

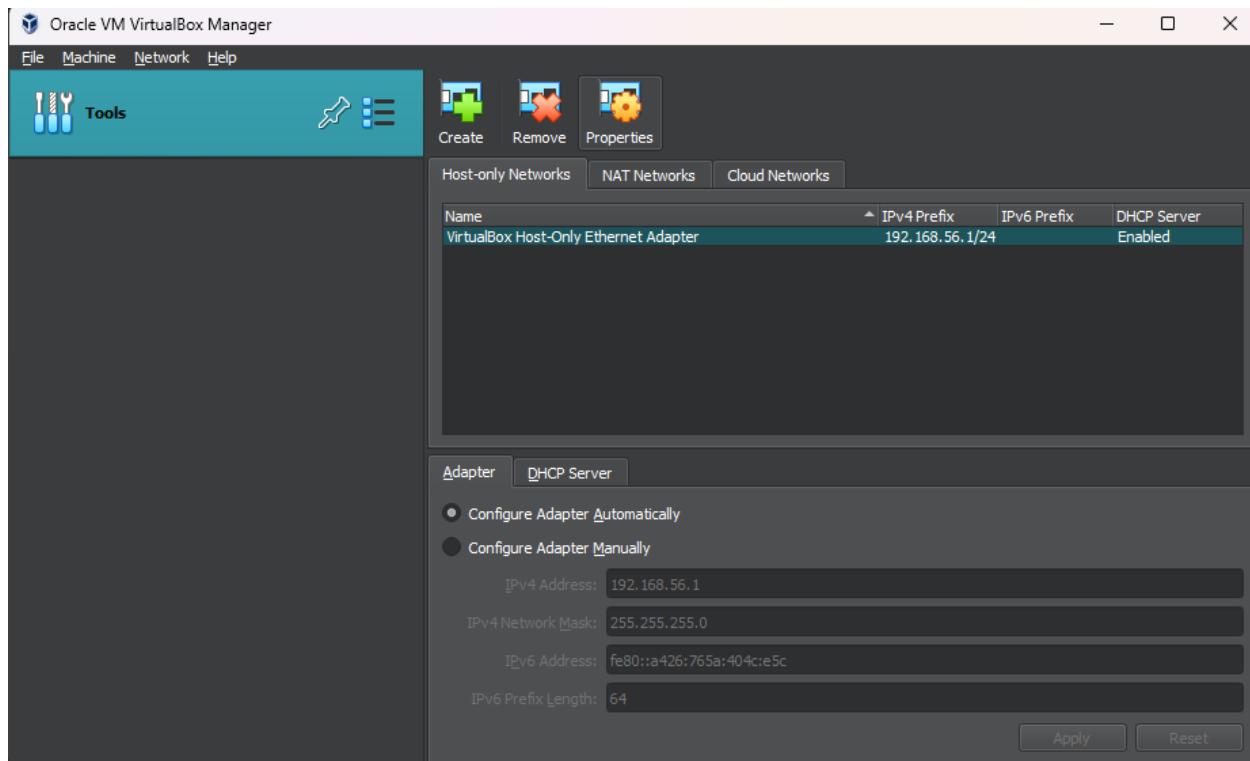
*AI-Assisted Incident Triage in a Splunk SIEM
Environment*

Drilon Toska

CSCI 6805_91

Lab Environment Design and Implementation

Oracle VM VirtualBox will be used as the virtualization platform for this project to create and manage the lab environment. VirtualBox allows multiple operating systems to run on a single host system, making it possible to build an isolated and controlled environment for testing security scenarios. Using VirtualBox, I will deploy virtual machines running Kali Linux, Windows Server, and Windows 10, each serving a specific role within the lab.



To build the virtual lab environment, official ISO installation files were obtained for each required operating system. The Kali Linux ISO was downloaded from the official Kali Linux website, while the Windows Server and Windows 10 ISO files were obtained directly from Microsoft.

Kali Linux 2025.4 Changelog ⁸

x86_64 Apple Silicon (ARM64)

Recommended

Installer

Complete offline installation with customization

↓ 547 torrent sum

Microsoft | Software Download Windows Windows Insider Preview All Microsoft Search ⌂ Dylon

Download Windows 10

Before updating, please refer to the [Windows release information status](#) for known issues to confirm your device is not impacted.

Stay Secure with Essential Windows Updates: After October 14, 2025, Windows 10 will no longer receive free software updates, technical support, or security fixes. This means your PC will be more vulnerable to security threats and malware. **Consider Upgrading to Windows 11:** Move to the security, speed, and innovation that Windows 11 PCs provide, available at every price point. Upgrading to Windows 11 ensures you continue to receive the latest security updates, features, and technical support, keeping your PC safe and efficient. For more information on preparing for Windows 10 end of support, see our [Windows blog post](#).

Windows 10 2022 Update | Version 22H2

The Update Assistant can help you update to the latest version of Windows 10. To get started, click **Update now**.

Update now

Create Windows 10 installation media

To get started, you will first need to have a license to install Windows 10. You can then download and run the media creation tool. For more information on how to use the tool, see the instructions below.

Download Now



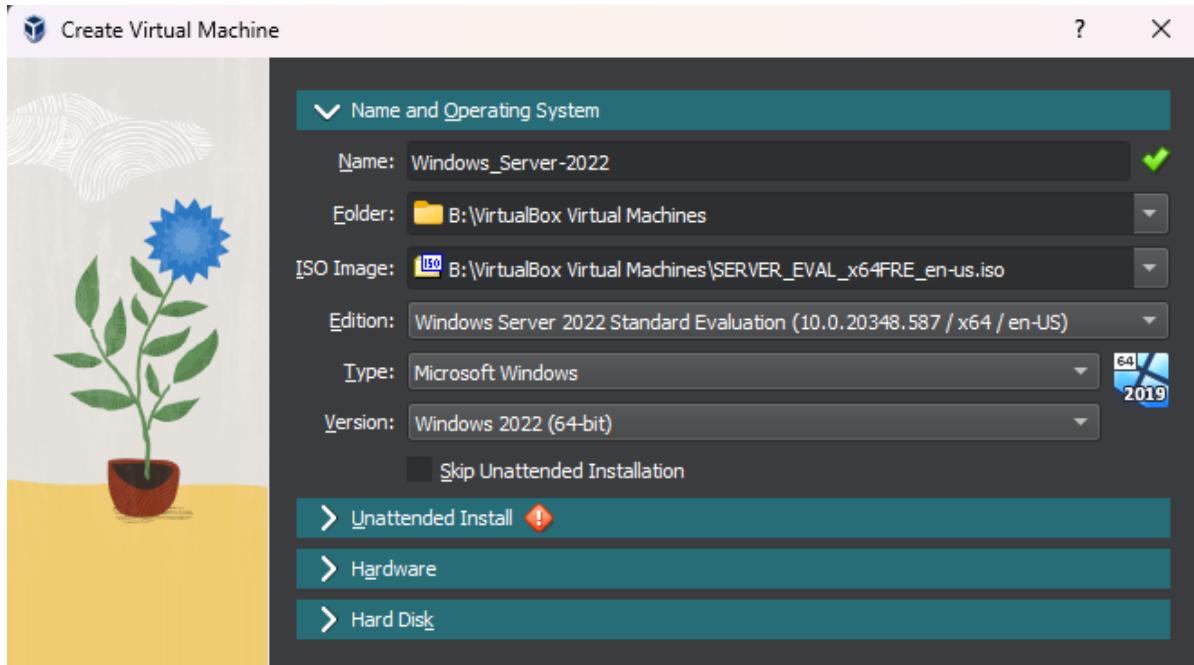
Microsoft | Evaluation Center Windows Windows Server SQL Server System Center Microsoft Security Additional products All Microsoft

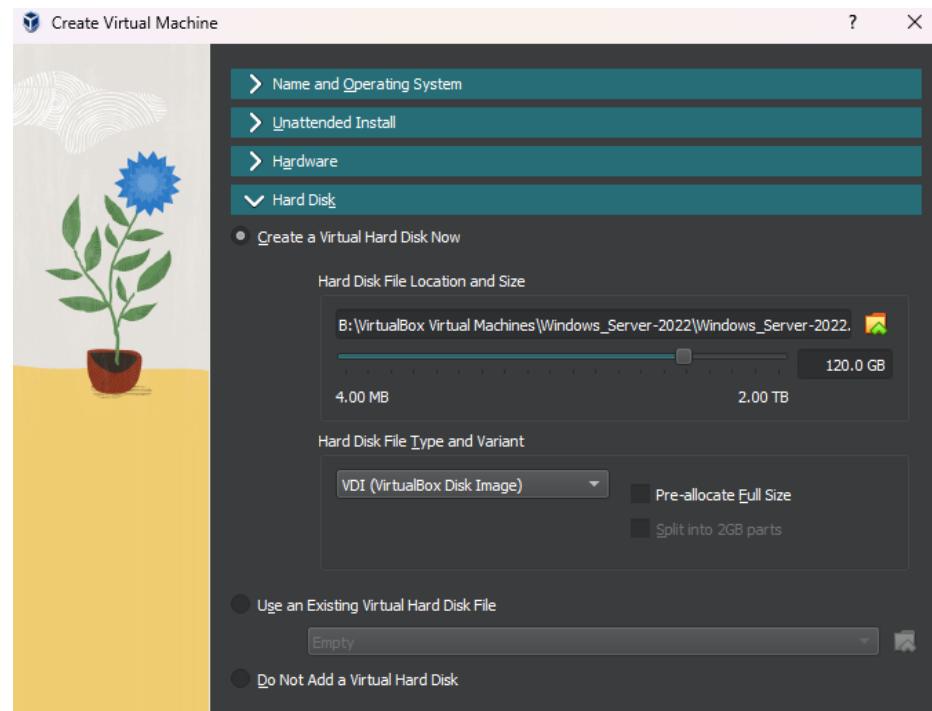
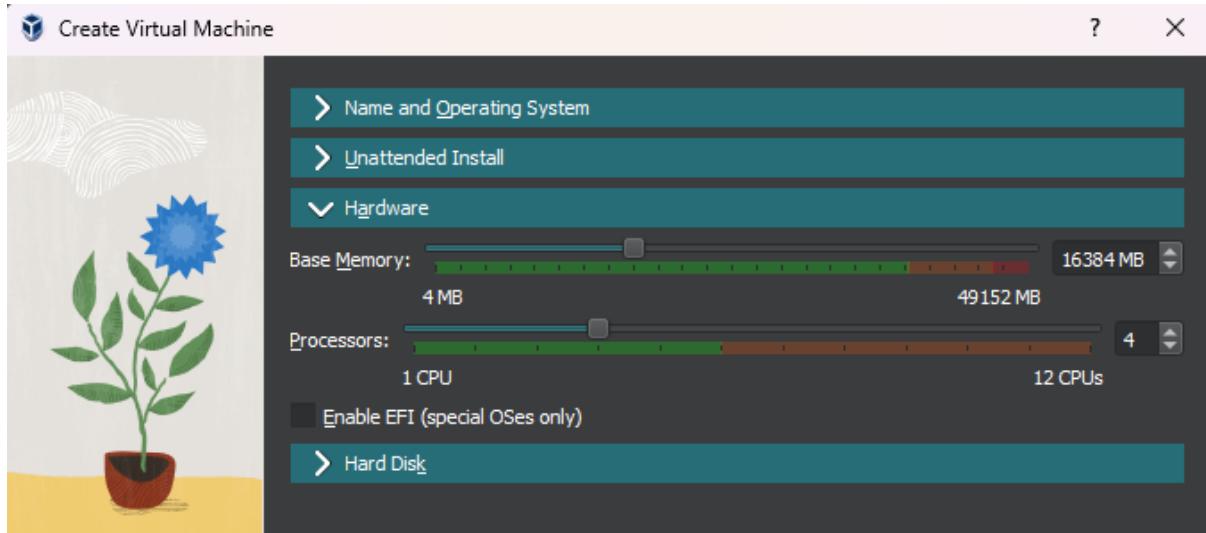
Please select your Windows Server 2022 download

English (United States)	ISO downloads 64-bit edition >	VHD download 64-bit edition >	Try on Azure Learn more >	Create a VM in Azure Learn more >
-------------------------	--	---	--	--

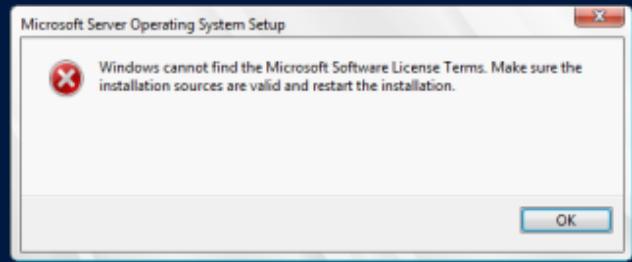
After obtaining the required ISO files, the virtual machines were created using VirtualBox. Separate virtual machines were configured for Kali Linux, Windows Server, and Windows 10, with each system assigned resources appropriate to its role in the lab environment. The Windows Server virtual machine was provisioned to support domain services and host the Splunk SIEM, while the Windows 10 virtual machine was intended to function as a domain-joined endpoint generating user and system activity. The Kali Linux virtual machine was configured as an attacker system used to simulate adversarial behavior. During creation, CPU, memory, and disk resources were allocated to ensure stable performance while maintaining isolation between systems.

Creation of Windows Server VM



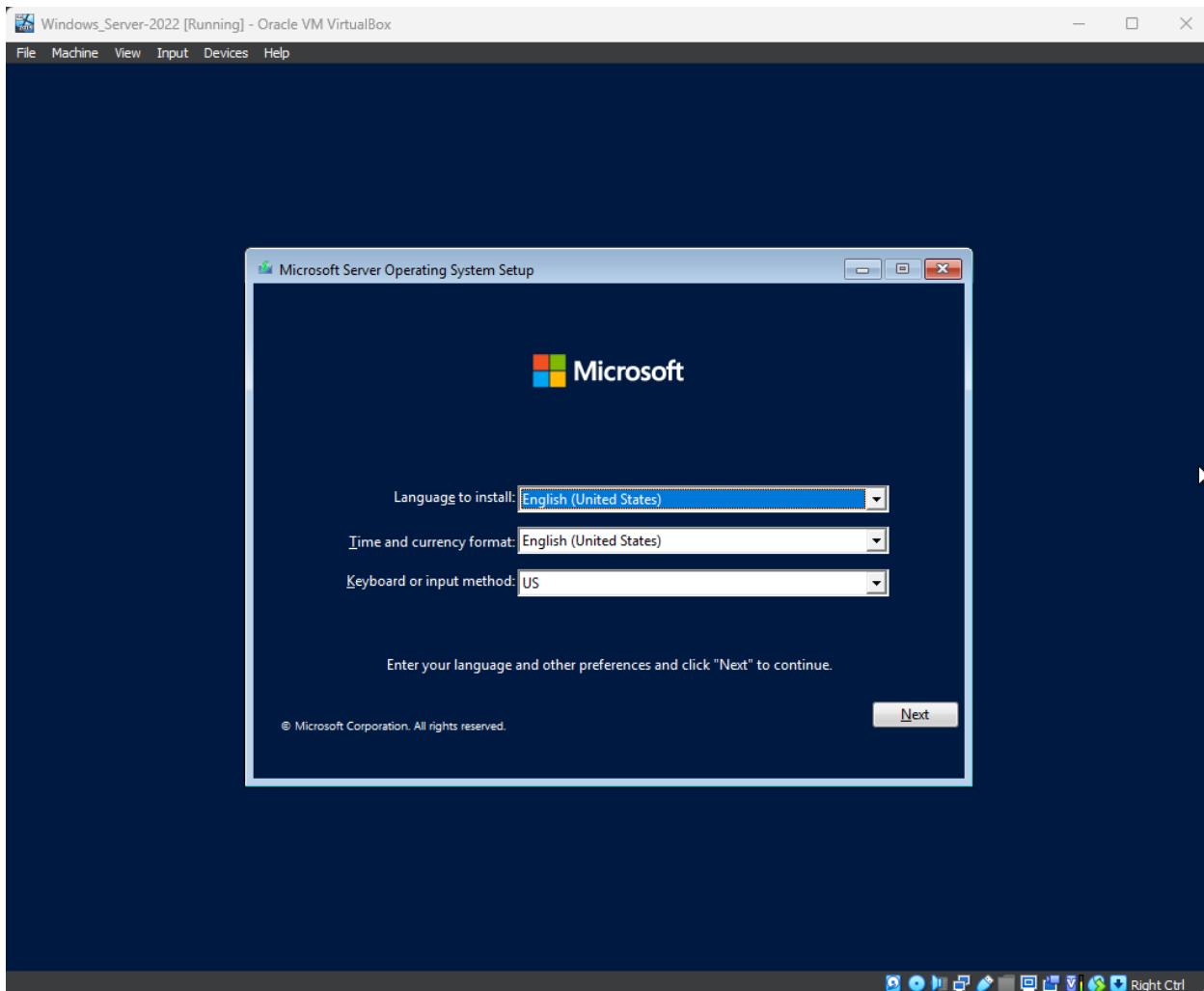


The first time I booted the server, I got this error:

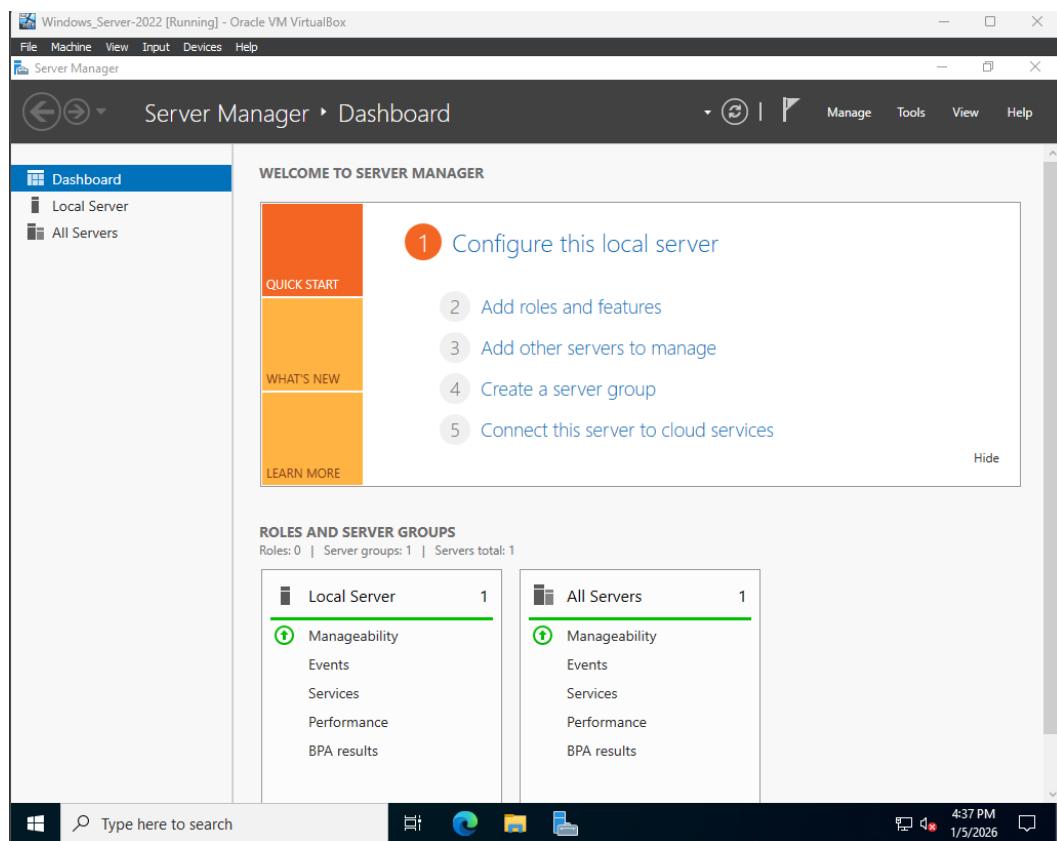


Setup is starting

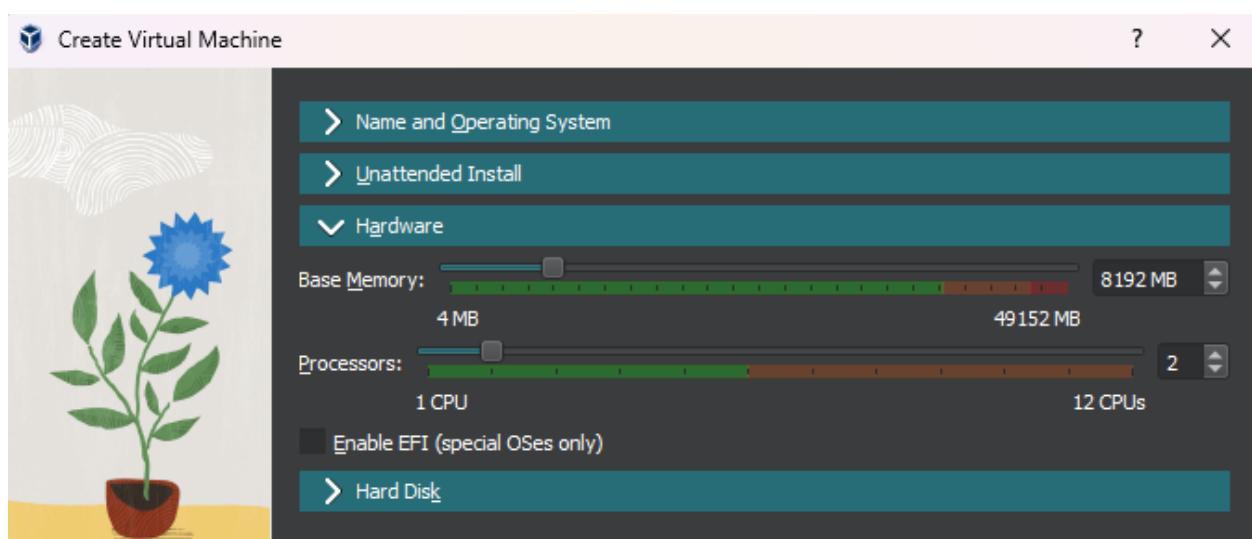
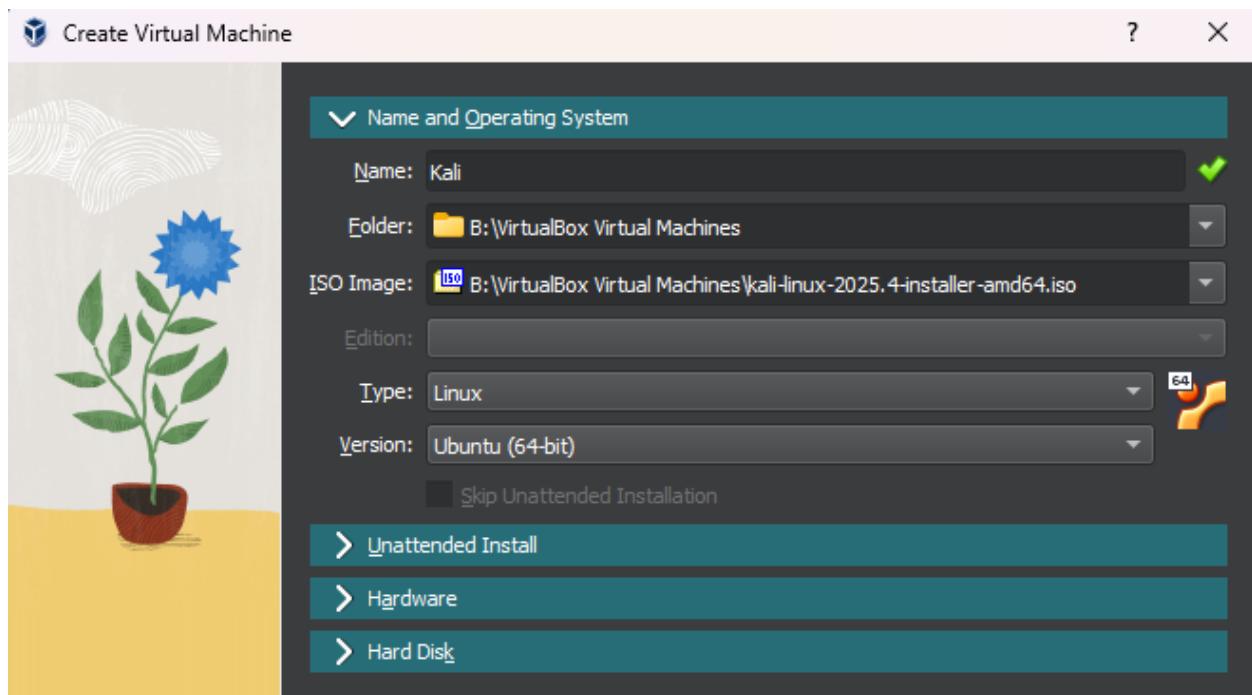
After some research, I enabled the “Skip Unattended Installation” and it booted just fine.

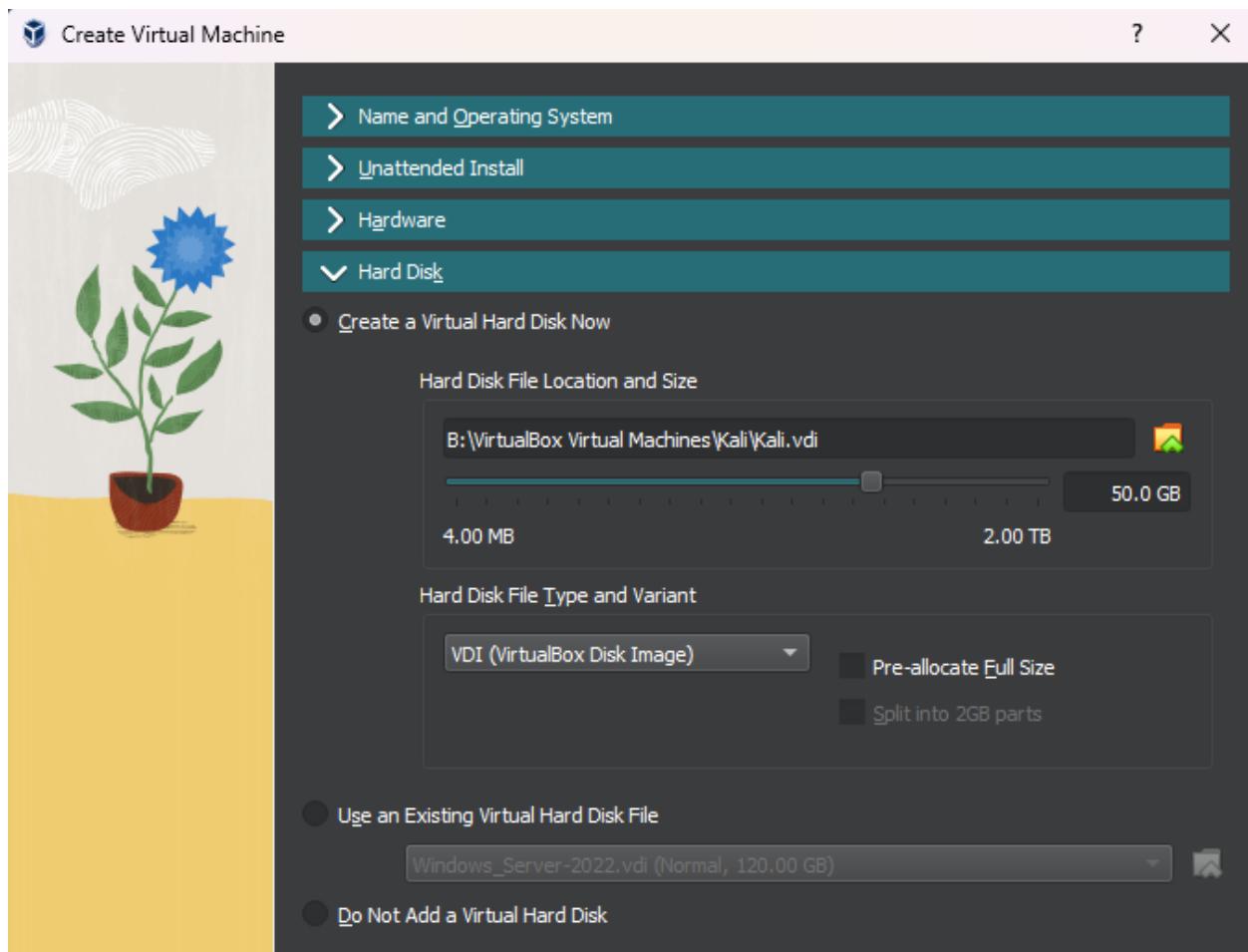


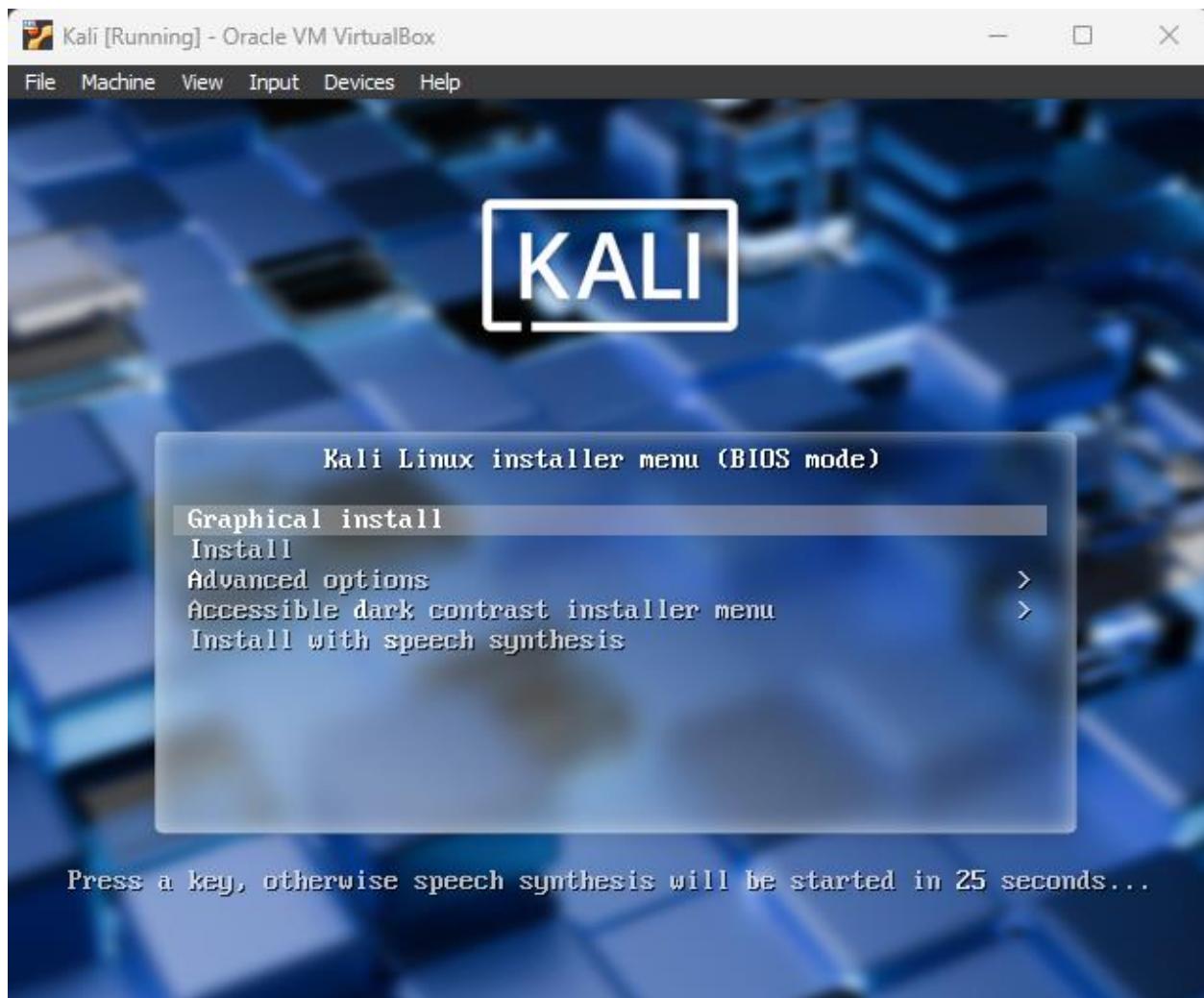
Finished installation of server:

