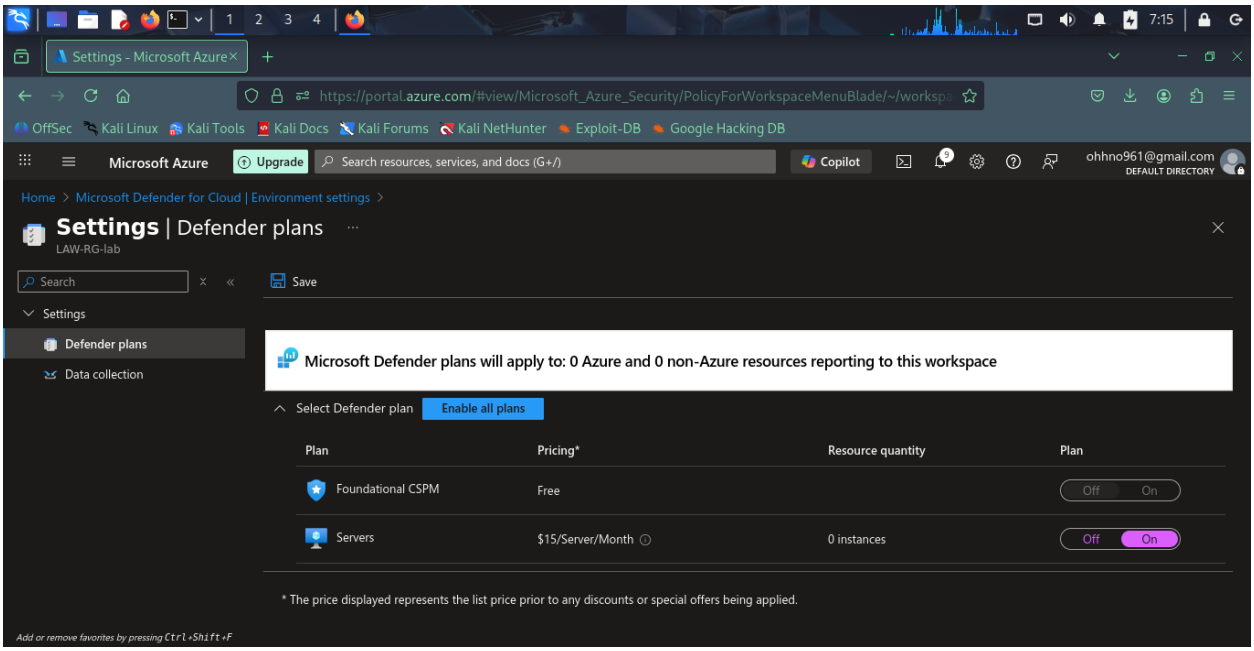

Watchlist wizard - Micros
azure-soc-honeynet/geoi
https://portal.azure.com/#view/Microsoft_Azure_SentinelUS/CreateWatchlistWizard.ReactView/subs
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Watchlist >
Watchlist wizard
General
Source
Review + create
Drag and drop the files or
Browse for files
SearchKey *
network
Reset
network
latitude
longitude
cityname
countryname
1.22.0.0/16
12.9634
77.5855
Bengaluru
India
1.23.0.0/16
19.1963
72.9675
Thane
India
1.24.0.0/16
19.1954
72.9646
Thane
India
1.25.0.0/16
19.195
72.969
Thane
India
1.26.0.0/16
19.1874
72.965
Thane
India
1.27.0.0/16
19.2048
72.9588
Thane
India
1.28.0.0/16
19.1879
72.9592
Thane
India
< Previous
Next : Review + create >
Give feedback

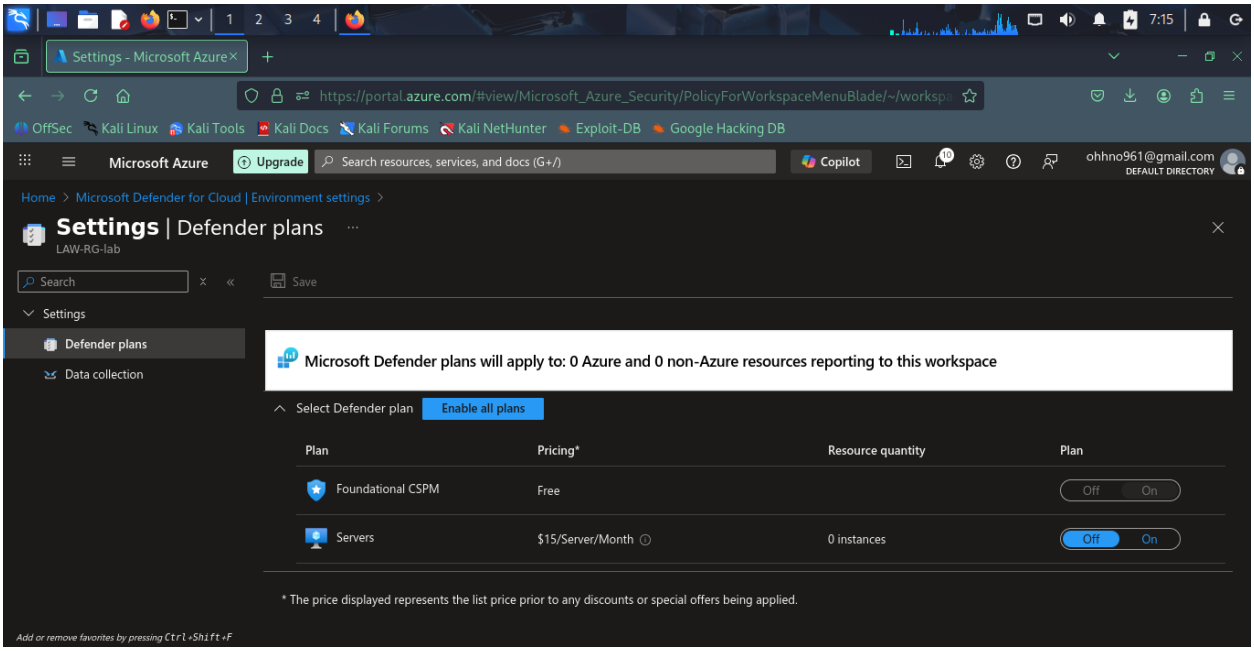

Microsoft Sentinel - Micr
azure-soc-honeynet/geoi
https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/Watchlist/subs
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel
Microsoft Sentinel | Watchlist
Selected workspace: 'law-rg-lab'
Search
Refresh
New
Delete
Update watchlist
Columns
Guides & Feedback
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
Watchlist
Automation
Settings
0
Watchlists
0
Watchlist Items
My Watchlists
Templates (Preview)
Search by name, alias and description
Add filter
Name
Alias
Source
Create...
Last u...
geoip
geoip
geoip-summarized.csv
7/25/2025
7/25/2025
Add or remove favorites by pressing Ctrl+Shift+F

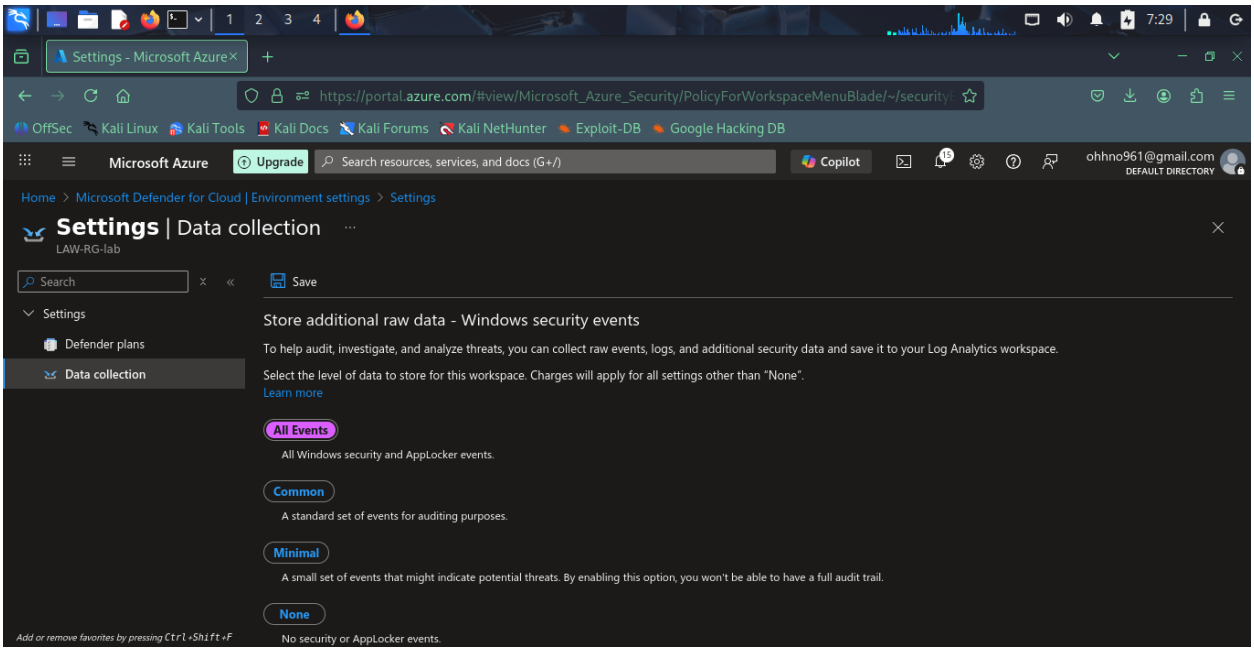

LAW-RG-lab - Microsoft
https://portal.azure.com/#@ohhno961gmail.onmicrosoft.com/resource/subscriptions/632d7a25-d64
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Log Analytics workspaces > LAW-RG-lab
Log Analytics ...
Default Directory
Create
Open recycle bin
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
LAW-RG-lab
Sentinel-Defender-Lab
Showing 1 - 2 of 2. Display count:
auto
LAW-RG-lab | Logs
Log Analytics workspace
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
New Query 1*
New Query 2
Queries hub
Watchlist
Time range : Last 24 hours
Simple mode
Show : 1000 results
Add
Results
Chart
TimeGenerated [UTC]
AzureTenantId
WatchlistId
7/25/2025, 4:51:36.299 PM
f8949756-0e91-46dd-b912-aac4b2c5dc18
8d073b22-a8ea-42e8-92d5-6c
Columns
Add or remove favorites by pressing Ctrl+Shift+F

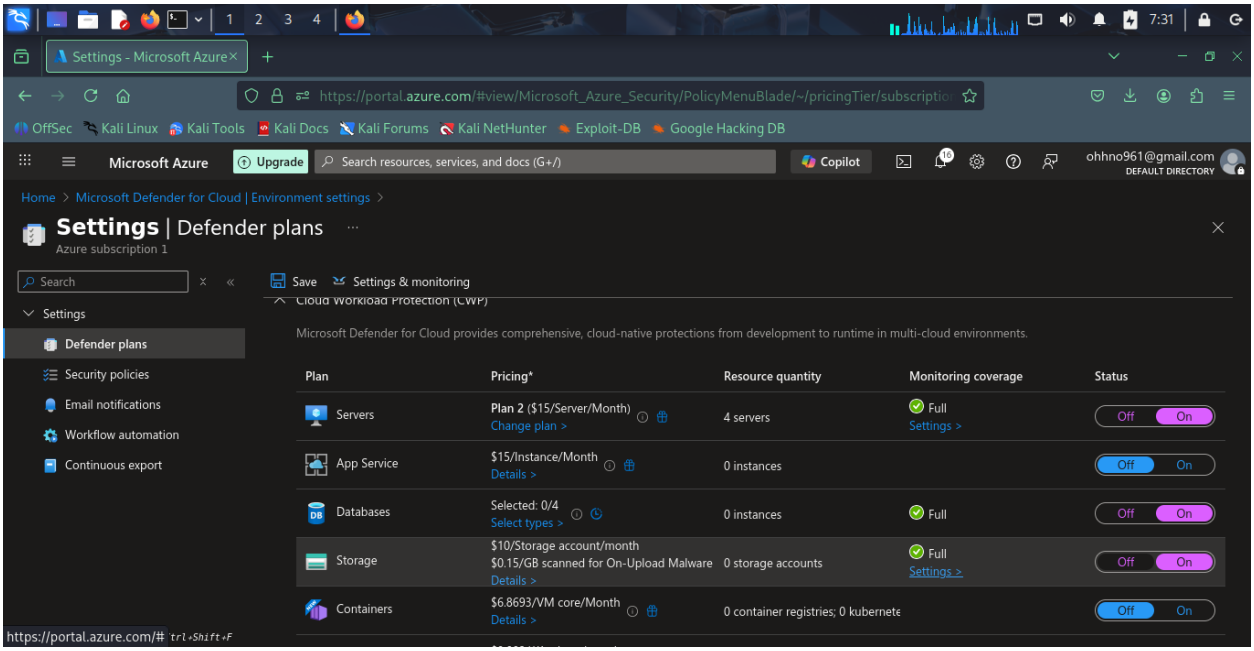

LAW-RG-lab - Microsoft
https://portal.azure.com/#@ohhno961gmail.onmicrosoft.com/resource/subscriptions/632d7a25-d64
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Log Analytics workspaces > LAW-RG-lab
Log Analytics ...
Default Directory
Create
Open recycle bin
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
LAW-RG-lab
Sentinel-Defender-Lab
Showing 1 - 2 of 2. Display count:
auto
LAW-RG-lab | Logs
Log Analytics workspace
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
Add or remove favorites by pressing Ctrl+Shift+F
New Query 1*
New Query 2
Queries hub
Run
Time range : Last 24 hours
Show : 1000 results
KQL mode
1 GetWatchlist("geoip")
2 | count
Results
Chart
Count
50000
Columns