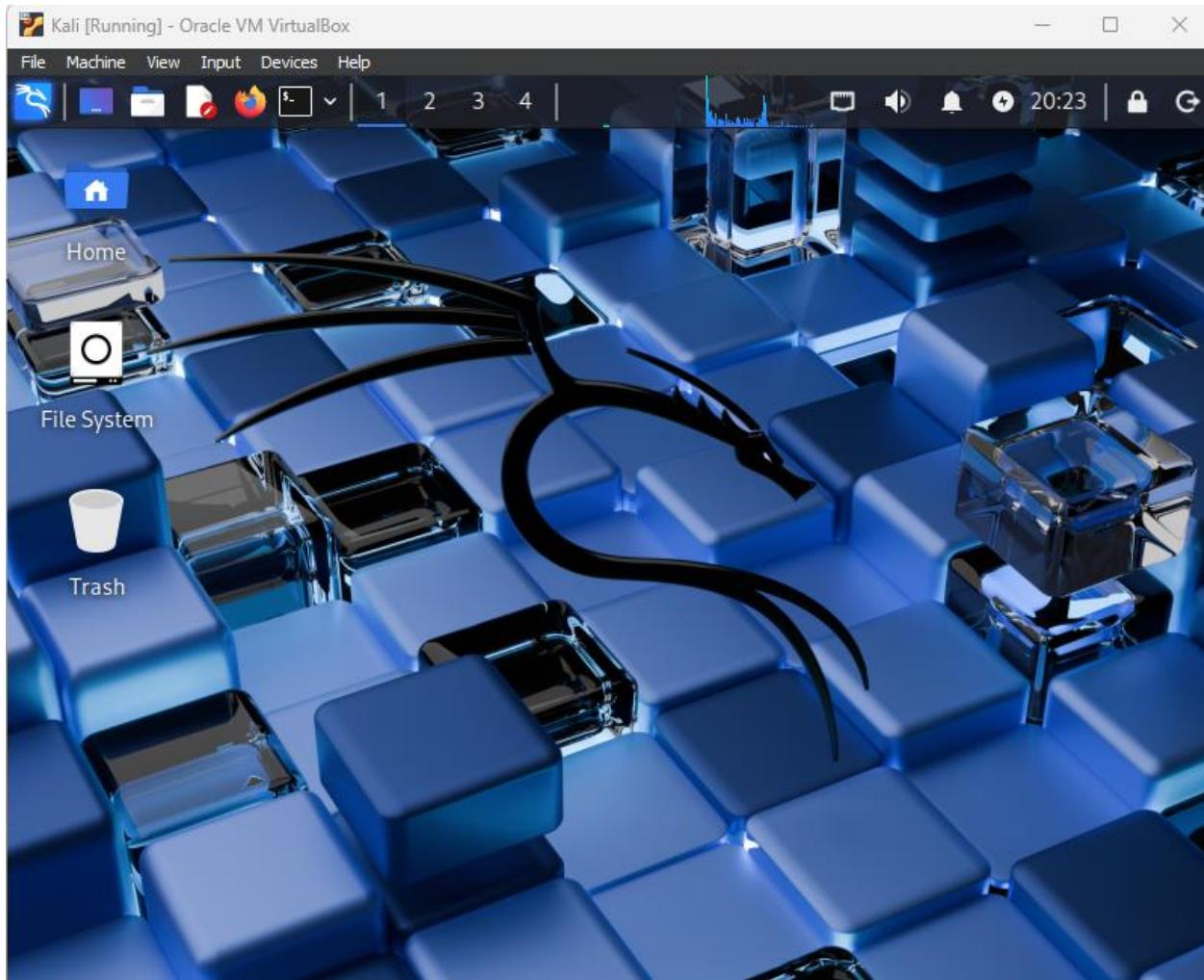


Creation of Kali Linux VM

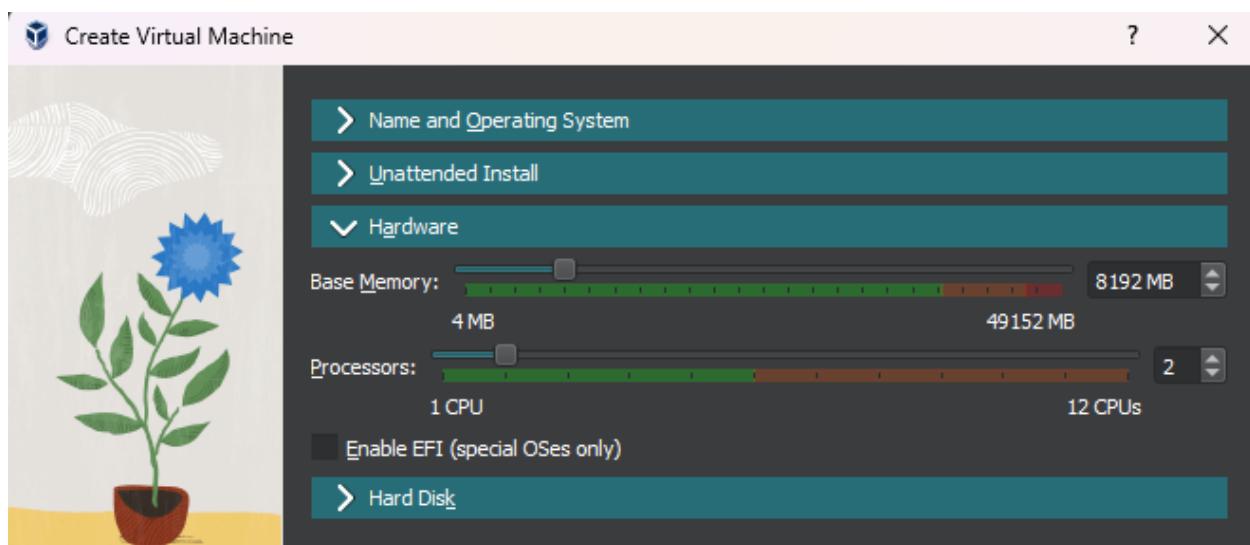
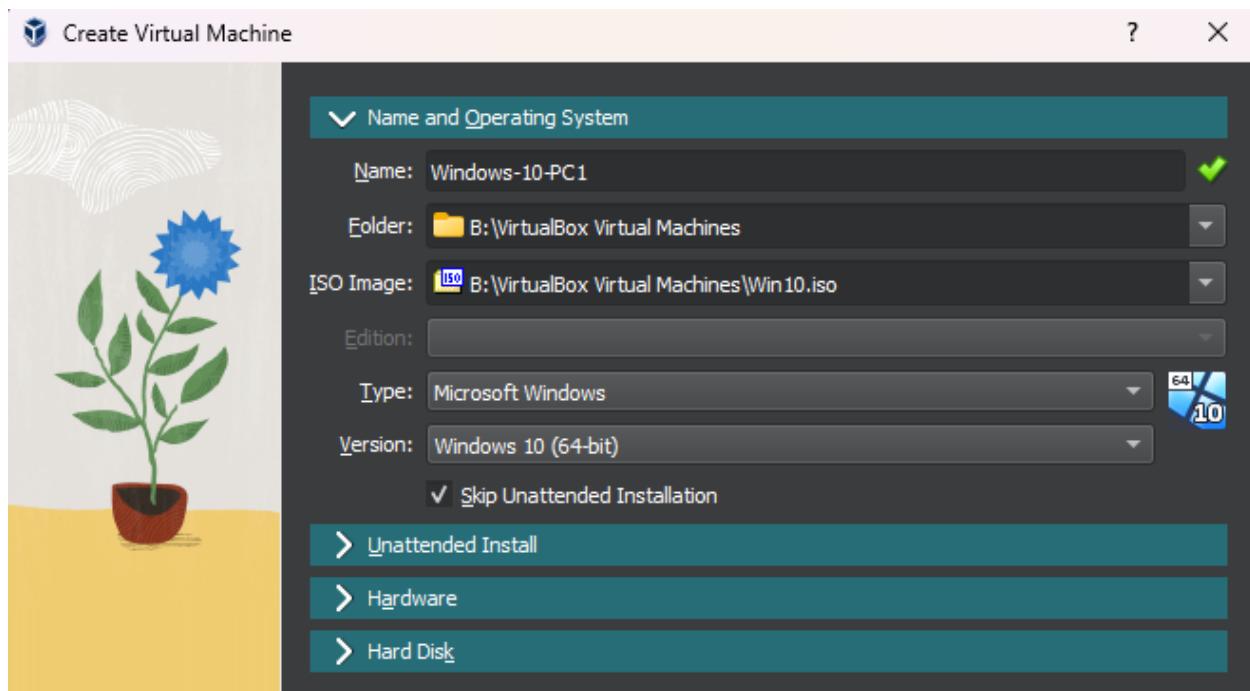


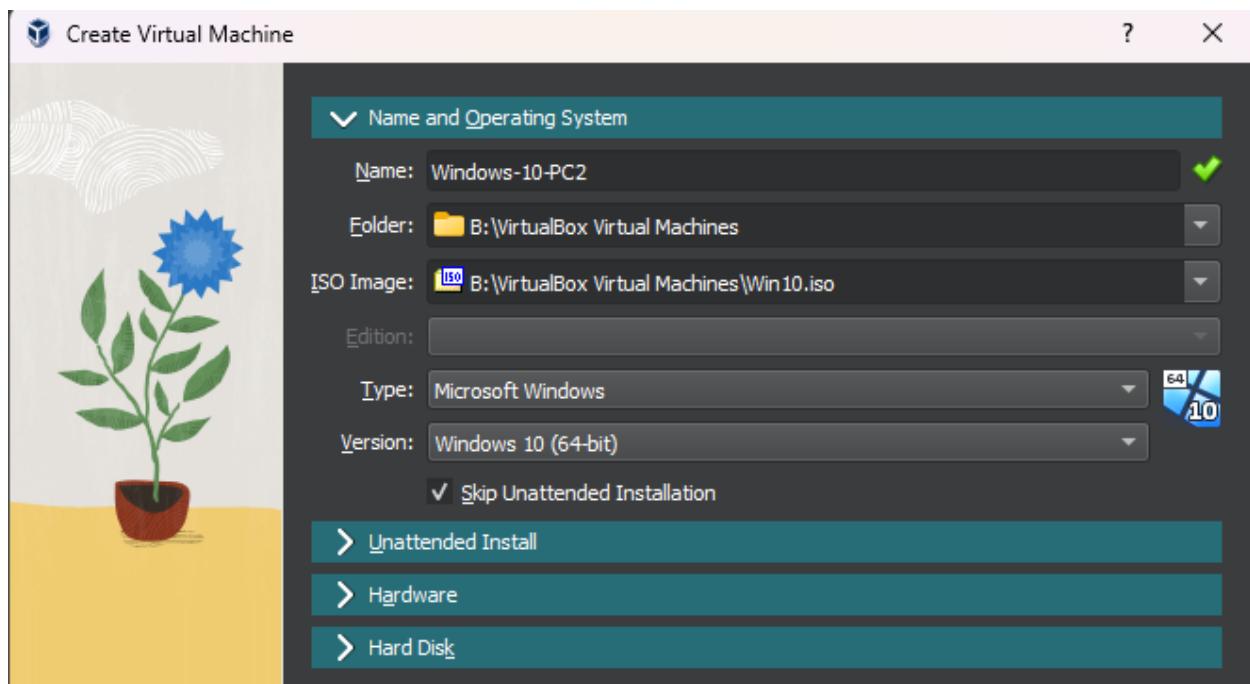
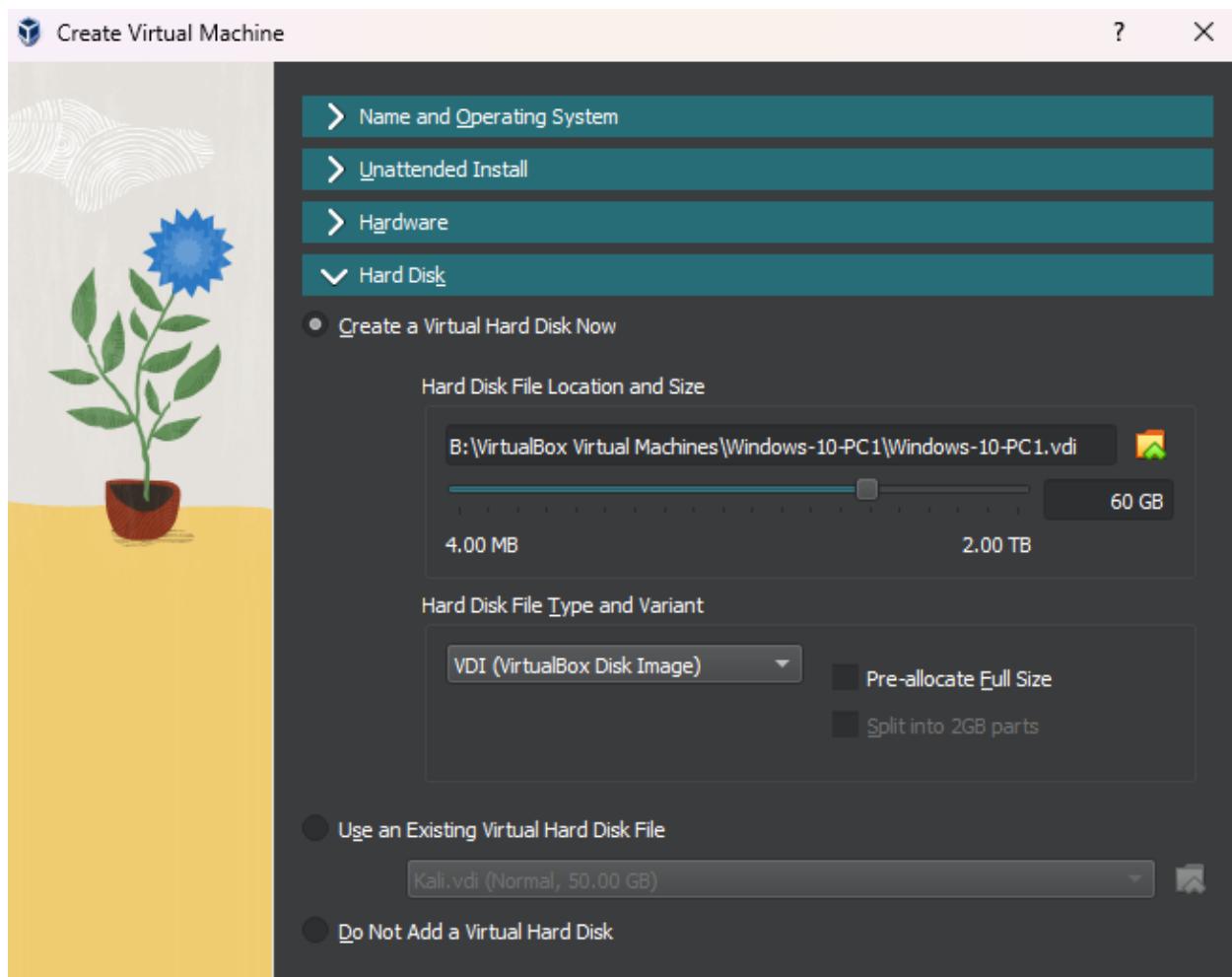


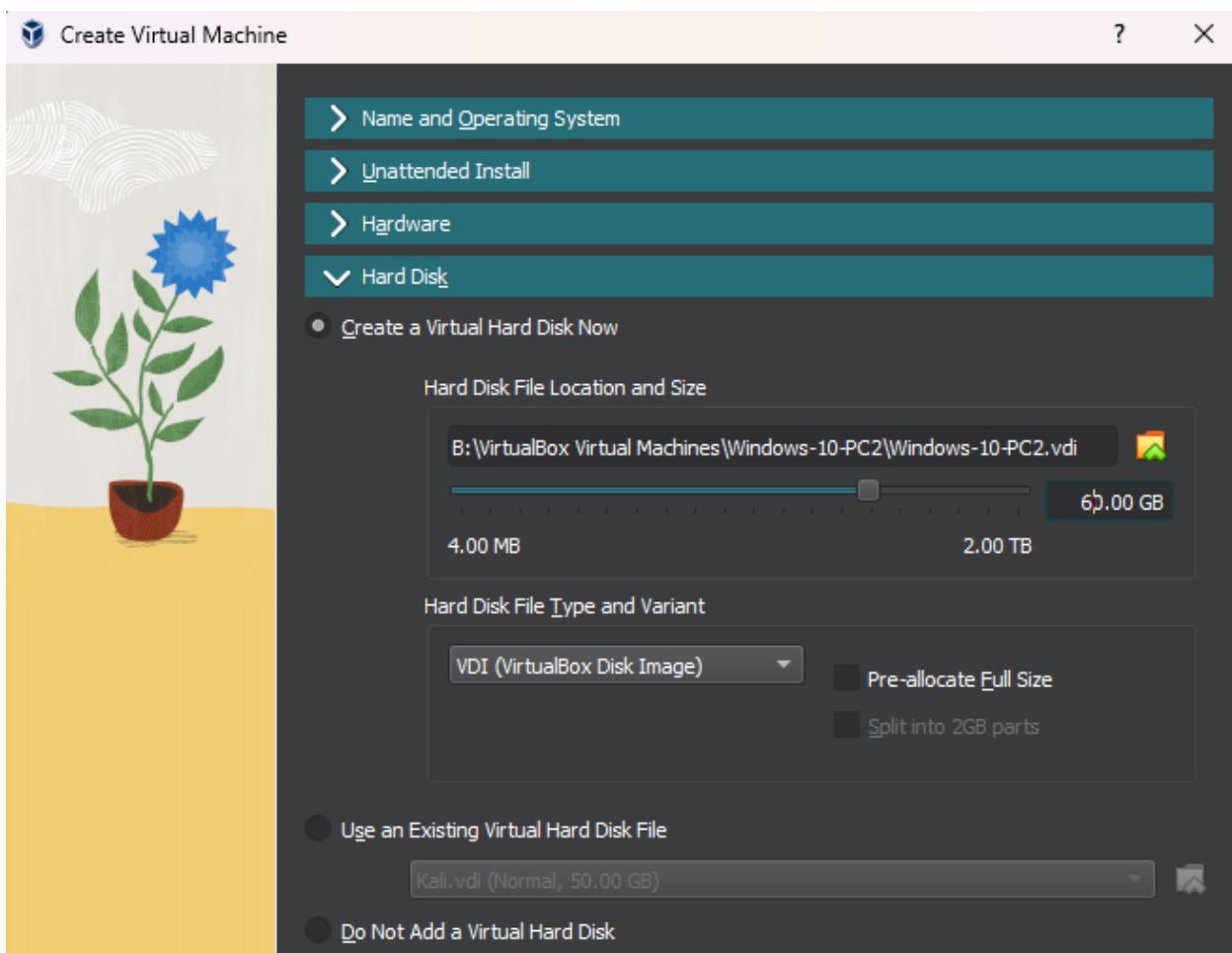
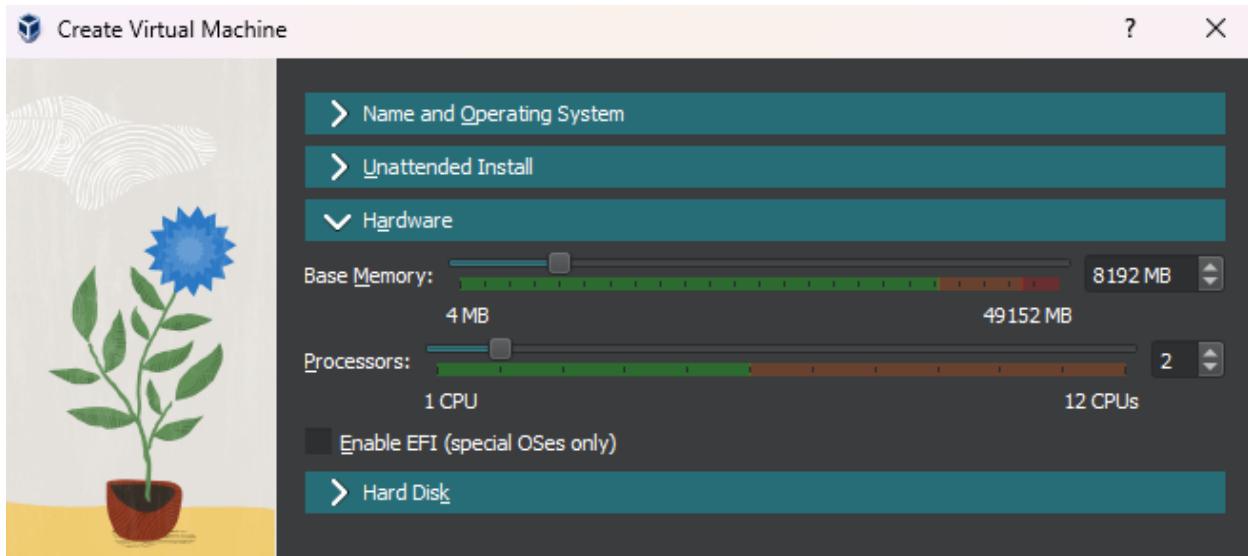




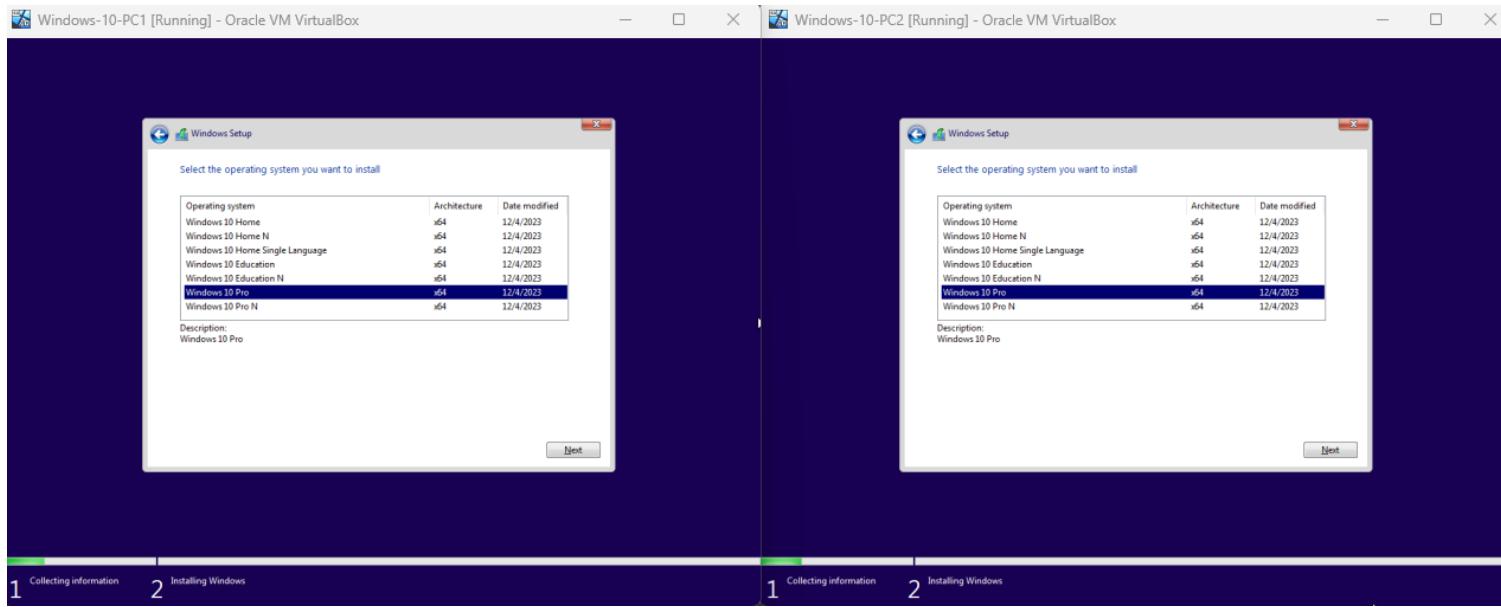
Creation of two Windows 10 Machines



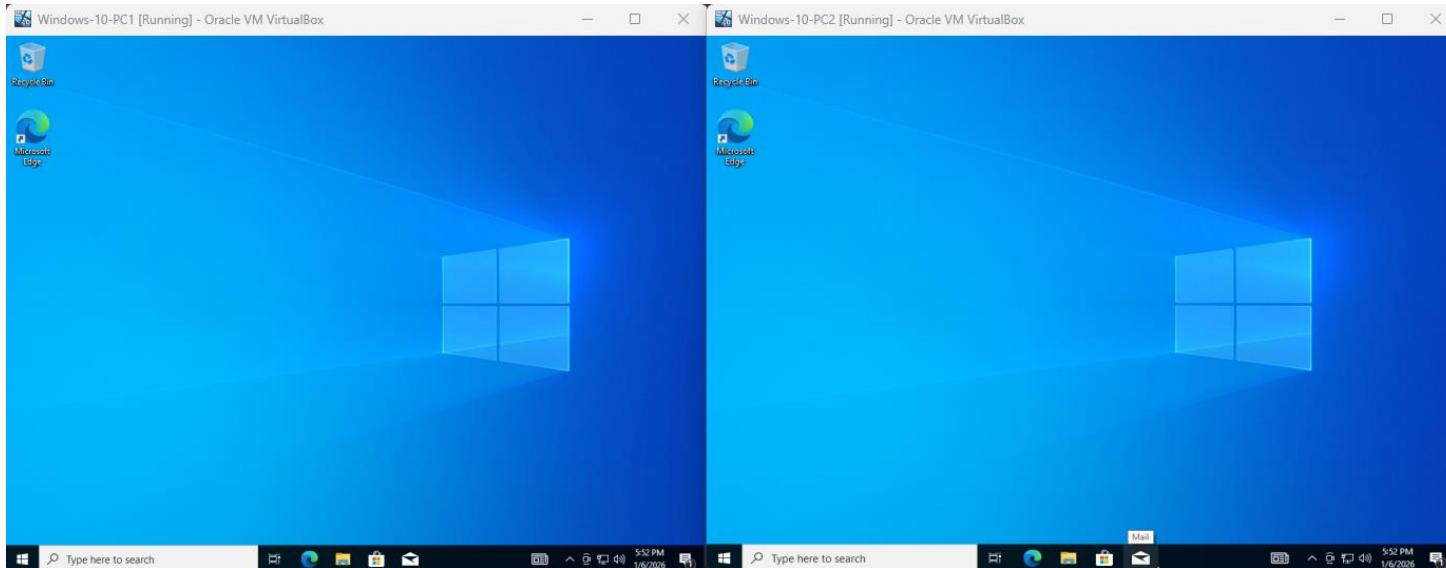




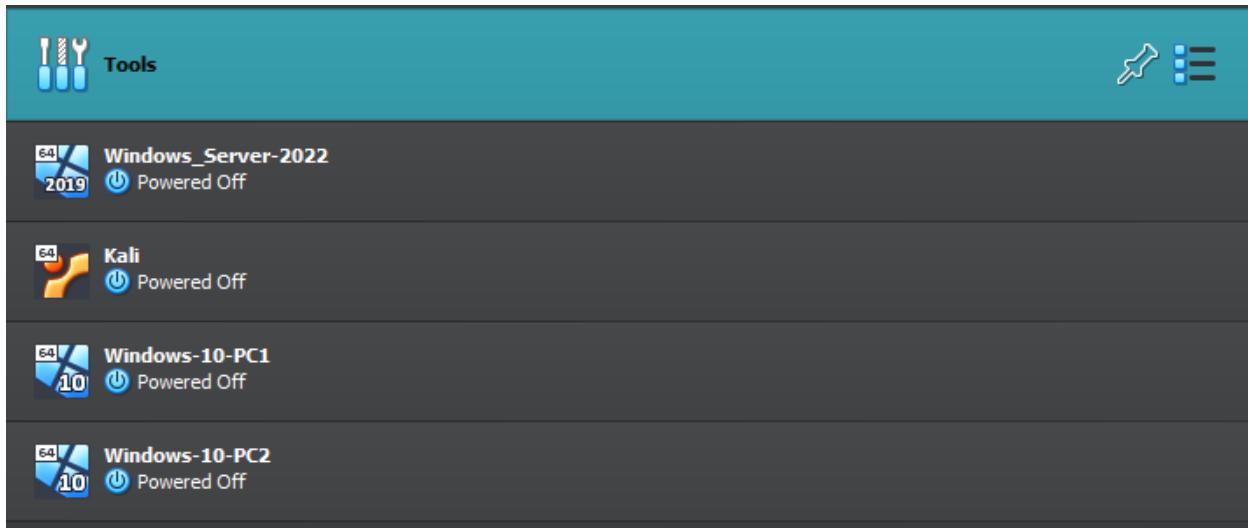
Both Windows 10 PCs successfully booted and are installing Windows 10 Pro Edition.



Both Windows 10 PCs are successfully running.



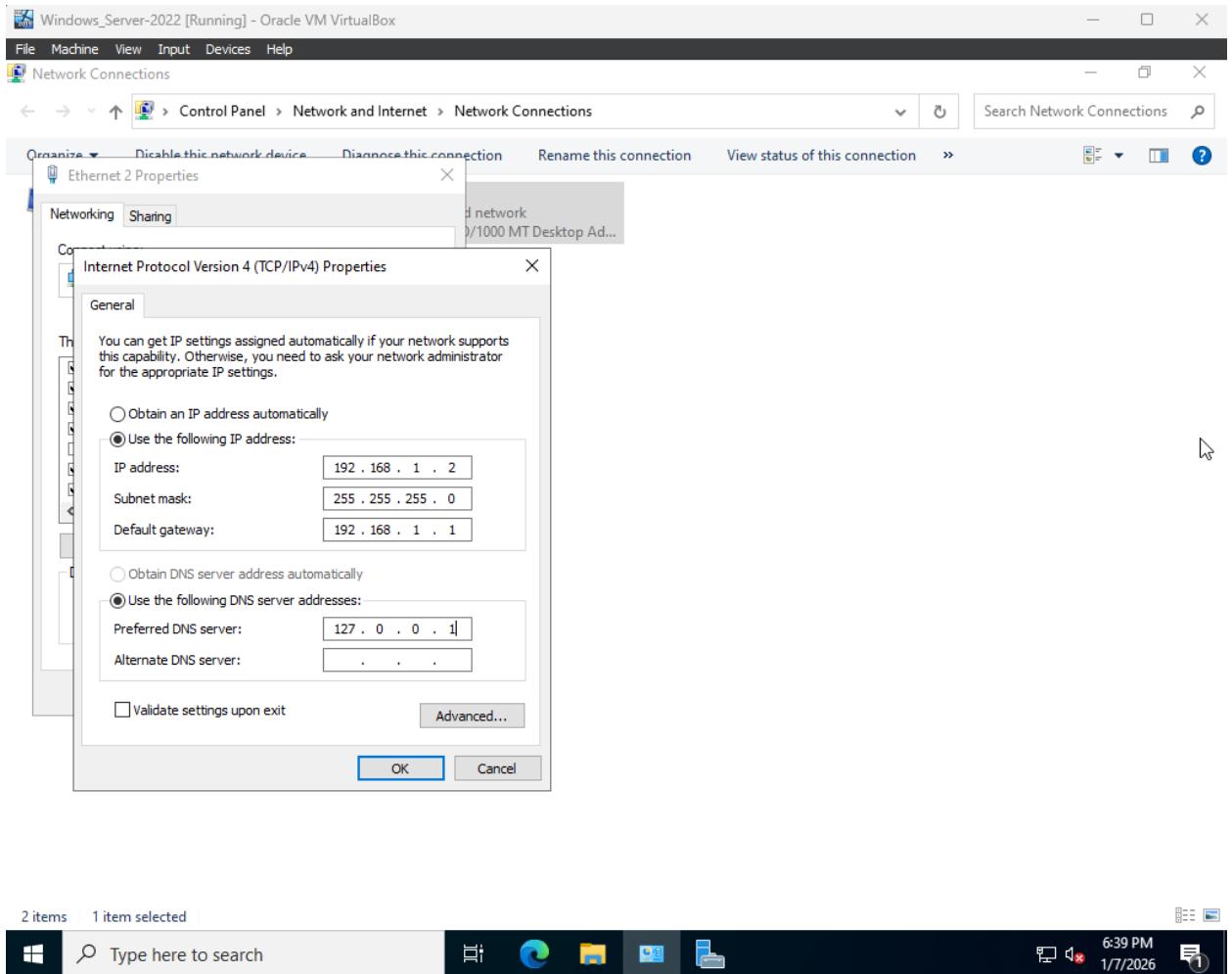
All VMs Have Been Created



Active Directory Domain Services Promotion

The Windows Server 2022 virtual machine will be promoted to a Domain Controller by installing Active Directory Domain Services. This allows the server to handle user authentication, group management, and domain-based access for the lab environment. As part of this process, DNS services will also be configured on the server so that domain-joined systems can properly locate and communicate with the domain controller. Promoting the server to Active Directory creates a more realistic enterprise setup and provides the authentication and security activity needed for later analysis in Splunk.

Statically assign the IP address and set the DNS IP to point at itself.



Disable Windows Defender Firewall to allow ICMP requests and to leave the system intentionally vulnerable.

The screenshot shows the Windows Server 2022 Control Panel window titled "Windows_Server-2022 [Running] - Oracle VM VirtualBox". The menu bar includes File, Machine, View, Input, Devices, and Help. The title bar says "Windows Defender Firewall". The main content area displays the Windows Defender Firewall settings. It starts with a section titled "Help protect your PC with Windows Defender Firewall" which states that Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network. A button labeled "Use recommended settings" is present. Below this, there are two network categories: "Private networks" (Not connected) and "Guest or public networks" (Connected). The "Guest or public networks" section is expanded, showing "Network" and "Unidentified network" under "Active public networks". Other settings include "Windows Defender Firewall state: Off", "Incoming connections: Block all connections to apps that are not on the list of allowed apps", and "Notification state: Do not notify me when Windows Defender Firewall blocks a new app".

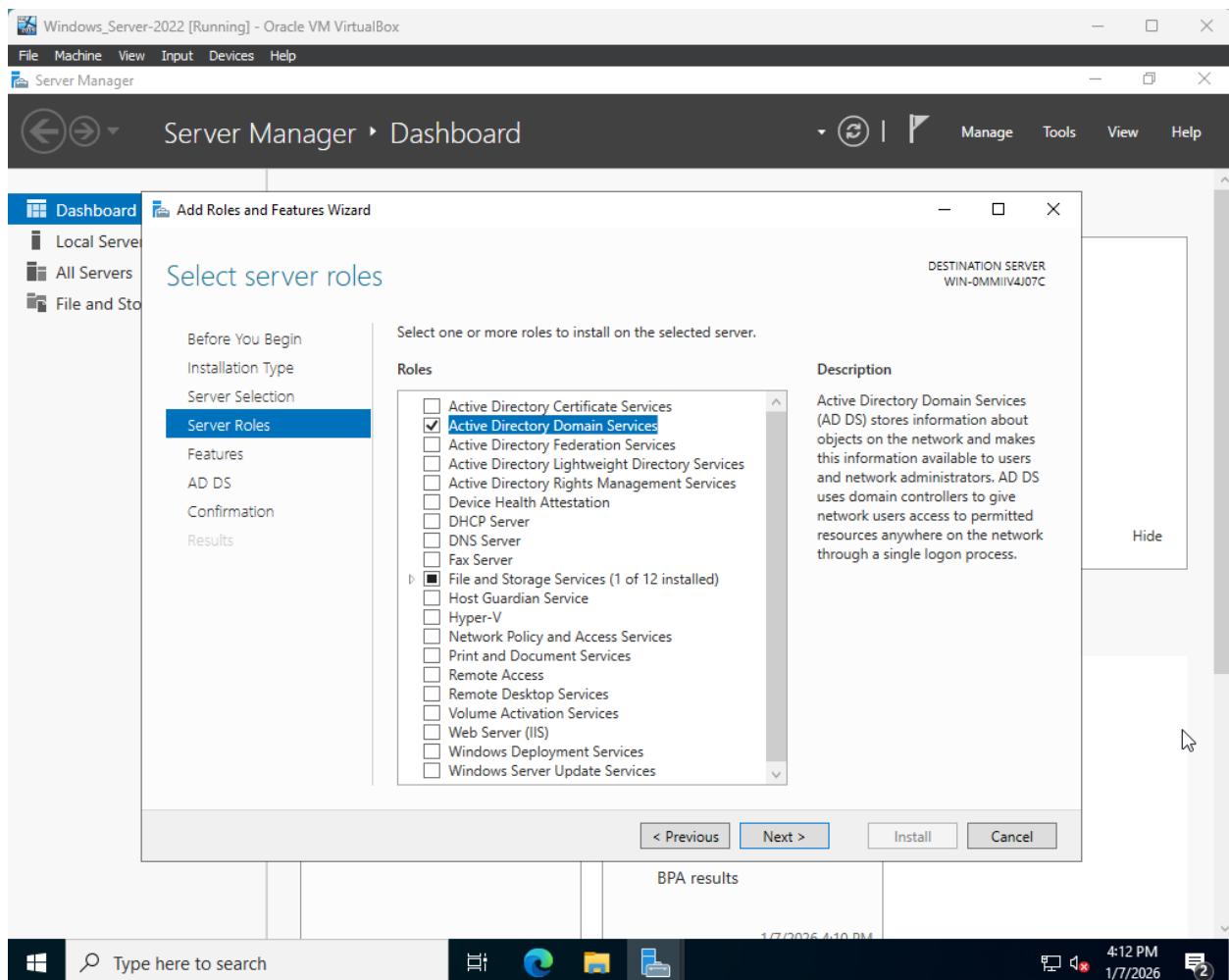
See also

- Security and Maintenance
- Network and Sharing Center

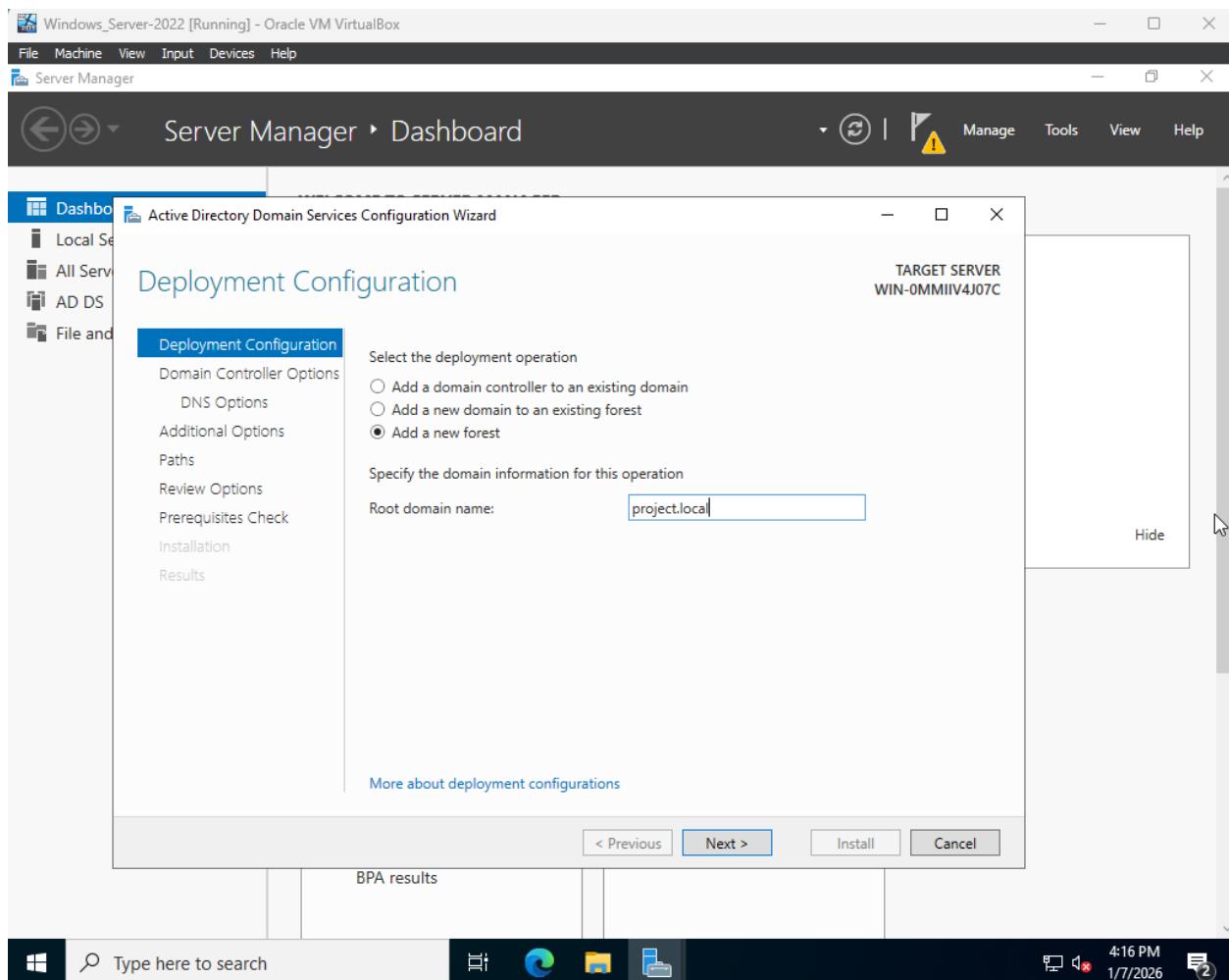
Type here to search

3:55 PM
1/7/2026

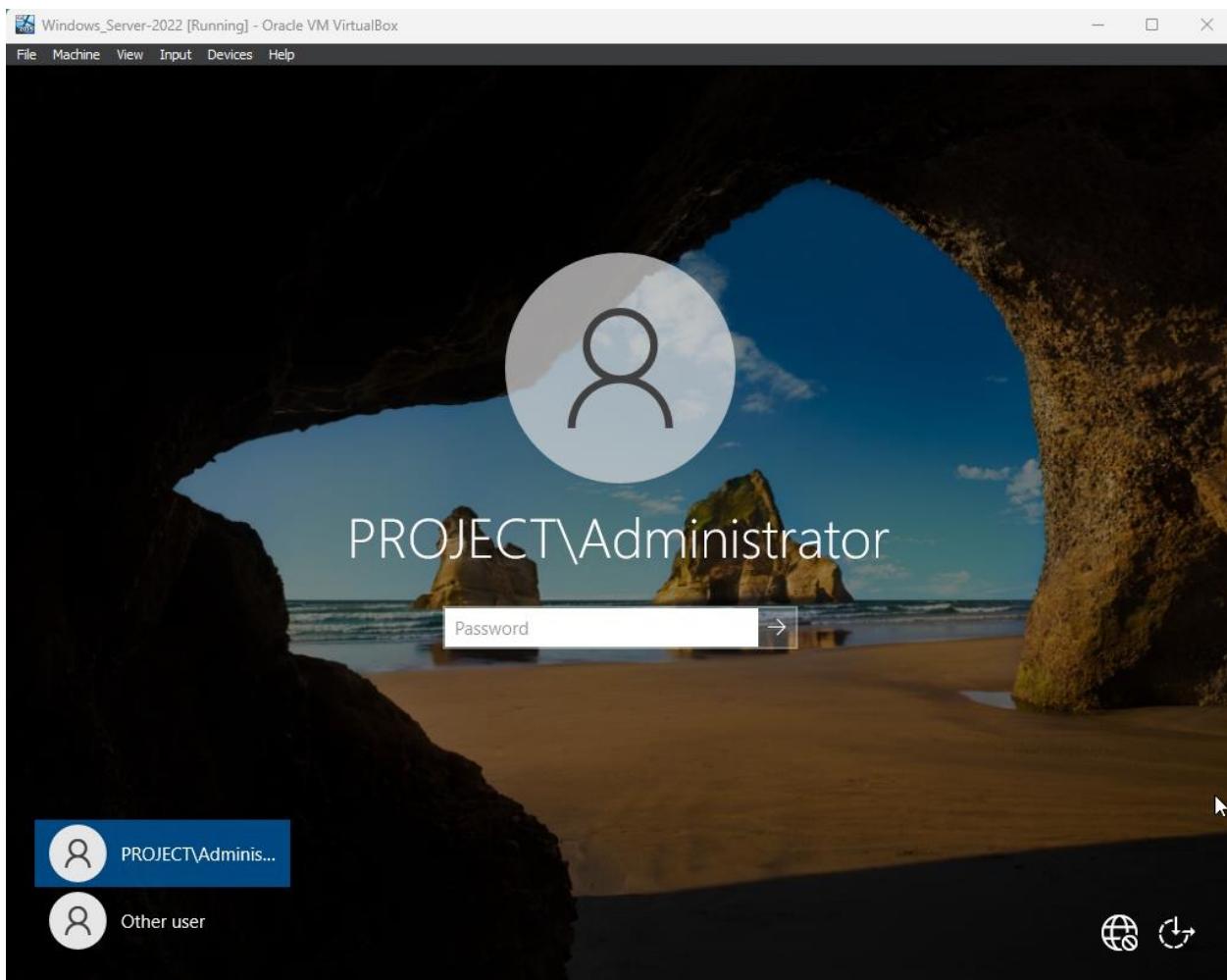
Installing the AD DS service to promote the server to a domain controller.



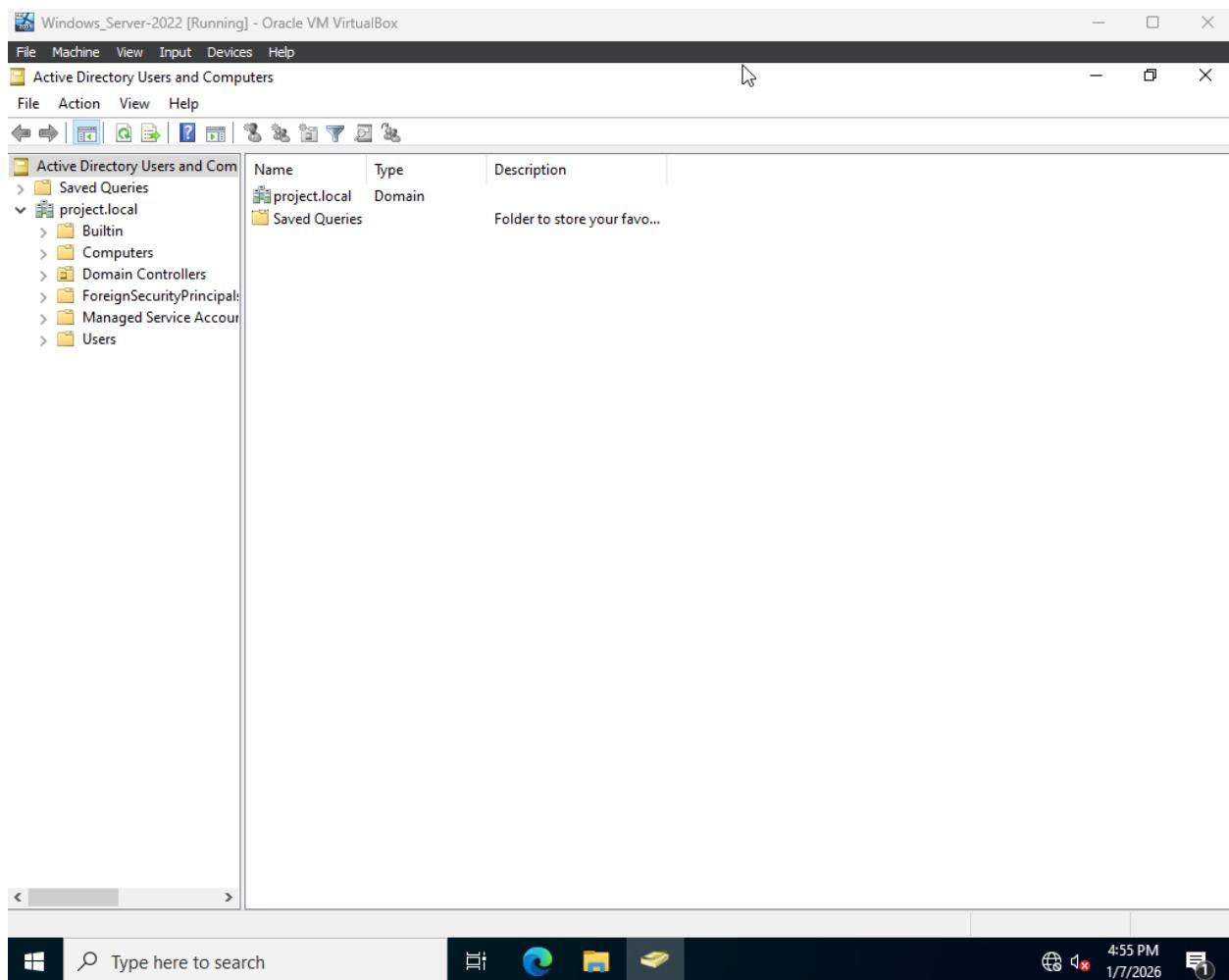
In the process of promoting the server to DC.



After the automatic reboot that followed the installation, you can see the server is now a domain controller.



In the Active Directory application.



Creating two domain users and two groups for realism purposes.

Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com
Saved Queries
project.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Account
Users
Groups

Name	Type	Description
Administrator	User	Built-in account for ad...
Guest	User	Built-in account for gue...

New Object - User

Create in: project.local/Users

First name: John Initials:
Last name: Smith
Full name: John Smith

User logon name: @project.local

User logon name (pre-Windows 2000):

< Back Next > Cancel

Type here to search

4:58 PM 1/7/2026

Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com
Saved Queries
project.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Groups

Name	Type	Description
Administrator	User	Built-in account for ad...
Guest	User	Built-in account for gue...
John Smith	User	

New Object - User

Create in: project.local/Users

First name: Mike Initials:
Last name: Shirley
Full name: Mike Shirley

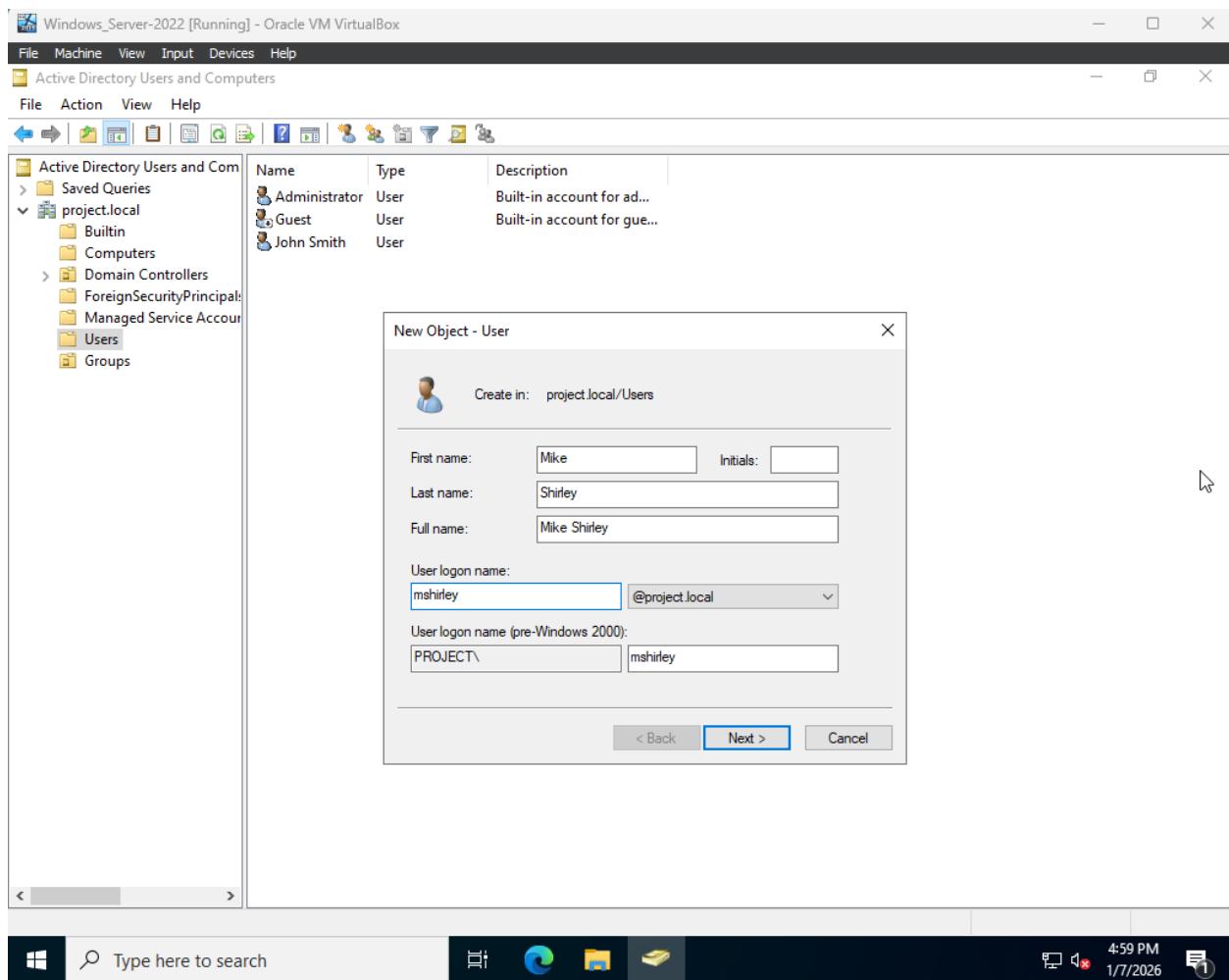
User logon name:
mshirley @project.local

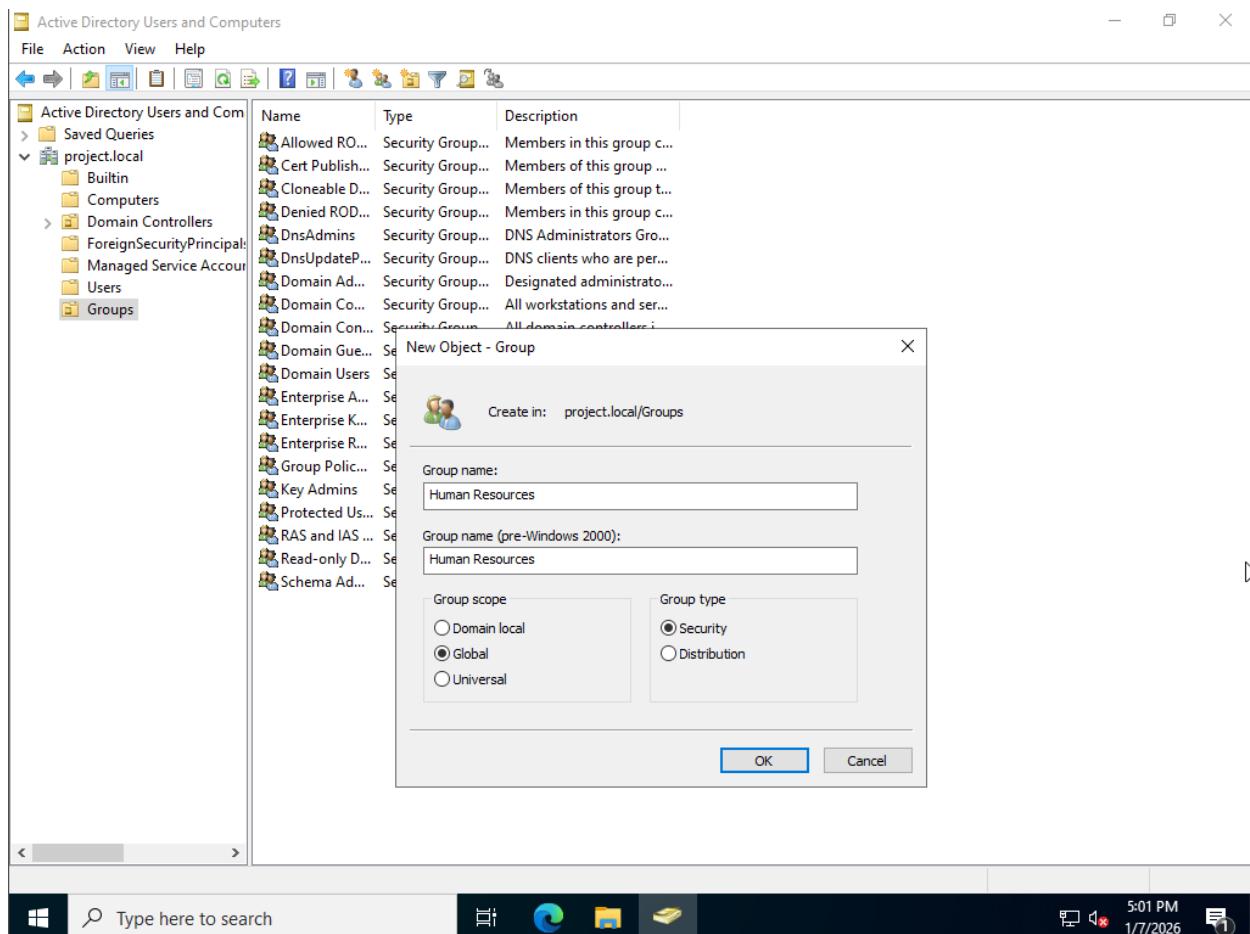
User logon name (pre-Windows 2000):
PROJECT\mshirley

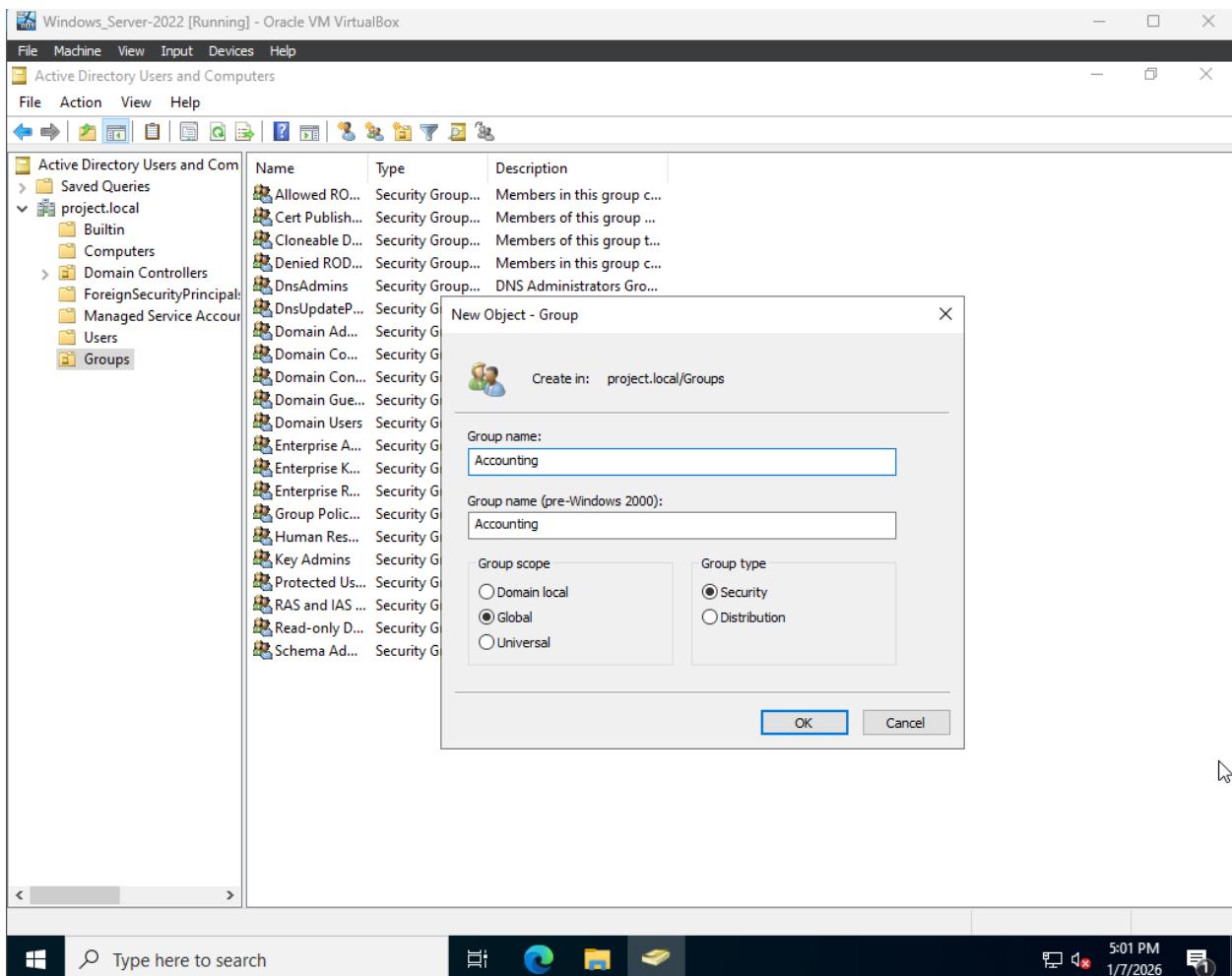
< Back Next > Cancel

Type here to search

4:59 PM 1/7/2026







Network Configuration and Connectivity

The project uses a single shared NAT Network in VirtualBox to allow all virtual machines to communicate while remaining isolated from the external environment. NAT Network mode was chosen because it provides internal LAN-style connectivity as well as outbound internet access for software installation and updates. All systems in the lab were intentionally connected to the same virtual subnet to simulate a small organizational network.

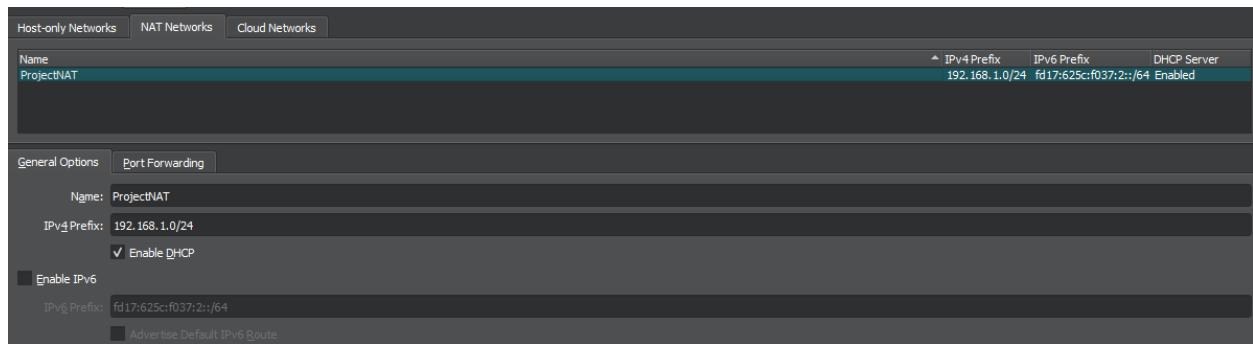
Static IP addressing is planned for the Windows Server and Windows 11 virtual machines to provide consistent network communication. Assigning fixed addresses makes it easier to reference systems, configure Splunk forwarders, and reproduce security scenarios without

relying on changing DHCP leases. This also allows alerts and logs in Splunk to clearly map to specific hosts throughout the project.

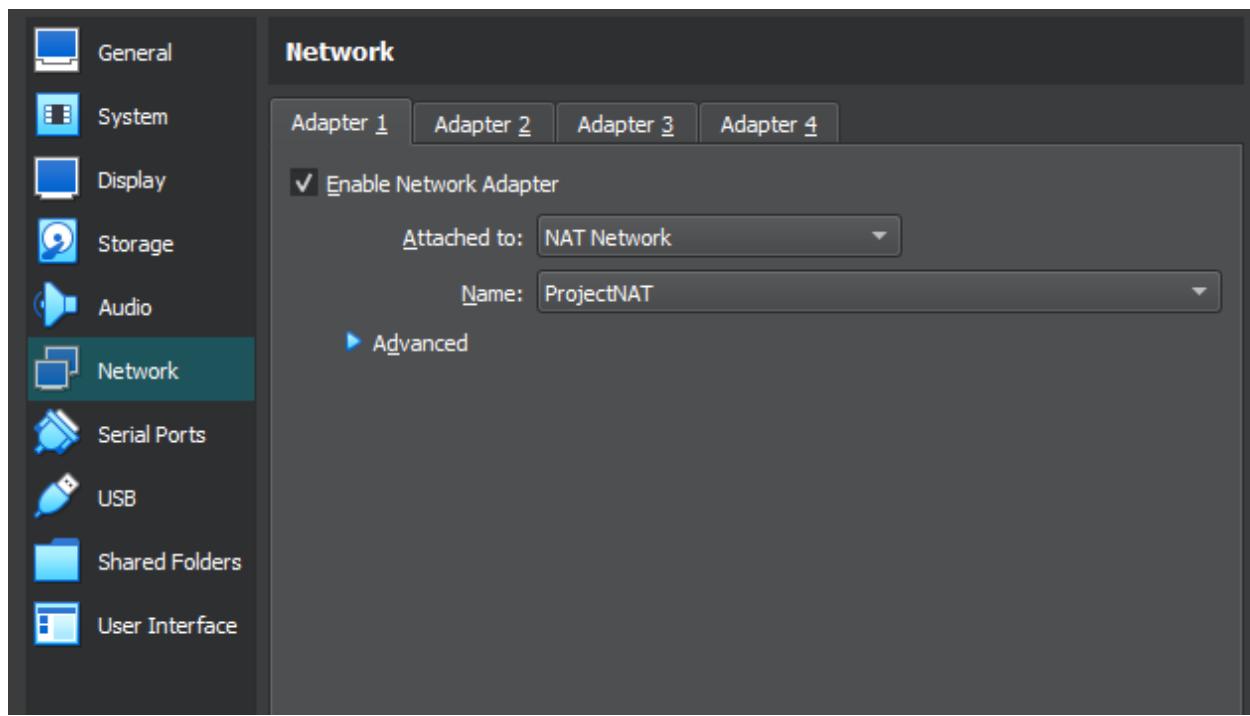
The Windows Server 2022 virtual machine will be promoted to a Domain Controller using Active Directory Domain Services. This creates a realistic enterprise environment where authentication, group membership, and administrative actions occur within a Windows domain. Operating the endpoints as domain-joined systems will give me meaningful security information to detect behaviors like login abuse and privilege changes in Splunk.

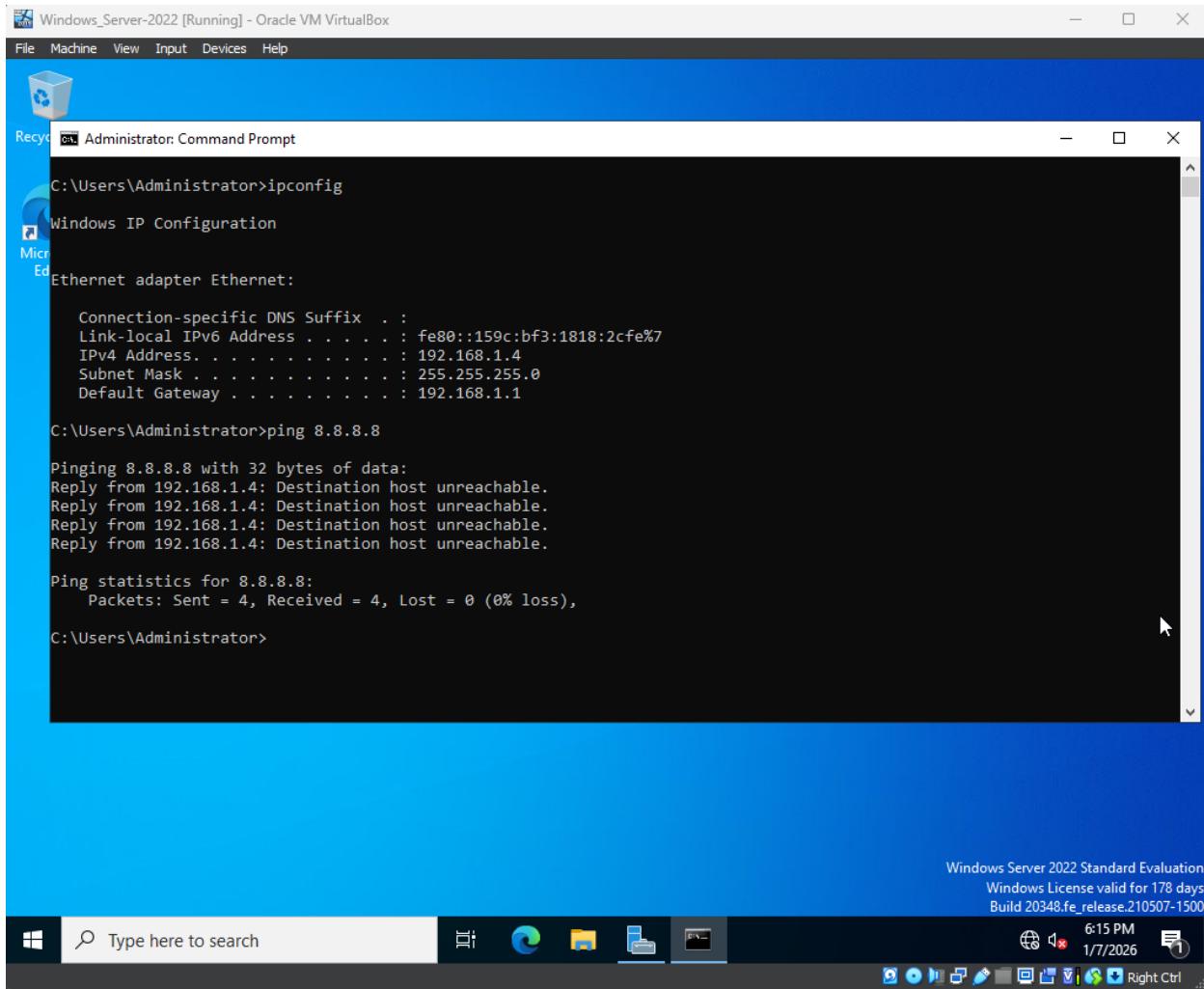
For the Windows 11 endpoint virtual machines to operate as domain-joined systems, their DNS settings will be pointed directly to the IP address of the Windows Server domain controller. After the server is promoted to a Domain Controller, it will also host the primary DNS service for the Active Directory domain. Each endpoint will be configured so that its network adapter uses the domain controller's static IP as the preferred DNS server, ensuring that all authentication and name resolution requests are handled internally by the domain. This configuration allows the Windows clients to locate domain resources such as AD, Group Policy, and later the Splunk server by hostname, which is required for a realistic security logging environment.