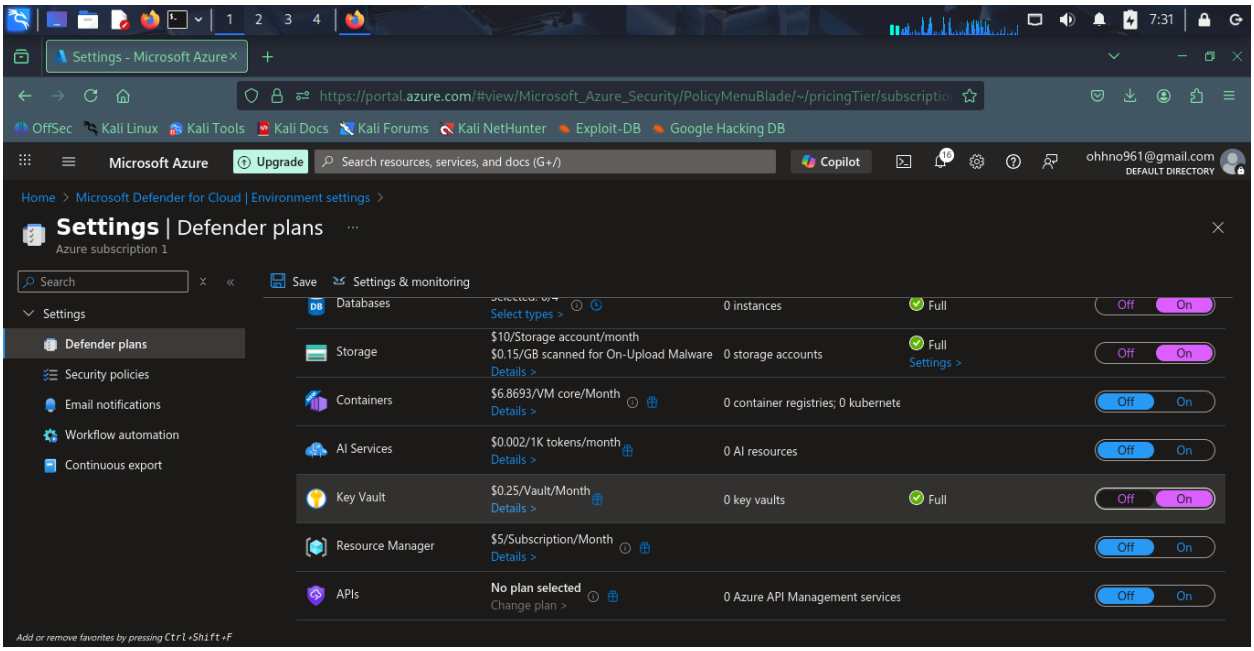

LAW-RG-lab - Microsoft
https://portal.azure.com/#@ohhno961gmail.onmicrosoft.com/resource/subscriptions/632d7a25-d64
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Log Analytics workspaces > LAW-RG-lab
Log Analytics ...
Default Directory
Create
Open recycle bin
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
LAW-RG-lab
Sentinel-Defender-Lab
Showing 1 - 2 of 2. Display count:
auto
LAW-RG-lab | Logs
Log Analytics workspace
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
Add or remove favorites by pressing Ctrl+Shift+F
New Query 1*
New Query 2
Queries hub
Run
Time range : Last 24 hours
Show : 1000 results
KQL mode
1 GetWatchlist("geoip")
2 | count
Results
Chart
Count
54803
Columns


Settings - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Security/PolicyForWorkspaceMenuBlade/~/workspa
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Defender for Cloud | Environment settings >
Settings | Defender plans
LAW-RG-lab
Search
Save
Settings
Defender plans
Data collection
Microsoft Defender plans will apply to: 0 Azure and 0 non-Azure resources reporting to this workspace
Select Defender plan
Enable all plans
Plan
Pricing*
Resource quantity
Plan
Foundational CSPM
Free
Off
On
Servers
$15/Server/Month
0 instances
Off
On
* The price displayed represents the list price prior to any discounts or special offers being applied.
Add or remove favorites by pressing Ctrl+Shift+F


Settings - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Security/PolicyForWorkspaceMenuBlade/~/workspa
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Defender for Cloud | Environment settings >
Settings | Defender plans
LAW-RG-lab
Search
Save
Settings
Defender plans
Data collection
Microsoft Defender plans will apply to: 0 Azure and 0 non-Azure resources reporting to this workspace
Select Defender plan
Enable all plans
Plan
Pricing*
Resource quantity
Plan
Foundational CSPM
Free
Off
On
Servers
$15/Server/Month
0 instances
Off
On
* The price displayed represents the list price prior to any discounts or special offers being applied.
Add or remove favorites by pressing Ctrl+Shift+F


Settings - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Security/PolicyForWorkspaceMenuBlade/~/security
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Defender for Cloud | Environment settings > Settings
Settings | Data collection
LAW-RG-lab
Search
Save
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.
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.
Add or remove favorites by pressing Ctrl+Shift+F

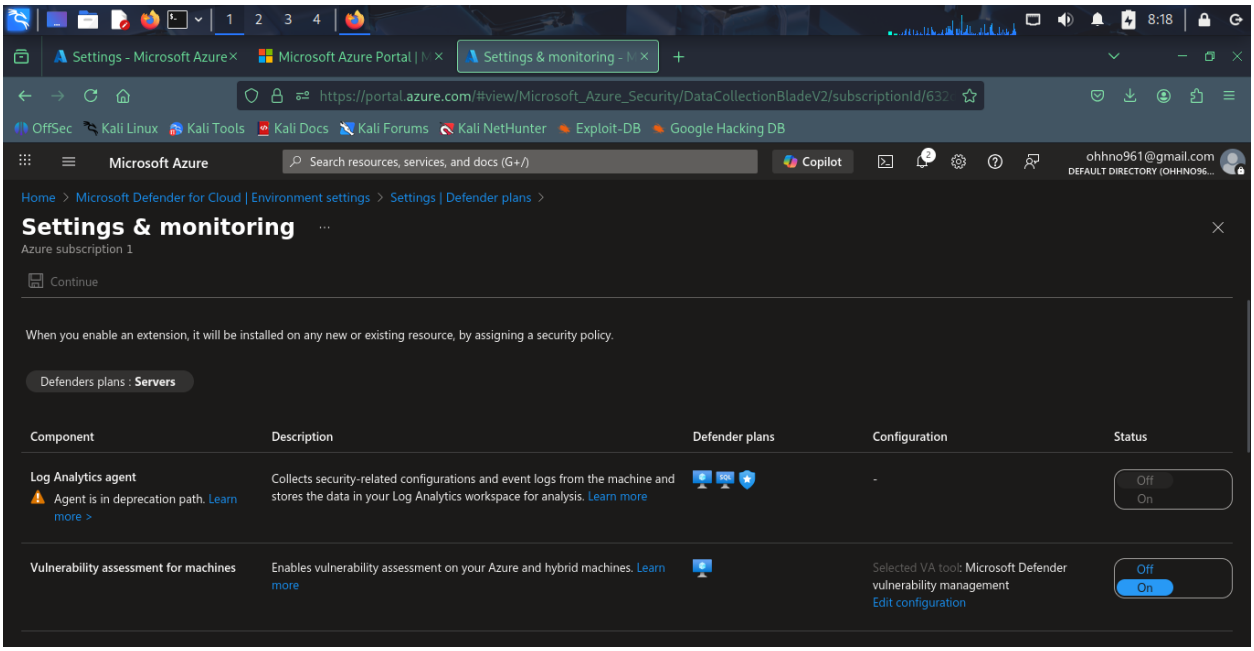
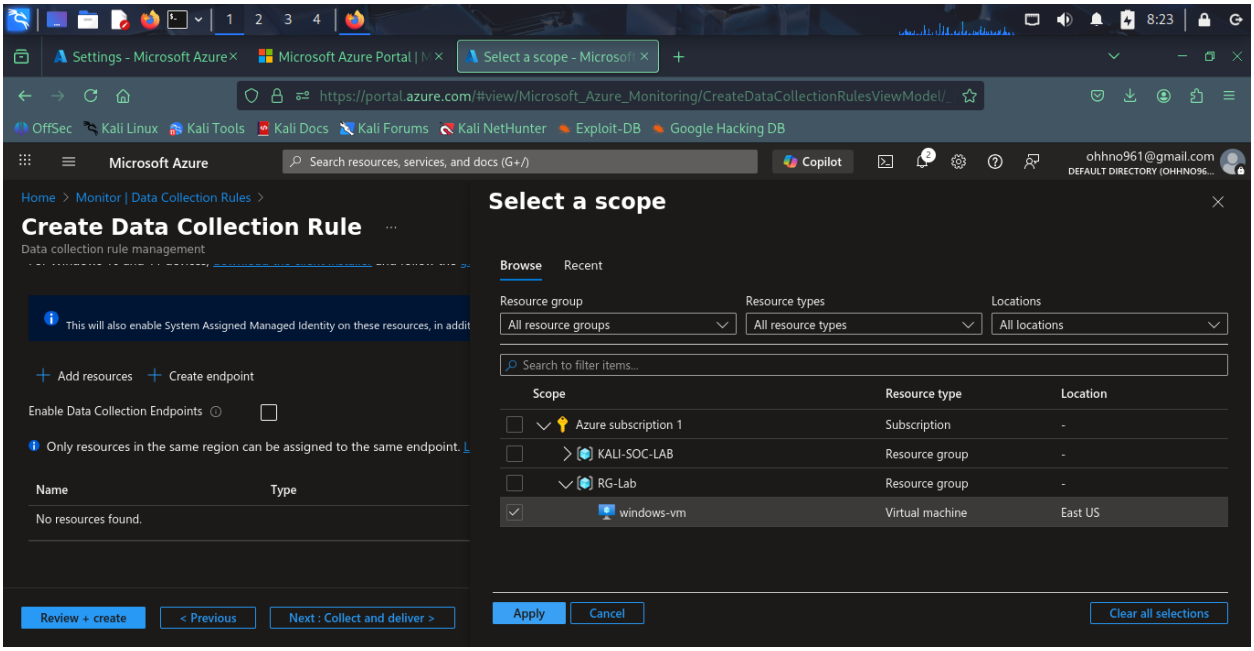

Settings - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Security/PolicyMenuBlade/~/pricingTier/subscriptio
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Defender for Cloud | Environment settings >
Settings | Defender plans
Azure subscription 1
Search
Save
Settings & monitoring
Settings
Defender plans
Security policies
Email notifications
Workflow automation
Continuous export
Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.
Plan
Pricing*
Resource quantity
Monitoring coverage
Status
Servers
Plan 2 ($15/Server/Month)
Change plan >
4 servers
Full
Settings >
Off On
App Service
$15/Instance/Month
Details >
0 instances
Off On
Databases
Selected: 0/4
Select types >
0 instances
Full
Off On
Storage
$10/Storage account/month
$0.15/GB scanned for On-Upload Malware
Details >
0 storage accounts
Full
Settings >
Off On
Containers
$6.8693/VM core/Month
Details >
0 container registries; 0 kubernete
Off On
https://portal.azure.com/# Ctrl+Shift+F