Create One Shared NAT Network

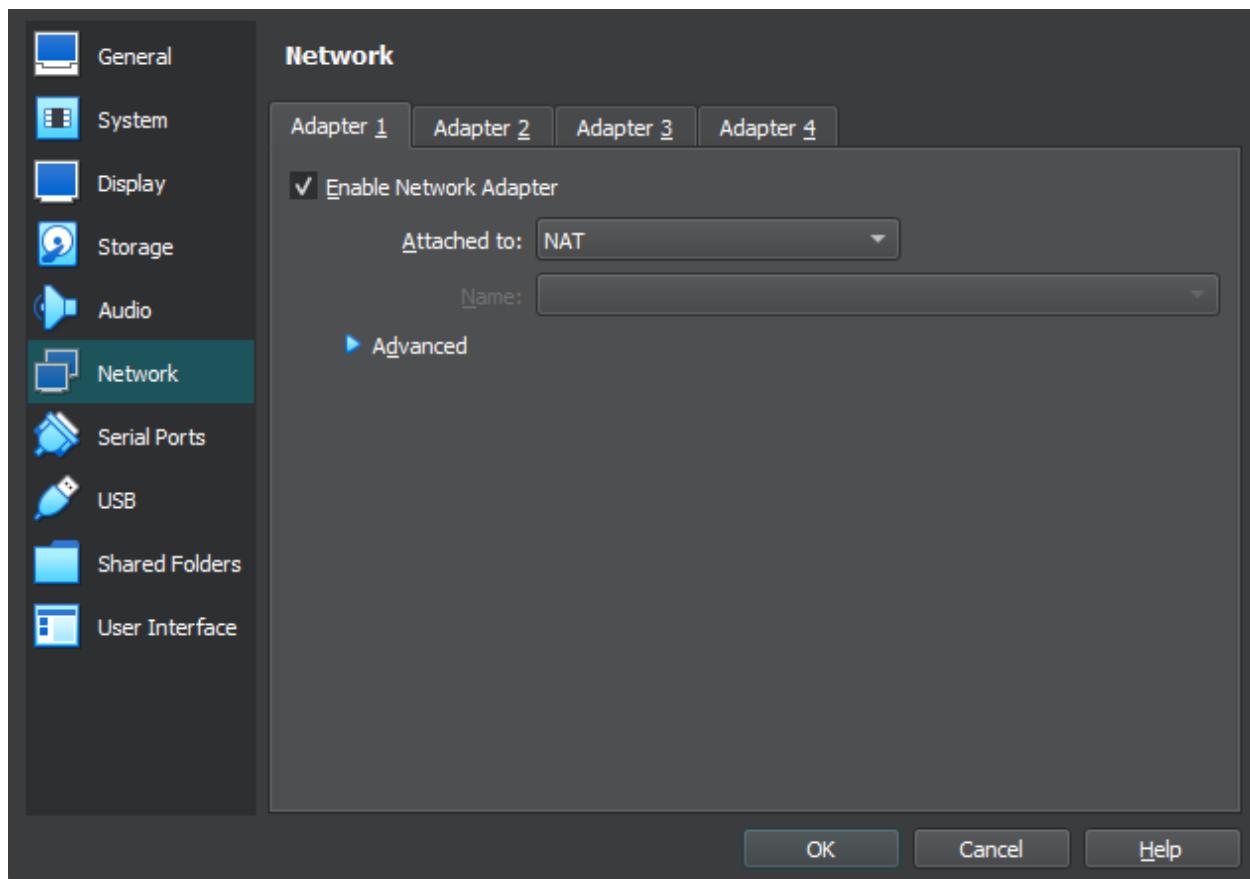


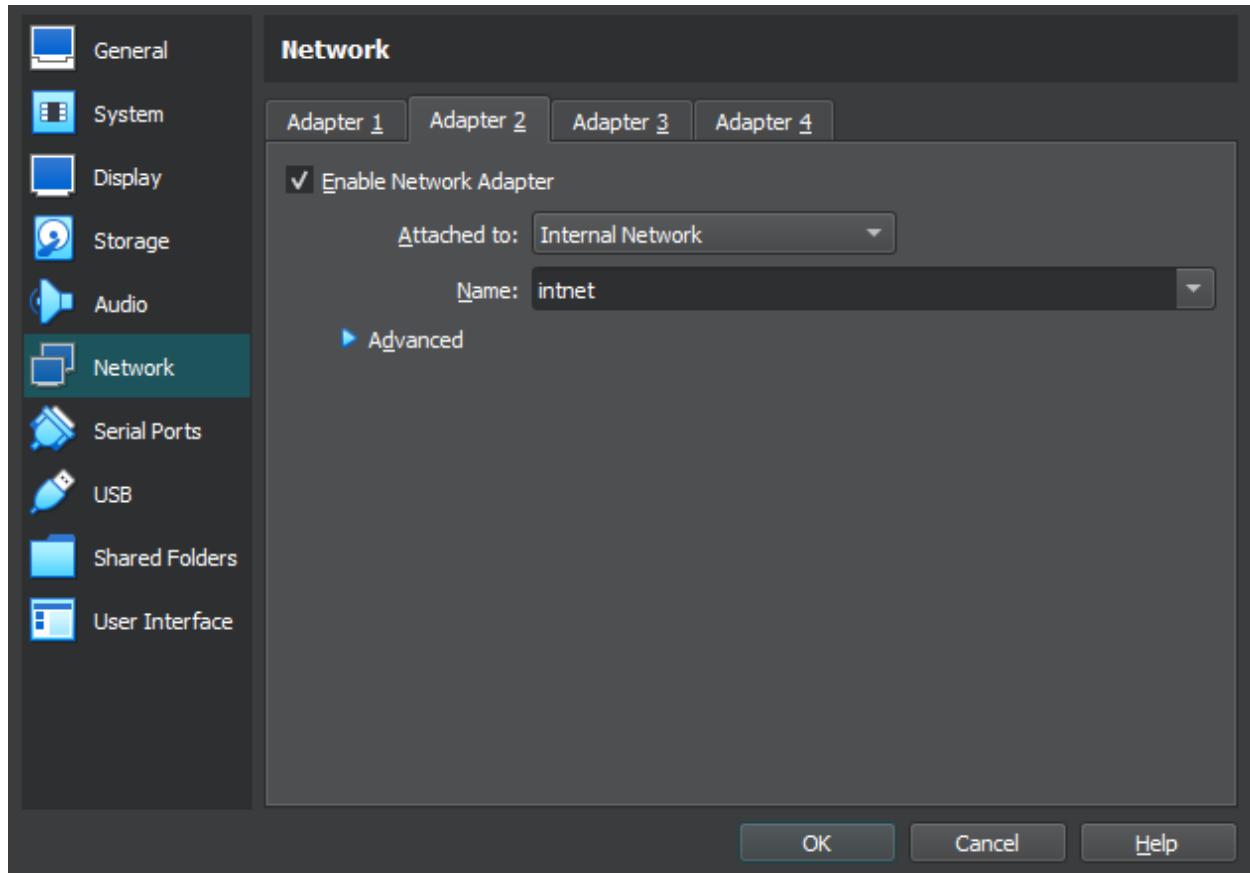
Now that the NAT network has been created, it will need to be added to each VMs network adapter in the settings while all of them are powered off.





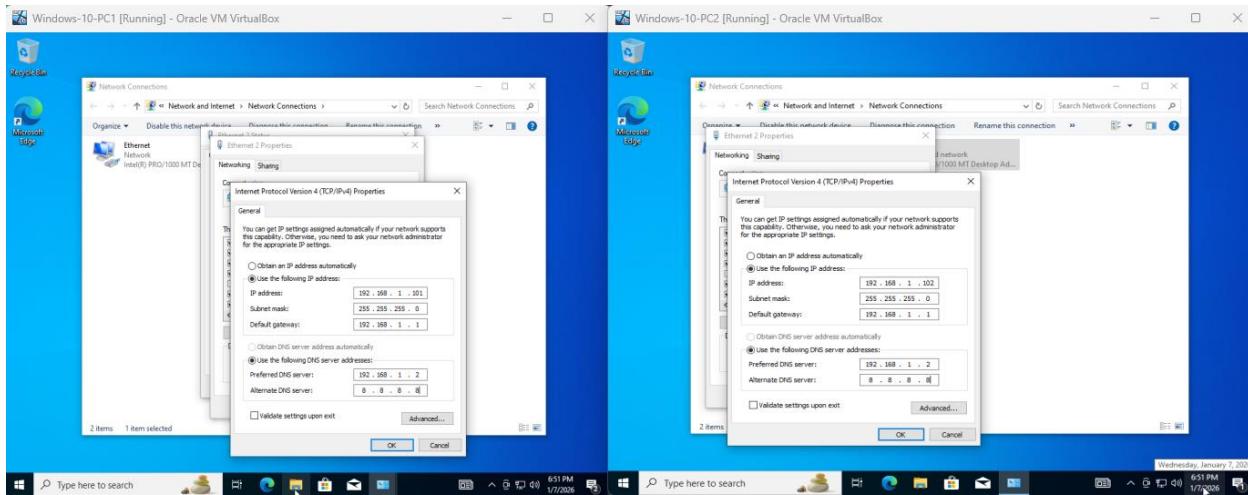
After powering the server to test this connection, I realized the NAT Network was not working properly. Although the systems were able to obtain IP addresses, internet connectivity could not be established even after spending significant time troubleshooting the configuration (See the screenshot above). After verifying that standard NAT worked correctly and testing multiple network settings, it became clear that the issue was related to VirtualBox's NAT Network rather than the virtual machines themselves. To avoid further delays, the lab will instead use two network adapters: one NAT adapter for internet access and one internal network adapter for communication between virtual machines.



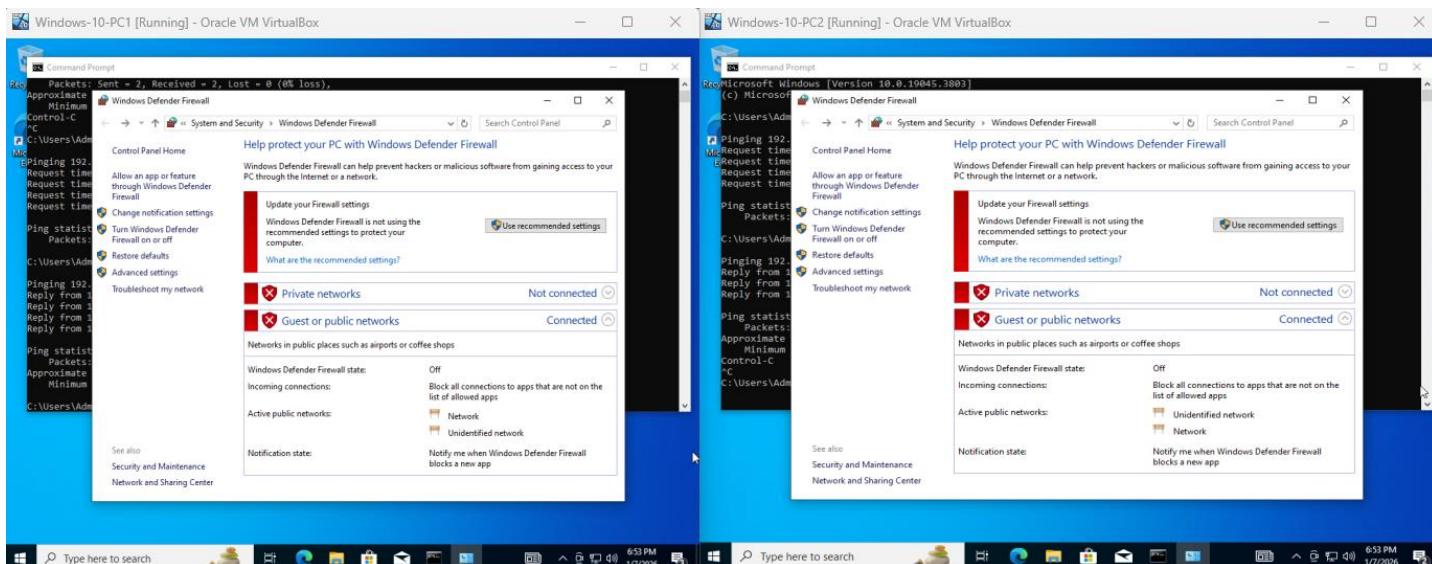


Statically Assigning IP Addresses

Now, I will assign static IP addresses to the Kali and both Windows VMs (Server was already done earlier). Using static addressing ensures consistent communication between the domain controller, endpoints, and attack system, and prevents issues caused by changing IP addresses. This is especially important for Active Directory, DNS resolution, and Splunk log forwarding, where systems must reliably reference one another throughout the lab environment. I will also set the preferred DNS IP address to the servers' IP on the Windows VMs as well.



Turned off Windows Defender to allow incoming ICMP requests. This is needed for the “ping” command to work. This was also done to leave the system intentionally vulnerable for the Kali machine later.



Successful ping between the computers and the server. An internal network has been established between these devices.

```

Windows-10-PC1 [Running] - Oracle VM VirtualBox
Command Prompt
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::98c:143:fe0a:3d2b%10
IPv4 Address . . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.2

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::cb29:7c0d:8533:6d5d%10
IPv4 Address . . . . . : 192.168.1.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

C:\Users\Admin>ping 192.168.1.2

Ping statistics for 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Admin>

Windows-10-PC2 [Running] - Oracle VM VirtualBox
Command Prompt
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::360c:c14d:17c3:7e5b%10
IPv4 Address . . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.2

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::74b8:43bb:cf62:5882%10
IPv4 Address . . . . . : 192.168.1.102
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

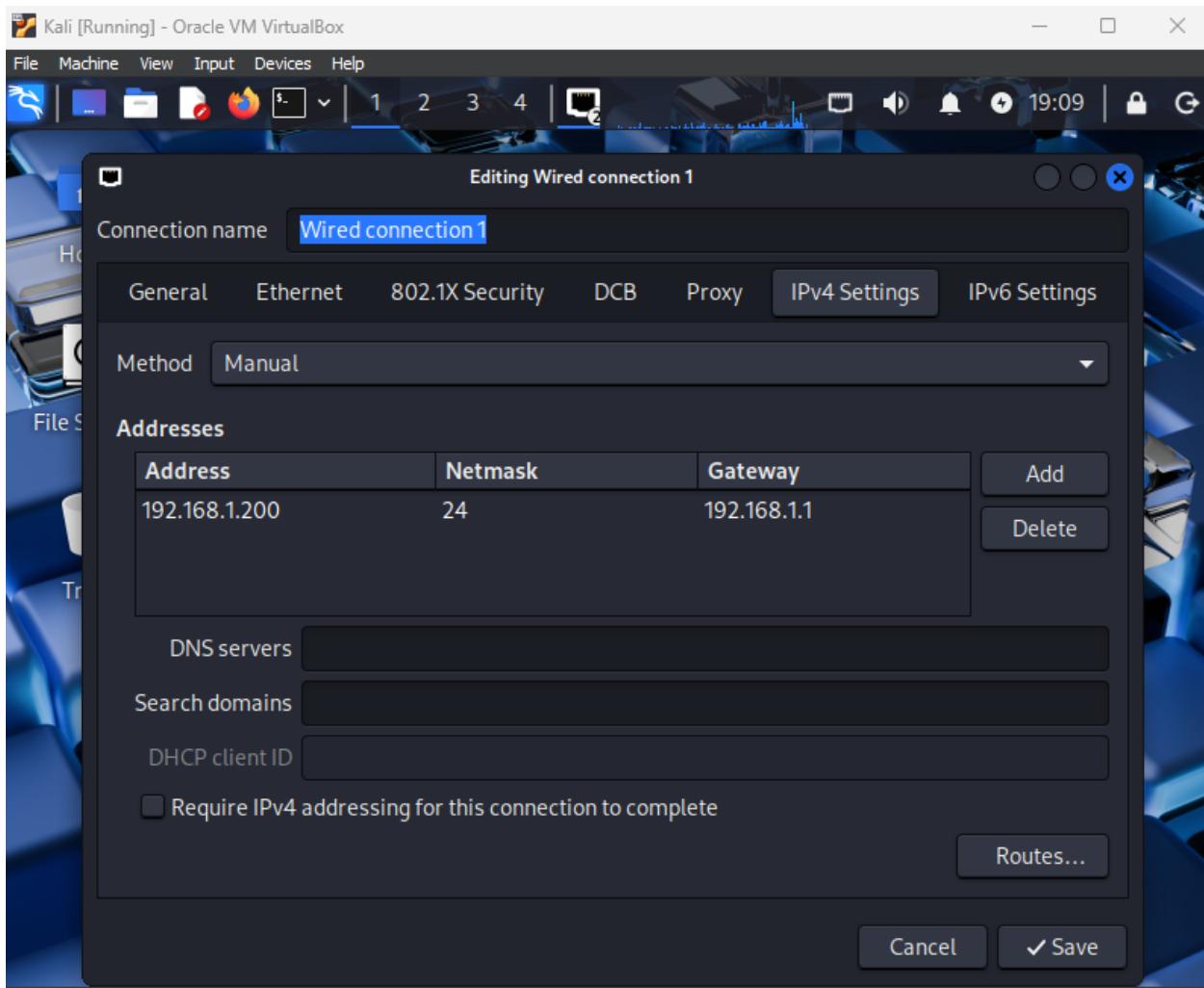
C:\Users\Admin>ping 192.168.1.2

Ping statistics for 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

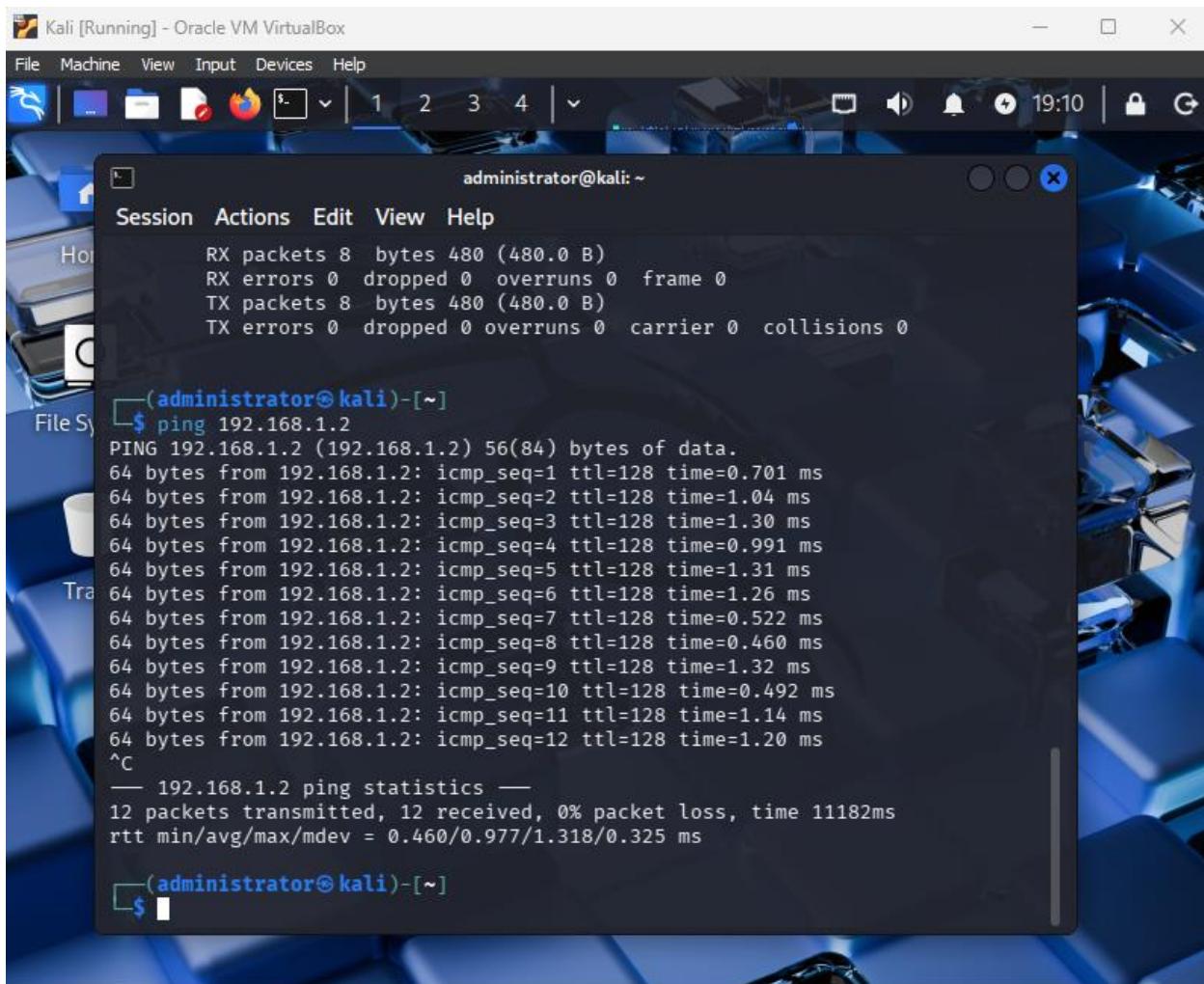
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Admin>

```



Kali machine can ping the server. This means that all devices are able to communicate with each other now.



The screenshot shows a terminal window titled "administrator@kali: ~" running on a Kali Linux desktop. The terminal displays the following output:

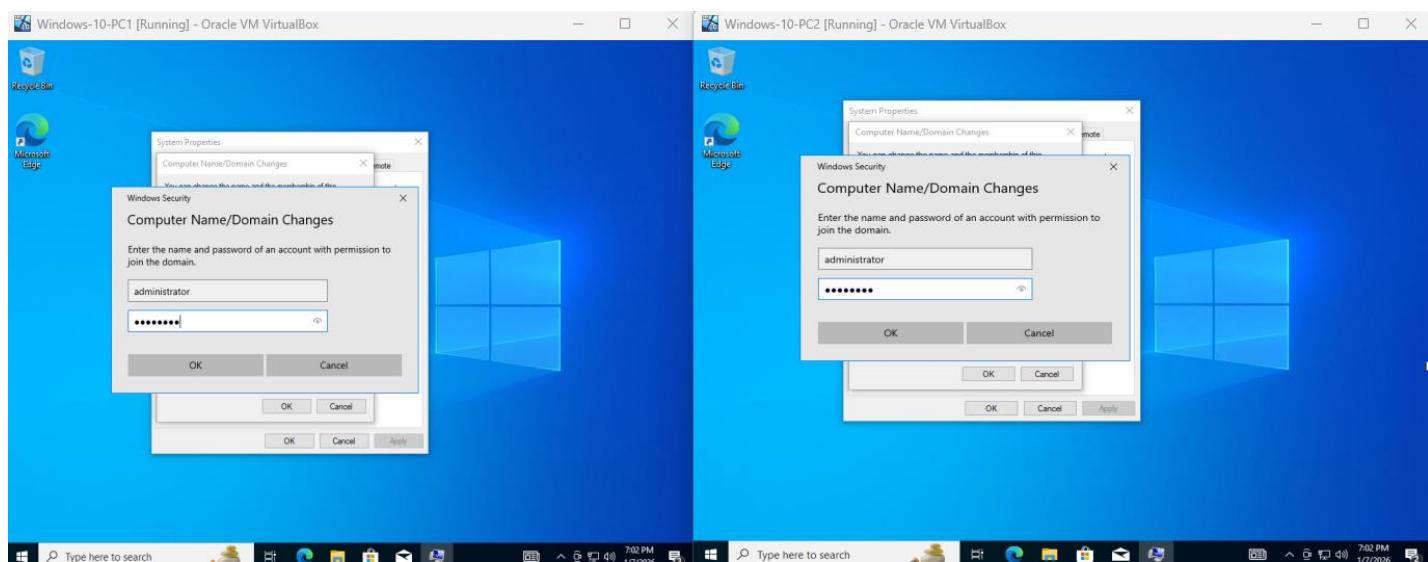
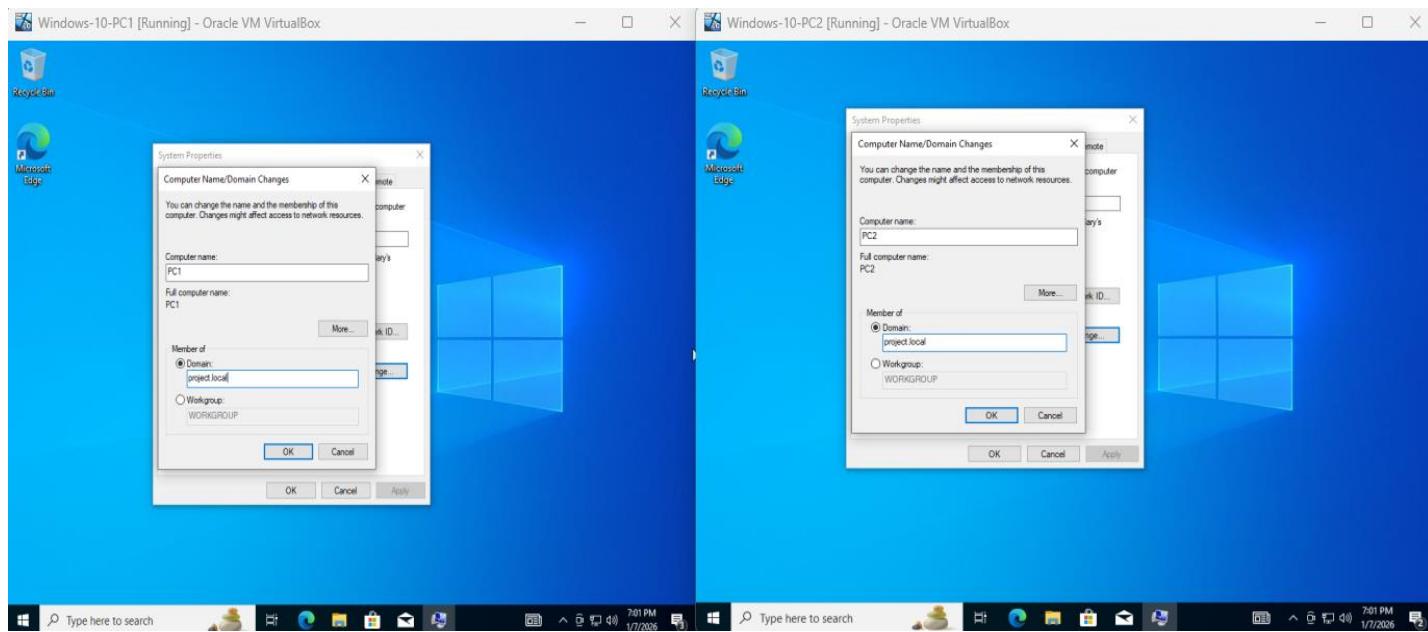
```
Session Actions Edit View Help
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

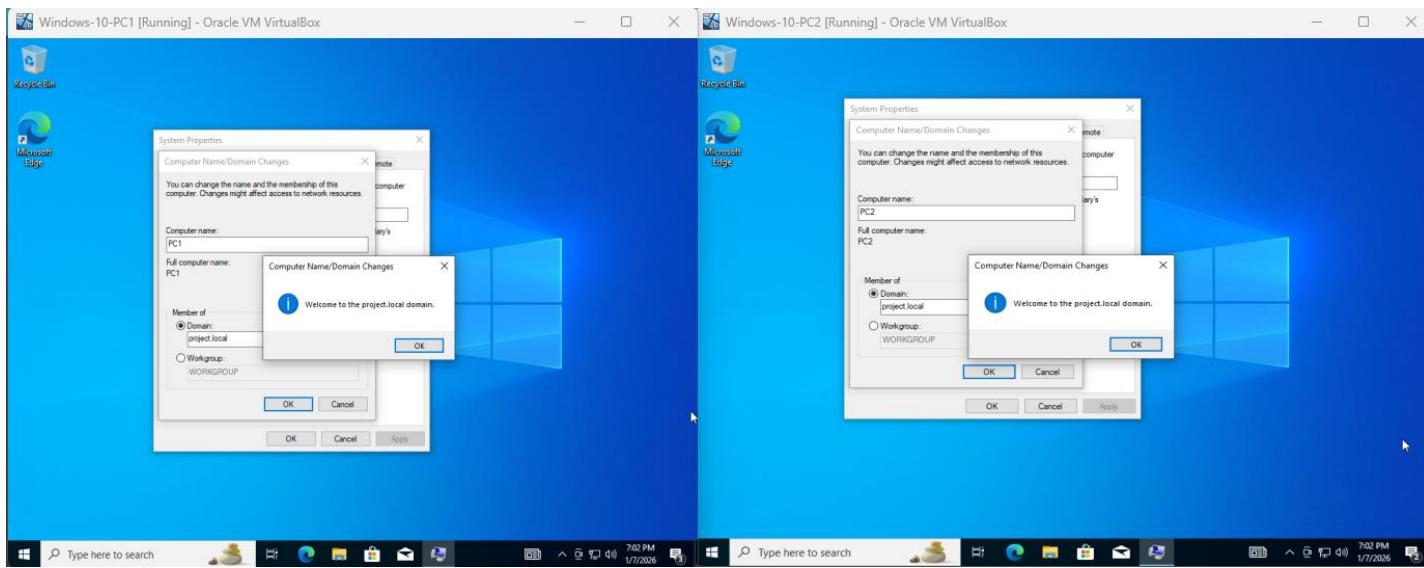
(administrator@kali)-[~]
$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=0.701 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=128 time=1.04 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=128 time=1.30 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=128 time=0.991 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=128 time=1.31 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=128 time=1.26 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=128 time=0.522 ms
64 bytes from 192.168.1.2: icmp_seq=8 ttl=128 time=0.460 ms
64 bytes from 192.168.1.2: icmp_seq=9 ttl=128 time=1.32 ms
64 bytes from 192.168.1.2: icmp_seq=10 ttl=128 time=0.492 ms
64 bytes from 192.168.1.2: icmp_seq=11 ttl=128 time=1.14 ms
64 bytes from 192.168.1.2: icmp_seq=12 ttl=128 time=1.20 ms
^C
— 192.168.1.2 ping statistics —
12 packets transmitted, 12 received, 0% packet loss, time 11182ms
rtt min/avg/max/mdev = 0.460/0.977/1.318/0.325 ms

(administrator@kali)-[~]
$
```

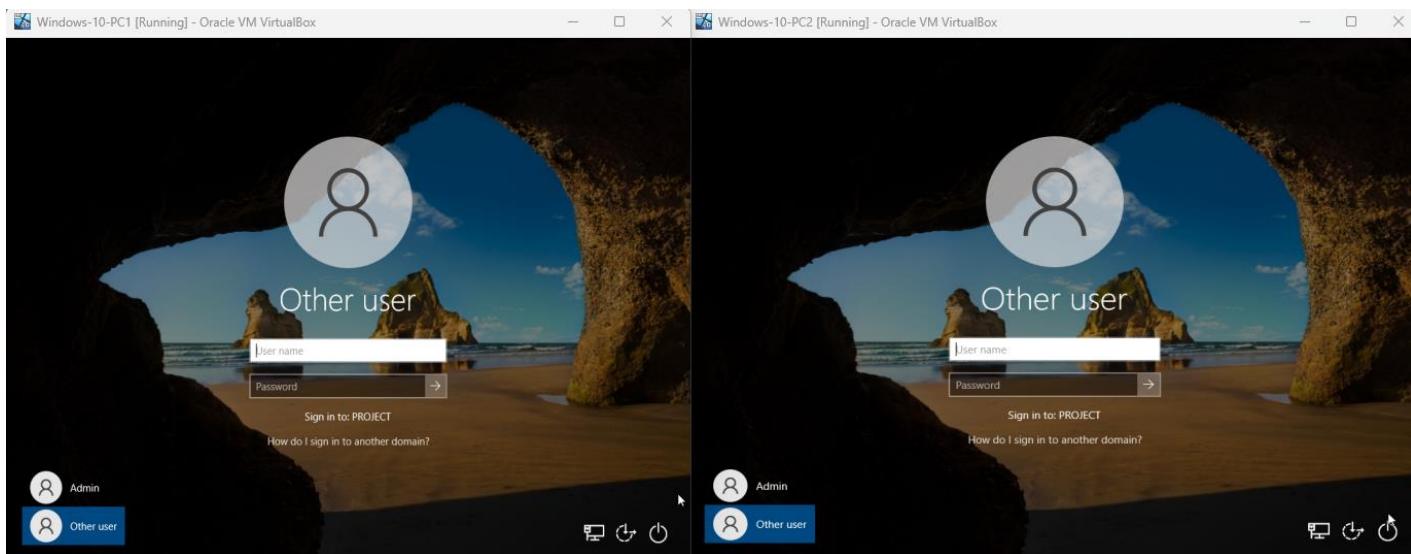
Domain Joining Windows Endpoints

With the domain controller and network configuration in place, the two Windows 11 endpoint virtual machines will now be joined to the Active Directory domain. Joining the endpoints to the domain allows user authentication, group policies, and domain-based activity to be centrally managed by the server. This step completes the core enterprise setup and enables the generation of realistic authentication and endpoint security events for later analysis in Splunk.





Both PCs are now domain joined.

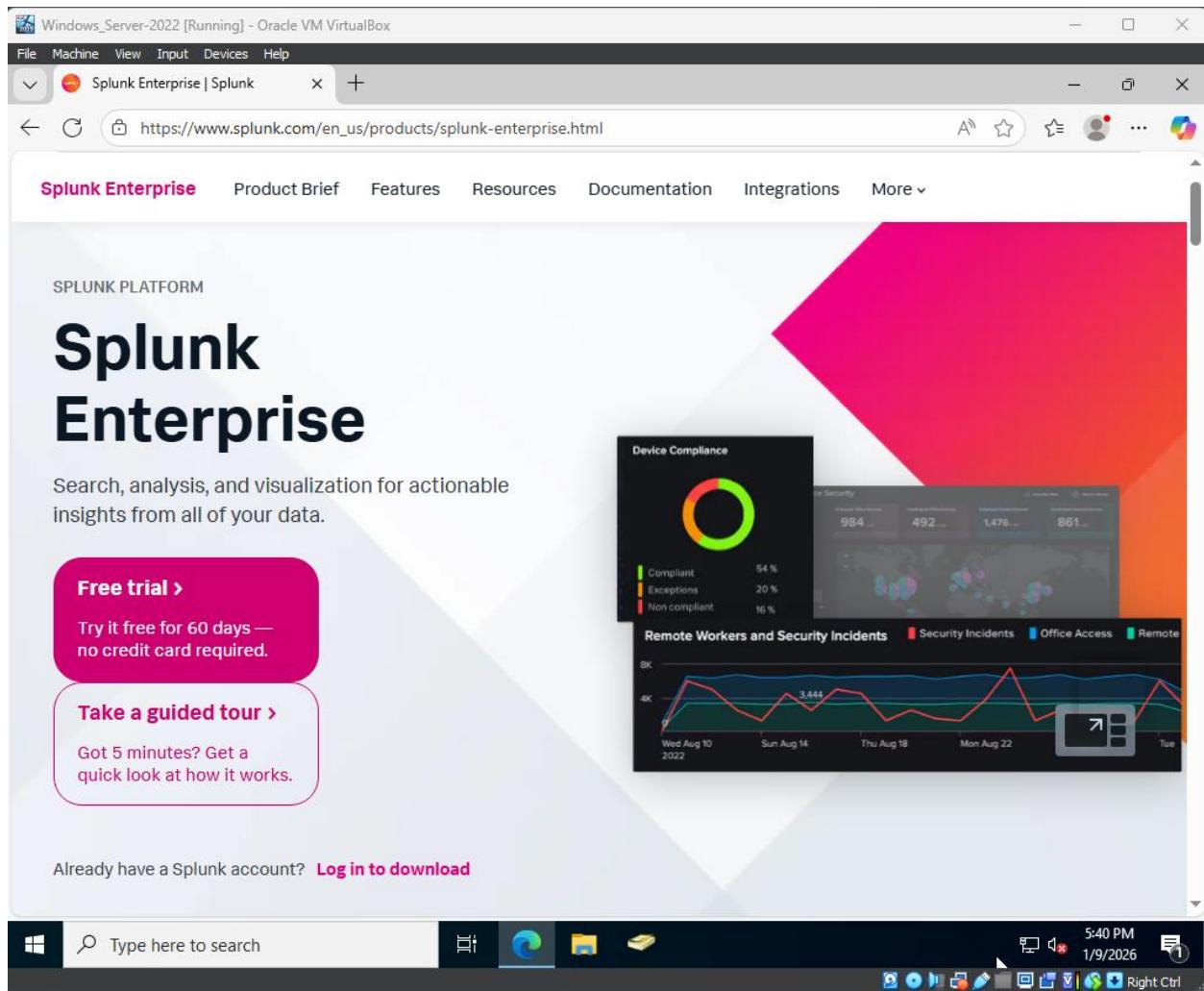


At this stage, the Active Directory domain has been successfully created, establishing a centralized authentication and management system that represents a small enterprise network. The Windows endpoints are domain-joined and generate realistic user and administrative activity within the environment. The Kali Linux machine is also connected to the internal network, allowing it to interact with domain systems and simulate adversarial behavior. This setup creates a more realistic lab environment and improves the quality of security alerts generated for later analysis in Splunk.

Splunk Installation and Setup

With the domain environment in place, Splunk will be installed and configured on the Windows Server to serve as the centralized SIEM for the lab. This includes setting up Splunk Enterprise, verifying basic functionality, and preparing the system to receive logs from the domain-joined endpoints. Establishing Splunk at this stage allows security events generated across the environment to be collected, searched, and analyzed as the foundation for later detection development and AI-assisted triage.

I will be using the free trial.



Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Splunk Enterprise Free Trial | Splunk

https://www.splunk.com/en_us/download/splunk-enterprise.html?locale=en_us

GET STARTED

Choose Your Download

Splunk Enterprise 10.0.2

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

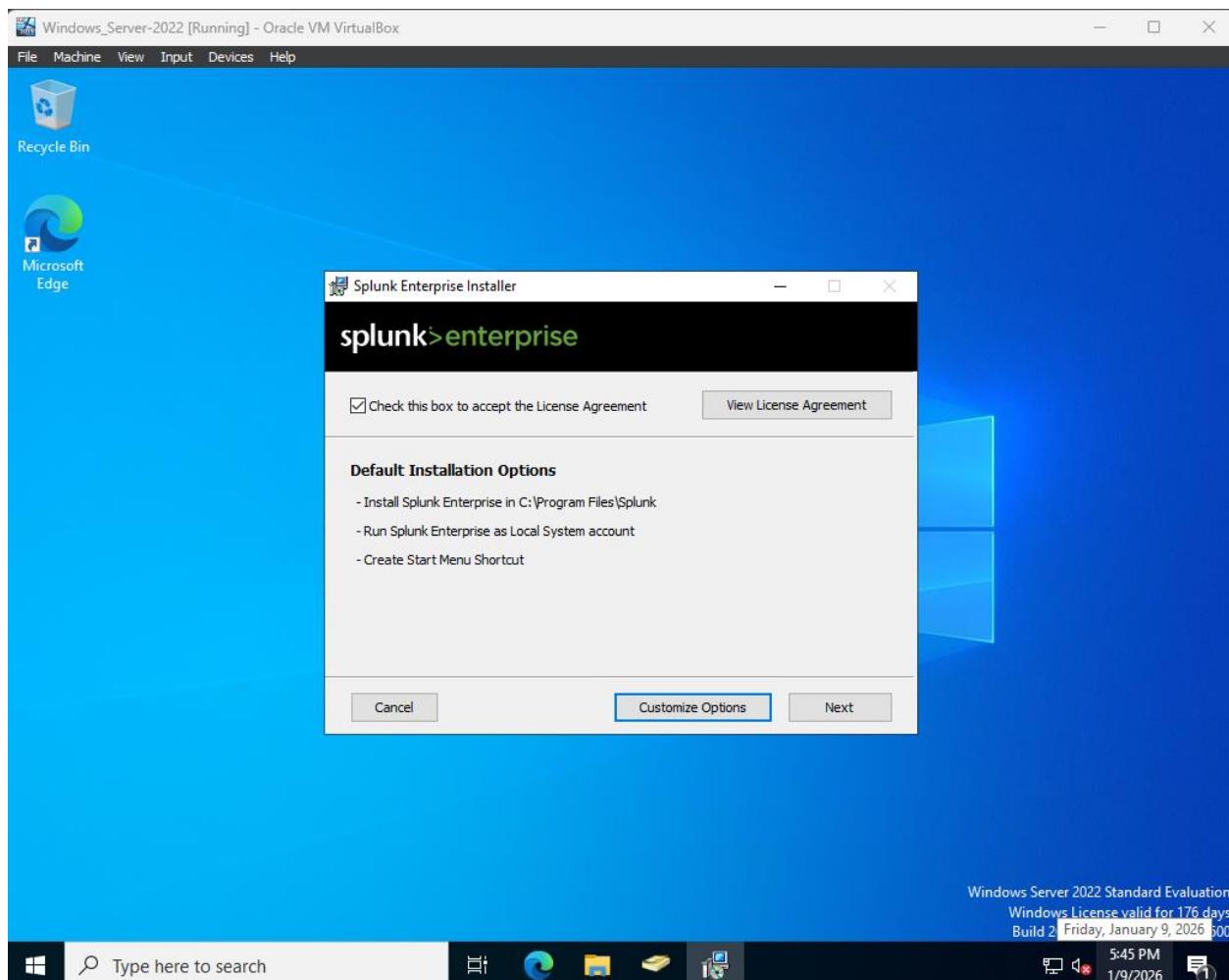
Windows **Linux** **Mac OS**

64-bit **Windows Server 2019, 2022, 2025** **.msi** 915.41 MB **Download Now** **Copy wget link** More

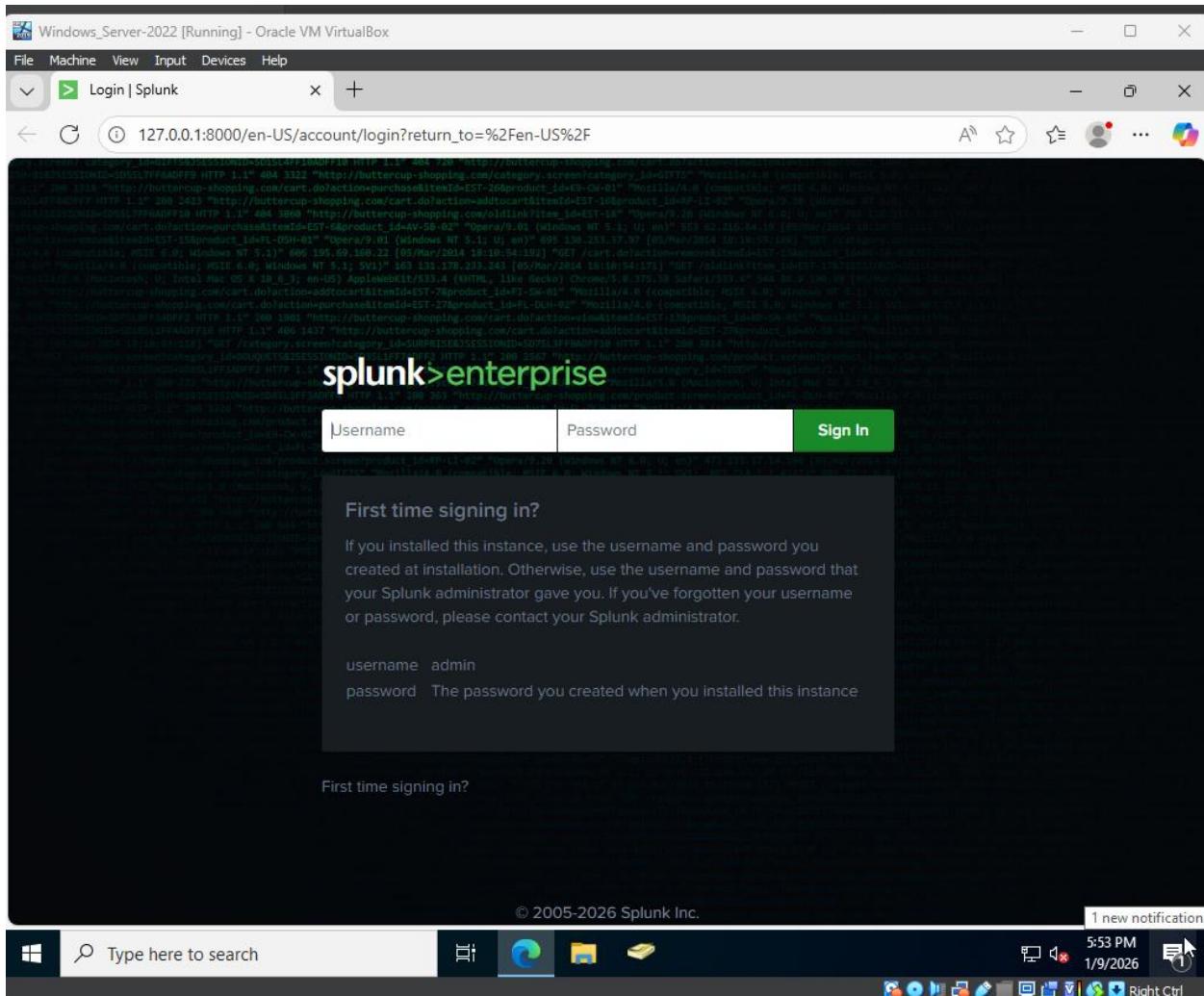
[Release Notes](#) | [System Requirements](#) | [Previous Releases](#) | [All Other Downloads](#)

Type here to search

5:43 PM
1/9/2026



The web UI of Splunk Enterprise after installation.

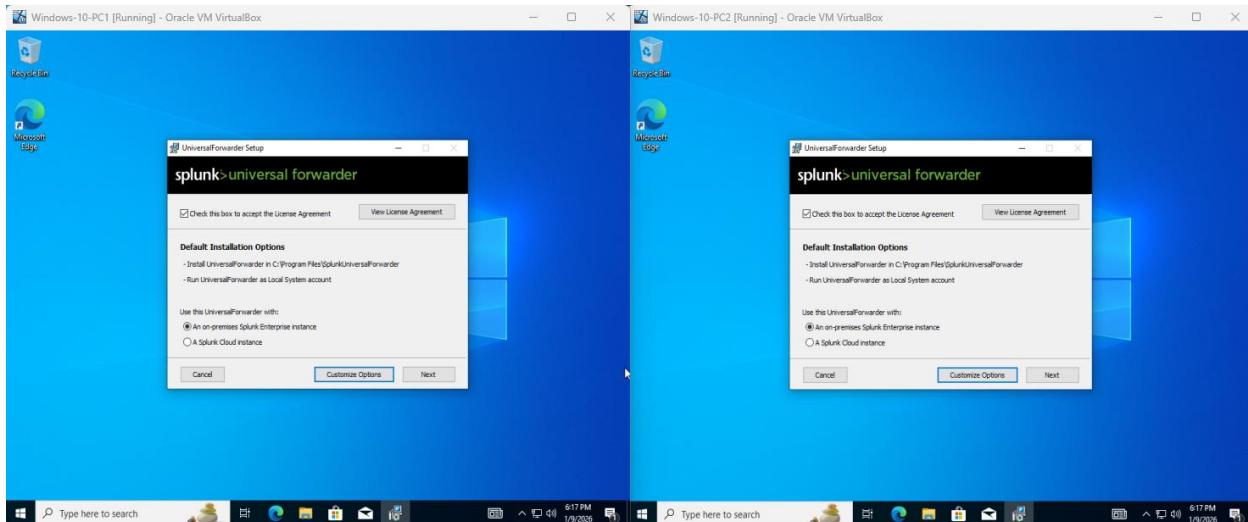


Once I logged, I navigated to the settings page. From there I went into forwarding and receiving in order to add a receiving port. This is needed to add the Windows 10 PCs.

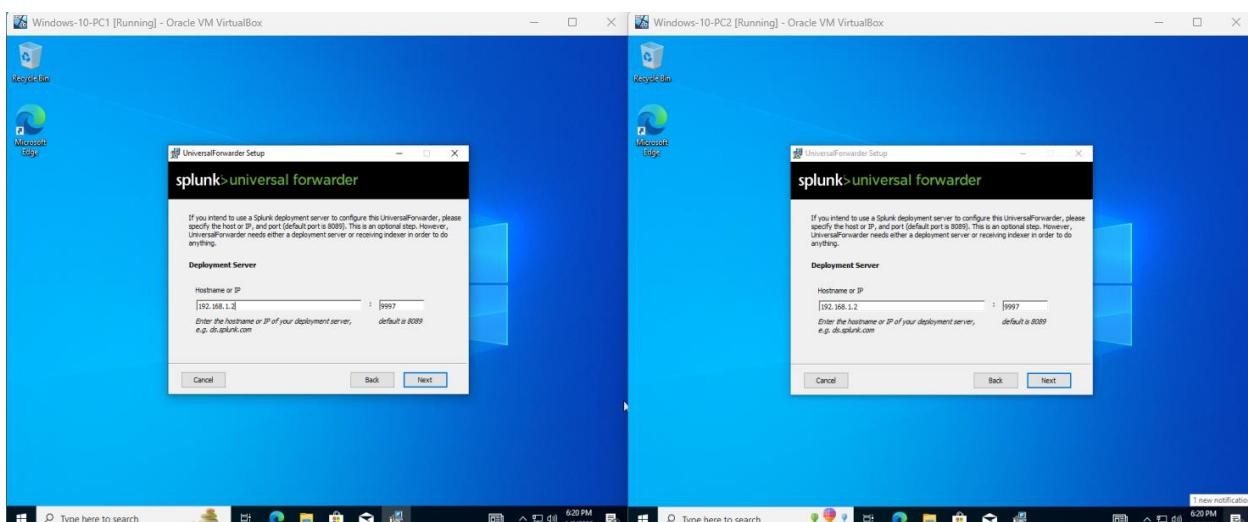
The screenshot shows the Splunk Enterprise Settings interface. The title bar reads "Windows_Server-2022 [Running] - Oracle VM VirtualBox". The main window is titled "Settings | Splunk" and displays the "Receive data" section. The URL in the address bar is "127.0.0.1:8000/en-US/manager/launcher/data/inputs/tcp/cooked". The top navigation bar includes "splunk>enterprise", "Apps", "Administra...", "Messages", "Settings", "Activity", "Help", "Find", and a search icon. A green button labeled "New Receiving Port" is visible in the top right. The main content area shows a table with one item: "Listen on this port" (9997), "Status" (Enabled), and an "Actions" column with a "Delete" link. Below the table are "filter" and "25 per page" buttons. The bottom of the screen shows a Windows taskbar with the date and time as "5:56 PM 1/9/2026".

Installing the Splunk Universal Forwarder on the two Windows 10 PCs.

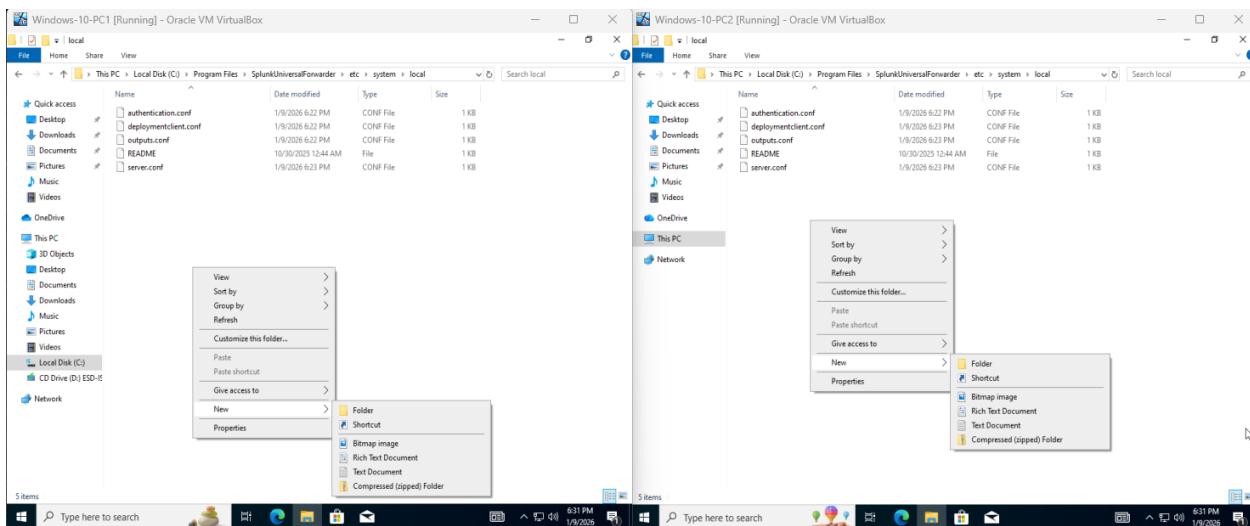
The screenshot shows two side-by-side web browser windows, both displaying the download page for the Splunk Universal Forwarder 10.0.2. The left window is for "Windows-10-PC1" and the right is for "Windows-10-PC2", both running in Oracle VM VirtualBox. The URL in both browser bars is "https://www.splunk.com/en_us/download/universal-forwarder.html?utm_campaign=bing_amer_en_search...". The page content is identical, featuring the title "Splunk Universal Forwarder 10.0.2" and a brief description of what universal forwarders do. It then prompts the user to "Choose Your Installation Package" for Windows, Linux, Mac OS, FreeBSD, Solaris, or AIX. Under the Windows section, there are two options: "Windows 10" (32-bit) and "Windows 10, 11 Windows Server 2019, 2022, 2025" (64-bit). Each option has a ".msi" file size (64.9 MB and 158.75 MB respectively), a "Download Now" button, a "Copy wget link" button, and a "More" dropdown menu. At the bottom of each window, there are links for "Release Notes", "System Requirements", "Previous Releases", and "All Other Downloads". The bottom of the screen shows a Windows taskbar with the date and time as "6:15 PM 1/9/2026".



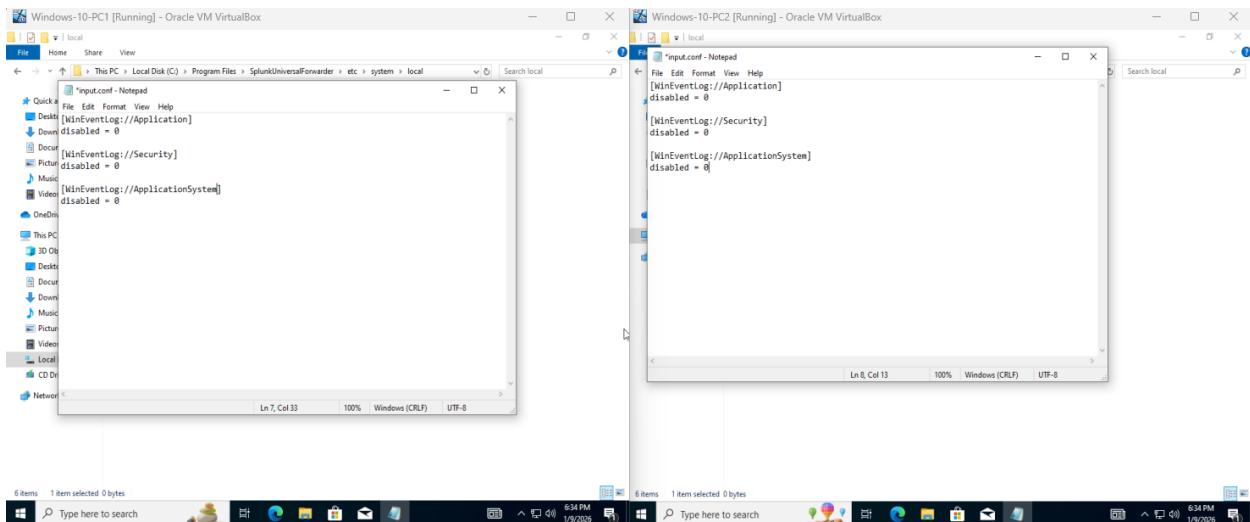
Added the private IP of the server along with the port we configured to receive.



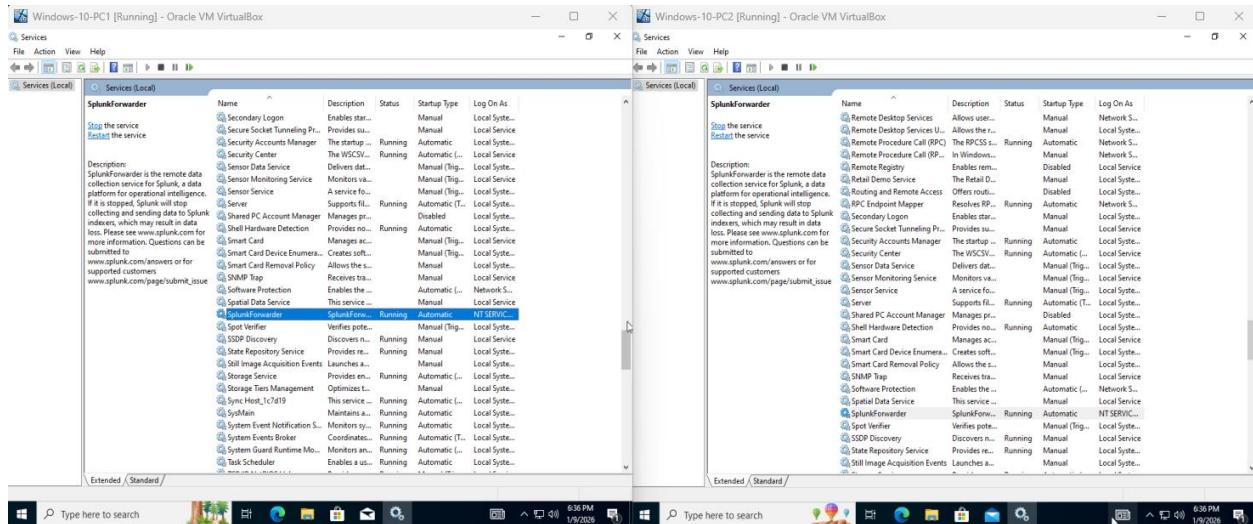
After the install, I will need to create a new text file in the SplunkUniversalForwarder folder that is now in the C drive. This text file will be called inputs.conf.



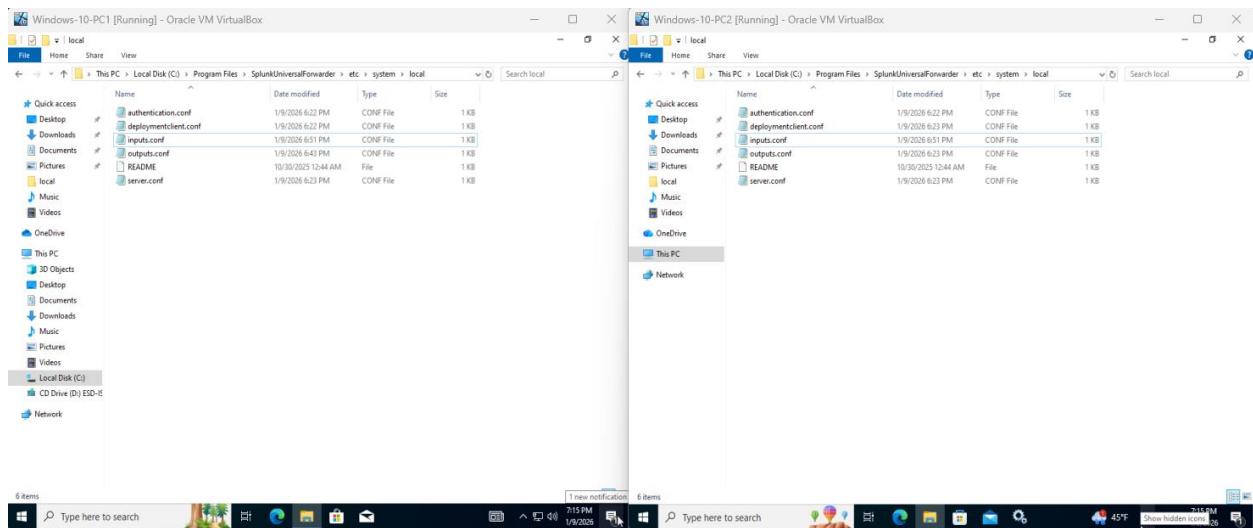
I include this bit of writing in the text files and save them.



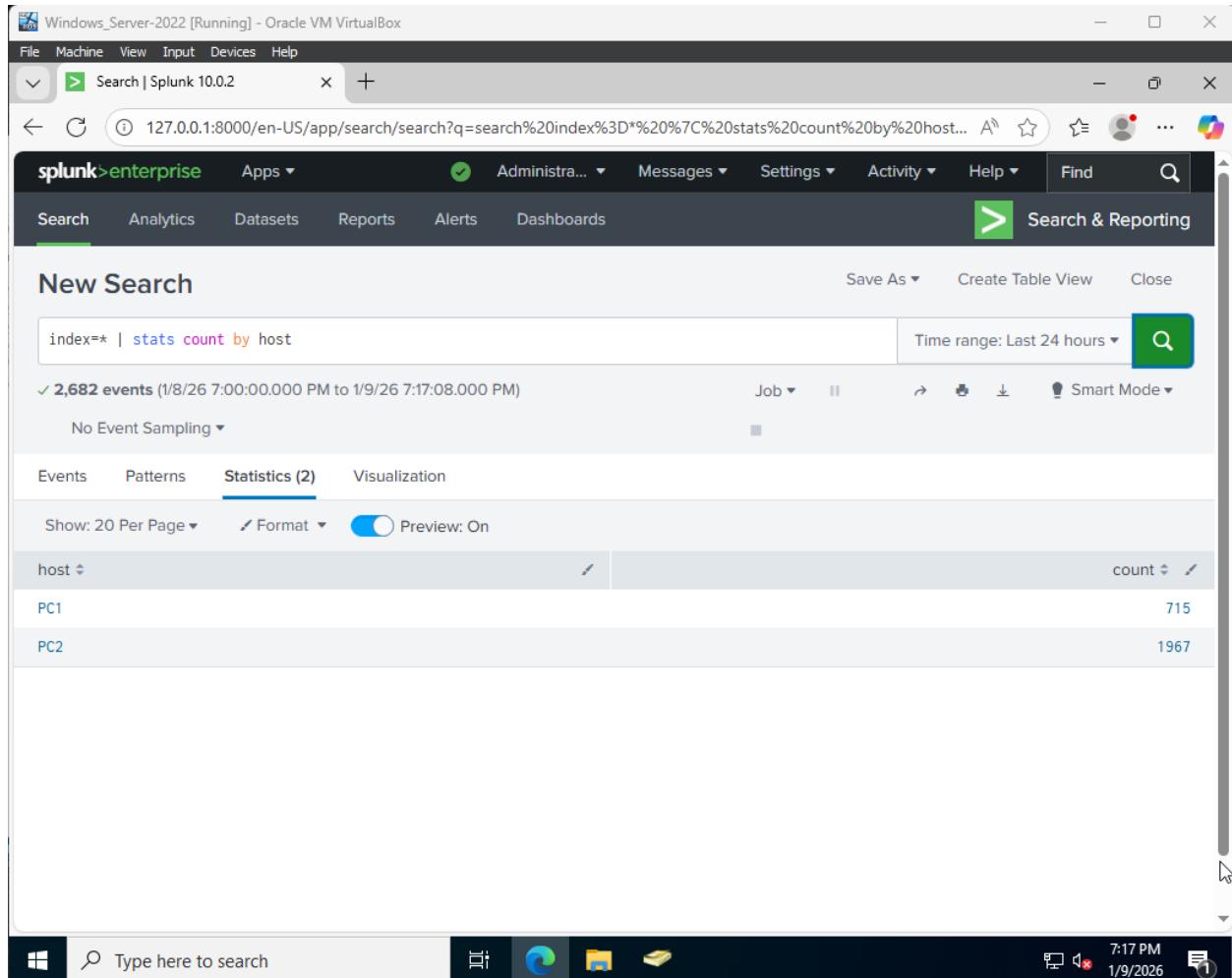
In the services application, I had to restart the SplunkForwarder service.



The two PCs were not showing up in the portal. After some time of troubleshooting, I changed the file type to a CONF file and it worked. I had to view the hidden file extensions to see it was inputs.conf.txt instead of inputs.conf.

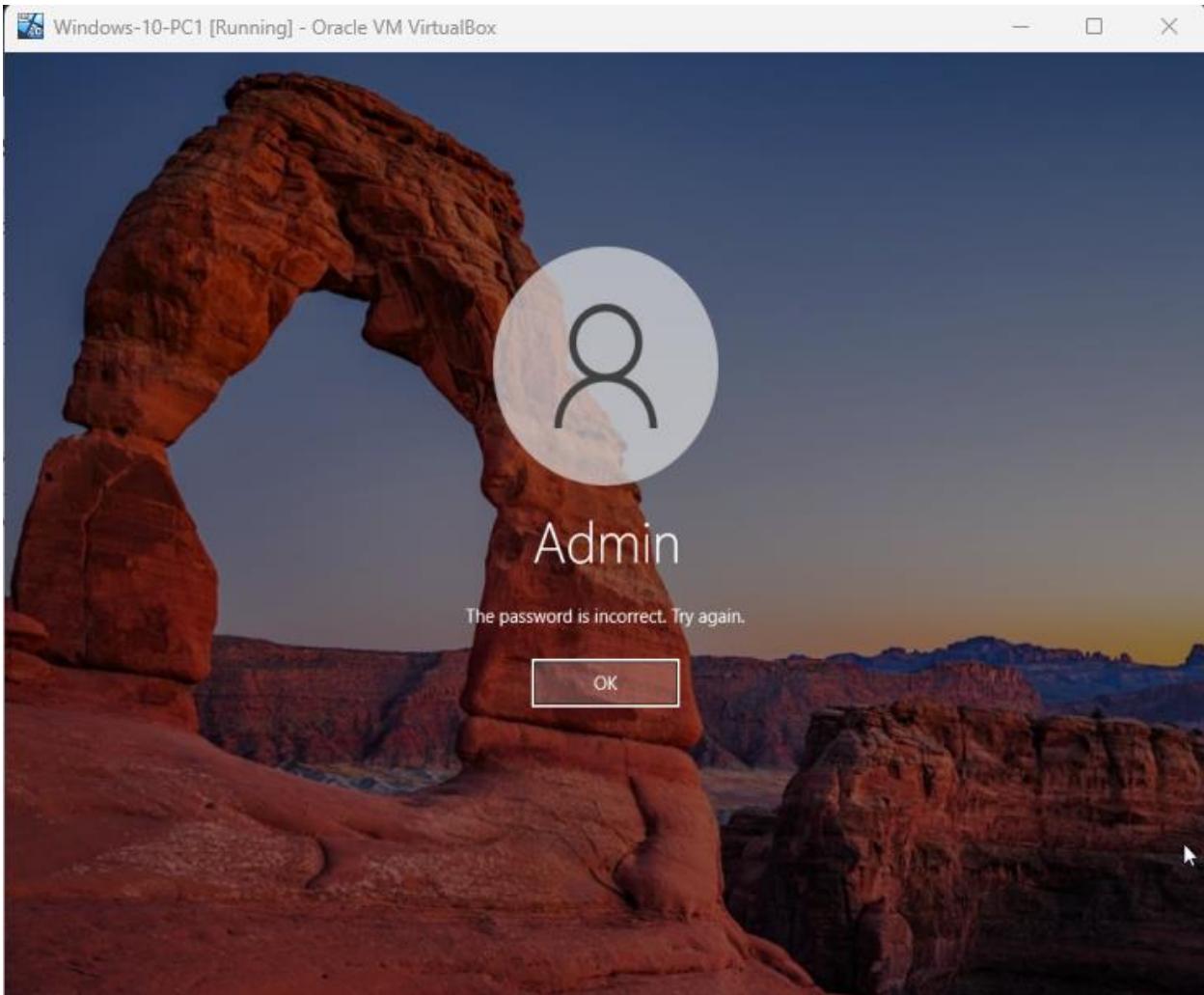


As you can see, the two PCs are now seen in the portal with all of their logs.



Setting Up SPL

Splunk Processing Language (SPL) was used to search, filter, and analyze security logs collected from domain-joined systems within the lab environment. SPL queries allow for real-time visibility into authentication activity, system events, and user behavior by correlating data across multiple hosts. These searches were further refined to detect suspicious patterns such as repeated failed login attempts.



Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Search | Splunk 10.0.2

Search | Splunk 10.0.2 127.0.0.1:8000

splunk enterprise Apps Administra... Messages Settings Activity Help Find Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

New Search

Save As Create Table View Close

index=* sourcetype="WinEventLog:Security" EventCode=4625 earliest=-5m | stats count as failed_logins by host, user | where failed_logins>= 3 | sort - failed_logins

Time range: Last 24 hours

3 events (1/12/26 7:10:17.000 PM to 1/12/26 7:15:18.179 PM) No Event Sampling Job ▾ II ▾ Verbose Mode ▾

Events (3) Patterns Statistics (0) Visualization

Timeline format ▾ – Zoom Out + Zoom to Selection × Deselect 1 minute per column

Format Show: 20 Per Page View: List

Hide Fields All Fields

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

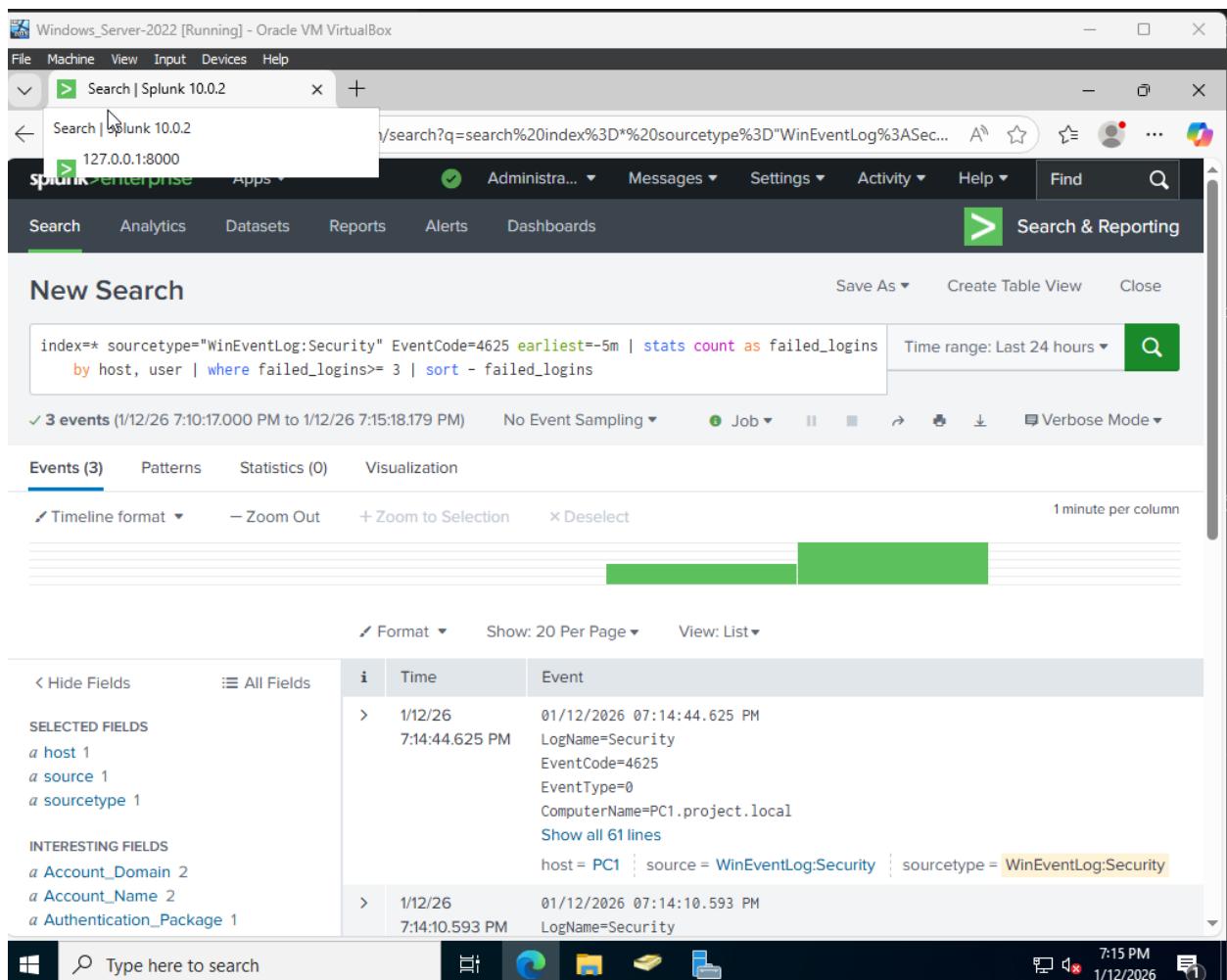
INTERESTING FIELDS

a Account_Domain 2
a Account_Name 2
a Authentication_Package 1

i	Time	Event
>	1/12/26 7:14:44.625 PM	01/12/2026 07:14:44.625 PM LogName=Security EventCode=4625 EventType=0 ComputerName=PC1.project.local Show all 61 lines host = PC1 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	1/12/26 7:14:10.593 PM	01/12/2026 07:14:10.593 PM LogName=Security