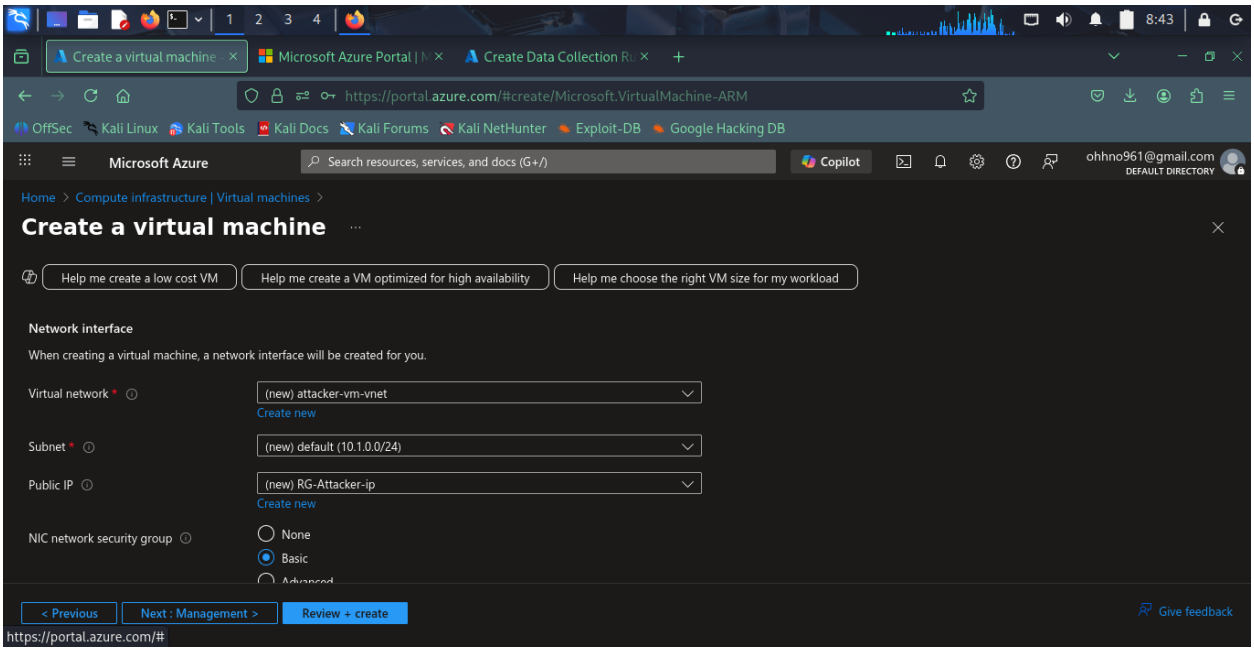


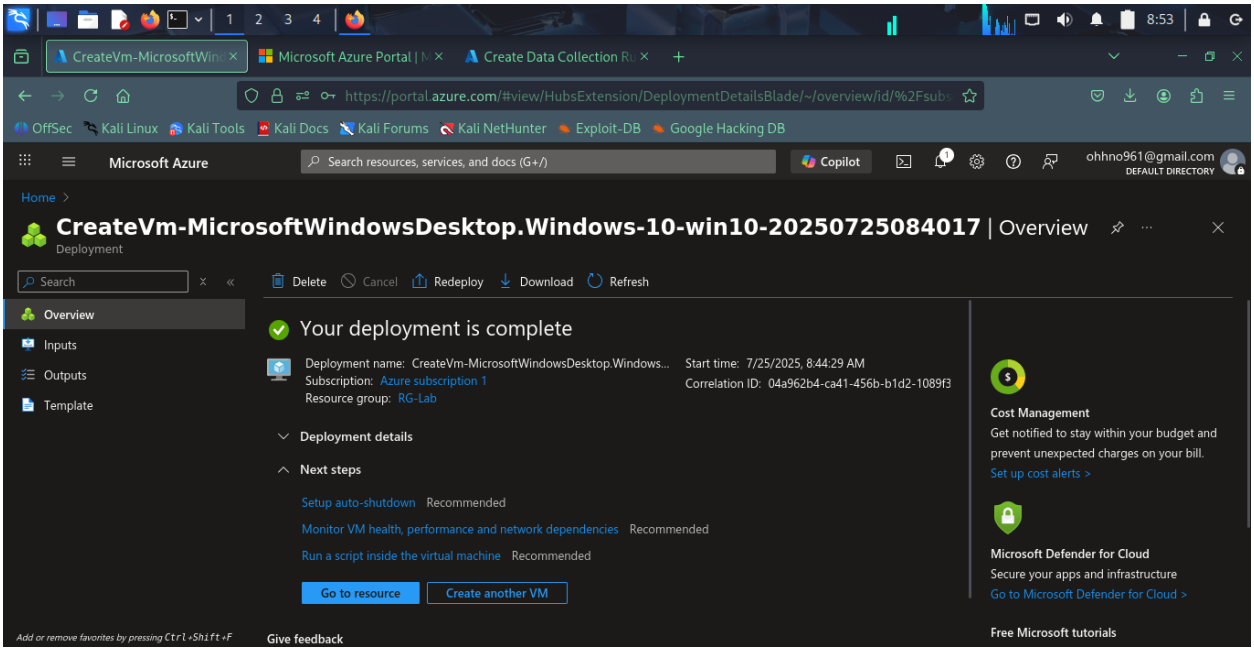
- **7. Deployment Challenges**

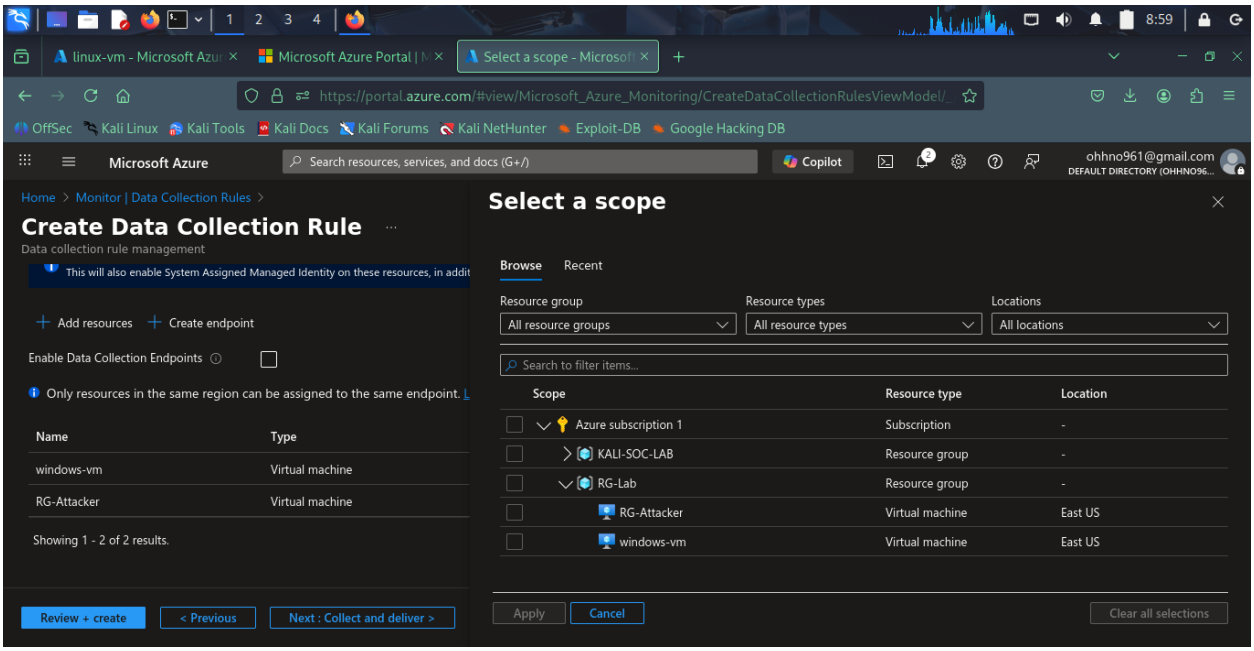
Issue	Attempted Fix	Outcome
NSG Flow Logs not available	Tried setting via Diagnostic Settings	Feature deprecated; failed to activate
Log Analytics Agent could not be deployed	Tried using Data Collection Rules (DCR) for each VM	Partially configured; not fully functional
Event Hub setup	Created namespace	Did not proceed with integration
Azure CLI on VMs	Tried SSH and manual configuration	Unsuccessful