Type here to search

7:15 PM 1/12/2026



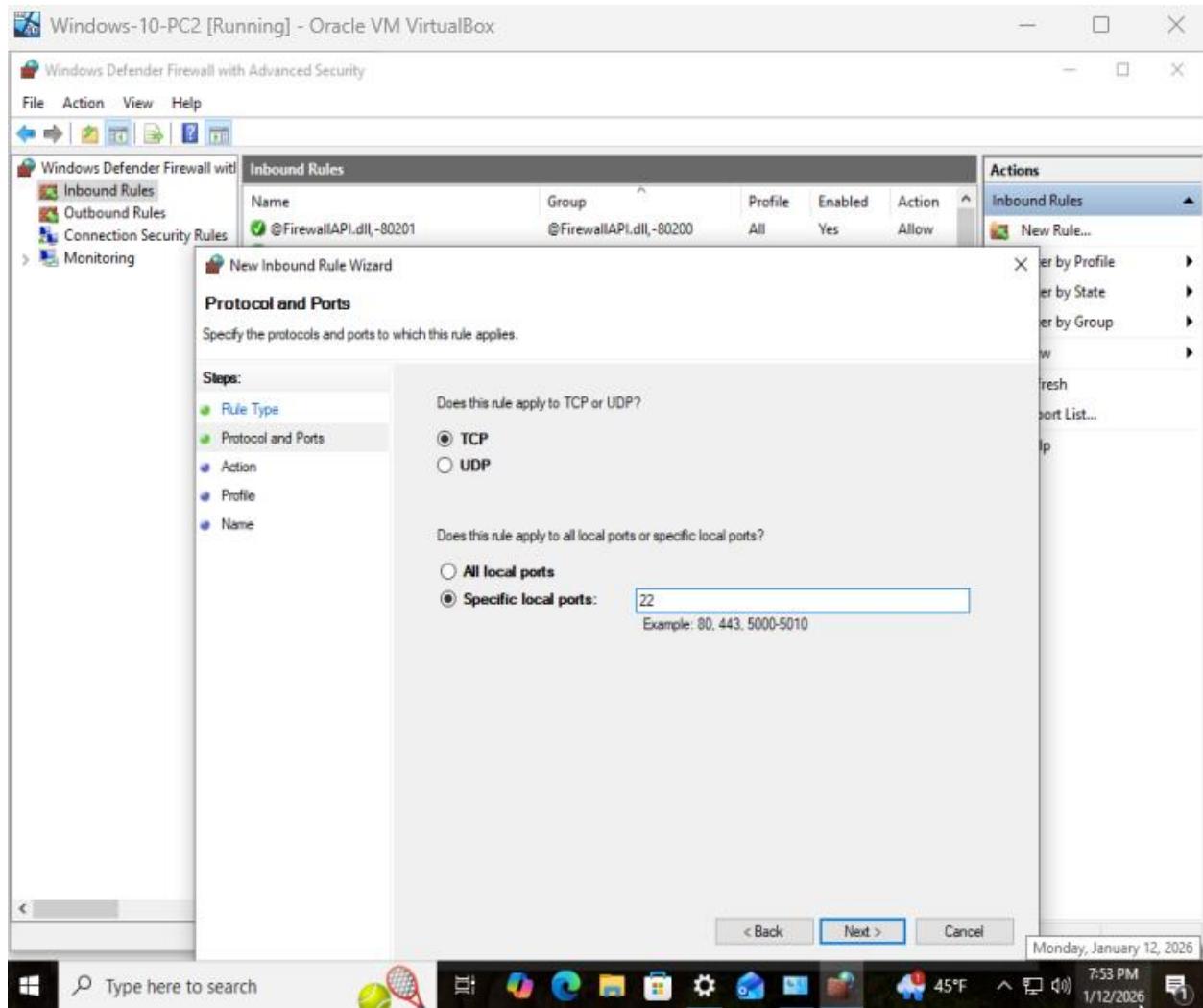
The screenshot shows a Splunk search interface running in Oracle VM VirtualBox. The search results are displayed in a table with columns for Time, Event, and several other fields. The table shows five events, all of which are failed log-in attempts (EventCode=4625) from the host PC1. The events occurred on 1/12/26 at various times between 6:51:27 PM and 6:50:43 PM. The logs indicate that the source is the WinEventLog:Security and the sourcetype is WinEventLog:Security. The ComputerName is consistently listed as PC1.project.local. The Splunk interface also displays a sidebar with selected and interesting fields, and a bottom navigation bar with standard Windows icons.

	i	Time	Event
< Hide Fields	All Fields	1/12/26 6:51:27.273 PM	01/12/2026 06:51:52.273 PM LogName=Security EventCode=4625 EventType=0 ComputerName=PC1.project.local Show all 61 lines host = PC1 source = WinEventLog:Security sourcetype = WinEventLog:Security
SELECTED FIELDS		1/12/26 6:50:48.669 PM	01/12/2026 06:50:48.669 PM LogName=Security EventCode=4625 EventType=0 ComputerName=PC1.project.local Show all 61 lines host = PC1 source = WinEventLog:Security sourcetype = WinEventLog:Security
INTERESTING FIELDS		1/12/26 6:50:46.299 PM	01/12/2026 06:50:46.299 PM LogName=Security EventCode=4625 EventType=0 ComputerName=PC1.project.local Show all 61 lines host = PC1 source = WinEventLog:Security sourcetype = WinEventLog:Security
		1/12/26 6:50:43.901 PM	01/12/2026 06:50:43.901 PM LogName=Security EventCode=4625 EventType=0 ComputerName=PC1.project.local Show all 61 lines host = PC1 source = WinEventLog:Security sourcetype = WinEventLog:Security

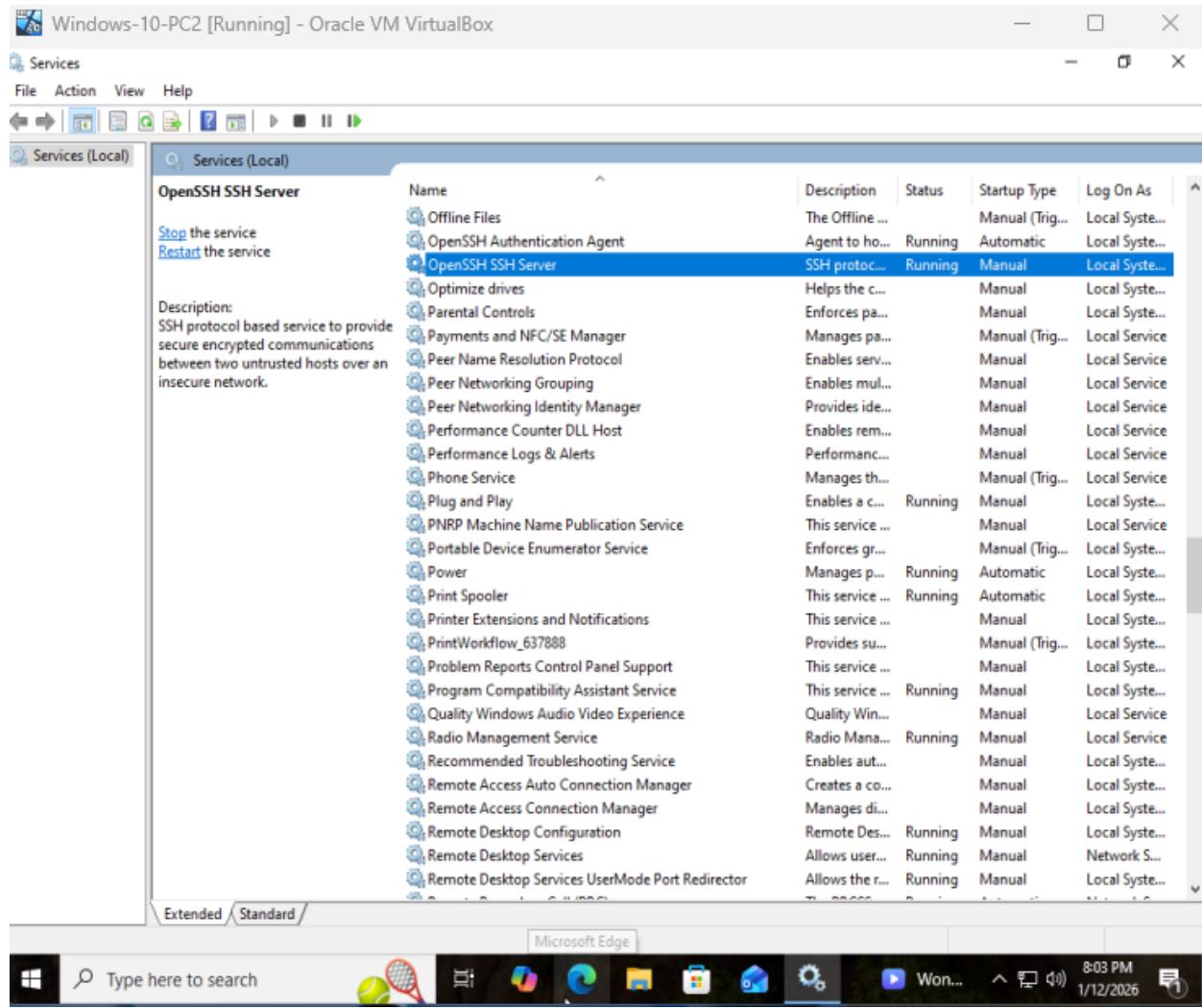
As you can see, the failed log in attempts have been sent over to the server.

Using Kali to Brute Force into the System and Create Logs

Enabling port 22 for SSH to allow for vulnerabilities. Kali will attack using SSH.



Starting up the SSH Server service to allow for SSH connections.



Testing the SSH and seeing that does indeed work.

Kali [Running] - Oracle VM VirtualBox

Administrator: C:\Windows\system32\conhost.exe

Session Actions Edit View Help

```
(administrator@kali)-[~]
$ ssh Admin@192.168.1.102
The authenticity of host '192.168.1.102 (192.168.1.102)' can't be established
.
ED25519 key fingerprint is: SHA256:C24j0qsQ2KR80xHQ1c46wCAF06oE0pfLyevTWSr0LL
E
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.102' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
Admin@192.168.1.102's password:
```

Microsoft Windows [Version 10.0.19045.6456]
(c) Microsoft Corporation. All rights reserved.

```
admin@PC2 C:\Users\Admin>
```

Using a basic Hydra tool command to attempt the SSH connection.

Kali [Running] - Oracle VM VirtualBox

Session Actions Edit View Help

```
Enter the service to attack (eg: ftp, ssh, http-post-form): ssh
Enter the target to attack (or filename with targets): 192.168.1.102
Enter a username to test or a filename: Admin
Enter a password to test or a filename: P@ssword
If you want to test for passwords (s)ame as login, (n)ull or (r)everse login, enter these letters without spaces (e.g. "sr") or leave empty otherwise:
Port number (press enter for default):
```

The following options are supported by the service module:
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2026-01-12 20:06:31

Help for module ssh:

The Module ssh does not need or support optional parameters

If you want to add module options, enter them here (or leave empty):

The following command will be executed now:
hydra -l Admin -p P@ssword -u 192.168.1.102 ssh

Do you want to run the command now? [Y/n] y

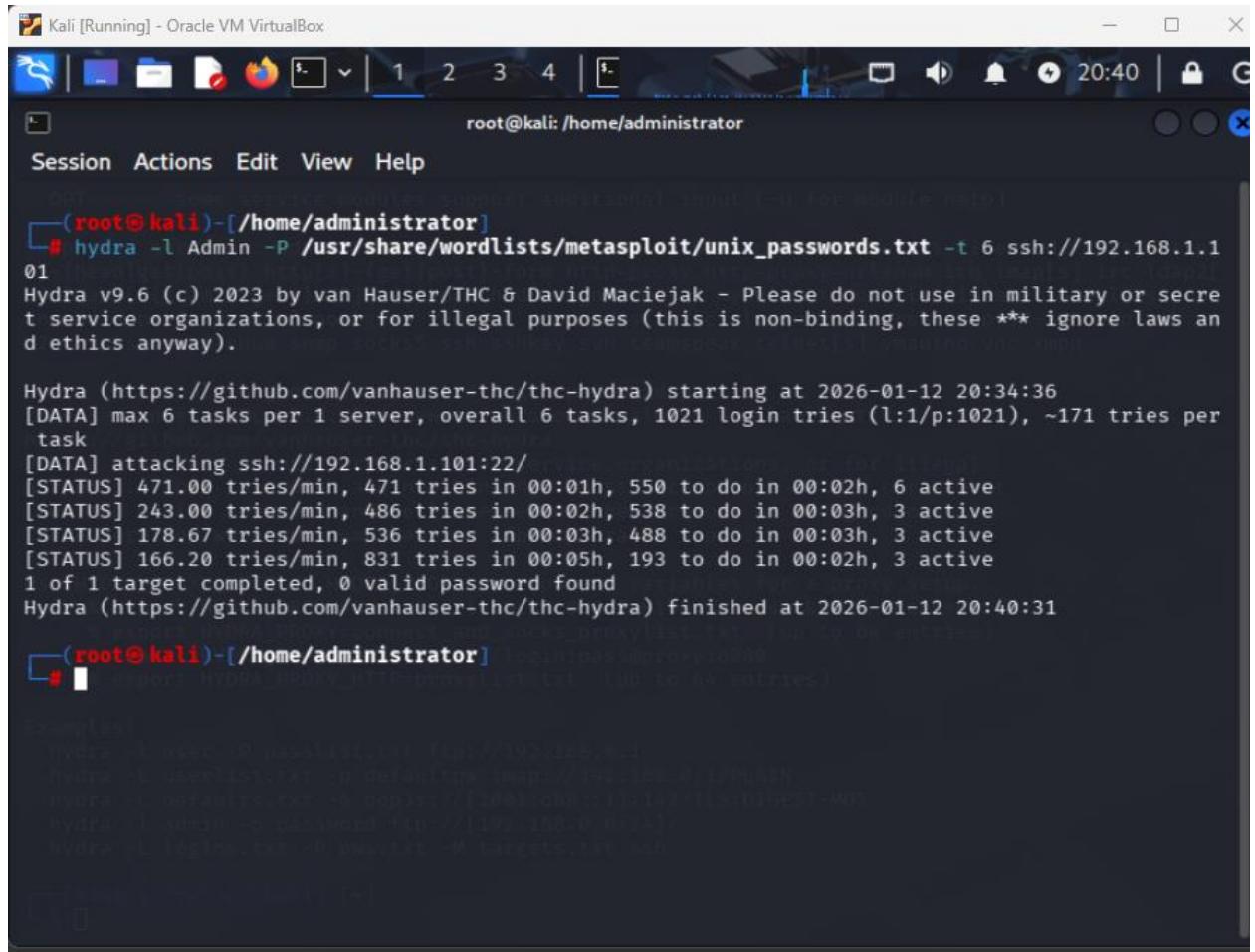
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

```
Kali [Running] - Oracle VM VirtualBox
administrator@kali: ~
Session Actions Edit View Help
t service organizations, or for illegal purposes (this is non-binding, these ** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-12 20:06:31
Help for module ssh:
The Module ssh does not need or support optional parameters
If you want to add module options, enter them here (or leave empty):
The following command will be executed now:
hydra -l Admin -p P@ssword -u 192.168.1.102 ssh
Do you want to run the command now? [Y/n] y
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secre
t service organizations, or for illegal purposes (this is non-binding, these ** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-12 20:06:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to redu
ce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.102:22/
[22][ssh] host: 192.168.1.102 login: Admin password: P@ssword
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-12 20:06:36
zsh: corrupt history file /home/administrator/.zsh_history
└─(administrator㉿kali)-[~]
$
```

Now that SSH and Hydra are both working as intended, I will use the command to crack the password by using a password list and check the logs on Splunk.



Kali [Running] - Oracle VM VirtualBox

root@kali: /home/administrator

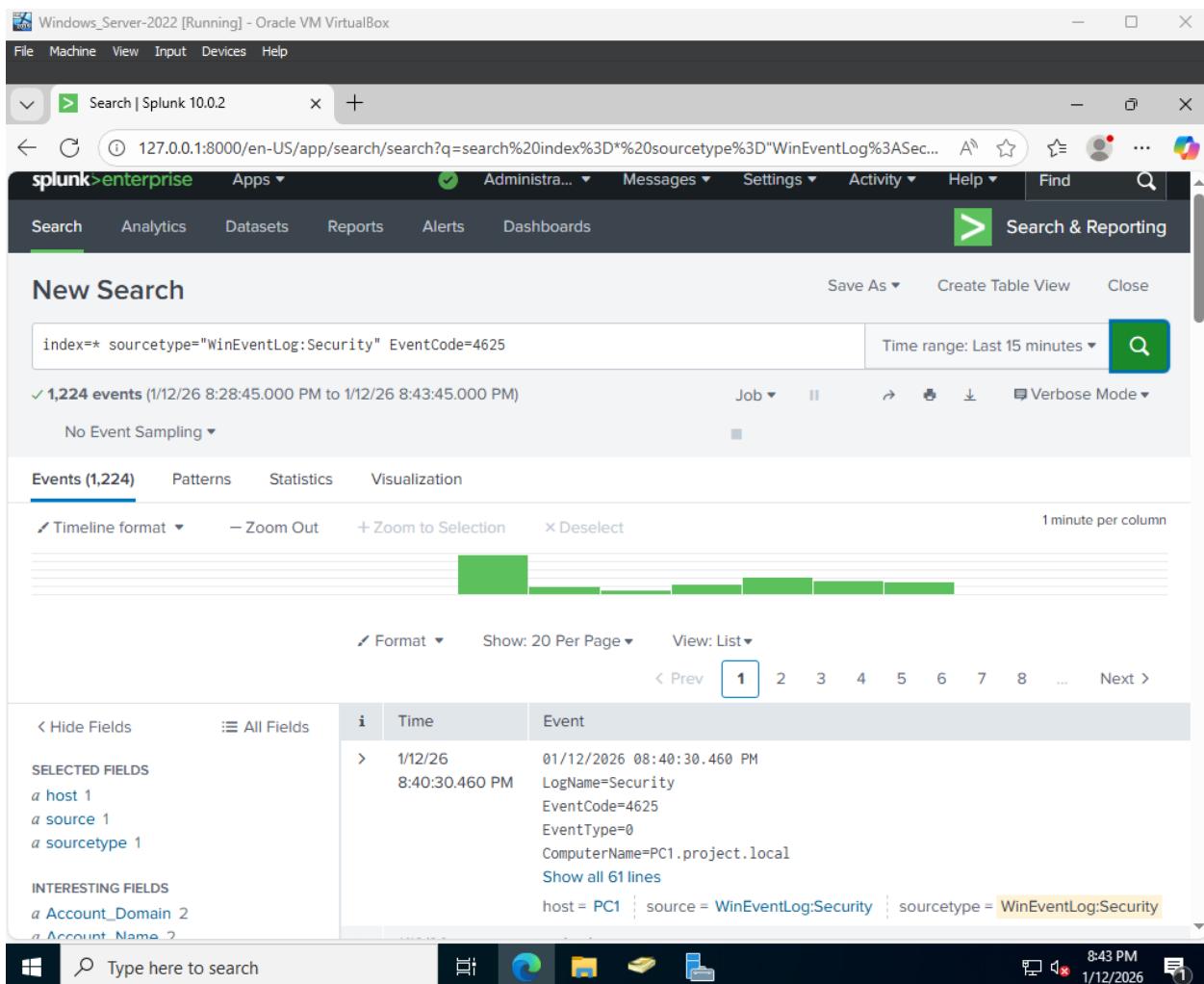
Session Actions Edit View Help

```
[root@kali ~]# hydra -l Admin -P /usr/share/wordlists/metasploit/unix_passwords.txt -t 6 ssh://192.168.1.1:01
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-12 20:34:36
[DATA] max 6 tasks per 1 server, overall 6 tasks, 1021 login tries (l:1/p:1021), ~171 tries per task
[DATA] attacking ssh://192.168.1.101:22/
[STATUS] 471.00 tries/min, 471 tries in 00:01h, 550 to do in 00:02h, 6 active
[STATUS] 243.00 tries/min, 486 tries in 00:02h, 538 to do in 00:03h, 3 active
[STATUS] 178.67 tries/min, 536 tries in 00:03h, 488 to do in 00:03h, 3 active
[STATUS] 166.20 tries/min, 831 tries in 00:05h, 193 to do in 00:02h, 3 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-12 20:40:31

[root@kali ~]#
```

As you can see, there are all the logs of the failed log in attempts. This search shows 1224 logs of failed attempts in the past 15 minutes. These were all generated by the Kali machine using the Hydra Tool.

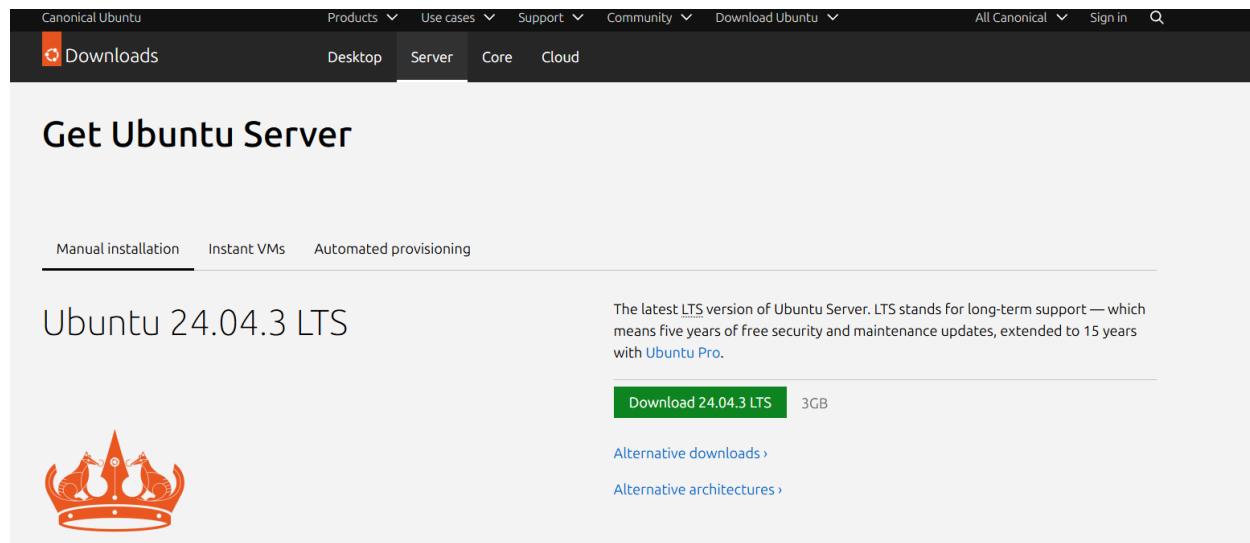


n8n and AI Integration Setup

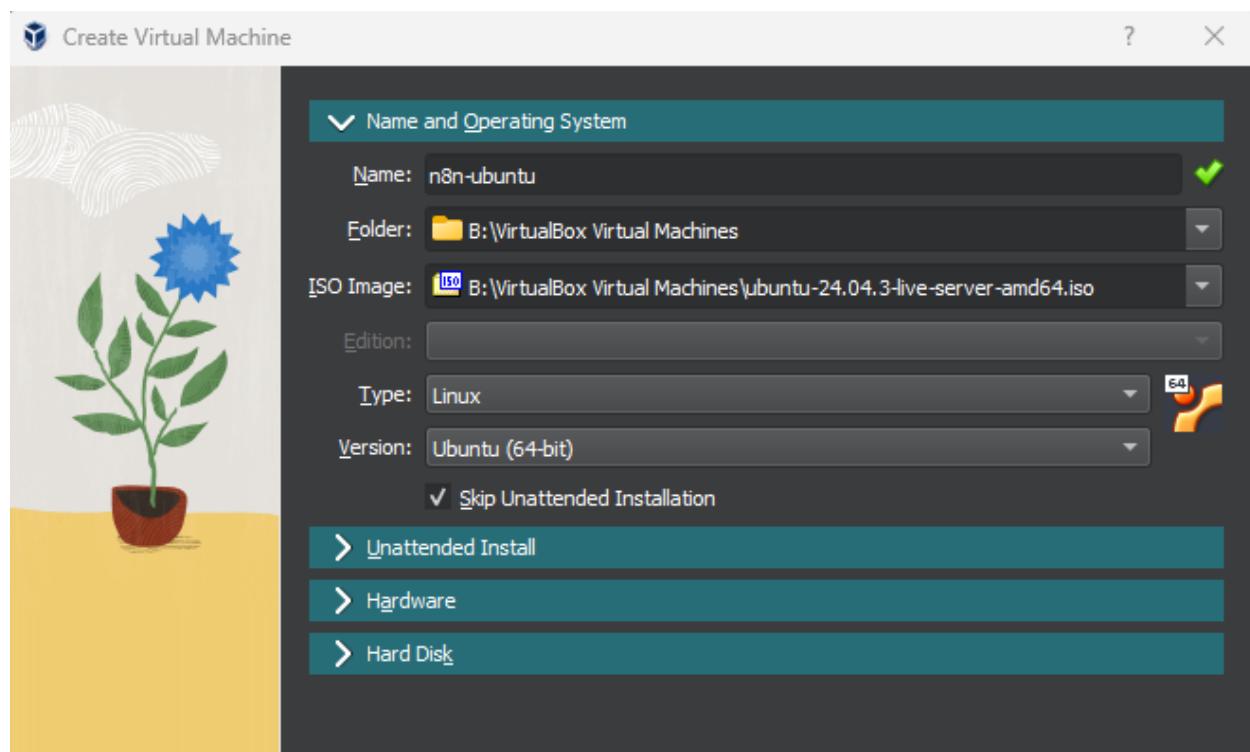
n8n is an open-source workflow automation tool that allows different systems and services to be connected using a visual, low-code interface. In this lab, n8n is used as the automation layer between Splunk and AI. Security events and logs generated from Kali attacks and collected by Splunk can be passed into n8n workflows, where they are processed and evaluated.

To support this, an Ubuntu virtual machine will be created to host n8n and manage the automation workflows. As the AI component, ChatGPT is integrated into n8n to analyze Splunk log data, summarize events, and provide context on potential security threats. This allows raw log data to be transformed into meaningful insights, simulating how AI can assist analysts in a

real enterprise environment. The combination of Splunk for detection, n8n for automation, and ChatGPT for analysis demonstrates a modern security monitoring and response workflow.



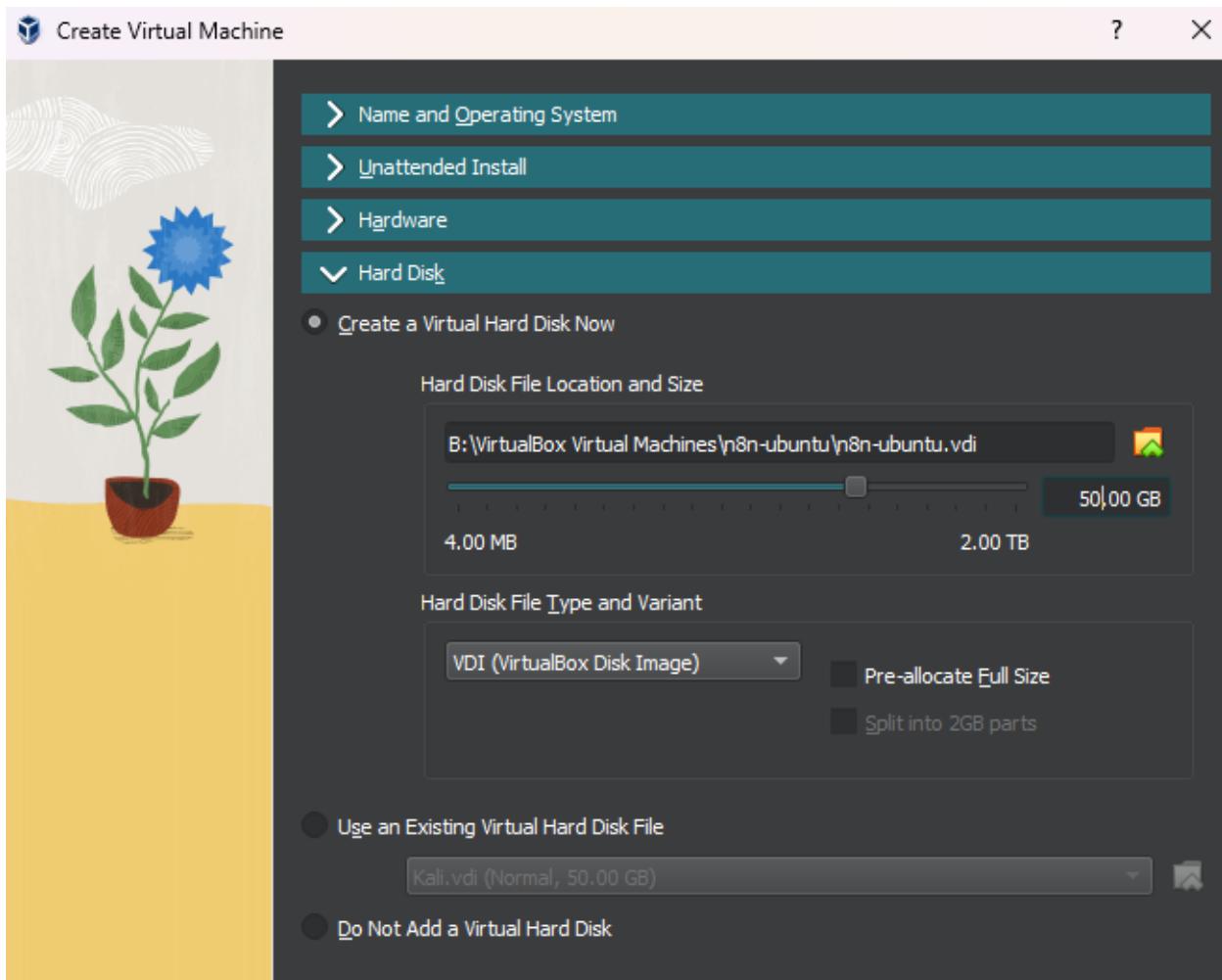
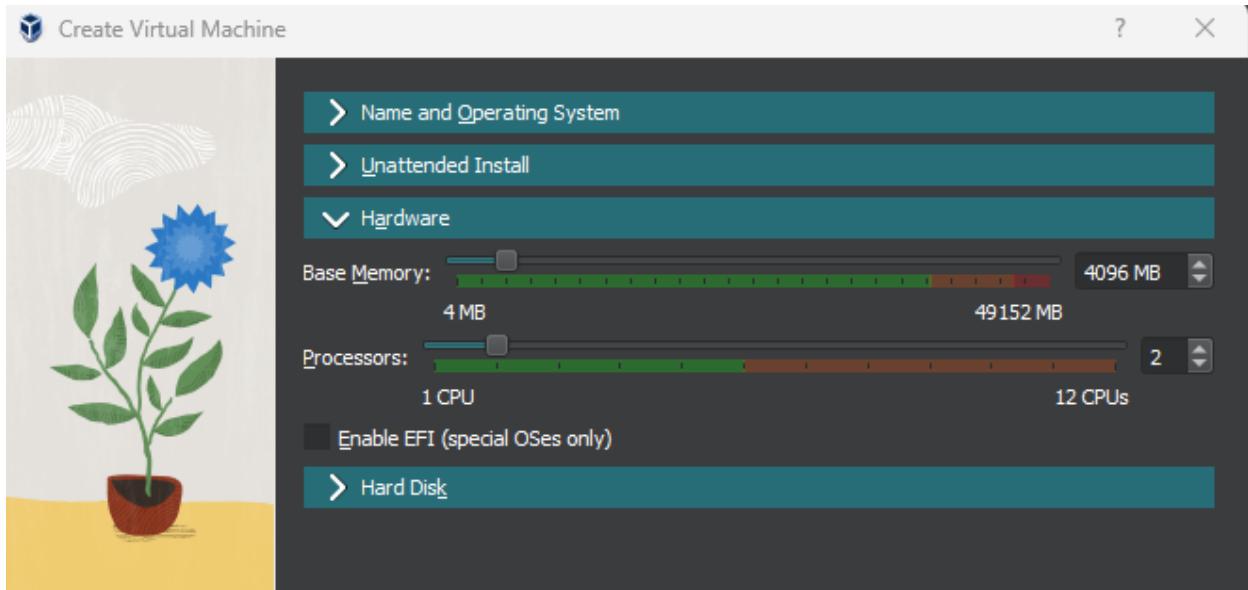
The screenshot shows the Canonical Ubuntu website's "Get Ubuntu Server" section. At the top, there are navigation links for "Products", "Use cases", "Support", "Community", "Download Ubuntu", "All Canonical", "Sign in", and a search bar. Below these are tabs for "Downloads" (highlighted in orange), "Desktop", "Server" (selected), "Core", and "Cloud". The main heading is "Get Ubuntu Server". Below it are three options: "Manual installation" (selected), "Instant VMs", and "Automated provisioning". A large image of a red crown is on the left. To the right, it says "Ubuntu 24.04.3 LTS" and provides a brief description: "The latest LTS version of Ubuntu Server. LTS stands for long-term support — which means five years of free security and maintenance updates, extended to 15 years with Ubuntu Pro." A green button labeled "Download 24.04.3 LTS" (3GB) is prominently displayed. Below the button are links for "Alternative downloads" and "Alternative architectures".