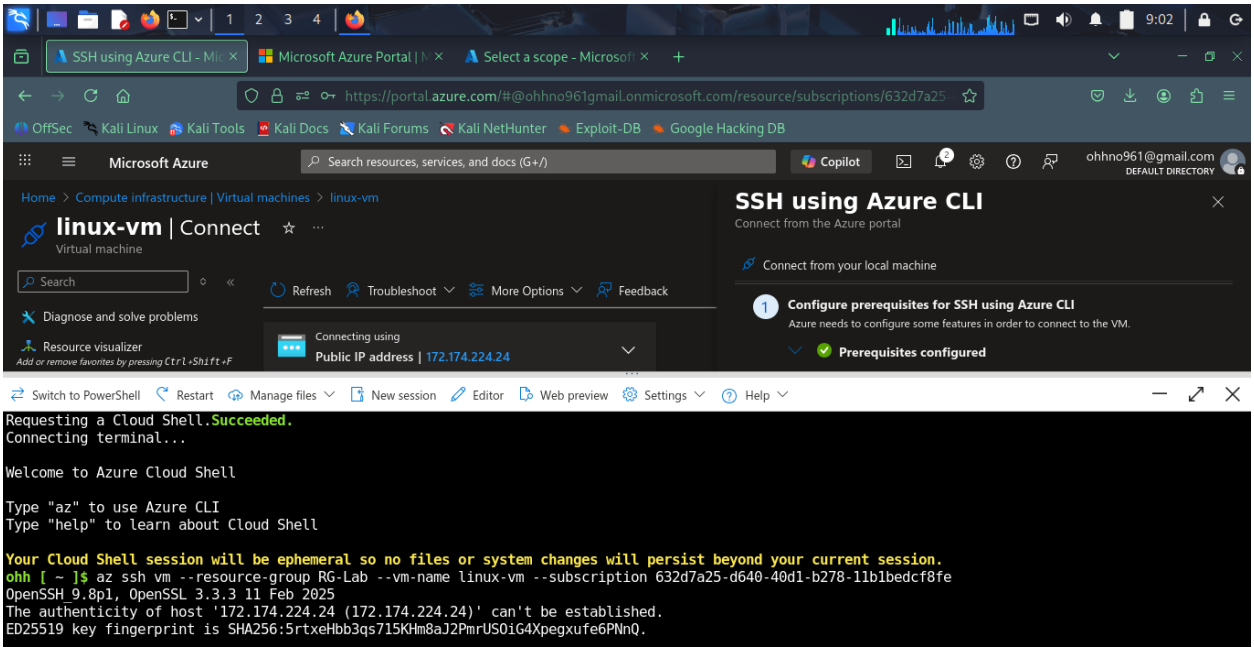
- ---

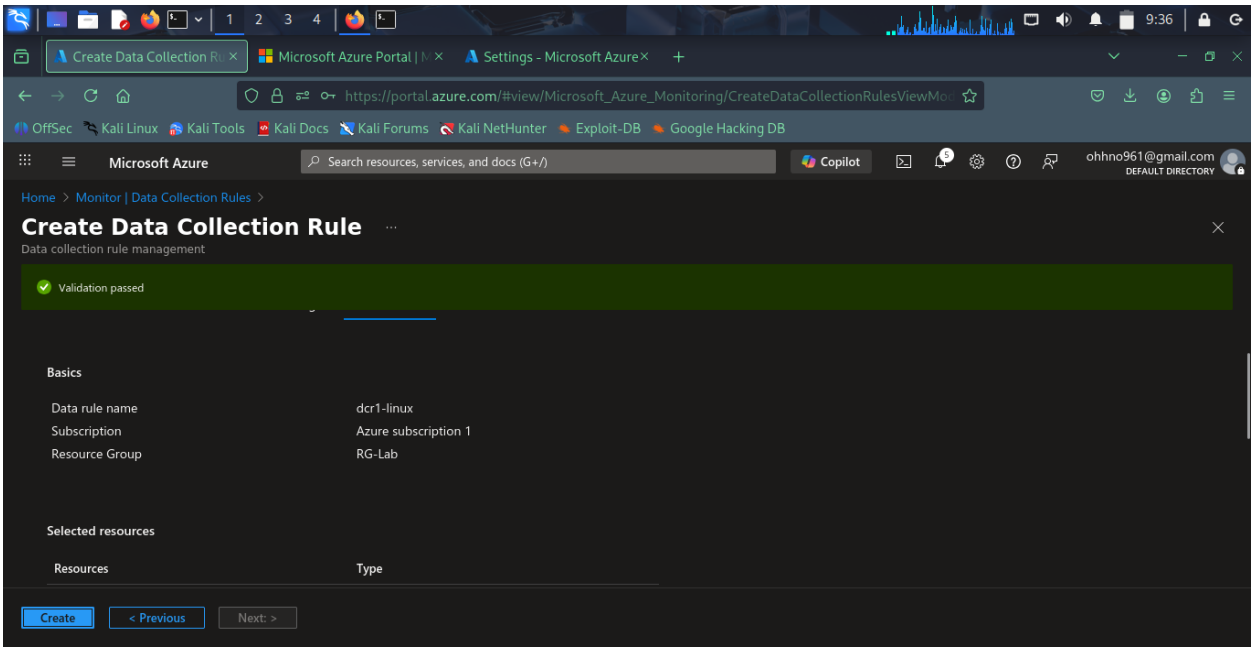
- 
Settings - Microsoft Azure
Microsoft Azure Portal
Settings & monitoring
https://portal.azure.com/#view/Microsoft_Azure_Security/DataCollectionBladeV2/subscriptionId/632
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
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.
Defenders plans : Servers
Component
Description
Defender plans
Configuration
Status
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
-
Off
On
Vulnerability assessment for machines
Enables vulnerability assessment on your Azure and hybrid machines. Learn more
Selected VA tool: Microsoft Defender vulnerability management
Edit configuration
Off
On
- 
Settings - Microsoft Azure
Microsoft Azure Portal
Select a scope - Microsoft
https://portal.azure.com/#view/Microsoft_Azure_Monitoring/CreateDataCollectionRulesViewModel/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Monitor | Data Collection Rules >
Create Data Collection Rule
Data collection rule management
This will also enable System Assigned Managed Identity on these resources, in addit
Add resources
Create endpoint
Enable Data Collection Endpoints
Only resources in the same region can be assigned to the same endpoint.
Name
Type
No resources found.
Review + create
< Previous
Next : Collect and deliver >
Select a scope
Browse
Recent
Resource group
All resource groups
Resource types
All resource types
Locations
All locations
Search to filter items...
Scope
Resource type
Location
Azure subscription 1
Subscription
KALI-SOC-LAB
Resource group
RG-Lab
Resource group
windows-vm
Virtual machine
East US
Apply
Cancel
Clear all selections

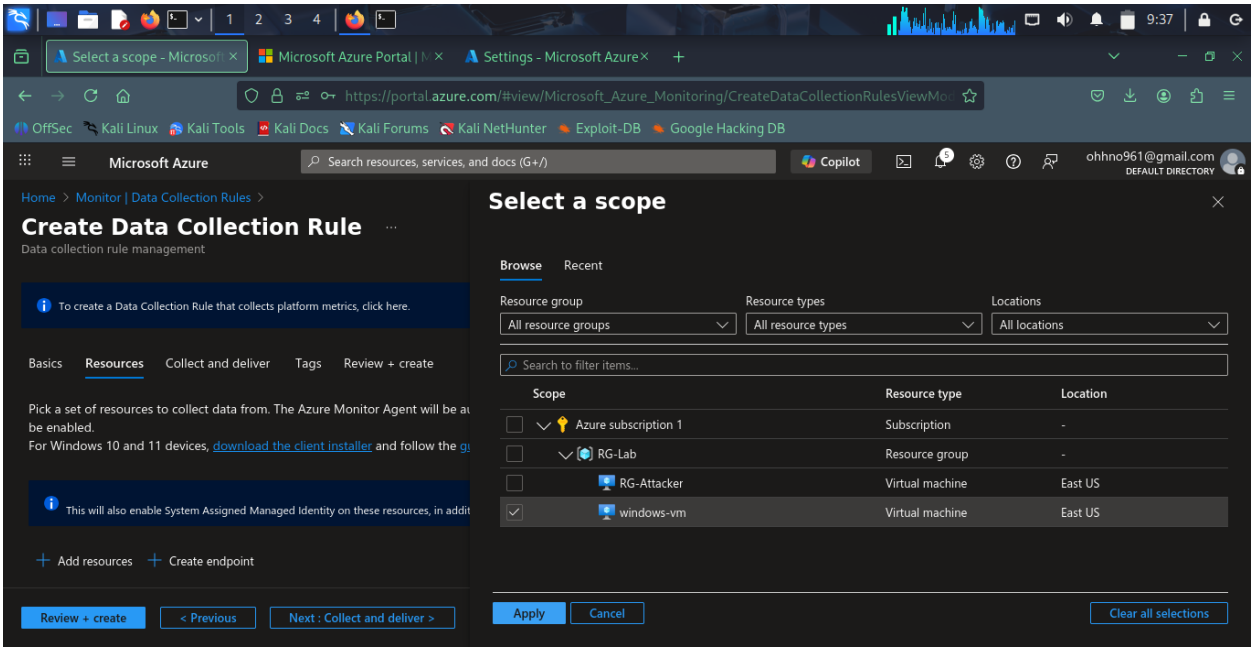

Create a virtual machine
Microsoft Azure Portal
Create Data Collection
https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Compute infrastructure | Virtual machines >
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Network interface
When creating a virtual machine, a network interface will be created for you.
Virtual network *
(new) attacker-vm-vnet
Create new
Subnet *
(new) default (10.1.0.0/24)
Public IP
(new) RG-Attacker-ip
Create new
NIC network security group
None
Basic
Advanced
< Previous
Next : Management >
Review + create
Give feedback
https://portal.azure.com/#

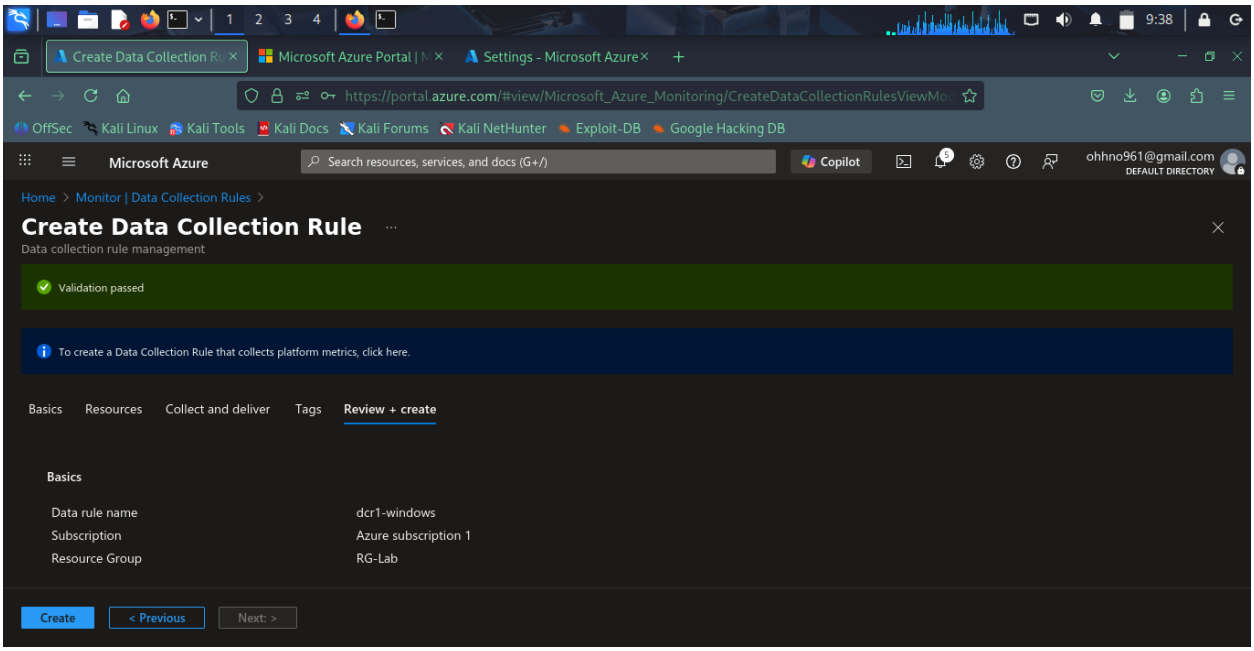

CreateVm-MicrosoftWin
Microsoft Azure Portal
Create Data Collection
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubs
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home >
CreateVm-MicrosoftWindowsDesktop.Windows-10-win10-20250725084017 | Overview
Deployment
Search
Delete
Cancel
Redeploy
Download
Refresh
Overview
Inputs
Outputs
Template
Your deployment is complete
Deployment name: CreateVm-MicrosoftWindowsDesktop.Windows...
Subscription: Azure subscription 1
Resource group: RG-Lab
Start time: 7/25/2025, 8:44:29 AM
Correlation ID: 04a962b4-ca41-456b-b1d2-1089f3
Deployment details
Next steps
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended
Go to resource
Create another VM
Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Add or remove favorites by pressing Ctrl+Shift+F
Give feedback

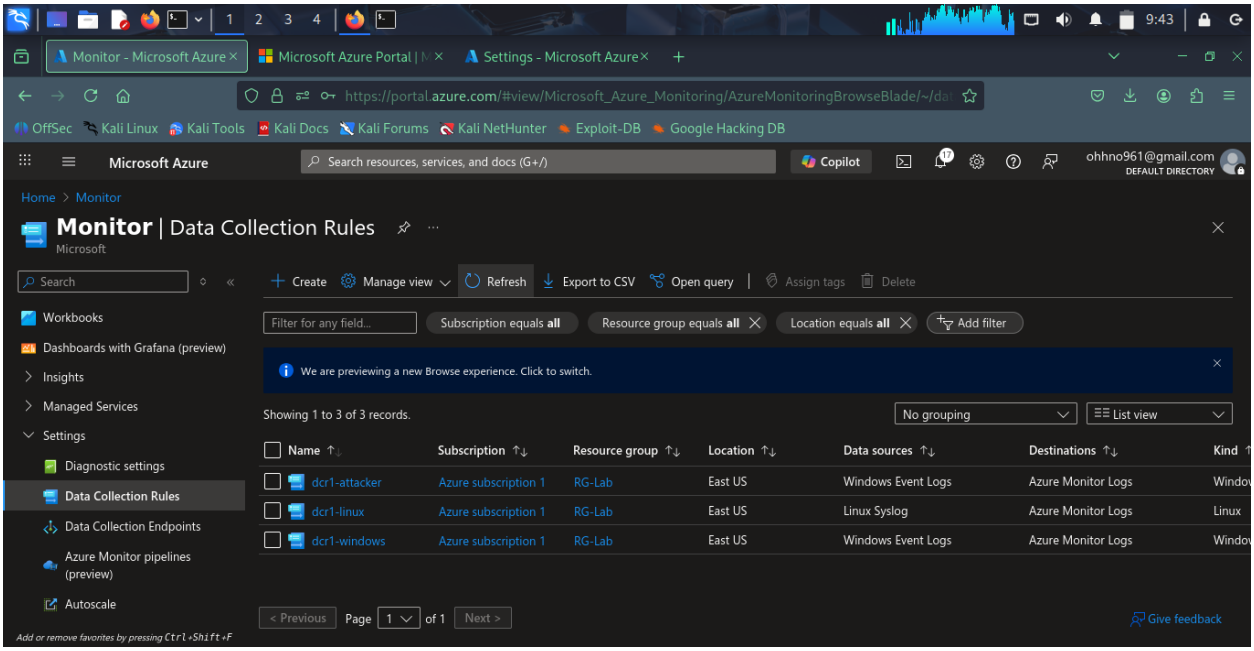

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Monitor | Data Collection Rules >
Create Data Collection Rule
Data collection rule management
This will also enable System Assigned Managed Identity on these resources, in addit
Add resources
Create endpoint
Enable Data Collection Endpoints
Only resources in the same region can be assigned to the same endpoint.
Name
Type
windows-vm
Virtual machine
RG-Attacker
Virtual machine
Showing 1 - 2 of 2 results.
Review + create
< Previous
Next : Collect and deliver >
Select a scope
Browse
Recent
Resource group
All resource groups
Resource types
All resource types
Locations
All locations
Search to filter items...
Scope
Resource type
Location
Azure subscription 1
Subscription
KALI-SOC-LAB
Resource group
RG-Lab
Resource group
RG-Attacker
Virtual machine
East US
windows-vm
Virtual machine
East US
Apply
Cancel
Clear all selections