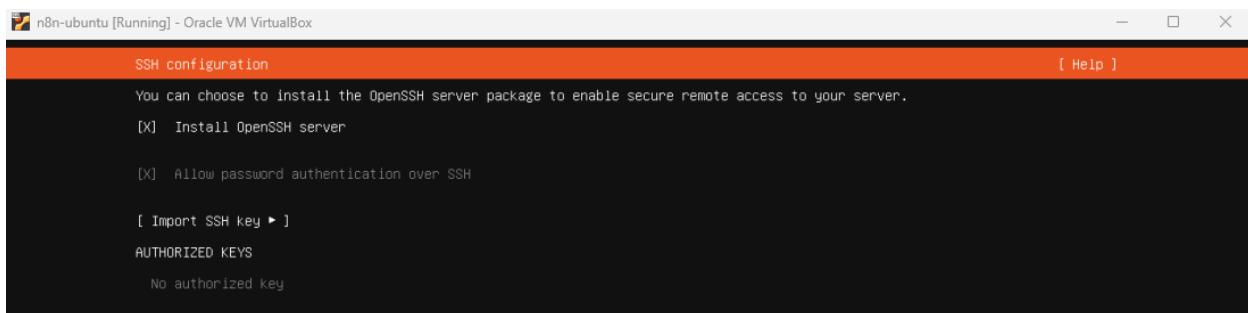
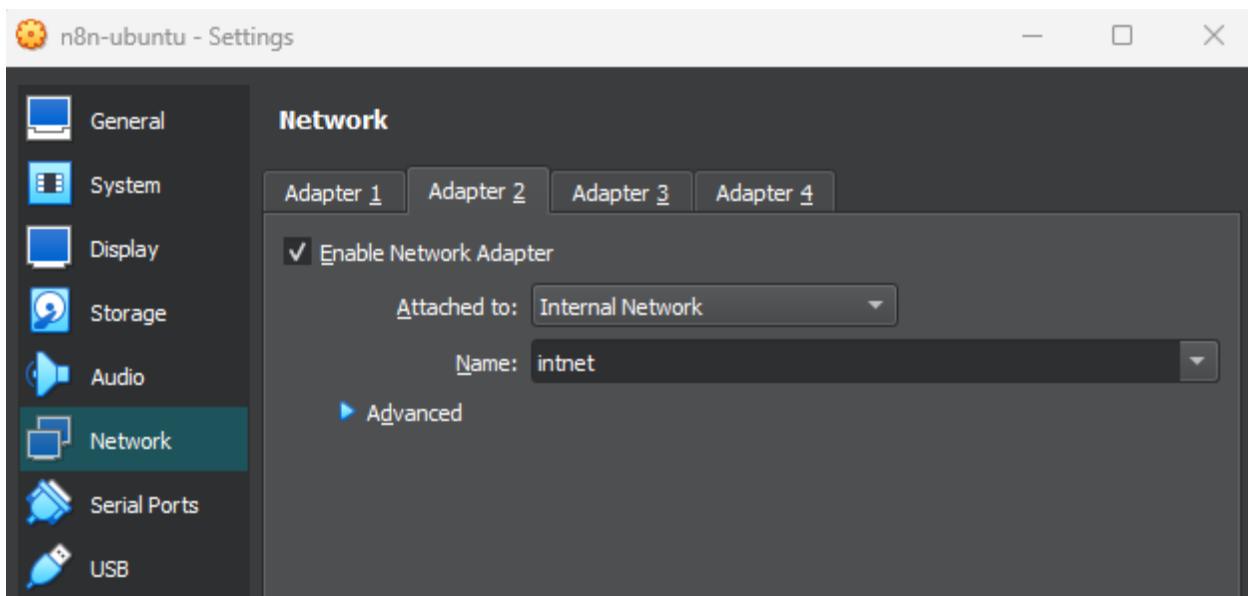


The screenshot shows the "Create Virtual Machine" dialog box from Oracle VM VirtualBox. The title bar says "Create Virtual Machine". On the left is a decorative illustration of a blue sunflower. The main area is titled "Name and Operating System". It contains the following fields:

- Name: n8n-ubuntu (with a green checkmark)
- Folder: B:\VirtualBox Virtual Machines
- ISO Image: B:\VirtualBox Virtual Machines\ubuntu-24.04.3-live-server-amd64.iso
- Edition: (empty dropdown)
- Type: Linux (with a 64-bit icon)
- Version: Ubuntu (64-bit)

A checked checkbox "Skip Unattended Installation" is present. Below the main section are three expandable categories: "Unattended Install", "Hardware", and "Hard Disk".





n8n-ubuntu [Running] - Oracle VM VirtualBox

Installing system [Help]

```
subiquity/Ad/apply_autoinstall_config:  
subiquity/Late/apply_autoinstall_config:  
configuring apt  
curtin command in-target  
installing system  
executing curtin install initial step  
executing curtin install partitioning step  
curtin command install  
configuring storage  
running 'curtin block-meta simple'  
curtin command block-meta  
removing previous storage devices  
configuring disk: disk-sda  
configuring partition: partition-0  
configuring partition: partition-1  
configuring format: format-0  
configuring partition: partition-2  
configuring lvm_volvgroup: lvm_volvgroup-0  
configuring lvm_partition: lvm_partition-0  
configuring format: format-1  
configuring mount: mount-1  
configuring mount: mount-0  
executing curtin install extract step  
curtin command install  
writing install sources to disk  
running 'curtin extract'  
curtin command extract  
acquiring and extracting image from cp:///tmp/tmpi3rql_zr/mount  
configuring keyboard  
curtin command in-target  
executing curtin install curthooks step  
curtin command install  
configuring installed system  
running 'curtin curthooks'  
curtin command curthooks  
configuring apt configuring apt  
Installing missing packages  
Installing packages on target system: ['grub-pc']  
configuring iscsi service  
configuring raid (mdadm) service  
configuring NVMe over TCP  
installing kernel \
```

[View full log]

n8n-ubuntu [Running] - Oracle VM VirtualBox

GNU nano 7.2

```
network:  
  version: 2  
  ethernets:  
    enp0s3:  
      dhcp4: true  
      nameservers:  
        addresses: [8.8.8.8]  
    enp0s8:  
      dhcp4: false  
      addresses:  
        - 192.168.1.3/24
```

```
n8n@n8n-ubuntu:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=0.922 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=128 time=0.613 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=128 time=0.414 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=128 time=0.400 ms
```

Now that the Ubuntu machine is running and connected to the internal network, n8n will need to be installed.

```
n8n@n8n-ubuntu [Running] - Oracle VM VirtualBox
Selecting previously unselected package bridge-utils.
Preparing to unpack .../1-bridge-utils_1.7.1-1ubuntu2_amd64.deb ...
Unpacking bridge-utils (1.7.1-1ubuntu2) ...
Selecting previously unselected package runc.
Preparing to unpack .../2-runc_1.3.3-0ubuntu1~24.04.3_amd64.deb ...
Unpacking runc (1.3.3-0ubuntu1~24.04.3) ...
Selecting previously unselected package containerd.
Preparing to unpack .../3-containerd_1.7.28-0ubuntu1~24.04.1_amd64.deb ...
Unpacking containerd (1.7.28-0ubuntu1~24.04.1) ...
Selecting previously unselected package dns-root-data.
Preparing to unpack .../4-dns-root-data_2024071801~ubuntu0.24.04.1_all.deb ...
Unpacking dns-root-data (2024071801~ubuntu0.24.04.1) ...
Selecting previously unselected package dnsmasq-base.
Preparing to unpack .../5-dnsmasq-base_2.90-2ubuntu0.1_amd64.deb ...
Unpacking dnsmasq-base (2.90-2ubuntu0.1) ...
Selecting previously unselected package docker.io.
Preparing to unpack .../6-docker.io_20.2.2-0ubuntu1~24.04.1_amd64.deb ...
Unpacking docker.io (20.2.2-0ubuntu1~24.04.1) ...
Selecting previously unselected package ubuntu-fan.
Preparing to unpack .../7-ubuntu-fan_0.12.16+24.04.1_all.deb ...
Unpacking ubuntu-fan (0.12.16+24.04.1) ...
Setting up dnsmasq-base (2.90-2ubuntu0.1) ...
Setting up runc (1.3.3-0ubuntu1~24.04.3) ...
Setting up dns-root-data (2024071801~ubuntu0.24.04.1) ...
Setting up bridge-utils (1.7.1-1ubuntu2) ...
Setting up pigz (2.8-1) ...
Setting up containerd (1.7.28-0ubuntu1~24.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/containerd.service → /usr/lib/systemd/system/containerd.service.
Setting up ubuntu-fan (0.12.16+24.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/ubuntu-fan.service → /usr/lib/systemd/system/ubuntu-fan.service.
Setting up docker.io (20.2.2-0ubuntu1~24.04.1) ...
Info: Selecting GID from range 100 to 999 ...
Info: Adding group 'docker' (GID 110) ...
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /usr/lib/systemd/system/docker.service.
Created symlink /etc/systemd/system/sockets.target.wants/docker.socket → /usr/lib/systemd/system/docker.socket.
Processing triggers for dbus (1.14.10-4ubuntu4.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
n8n@n8n-ubuntu:~$
```

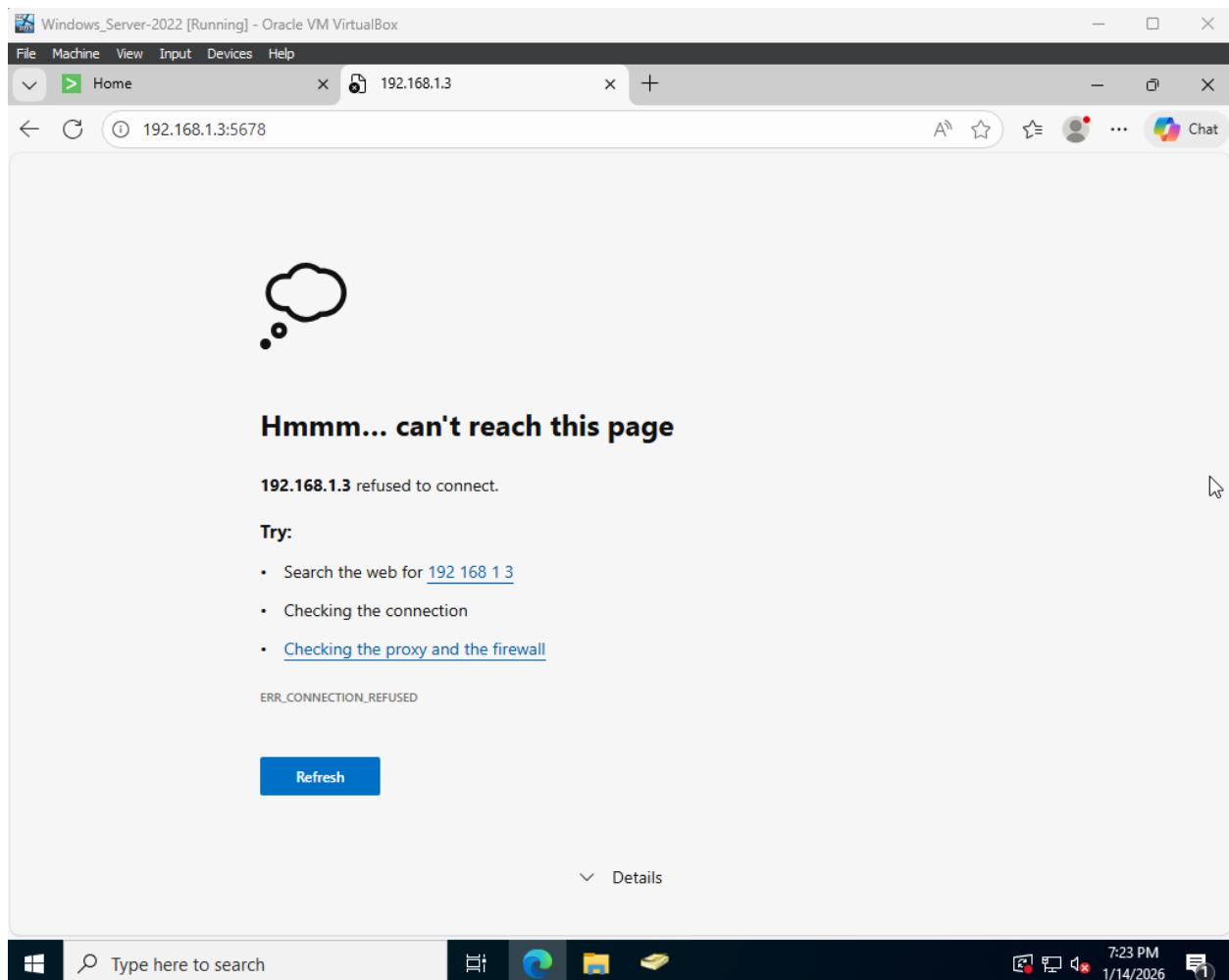
```
[n8n-ubuntu:~$] n8n-ubuntu [Running] - Oracle VM VirtualBox
[n8n-ubuntu:~$] get:7 http://us.archive.ubuntu.com/ubuntu noble/universe amd64 python3-compose all 1.29.2-6ubuntu1 [84.6 kB]
[n8n-ubuntu:~$] get:8 http://us.archive.ubuntu.com/ubuntu noble/universe amd64 docker-compose all 1.29.2-6ubuntu1 [14.0 kB]
[n8n-ubuntu:~$] fetched 297 kB in 0s (2,976 kB/s)
[n8n-ubuntu:~$] Selecting previously unselected package python3-websocket.
[n8n-ubuntu:~$] Reading database ... 87792 files and directories currently installed.
[n8n-ubuntu:~$] Preparing to unpack .../0-python3-websocket_1.7.0-1_all.deb ...
[n8n-ubuntu:~$] Unpacking python3-websocket (1.7.0-1) ...
[n8n-ubuntu:~$] Selecting previously unselected package python3-docker.
[n8n-ubuntu:~$] Preparing to unpack .../1-python3-docker_5.0.3-1ubuntu1.1_all.deb ...
[n8n-ubuntu:~$] Unpacking python3-docker (5.0.3-1ubuntu1.1) ...
[n8n-ubuntu:~$] Selecting previously unselected package python3-dockerpty.
[n8n-ubuntu:~$] Preparing to unpack .../2-python3-dockerpty_0.4.1-5_all.deb ...
[n8n-ubuntu:~$] Unpacking python3-dockerpty (0.4.1-5) ...
[n8n-ubuntu:~$] Selecting previously unselected package python3-docopt.
[n8n-ubuntu:~$] Preparing to unpack .../3-python3-docopt_0.6.2-6_all.deb ...
[n8n-ubuntu:~$] Unpacking python3-docopt (0.6.2-6) ...
[n8n-ubuntu:~$] Selecting previously unselected package python3-dotenv.
[n8n-ubuntu:~$] Preparing to unpack .../4-python3-dotenv_1.0.1-1_all.deb ...
[n8n-ubuntu:~$] Unpacking python3-dotenv (1.0.1-1) ...
[n8n-ubuntu:~$] Selecting previously unselected package python3-texttable.
[n8n-ubuntu:~$] Preparing to unpack .../5-python3-texttable_1.6.7-1_all.deb ...
[n8n-ubuntu:~$] Unpacking python3-texttable (1.6.7-1) ...
[n8n-ubuntu:~$] Selecting previously unselected package python3-compose.
[n8n-ubuntu:~$] Preparing to unpack .../6-python3-compose_1.29.2-6ubuntu1_all.deb ...
[n8n-ubuntu:~$] Unpacking python3-compose (1.29.2-6ubuntu1) ...
[n8n-ubuntu:~$] Selecting previously unselected package docker-compose.
[n8n-ubuntu:~$] Preparing to unpack .../7-docker-compose_1.29.2-6ubuntu1_all.deb ...
[n8n-ubuntu:~$] Unpacking docker-compose (1.29.2-6ubuntu1) ...
[n8n-ubuntu:~$] Setting up python3-dotenv (1.0.1-1) ...
[n8n-ubuntu:~$] Setting up python3-texttable (1.6.7-1) ...
[n8n-ubuntu:~$] Setting up python3-docopt (0.6.2-6) ...
[n8n-ubuntu:~$] Setting up python3-websocket (1.7.0-1) ...
[n8n-ubuntu:~$] Setting up python3-dockerpty (0.4.1-5) ...
[n8n-ubuntu:~$] Setting up python3-docker (5.0.3-1ubuntu1.1) ...
[n8n-ubuntu:~$] Setting up python3-compose (1.29.2-6ubuntu1) ...
[n8n-ubuntu:~$] Setting up docker-compose (1.29.2-6ubuntu1) ...
[n8n-ubuntu:~$] Processing triggers for man-db (2.12.0-4build2) ...
[n8n-ubuntu:~$] Scanning processes...
[n8n-ubuntu:~$] Scanning linux images...
[n8n-ubuntu:~$] Running kernel seems to be up-to-date.
[n8n-ubuntu:~$] No services need to be restarted.
[n8n-ubuntu:~$] No containers need to be restarted.
[n8n-ubuntu:~$] No user sessions are running outdated binaries.
[n8n-ubuntu:~$] No VM guests are running outdated hypervisor (qemu) binaries on this host.
[n8n-ubuntu:~$]
```

```
[n8n-ubuntu:~$] n8n-ubuntu [Running] - Oracle VM VirtualBox
[n8n-ubuntu:~$] n8n@n8n-ubuntu:~$ mkdir n8n-compose
[n8n-ubuntu:~$] n8n@n8n-ubuntu:~$ cd n8n-compose/
[n8n-ubuntu:~$] n8n@n8n-ubuntu:~/n8n-compose$ sudo nano docker-compose.yaml
```

```
[n8n-ubuntu:~$] n8n-ubuntu [Running] - Oracle VM VirtualBox
[n8n-ubuntu:~$] GNU nano 7.2
[n8n-ubuntu:~$] services:
[n8n-ubuntu:~$]   n8n:
[n8n-ubuntu:~$]     image: n8nio/n8n:latest
[n8n-ubuntu:~$]     restart: always
[n8n-ubuntu:~$]     ports:
[n8n-ubuntu:~$]       - "5678:5678"
[n8n-ubuntu:~$]     environment:
[n8n-ubuntu:~$]       - N8N_HOST=192.168.1.3
[n8n-ubuntu:~$]       - N8N_PORT=5678
[n8n-ubuntu:~$]       - N8N_PROTOCOL=http
[n8n-ubuntu:~$]       - N8N_SECURE_COOKIE=false
[n8n-ubuntu:~$]       - GENERIC_TIMEZONE=America/Toronto
[n8n-ubuntu:~$]     volumes:
[n8n-ubuntu:~$]       - ./n8n_data:/home/node/.n8n
```

```
n8n@n8n-ubuntu:~/n8n-compose$ sudo docker-compose pull
Pulling n8n ... done
n8n@n8n-ubuntu:~/n8n-compose$ sudo docker-compose up -d
Creating network "n8n-compose_default" with the default driver
Creating n8n-compose_n8n_1 ... done
n8n@n8n-ubuntu:~/n8n-compose$
```

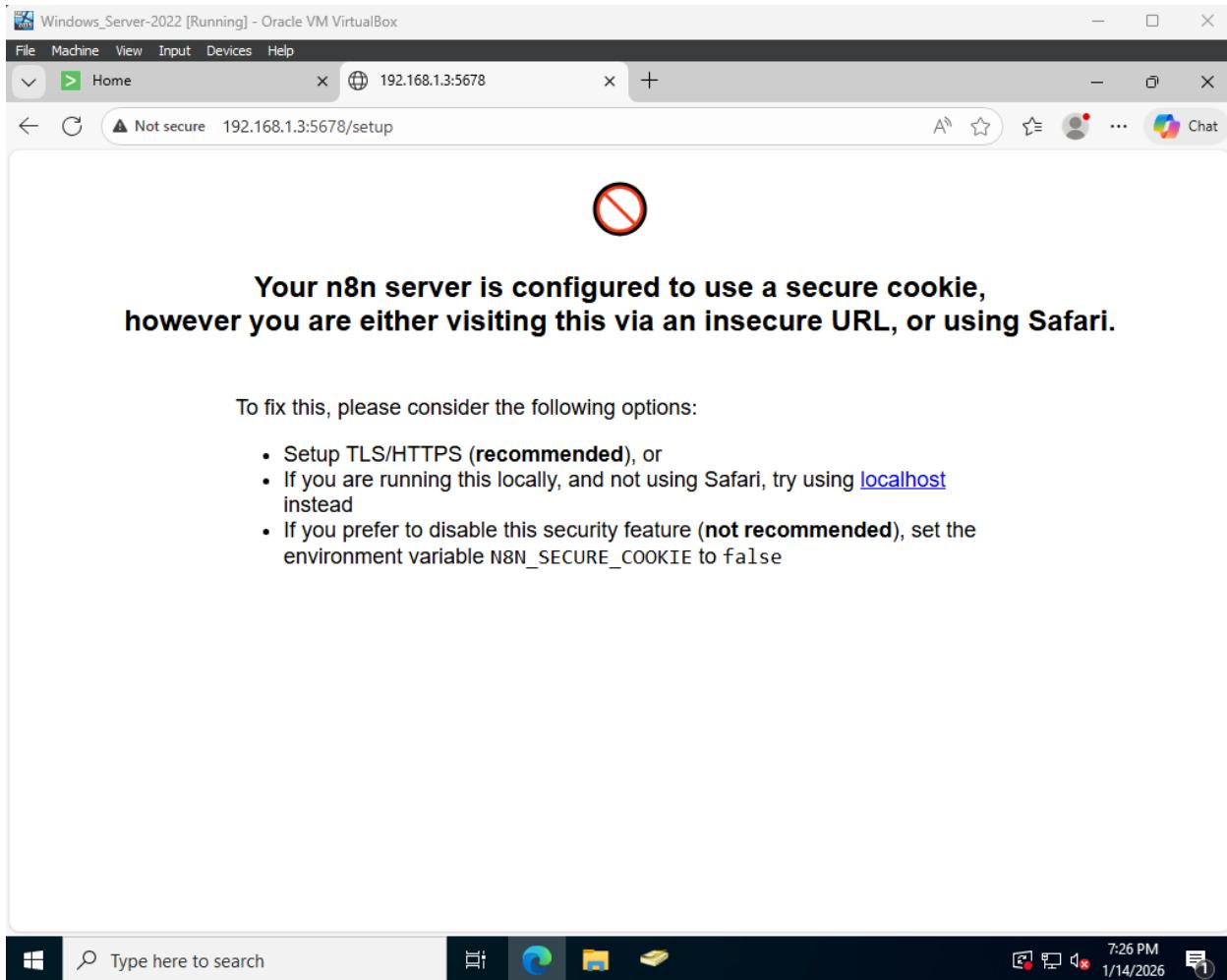
Now that the n8n is installed and running, I will access it through the server.



As you can see, I ran into an issue when attempting to access the servers' n8n service.

```
n8n@n8n-ubuntu:~/n8n-compose$ sudo docker-compose pull
Pulling n8n ... done
n8n@n8n-ubuntu:~/n8n-compose$ sudo docker-compose up -d
Creating network "n8n-compose_default" with the default driver
Creating n8n-compose_n8n_1 ... done
n8n@n8n-ubuntu:~/n8n-compose$ sudo ufw status
Status: inactive
n8n@n8n-ubuntu:~/n8n-compose$ ll
total 16
drwxrwxr-x 3 n8n  n8n  4096 Jan 15 00:20 ./
drwxr-x--- 5 n8n  n8n  4096 Jan 15 00:14 ../
-rw-r--r-- 1 root root  311 Jan 15 00:19 docker-compose.yaml
drwxr-xr-x 2 root root 4096 Jan 15 00:20 n8n_data/
n8n@n8n-ubuntu:~/n8n-compose$ sudo chown -R 1000:1000 n8n_data/
n8n@n8n-ubuntu:~/n8n-compose$ ll
total 16
drwxrwxr-x 3 n8n  n8n  4096 Jan 15 00:20 ./
drwxr-x--- 5 n8n  n8n  4096 Jan 15 00:14 ../
-rw-r--r-- 1 root root  311 Jan 15 00:19 docker-compose.yaml
drwxr-xr-x 2 n8n  n8n  4096 Jan 15 00:20 n8n_data/
n8n@n8n-ubuntu:~/n8n-compose$ sudo docker-compose down
Stopping n8n-compose_n8n_1 ... done
Removing n8n-compose_n8n_1 ... done
Removing network n8n-compose_default
n8n@n8n-ubuntu:~/n8n-compose$ sudo docker-compose up -d
Creating network "n8n-compose_default" with the default driver
Creating n8n-compose_n8n_1 ... done
n8n@n8n-ubuntu:~/n8n-compose$
```

I was able to fix the issue, but then I ran into a different one.



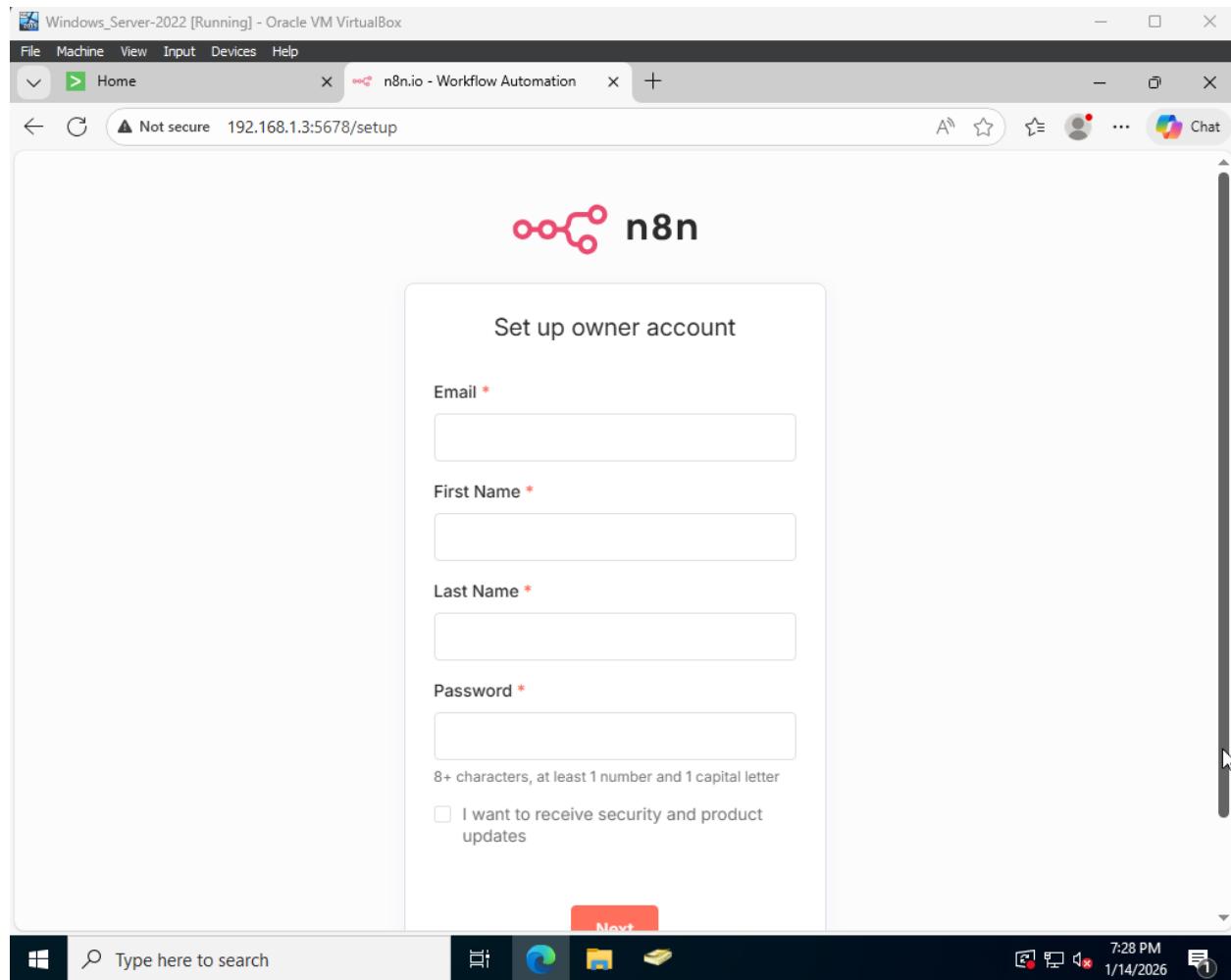
To fix this, please consider the following options:

- Setup TLS/HTTPS (**recommended**), or
- If you are running this locally, and not using Safari, try using localhost instead
- If you prefer to disable this security feature (**not recommended**), set the environment variable N8N_SECURE_COOKIE to false

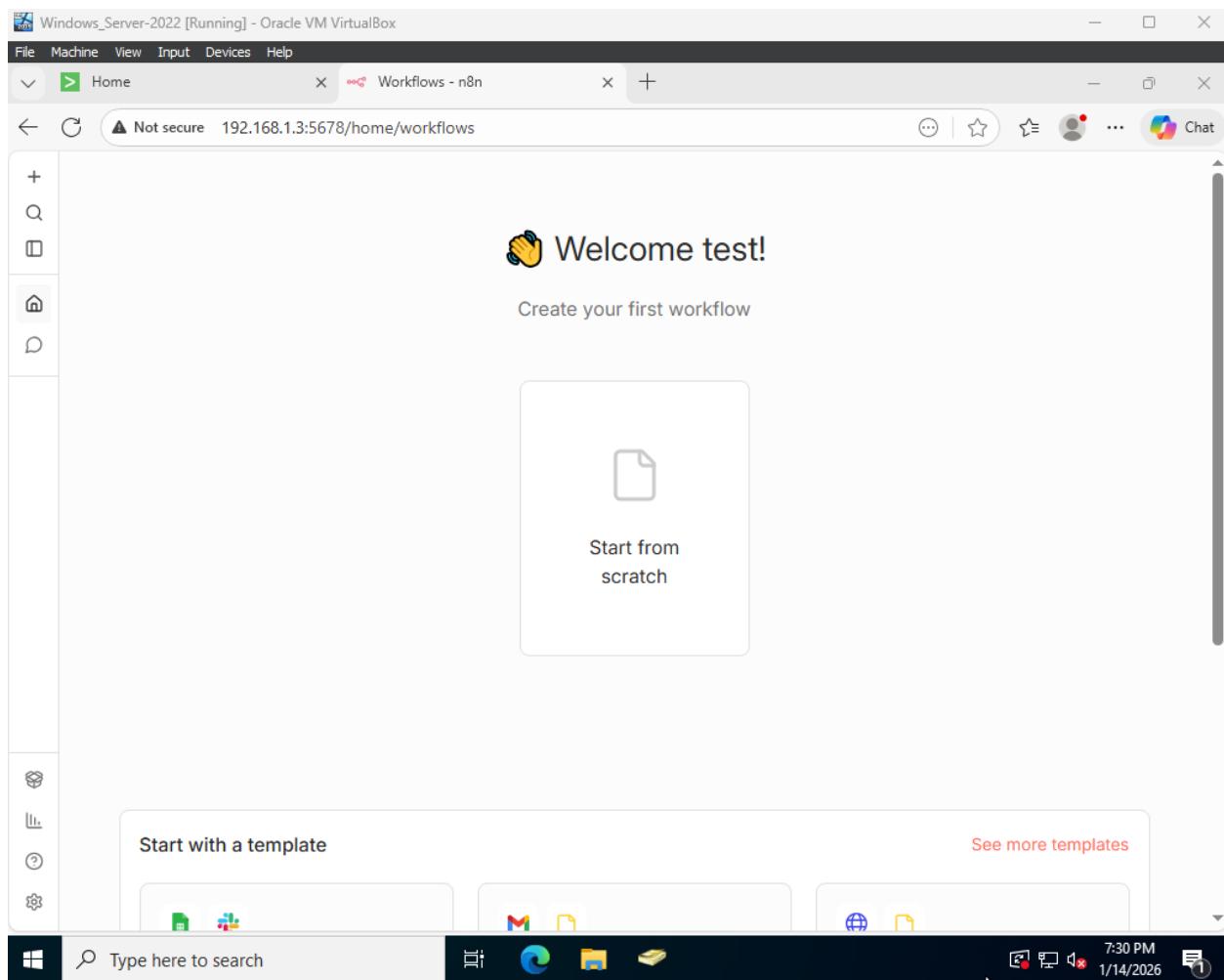
A screenshot of a terminal window titled "n8n-ubuntu [Running] - Oracle VM VirtualBox". The window displays a YAML configuration file for a Docker service named "n8n". The file includes definitions for "image", "restart", "ports", "environment" (with "N8N_SECURE_COOKIE=false"), and "volumes".

```
GNU nano 7.2
services:
  n8n:
    image: n8nio/n8n:latest
    restart: always
    ports:
      - "5678:5678"
    environment:
      - N8N_HOST=192.168.1.3
      - N8N_PORT=5678
      - N8N_PROTOCOL=http
      - N8N_SECURE_COOKIE=false
      - GENERIC_TIMEZONE=America/Toronto
    volumes:
      - ./n8n_data:/home/node/.n8n
```

I found that I had accidentally entered a – sign instead of an = sign int the .yaml file.



The service is now running and I can continue the setup.



Creating a Splunk Alert

Before continuing with the n8n automation, a Splunk alert must first be created. This alert will act as the trigger for the workflow by identifying relevant security events within the collected log data. Establishing the alert ensures that meaningful events are detected and passed forward for automated processing.

Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Search | Splunk 10.0.2 Workflows - n8n

splunk>enterprise Apps ▾ Administra... 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

New Search

index=* EventCode=4625 | stats count by _time,ComputerName,user,src_ip

Time range: Last 24 hours

✓ 3 events (1/13/26 7:00:00.000 PM to 1/14/26 7:38:41.000 PM) No Event Sampling Job

Events (3) Patterns Statistics (0) Visualization

✓ Timeline format - Zoom Out + Zoom to Selection × Deselect 1 hour per column

Format Show: 20 Per Page View: List

< Hide Fields : All Fields i Time Event

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

a Account_Domain 2
a Account_Name 2
a Authentication_Package 1
a Caller_Process_ID 1
a Caller_Process_Name 1

1/14/26 01/14/2026 07:38:36.909 PM LogName=Security EventCode=4625 EventType=0 ComputerName=PC1.project.local Show all 61 lines host = PC1 | source = WinEventLog:Security | sourcetype = WinEventLog:Security

1/14/26 01/14/2026 07:38:34.935 PM LogName=Security EventCode=4625

Type here to search

Network Internet access
Unidentified network No Internet access

i	Time	Event
>	1/14/26 7:38:36.909 PM	LogName=Security EventCode=4625 EventType=0 ComputerName=PC1.project.local Show all 61 lines host = PC1 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	1/14/26 7:38:34.935 PM	LogName=Security EventCode=4625

Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Search | Splunk 10.0.2 Workflows - n8n

127.0.0.1:8000/en-US/app/search/search?q=search%20index%3D%20EventCode%3D4625%20%7C%2...

splunk>enterprise Apps ▾ Administra... Messages Settings Activity Help Find & Reporting

Save As Alert

Settings

Title: Brute Force

Description: Failed log in credentials.