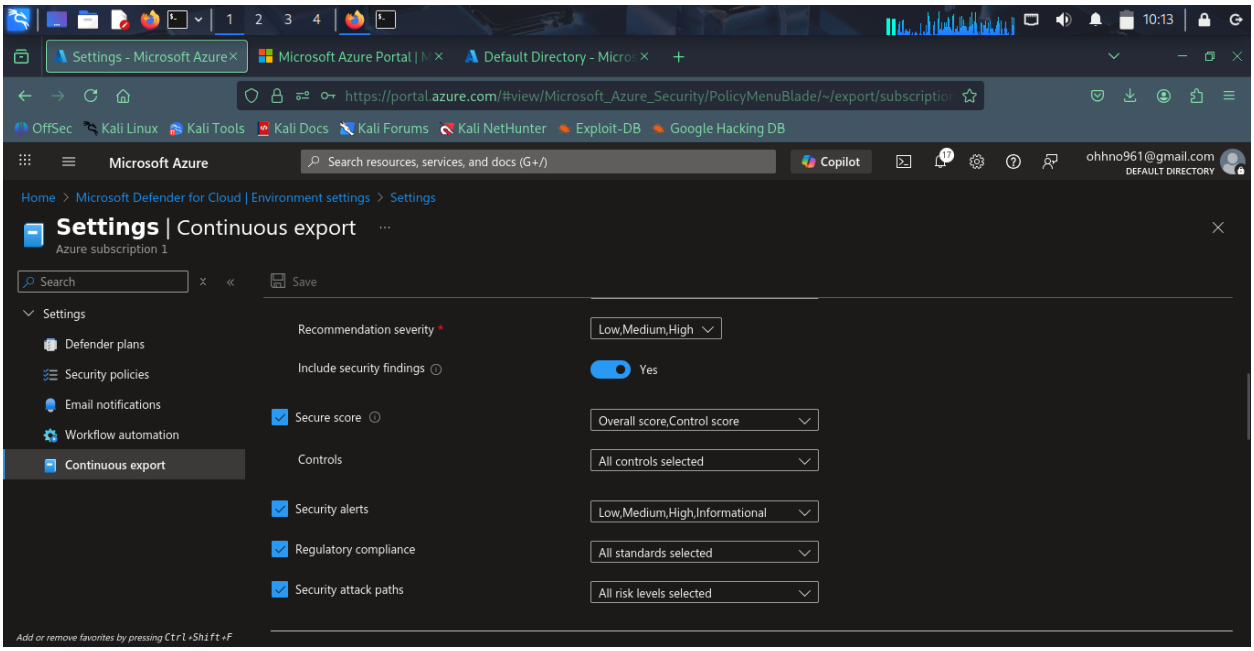

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Compute infrastructure | Virtual machines > linux-vm
linux-vm | Connect
Virtual machine
Search
Diagnose and solve problems
Resource visualizer
Refresh
Troubleshoot
More Options
Feedback
Connecting using
Public IP address | 172.174.224.24
SSH using Azure CLI
Connect from the Azure portal
Connect from your local machine
Configure prerequisites for SSH using Azure CLI
Azure needs to configure some features in order to connect to the VM.
Prerequisites configured
Switch to PowerShell
Restart
Manage files
New session
Editor
Web preview
Settings
Help
Requesting a Cloud Shell.Succeeded.
Connecting terminal...
Welcome to Azure Cloud Shell
Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell
Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
ohh [~]$ az ssh vm --resource-group RG-Lab --vm-name linux-vm --subscription 632d7a25-d640-40d1-b278-11b1bedcf8fe
OpenSSH_9.8p1, OpenSSL 3.3.3 11 Feb 2025
The authenticity of host '172.174.224.24 (172.174.224.24)' can't be established.
ED25519 key fingerprint is SHA256:5rtxeHbb3qs715KHm8aJ2PmrUSOiG4Xpegxufe6PNnQ.

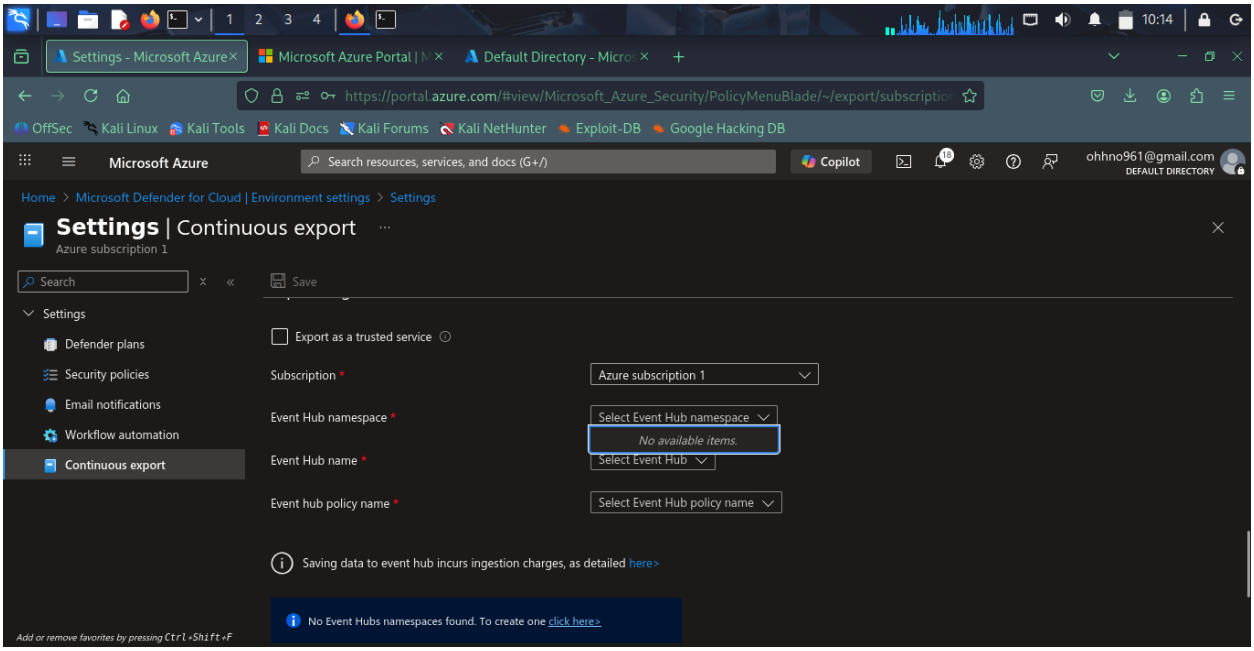

Create Data Collection R
Microsoft Azure Portal |
Settings - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Monitoring/CreateDataCollectionRulesViewMod
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Monitor | Data Collection Rules >
Create Data Collection Rule
Data collection rule management
Validation passed
Basics
Data rule name
dcr1-linux
Subscription
Azure subscription 1
Resource Group
RG-Lab
Selected resources
Resources
Type
Create
< Previous
Next: >

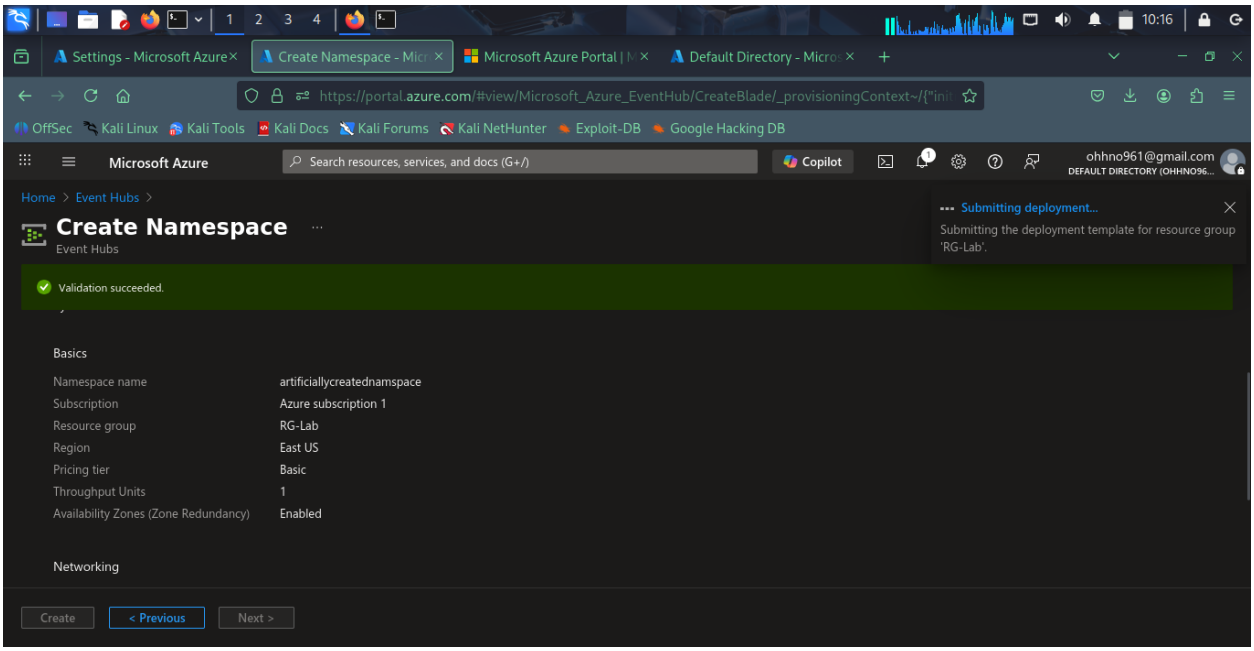

Select a scope - Microsoft
Microsoft Azure Portal |
Settings - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Monitoring/CreateDataCollectionRulesViewMod
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Monitor | Data Collection Rules >
Create Data Collection Rule
Data collection rule management
To create a Data Collection Rule that collects platform metrics, click here.
Basics
Resources
Collect and deliver
Tags
Review + create
Pick a set of resources to collect data from. The Azure Monitor Agent will be au
be enabled.
For Windows 10 and 11 devices, download the client installer and follow the g
This will also enable System Assigned Managed Identity on these resources, in addit
Add resources
Create endpoint
Review + create
< Previous
Next : Collect and deliver >
Select a scope
Browse
Recent
Resource group
All resource groups
Resource types
All resource types
Locations
All locations
Search to filter items...
Scope
Resource type
Location
Azure subscription 1
Subscription
-
RG-Lab
Resource group
-
RG-Attacker
Virtual machine
East US
windows-vm
Virtual machine
East US
Apply
Cancel
Clear all selections

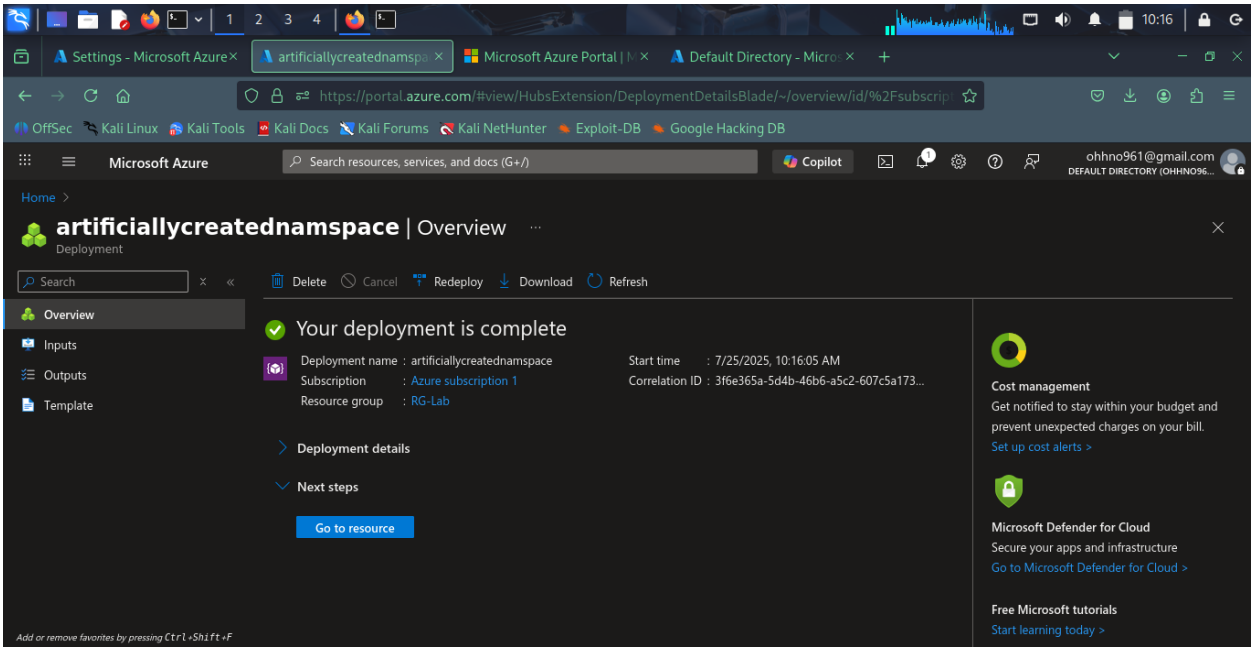

Create Data Collection Rule
Microsoft Azure Portal
Settings - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Monitoring/CreateDataCollectionRulesViewMod
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Monitor | Data Collection Rules >
Create Data Collection Rule
Data collection rule management
Validation passed
To create a Data Collection Rule that collects platform metrics, click here.
Basics Resources Collect and deliver Tags Review + create
Basics
Data rule name dcr1-windows
Subscription Azure subscription 1
Resource Group RG-Lab
Create
< Previous
Next: >

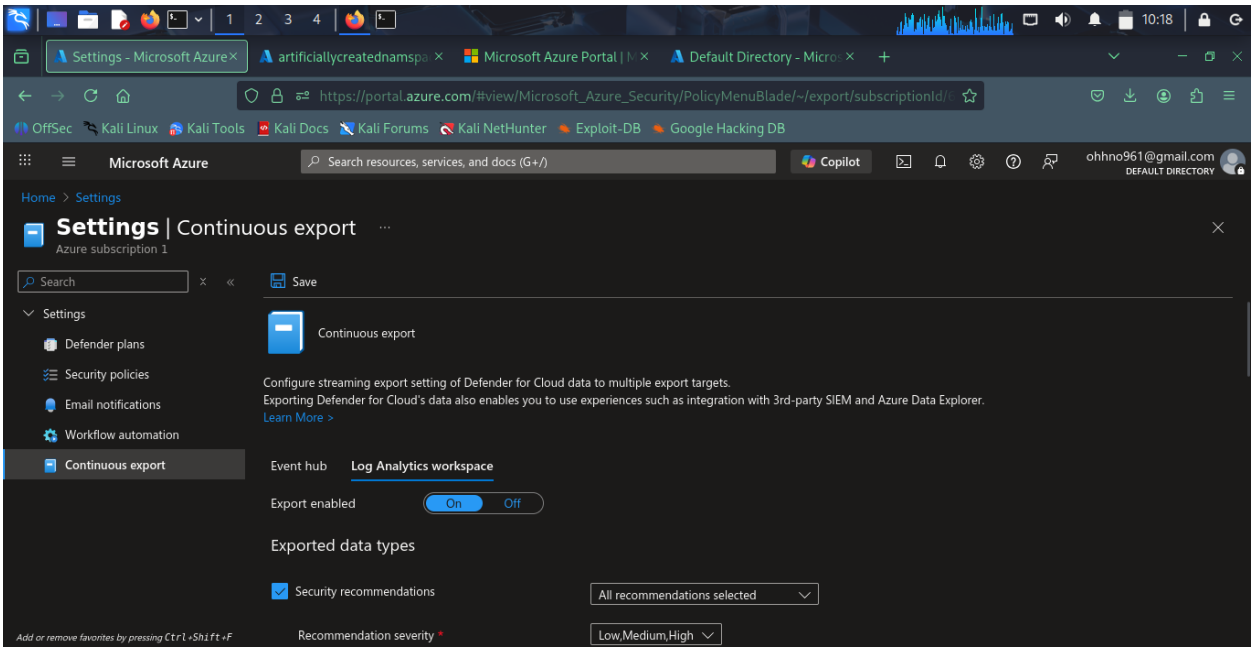

Monitor - Microsoft Azure
Microsoft Azure Portal
Settings - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Monitoring/AzureMonitoringBrowseBlade/~/da
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Monitor
Monitor | Data Collection Rules
Microsoft
Search
Workbooks
Dashboards with Grafana (preview)
Insights
Managed Services
Settings
Diagnostic settings
Data Collection Rules
Data Collection Endpoints
Azure Monitor pipelines (preview)
Autoscale
Add or remove favorites by pressing Ctrl+Shift+F
Create Manage view Refresh Export to CSV Open query Assign tags Delete
Filter for any field...
Subscription equals all
Resource group equals all
Location equals all
Add filter
We are previewing a new Browse experience. Click to switch.
Showing 1 to 3 of 3 records.
No grouping
List view
Name Subscription Resource group Location Data sources Destinations Kind
dcr1-attacker Azure subscription 1 RG-Lab East US Windows Event Logs Azure Monitor Logs
dcr1-linux Azure subscription 1 RG-Lab East US Linux Syslog Azure Monitor Logs Linux
dcr1-windows Azure subscription 1 RG-Lab East US Windows Event Logs Azure Monitor Logs
< Previous
Page 1 of 1
Next >
Give feedback

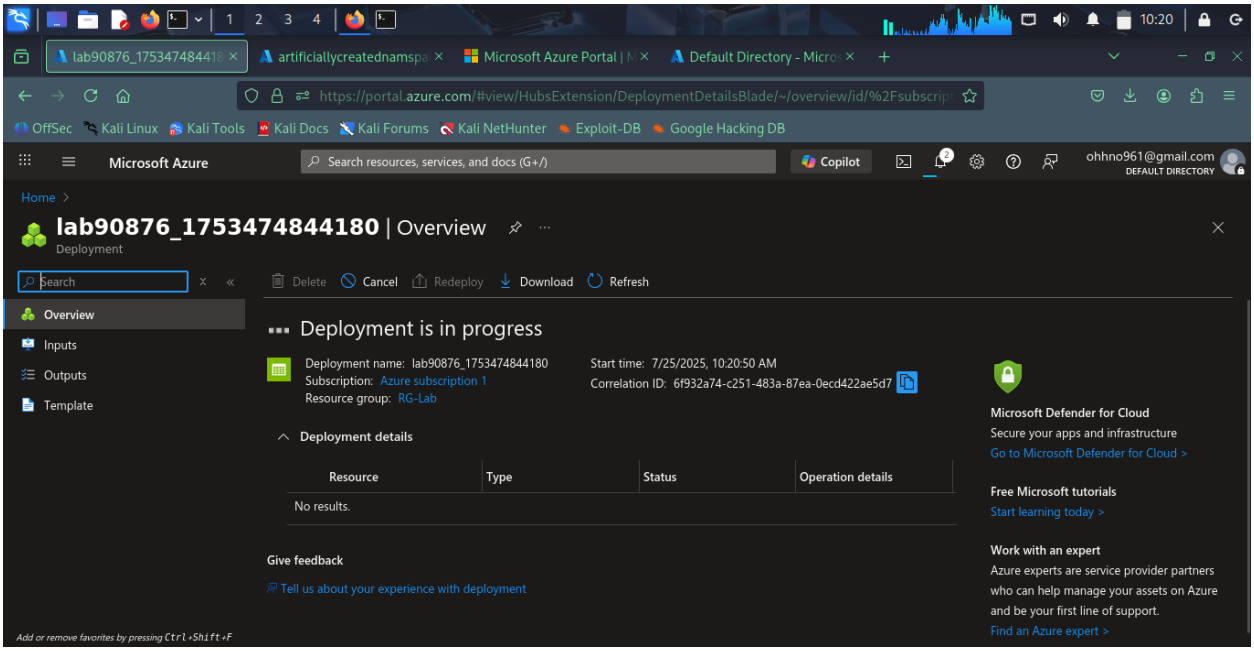

Settings - Microsoft Azure
Microsoft Azure Portal
Default Directory - Micro
https://portal.azure.com/#view/Microsoft_Azure_Security/PolicyMenuBlade/~/export/subscriptio
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Defender for Cloud | Environment settings > Settings
Settings | Continuous export
Azure subscription 1
Search
Save
Settings
Defender plans
Security policies
Email notifications
Workflow automation
Continuous export
Recommendation severity *
Low,Medium,High
Include security findings
Yes
Secure score
Overall score,Control score
Controls
All controls selected
Security alerts
Low,Medium,High,Informational
Regulatory compliance
All standards selected
Security attack paths
All risk levels selected
Add or remove favorites by pressing Ctrl+Shift+F

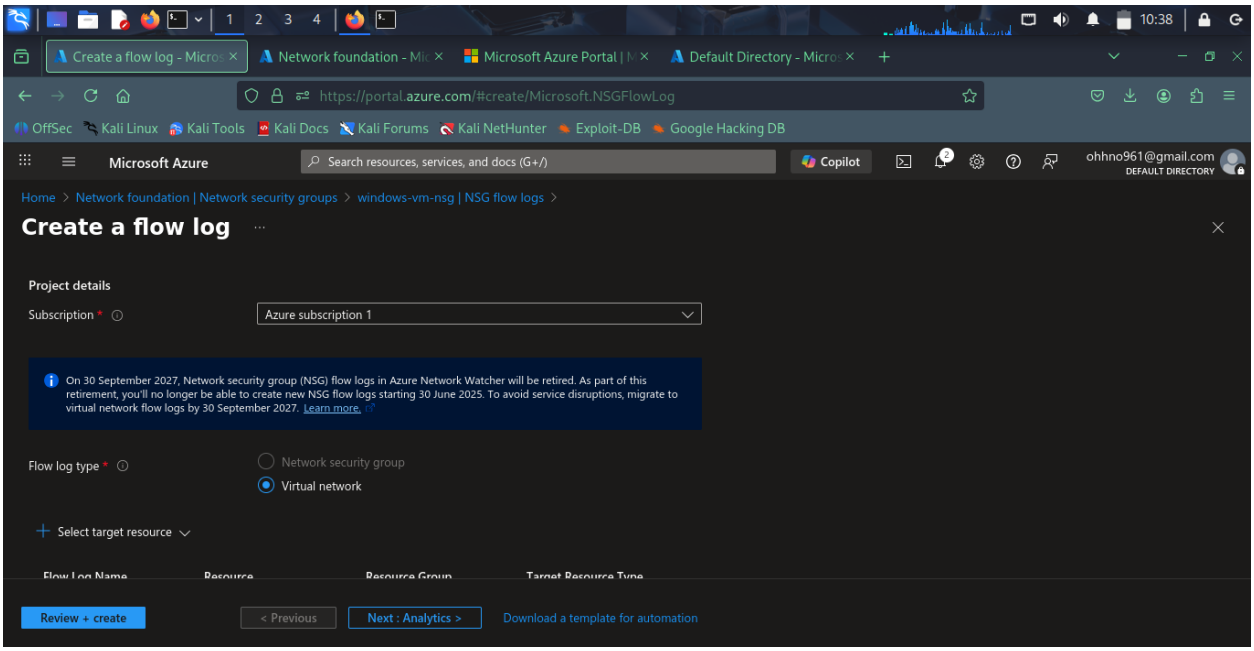

Settings - Microsoft Azure
Microsoft Azure Portal
Default Directory - Micro
https://portal.azure.com/#view/Microsoft_Azure_Security/PolicyMenuBlade/~/export/subscriptio
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Defender for Cloud | Environment settings > Settings
Settings | Continuous export
Azure subscription 1
Search
Save
Settings
Defender plans
Security policies
Email notifications
Workflow automation
Continuous export
Export as a trusted service
Subscription *
Azure subscription 1
Event Hub namespace *
Select Event Hub namespace
No available items.
Event Hub name *
Select Event Hub
Event hub policy name *
Select Event Hub policy name
Saving data to event hub incurs ingestion charges, as detailed here>
No Event Hubs namespaces found. To create one click here>
Add or remove favorites by pressing Ctrl+Shift+F

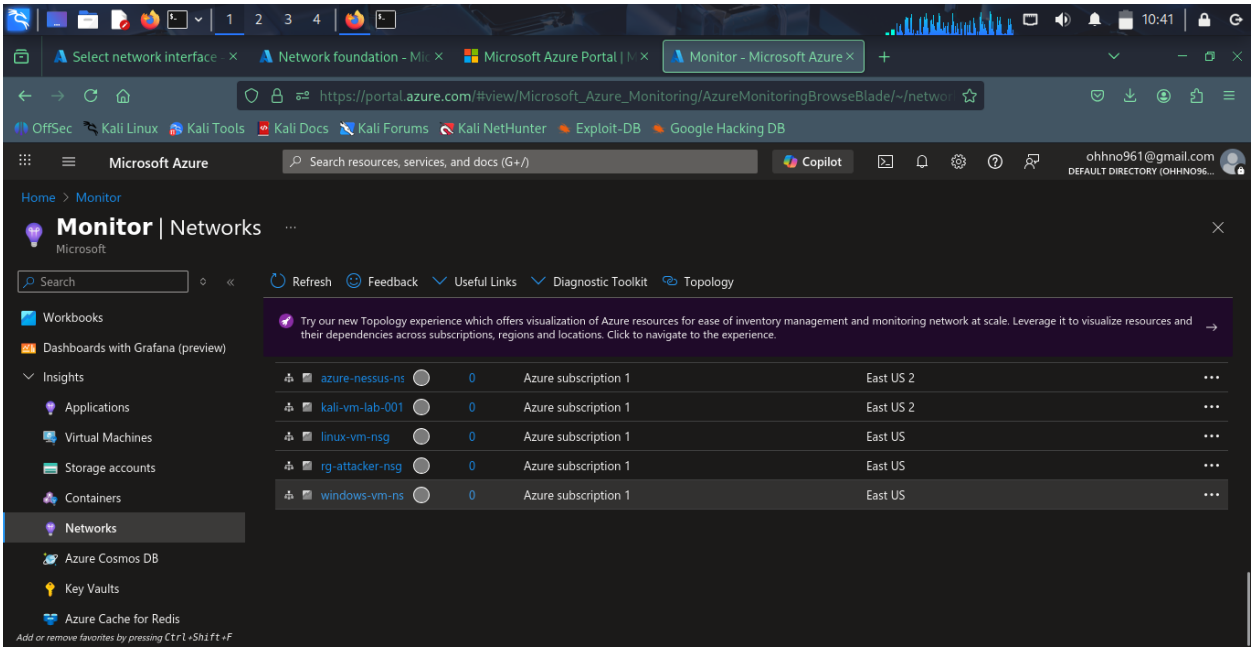

Settings - Microsoft Azure
Create Namespace - Micr
Microsoft Azure Portal | M
Default Directory - Micro
https://portal.azure.com/#view/Microsoft_Azure_EventHub/CreateBlade/_provisioningContext~/{"init
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Event Hubs >
Create Namespace
Event Hubs
Submitting deployment...
Submitting the deployment template for resource group 'RG-Lab'.
Validation succeeded.
Basics
Namespace name artificiallycreatednamspace
Subscription Azure subscription 1
Resource group RG-Lab
Region East US
Pricing tier Basic
Throughput Units 1
Availability Zones (Zone Redundancy) Enabled
Networking
Create
< Previous
Next >

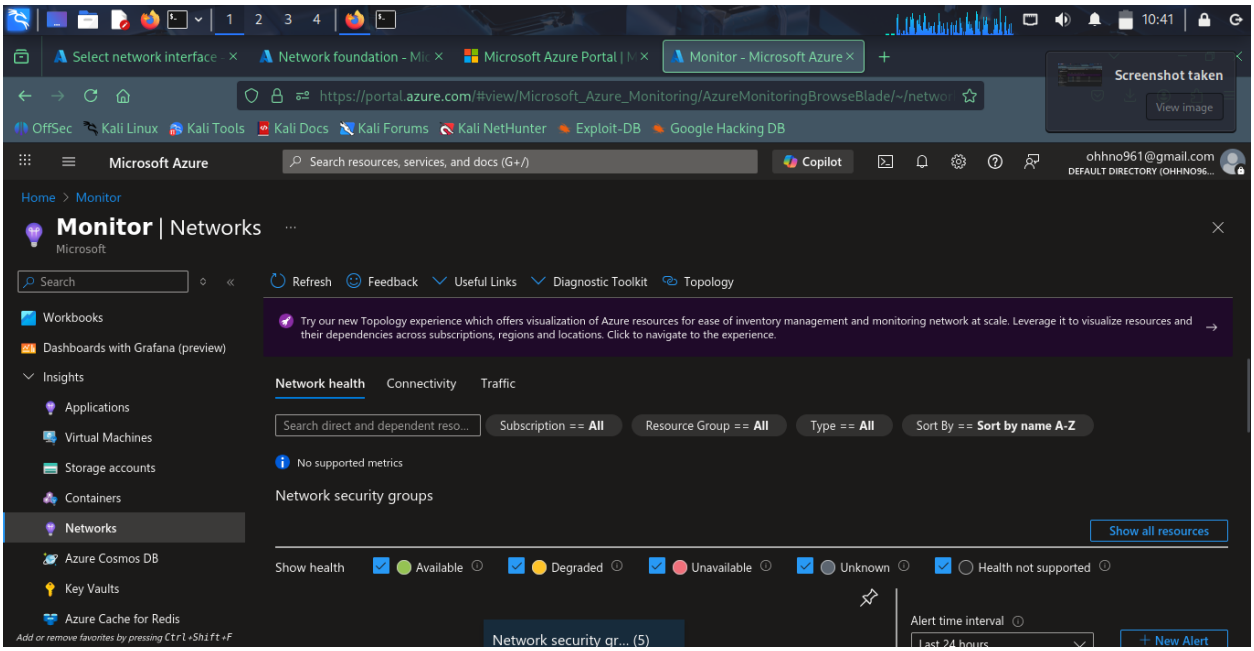

Settings - Microsoft Azure
artificiallycreatednamspa
Microsoft Azure Portal | M
Default Directory - Micro
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscript
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home >
artificiallycreatednamspace | Overview
Deployment
Search
Delete
Cancel
Redeploy
Download
Refresh
Overview
Inputs
Outputs
Template
Your deployment is complete
Deployment name : artificiallycreatednamspace
Subscription : Azure subscription 1
Resource group : RG-Lab
Start time : 7/25/2025, 10:16:05 AM
Correlation ID : 3f6e365a-5d4b-46b6-a5c2-607c5a173...
Deployment details
Next steps
Go to resource
Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Add or remove favorites by pressing Ctrl+Shift+F

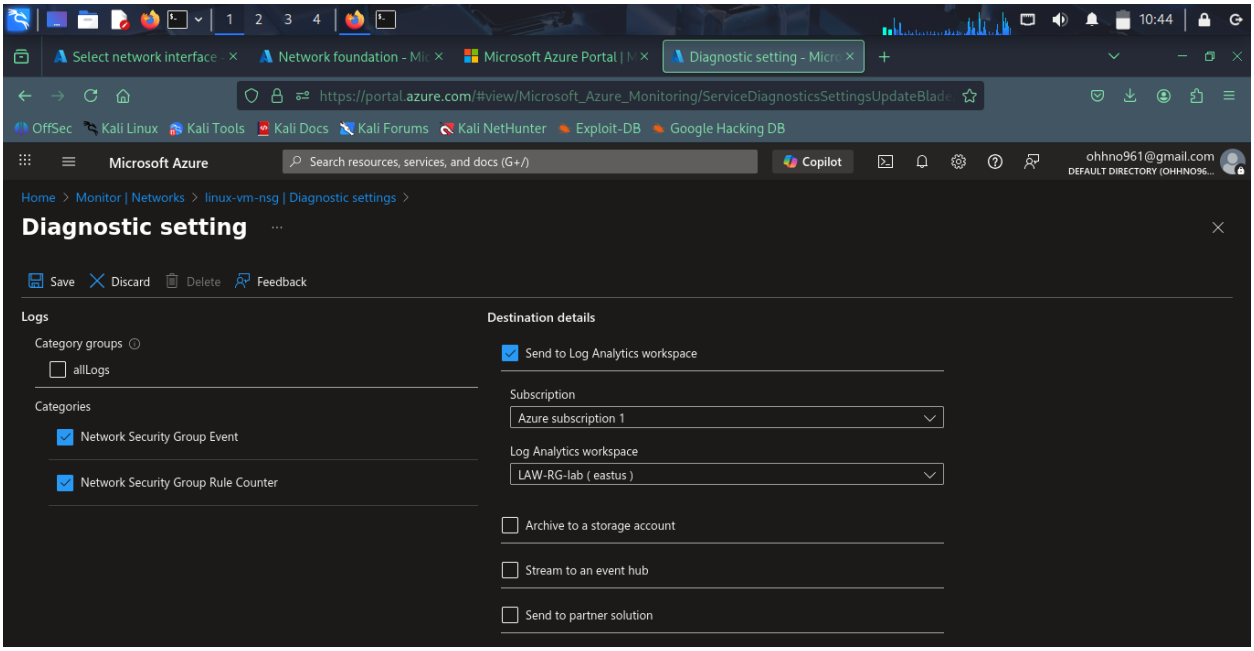

Settings - Microsoft Azure
Microsoft Azure Portal
Default Directory - Micro
https://portal.azure.com/#view/Microsoft_Azure_Security/PolicyMenuBlade/~/export/subscriptionId/
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Settings
Settings | Continuous export
Azure subscription 1
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
Off
Exported data types
Security recommendations
All recommendations selected
Recommendation severity *
Low,Medium,High
Add or remove favorites by pressing Ctrl+Shift+F

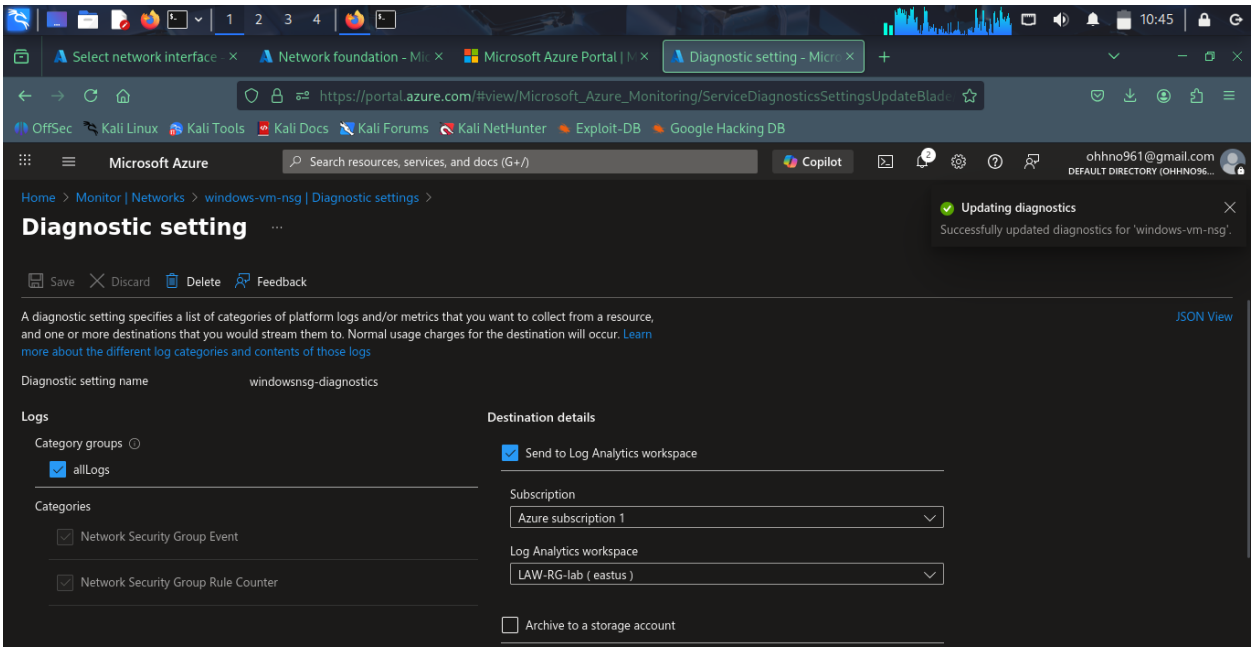

lab90876_1753474844180
artificiallycreatednamspa
Microsoft Azure Portal
Default Directory - Micro
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscript
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home >
lab90876_1753474844180 | Overview
Deployment
Search
Delete
Cancel
Redeploy
Download
Refresh
Overview
Inputs
Outputs
Template
Deployment is in progress
Deployment name: lab90876_1753474844180
Subscription: Azure subscription 1
Resource group: RG-Lab
Start time: 7/25/2025, 10:20:50 AM
Correlation ID: 6f932a74-c251-483a-87ea-0ecd422ae5d7
Deployment details
Resource
Type
Status
Operation details
No results.
Give feedback
Tell us about your experience with deployment
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >
Add or remove favorites by pressing Ctrl+Shift+F

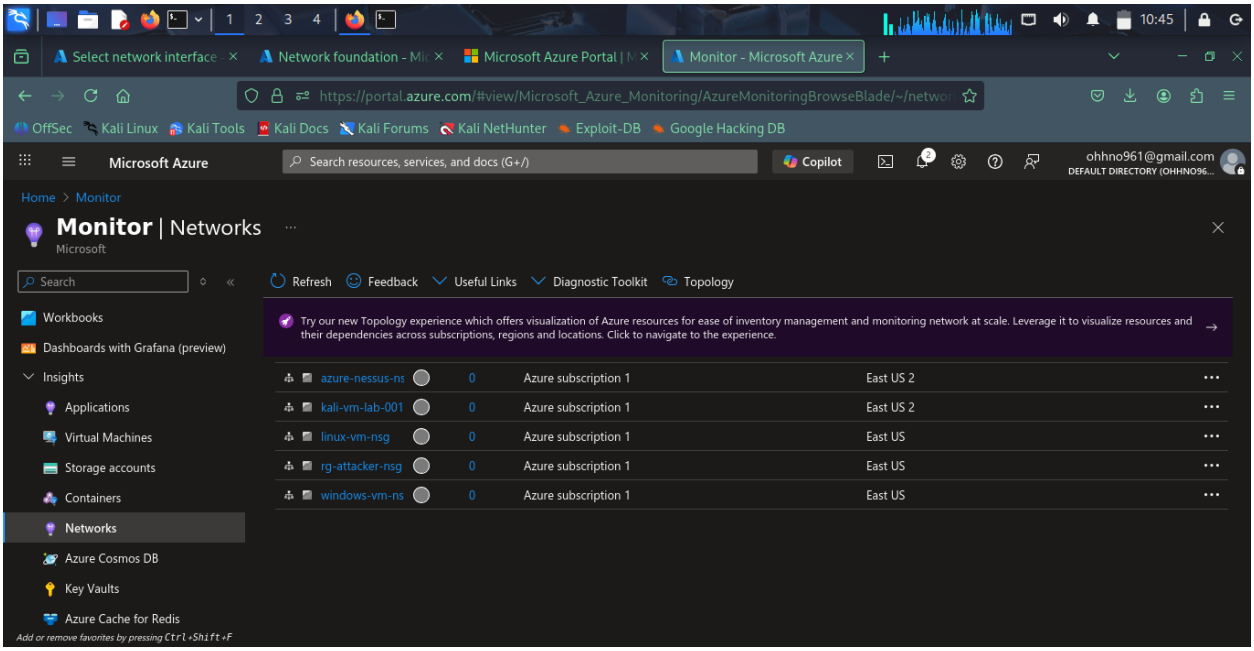

Create a flow log - Micros
Network foundation - Mic
Microsoft Azure Portal | M
Default Directory - Micros
https://portal.azure.com/#create/Microsoft.NSGFlowLog
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Network foundation | Network security groups > windows-vm-nsg | NSG flow logs >
Create a flow log
Project details
Subscription *
Azure subscription 1
On 30 September 2027, Network security group (NSG) flow logs in Azure Network Watcher will be retired. As part of this retirement, you'll no longer be able to create new NSG flow logs starting 30 June 2025. To avoid service disruptions, migrate to virtual network flow logs by 30 September 2027. Learn more.
Flow log type *
Network security group
Virtual network
Select target resource
Flow Log Name
Resource
Resource Group
Target Resource Type
Review + create
< Previous
Next : Analytics >
Download a template for automation

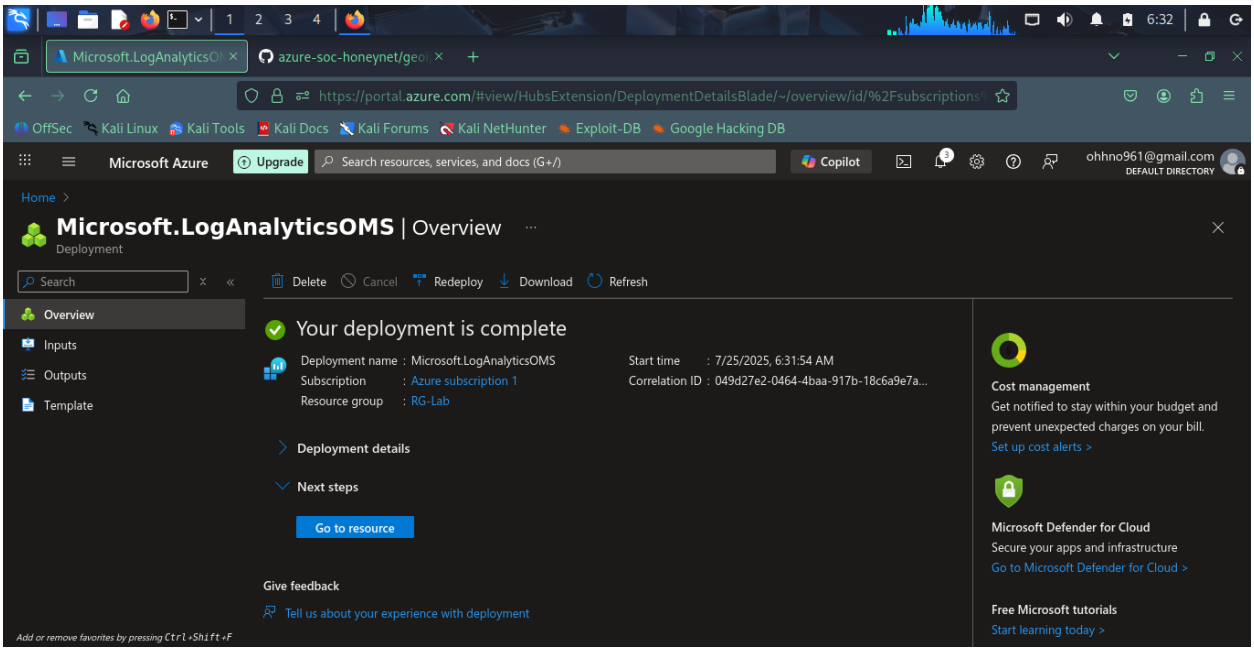

Select network interface
Network foundation - Mic
Microsoft Azure Portal | M
Monitor - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Monitoring/AzureMonitoringBrowseBlade/~/networ
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Monitor
Monitor | Networks
Microsoft
Search
Refresh
Feedback
Useful Links
Diagnostic Toolkit
Topology
Try our new Topology experience which offers visualization of Azure resources for ease of inventory management and monitoring network at scale. Leverage it to visualize resources and their dependencies across subscriptions, regions and locations. Click to navigate to the experience.
Workbooks
Dashboards with Grafana (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Add or remove favorites by pressing Ctrl+Shift+F
azure-nessus-ns 0 Azure subscription 1 East US 2
kali-vm-lab-001 0 Azure subscription 1 East US 2
linux-vm-nsg 0 Azure subscription 1 East US
rg-attacker-nsg 0 Azure subscription 1 East US
windows-vm-ns 0 Azure subscription 1 East US


Select network interface
Network foundation - Mic
Microsoft Azure Portal | M
Monitor - Microsoft Azure
Screenshot taken
View image
https://portal.azure.com/#view/Microsoft_Azure_Monitoring/AzureMonitoringBrowseBlade/~/networ
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Monitor
Monitor | Networks
Microsoft
Search
Refresh
Feedback
Useful Links
Diagnostic Toolkit
Topology
Workbooks
Dashboards with Grafana (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Add or remove favorites by pressing Ctrl+Shift+F
Try our new Topology experience which offers visualization of Azure resources for ease of inventory management and monitoring network at scale. Leverage it to visualize resources and their dependencies across subscriptions, regions and locations. Click to navigate to the experience.
Network health
Connectivity
Traffic
Search direct and dependent reso...
Subscription == All
Resource Group == All
Type == All
Sort By == Sort by name A-Z
No supported metrics
Network security groups
Show all resources
Show health
Available
Degraded
Unavailable
Unknown
Health not supported
Network security gr... (5)
Alert time interval
Last 24 hours
New Alert


Select network interface
Network foundation - Mic
Microsoft Azure Portal | M
Diagnostic setting - Micro
https://portal.azure.com/#view/Microsoft_Azure_Monitoring/ServiceDiagnosticsSettingsUpdateBlade
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Monitor | Networks > linux-vm-nsg | Diagnostic settings >
Diagnostic setting
Save
Discard
Delete
Feedback
Logs
Category groups
allLogs
Categories
Network Security Group Event
Network Security Group Rule Counter
Destination details
Send to Log Analytics workspace
Subscription
Azure subscription 1
Log Analytics workspace
LAW-RG-lab (eastus)
Archive to a storage account
Stream to an event hub
Send to partner solution


Select network interface
Network foundation - Mic
Microsoft Azure Portal | M
Diagnostic setting - Micro
https://portal.azure.com/#view/Microsoft_Azure_Monitoring/ServiceDiagnosticsSettingsUpdateBlade
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Monitor | Networks > windows-vm-nsg | Diagnostic settings
Diagnostic setting
Updating diagnostics
Successfully updated diagnostics for 'windows-vm-nsg'.
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
JSON View
Diagnostic setting name
windowsnsg-diagnostics
Logs
Category groups
allLogs
Categories
Network Security Group Event
Network Security Group Rule Counter
Destination details
Send to Log Analytics workspace
Subscription
Azure subscription 1
Log Analytics workspace
LAW-RG-lab (eastus)
Archive to a storage account


Select network interface
Network foundation - Mic
Microsoft Azure Portal | M
Monitor - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Monitoring/AzureMonitoringBrowseBlade/~/networ
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Monitor
Monitor | Networks
Microsoft
Search
Refresh Feedback Useful Links Diagnostic Toolkit Topology
Try our new Topology experience which offers visualization of Azure resources for ease of inventory management and monitoring network at scale. Leverage it to visualize resources and their dependencies across subscriptions, regions and locations. Click to navigate to the experience.
Workbooks
Dashboards with Grafana (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Add or remove favorites by pressing Ctrl+Shift+F
azure-nessus-ns 0 Azure subscription 1 East US 2
kali-vm-lab-001 0 Azure subscription 1 East US 2
linux-vm-nsg 0 Azure subscription 1 East US
rg-attacker-nsg 0 Azure subscription 1 East US
windows-vm-ns 0 Azure subscription 1 East US



8. Lessons Learned

1. **Cloud Security is Fast-Paced**: NSG Flow Logs were deprecated mid-project, highlighting the need to monitor Azure documentation closely.
2. **Real-World Honeypots Work**: SSH attacks began within minutes of VM exposure.
3. **Data Integration Complexity**: Sentinel setup requires precise resource linkage and permissions.
4. **Hands-on Beats Theory**: Despite technical roadblocks, this project built real muscle in Azure networking, logging, and detection workflows.

Final Reflection:

Although I couldn't fully complete the Sentinel integration in this project, I gained *far more than expected* through deep troubleshooting, real-world experimentation, and grappling with Azure's fast-evolving ecosystem.

- I discovered that **several features I relied on had been deprecated or renamed** (e.g., NSG Flow Logs), and even with an active Azure subscription, some **critical services were unavailable or restricted**, requiring creative workarounds.
- These blockers pushed me to **explore alternative paths**, including testing Data Collection Rules (DCR), GeoIP watchlists, and brute-force simulations across OS types.
- More importantly, I realized that **real-world cybersecurity doesn't follow a script**—things break, tools change, and documentation goes stale. That's when learning becomes *real*.

This project taught me how to:

- Architect cloud-based honeypot environments
- Simulate and detect attacks from both internal and external threat vectors
- Interpret logging systems across Windows and Linux
- Navigate Azure's shifting security landscape with persistence and critical thinking

I plan to **re-attempt this project soon**, building on these lessons, and will aim for full Microsoft Sentinel integration using custom DCR, Azure Monitor Agent, and third-party analytics pipelines.

In cybersecurity, progress isn't just measured by what *worked*—but by how much you *understood when things didn't*. This was one of those turning-point labs.