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Run on Cron Schedule ▾

Time Range: Last 24 hours ▾

Cron Expression: * * * * *

e.g. 00 18 *** (every day at 6PM). Learn More

Expires: 24 hour(s) ▾

Cancel Save

INTERESTING FIELDS

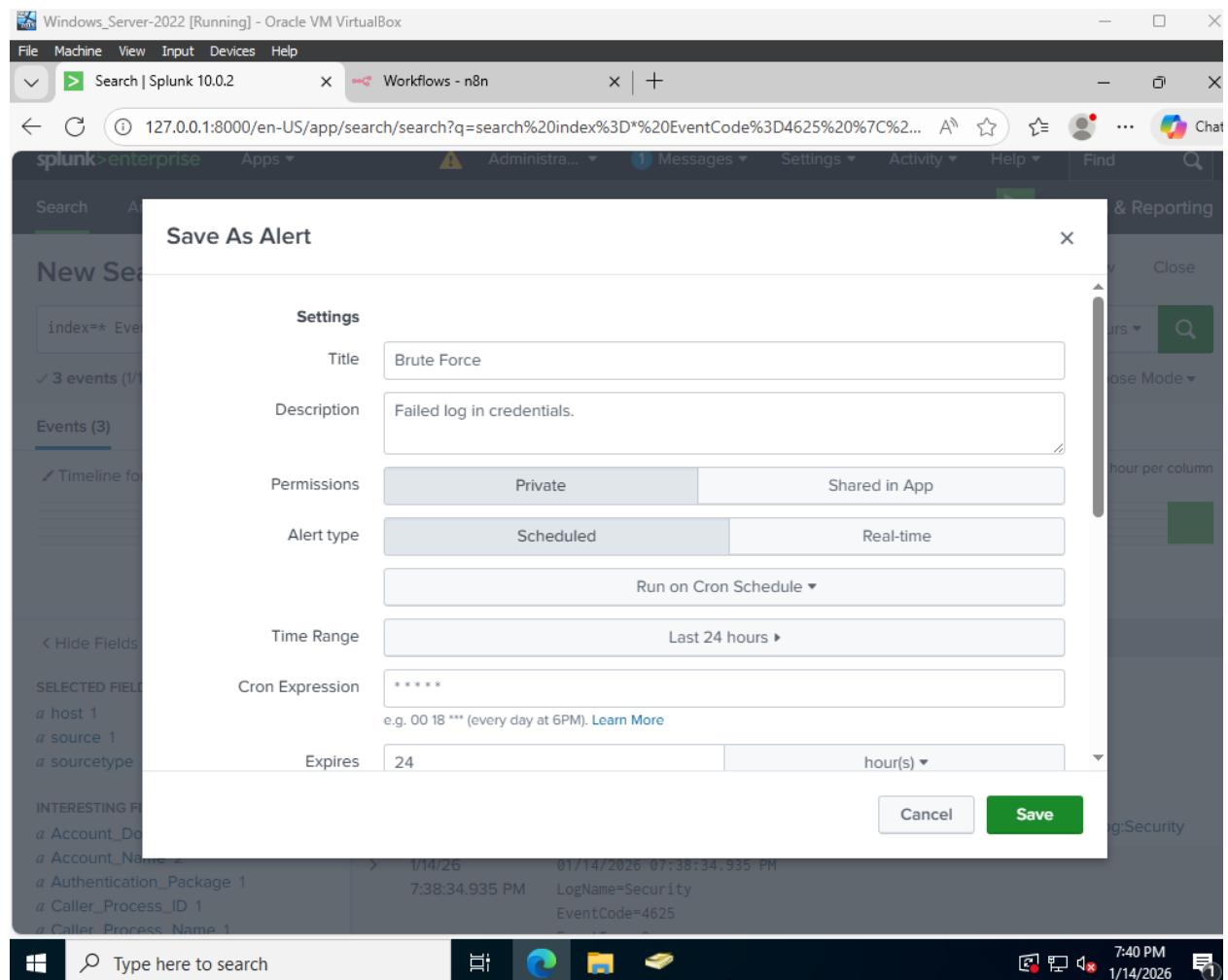
a host 1
a source 1
a sourcetype 1

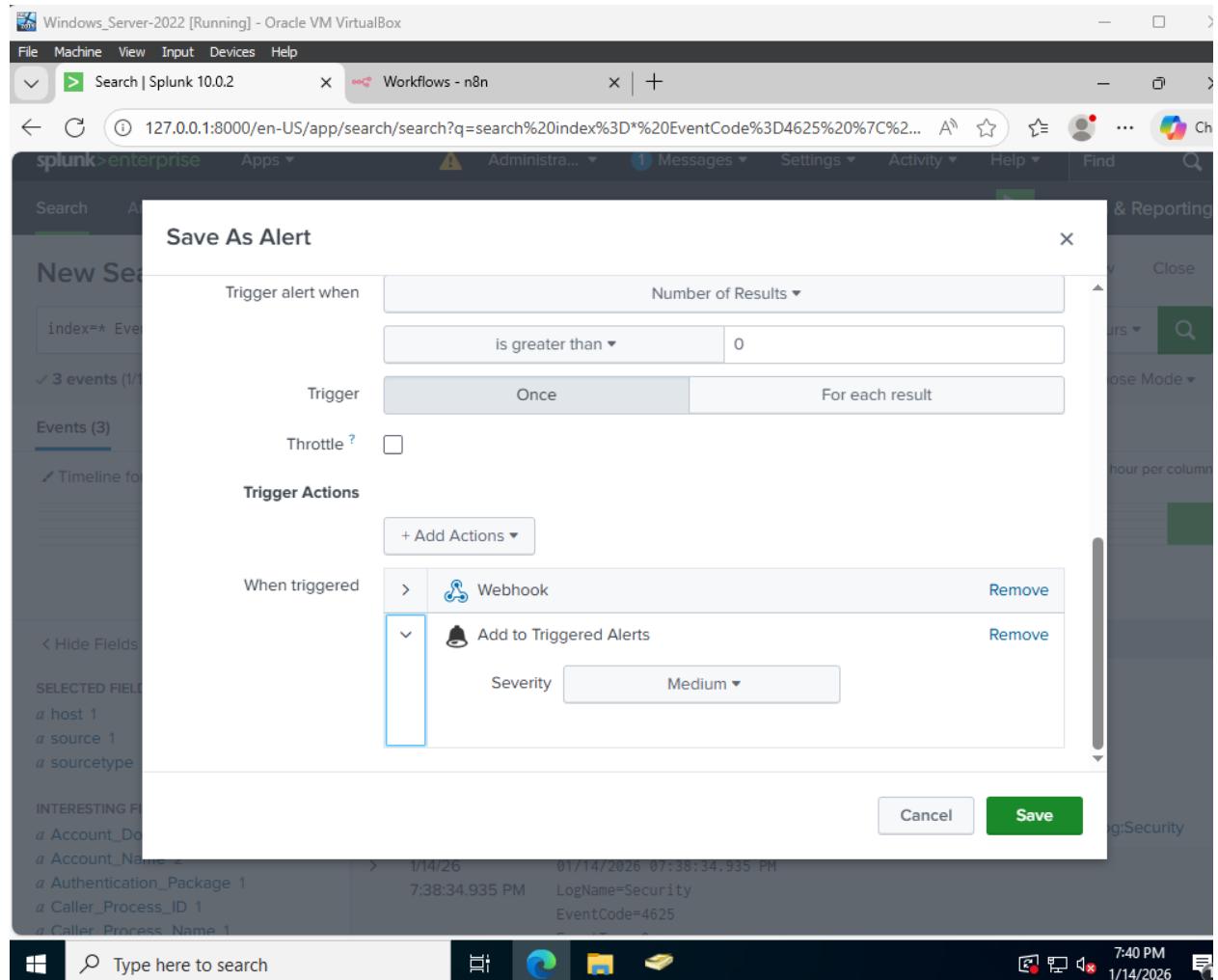
Account_Domain
Account_Name
Authentication_Package 1
Caller_Process_ID 1
Caller_Process_Name 1

1/14/26 7:38:34.935 PM LogName=Security EventCode=4625

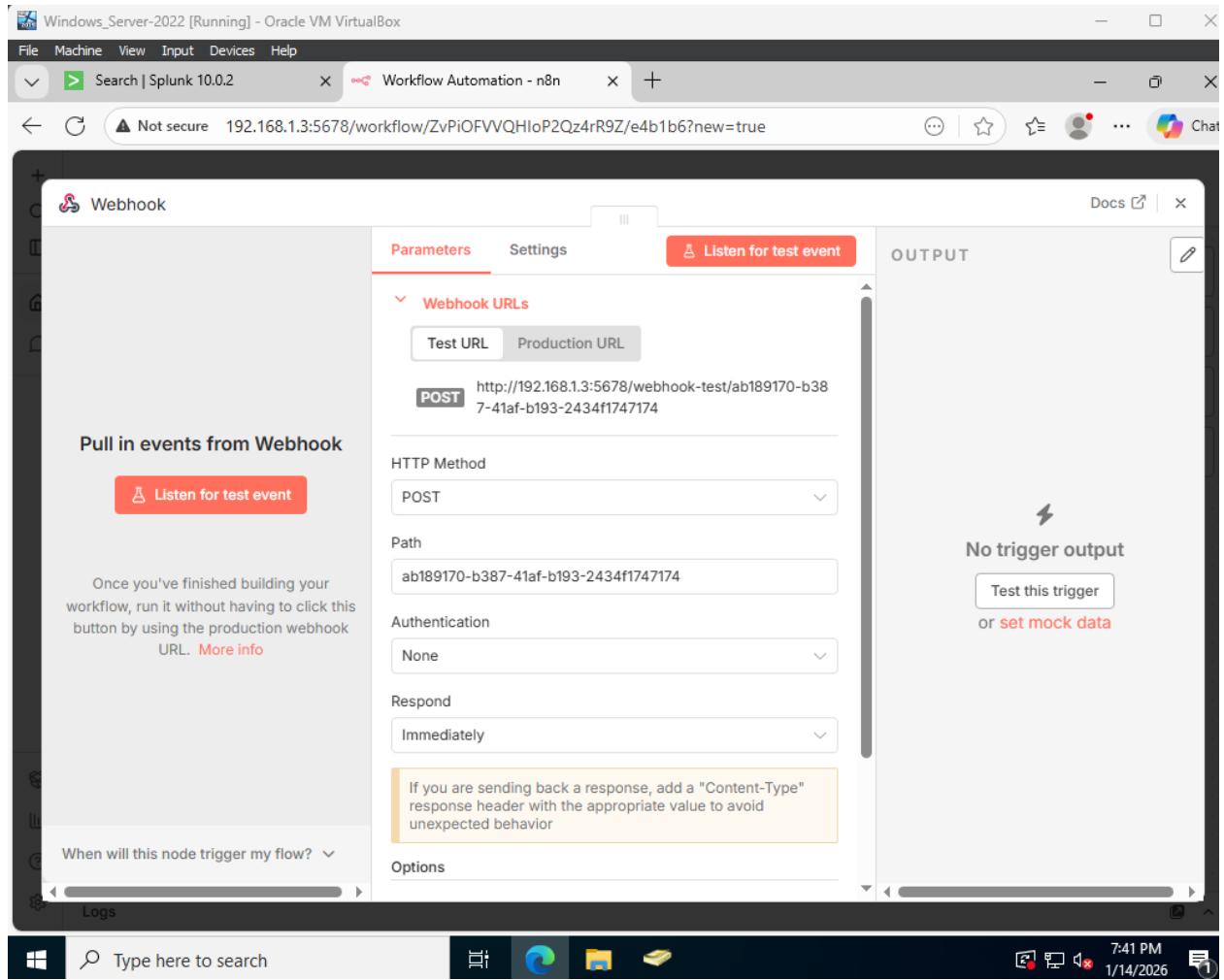
Type here to search

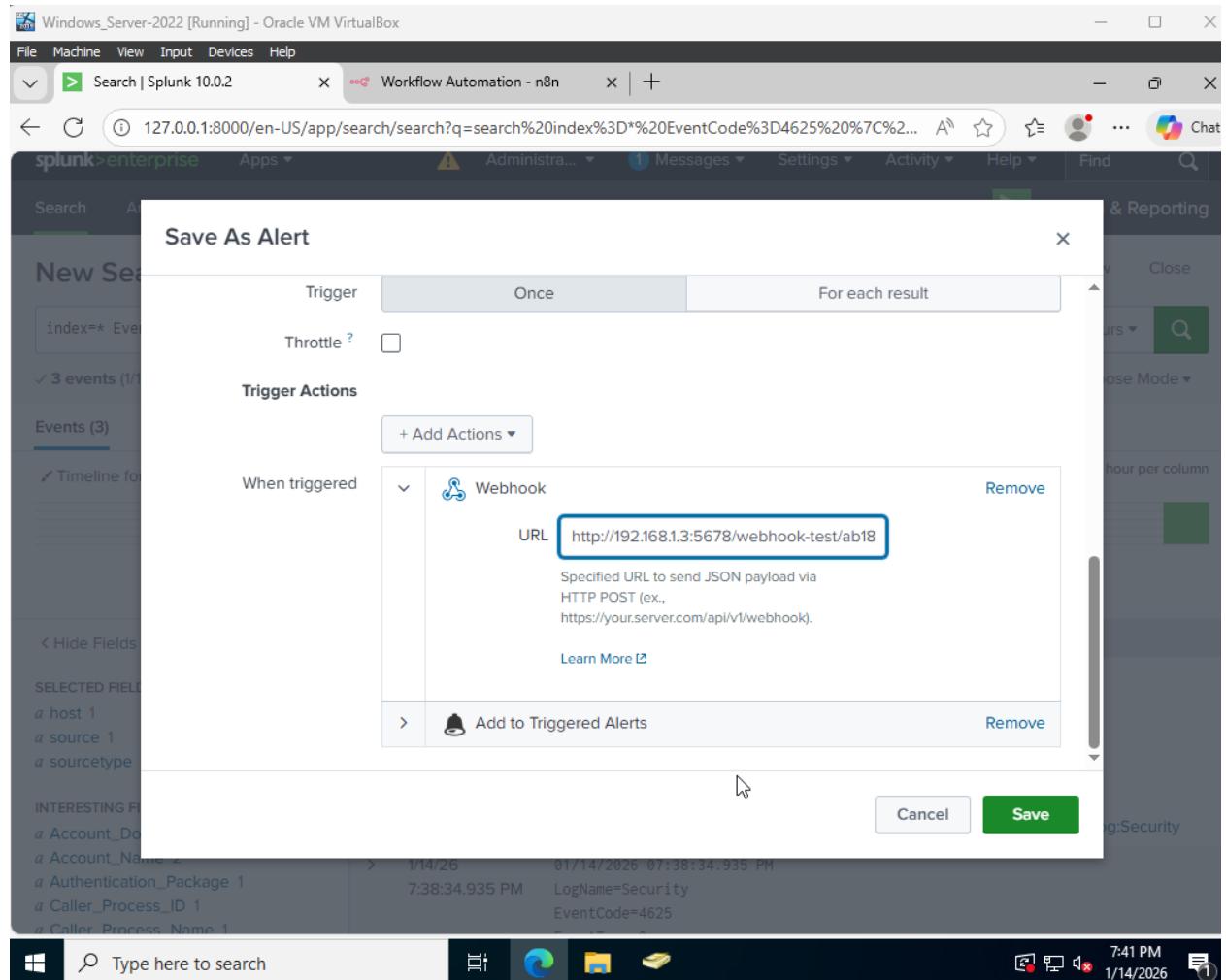
7:40 PM 1/14/2026





I will use the WebHook node to attach it to the alert. This will allow Splunk to send alerts to n8n.





As you can see, the alert has been created.

The screenshot shows a Splunk Enterprise interface. At the top, there's a navigation bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. Below it is a tab bar with 'Brute Force | Splunk 10.0.2' and 'Workflow Automation - n8n'. The main content area has a header 'splunk>enterprise' with 'Search & Reporting' highlighted. Below the header are tabs for 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. A search bar is on the right. The main content is titled 'Brute Force' and contains the message 'Failed log in credentials.' Below this, there are several configuration details:

Enabled: Yes. Disable	Trigger Condition: .. Number of Results is > 0. Edit
App: search	Actions: 2 Actions Edit
Permissions: Private. Owned by administrator. Edit	Add to Triggered Alerts
Modified: Jan 14, 2026 7:42:12 PM	Webhook
Alert Type: Scheduled. Cron Schedule. Edit	

At the bottom of the content area, there's a note: 'There are no fired events for this alert.' The bottom of the window shows a Windows taskbar with a search bar, pinned icons for File Explorer, Mail, and Task View, and system status icons.

After listening for a test event, the n8n node was able to detect the alert and produce the output.

Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Search | Splunk 10.0.2 > My workflow - n8n

Not secure 192.168.1.3:5678/workflow/ZvPiOFVVQHloP2Qz4rR9Z/e4b1b6

Webhook

Parameters Settings Listen for test event

Webhook URLs

Test URL Production URL

POST http://192.168.1.3:5678/webhook-test/ab189170-b387-41af-b193-2434f1747174

HTTP Method POST

Path ab189170-b387-41af-b193-2434f1747174

Authentication None

Respond Immediately

If you are sending back a response, add a "Content-Type" response header with the appropriate value to avoid unexpected behavior

Options

OUTPUT Docs Schema Table

1 item

body

sid : scheduler_administrator_search_RMD5C91acb01b27_at_1768449540_18

search_name : Brute Force

app : search

owner : administrator

results_link : http://WIN-OMMIV4J07C:8000/app/search/@go?sid=scheduler_administrator_search_RMD5C91acb01b27_at_1768449540_18

result

_time : 1768448311.182

ComputerName : PCI.project.local

user : Admin

src_ip : 127.0.0.1

count : 1

Pull in events from Webhook

Listen for test event

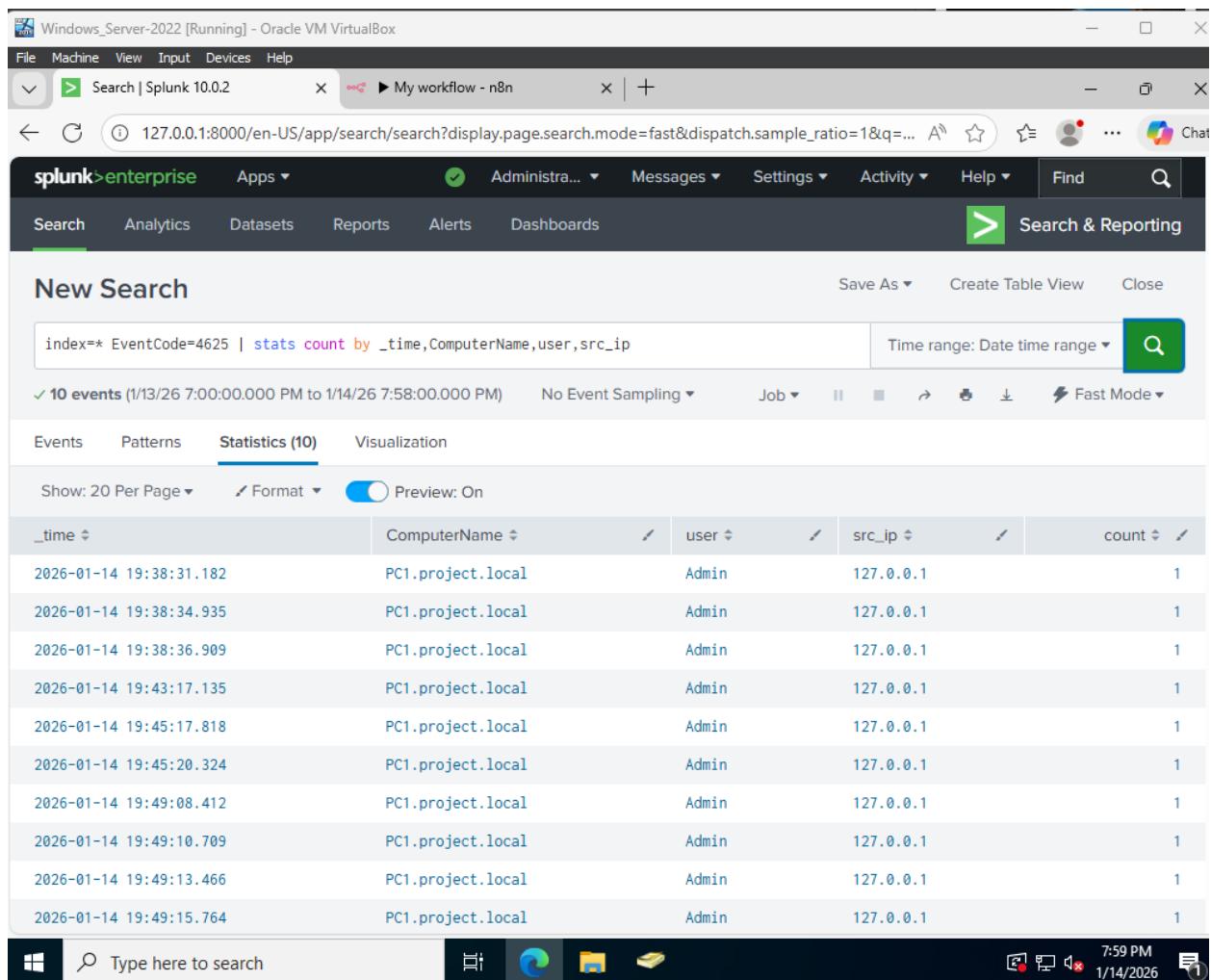
Once you've finished building your workflow, run it without having to click this button by using the production webhook URL. [More info](#)

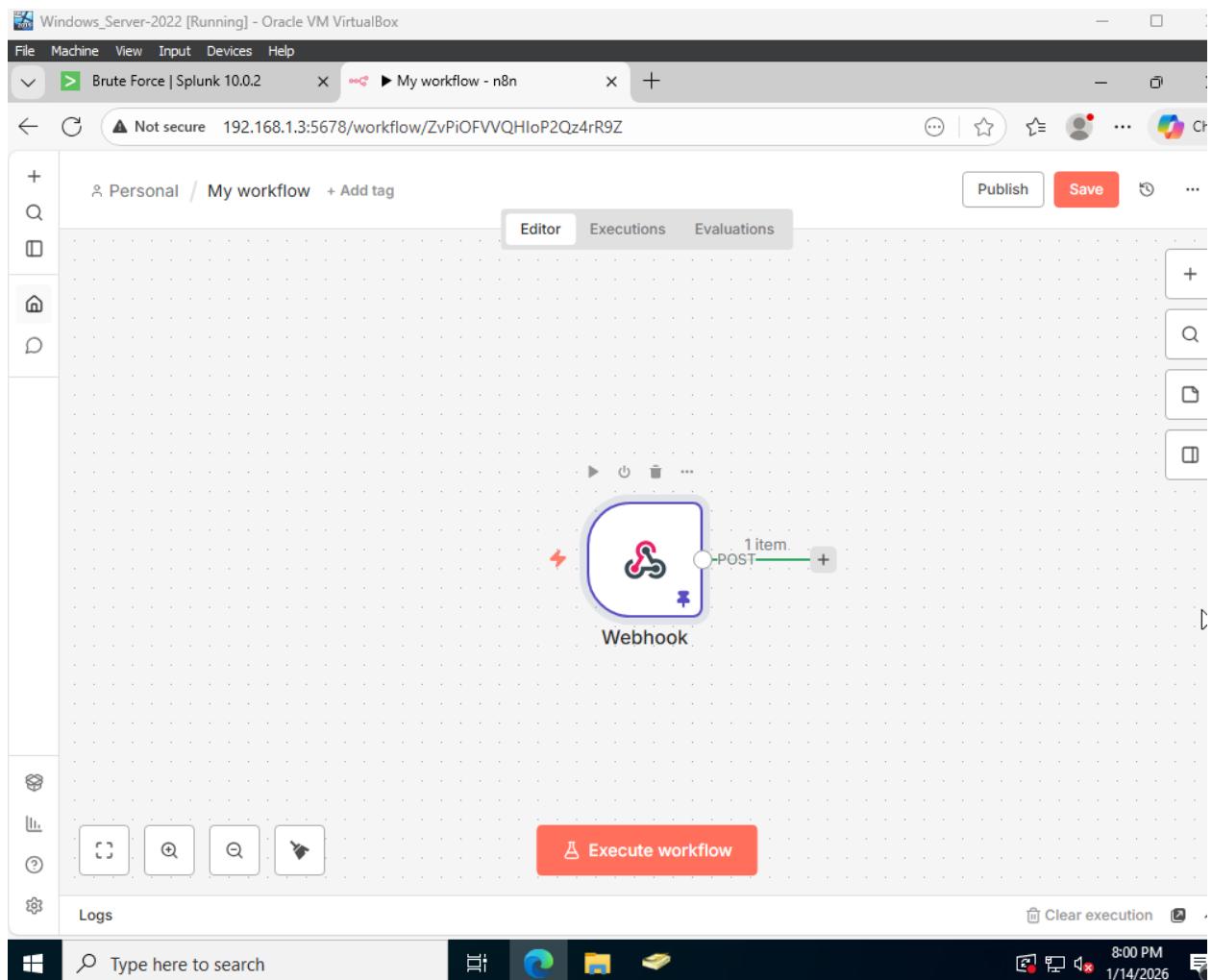
When will this node trigger my flow? ▾

Type here to search 7:59 PM 1/14/2026

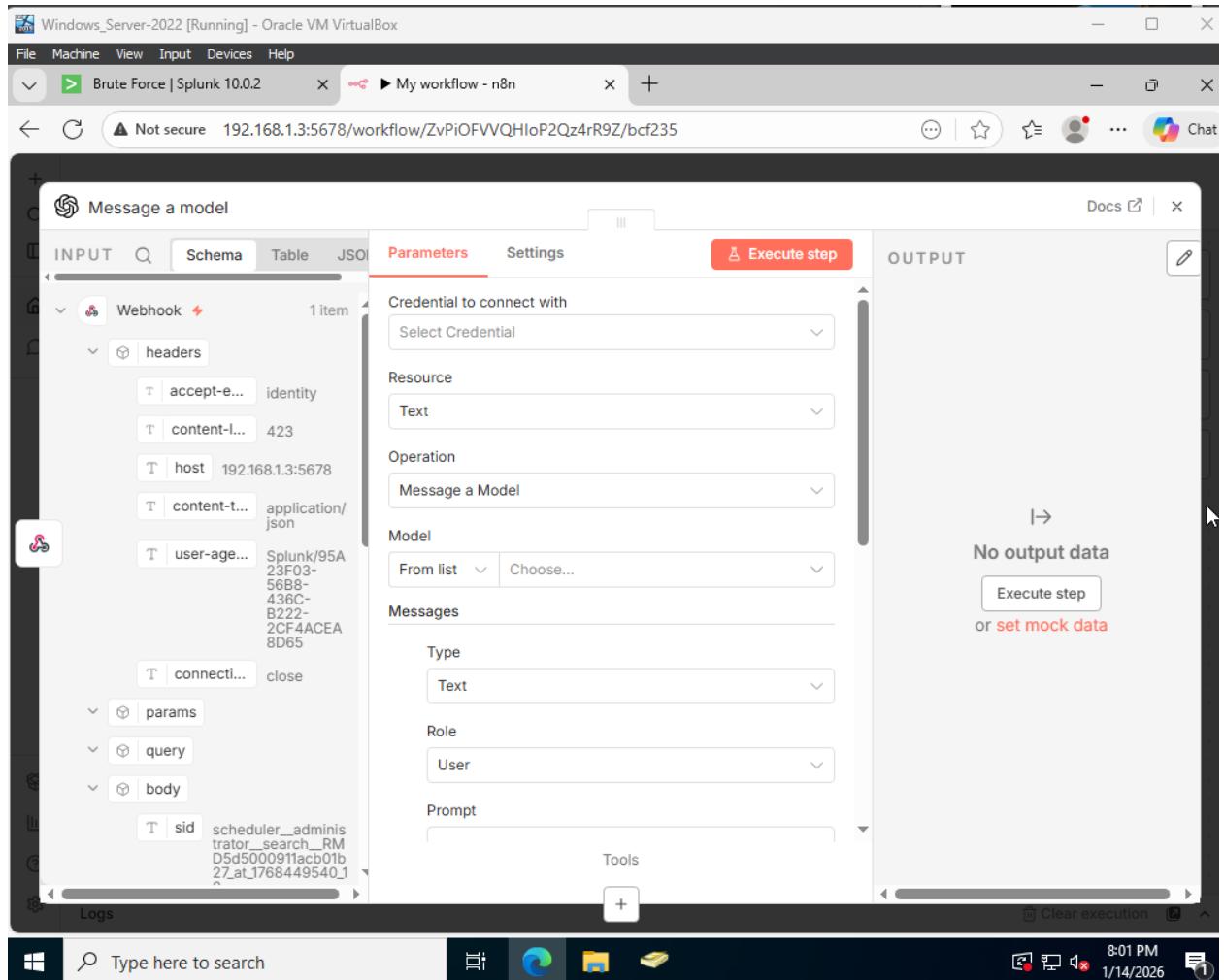
The screenshot shows the Splunk n8n interface. On the left, there's a sidebar with various icons. In the center, a 'Webhook' node is selected. The 'Parameters' tab is active, showing a 'Test URL' field containing 'http://192.168.1.3:5678/webhook-test/ab189170-b387-41af-b193-2434f1747174'. Below it, 'HTTP Method' is set to 'POST' and 'Path' is 'ab189170-b387-41af-b193-2434f1747174'. Under 'Authentication', 'None' is selected. The 'Respond' dropdown is set to 'Immediately'. A note below says: 'If you are sending back a response, add a "Content-Type" response header with the appropriate value to avoid unexpected behavior'. On the right, the 'OUTPUT' tab is selected, showing a single log entry in a table format. The log details a search operation: sid, search_name, app, owner, results_link, result, _time, ComputerName, user, src_ip, and count. At the bottom, a search bar says 'Type here to search' and shows the date and time '7:59 PM 1/14/2026'.

Here is the search of the alert showing all the logs:





I will now integrate ChatGPT as the AI. To do this I needed to add the OpenAI node and configure it.



Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Brute Force | Splunk 10.0 | My workflow - n8n | OpenAI Overview | OpenAI Platfo

https://platform.openai.com/docs/overview

OpenAI Platform

Search CTRL K

Get started

Overview

Quickstart

Models

Pricing

Libraries

Docs MCP

Latest: GPT-5.2

Core concepts

Add credits

Run your next API request by adding credits.

Go to Billing

Cookbook

Forum

OpenAI Platform

Developer quickstart

Make your first API request in minutes. Learn the basics of the OpenAI platform.

Get started

javascript ◊

```
1 import OpenAI from "openai";
2 const client = new OpenAI();
3
4 const response = await client.responses.create({
5   model: "gpt-5.2",
6   input: "Write a short bedtime story about a unicorn.",
7 });
8
9 console.log(response.output_text);
```

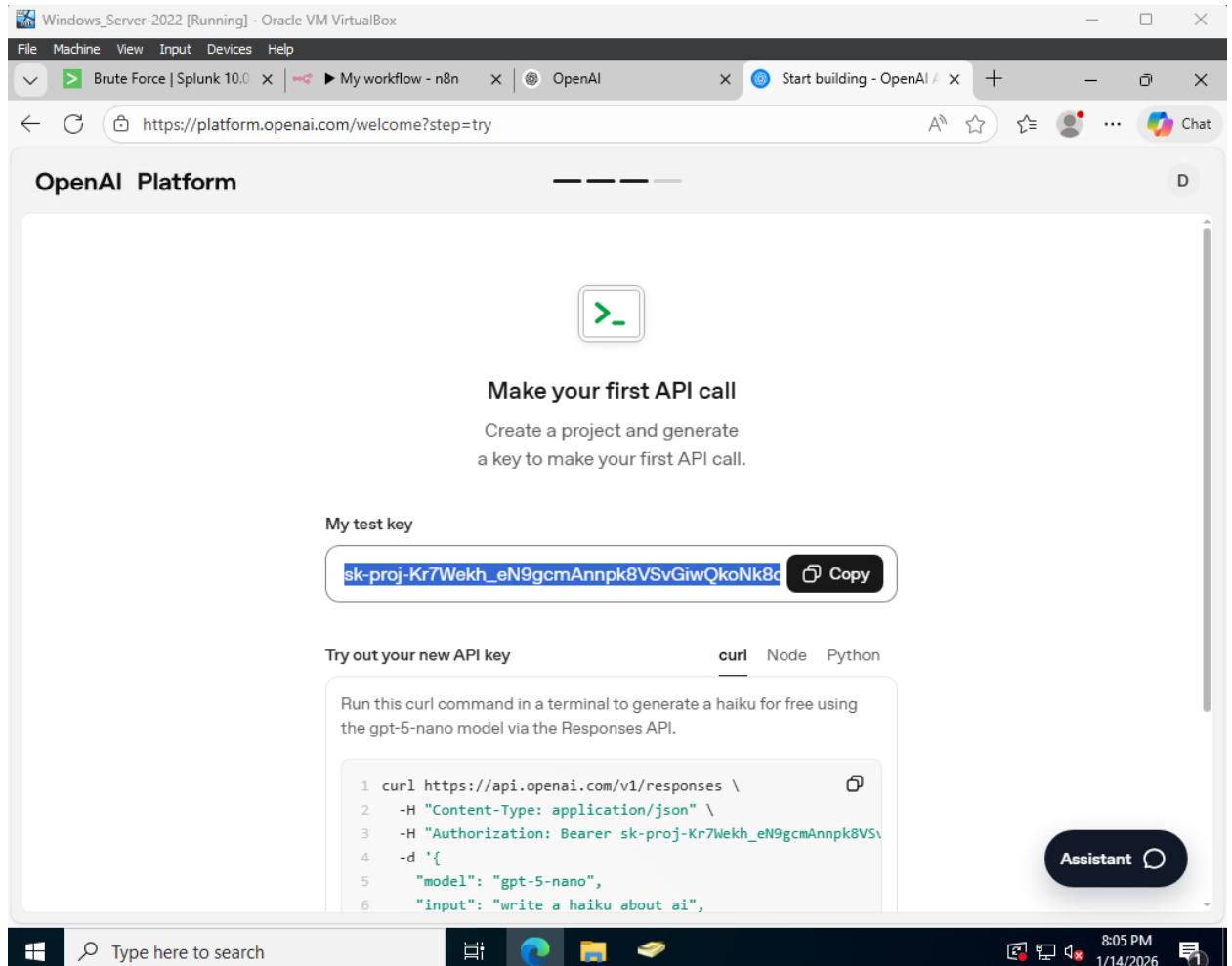
View all

Models

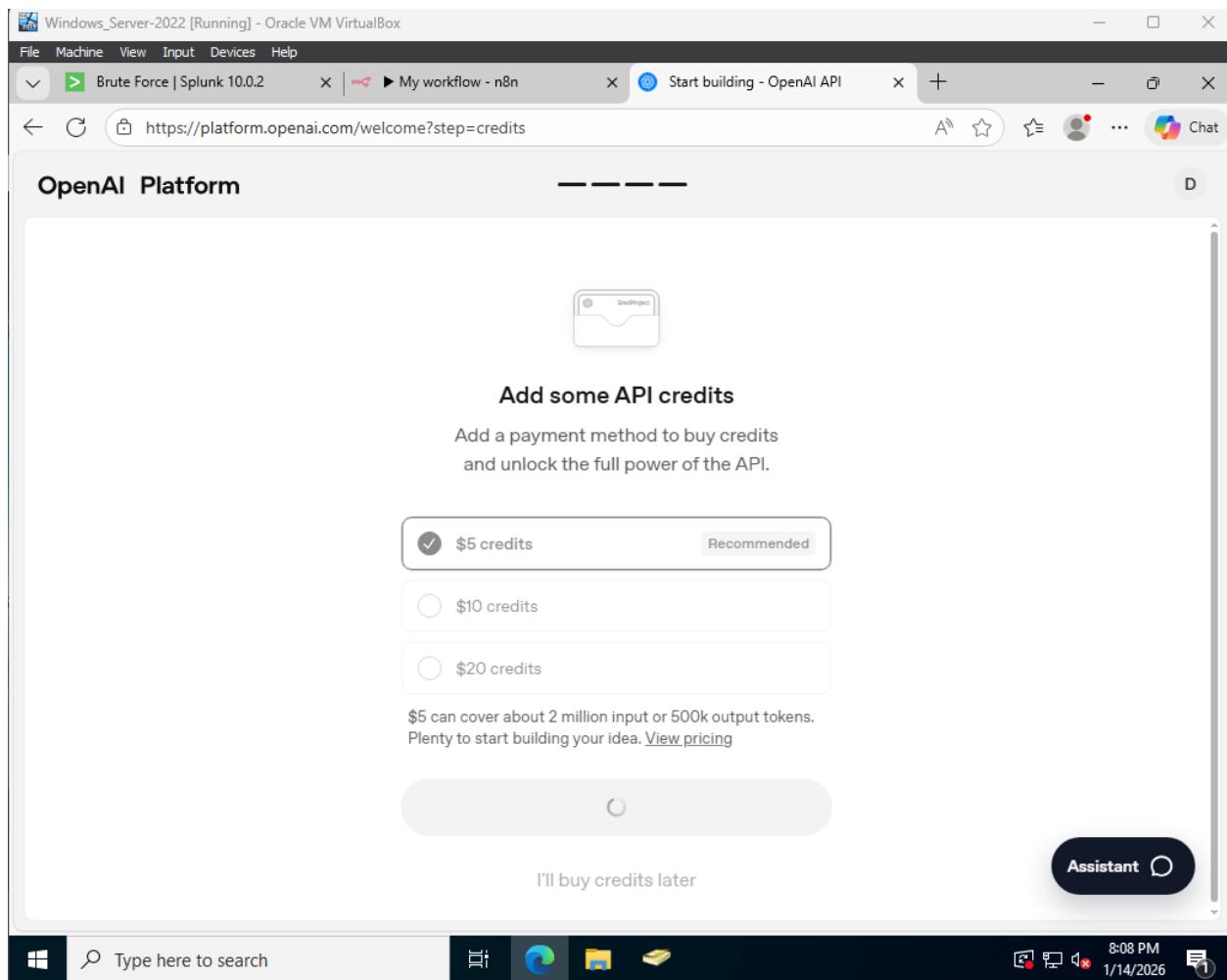
Assistant

Type here to search

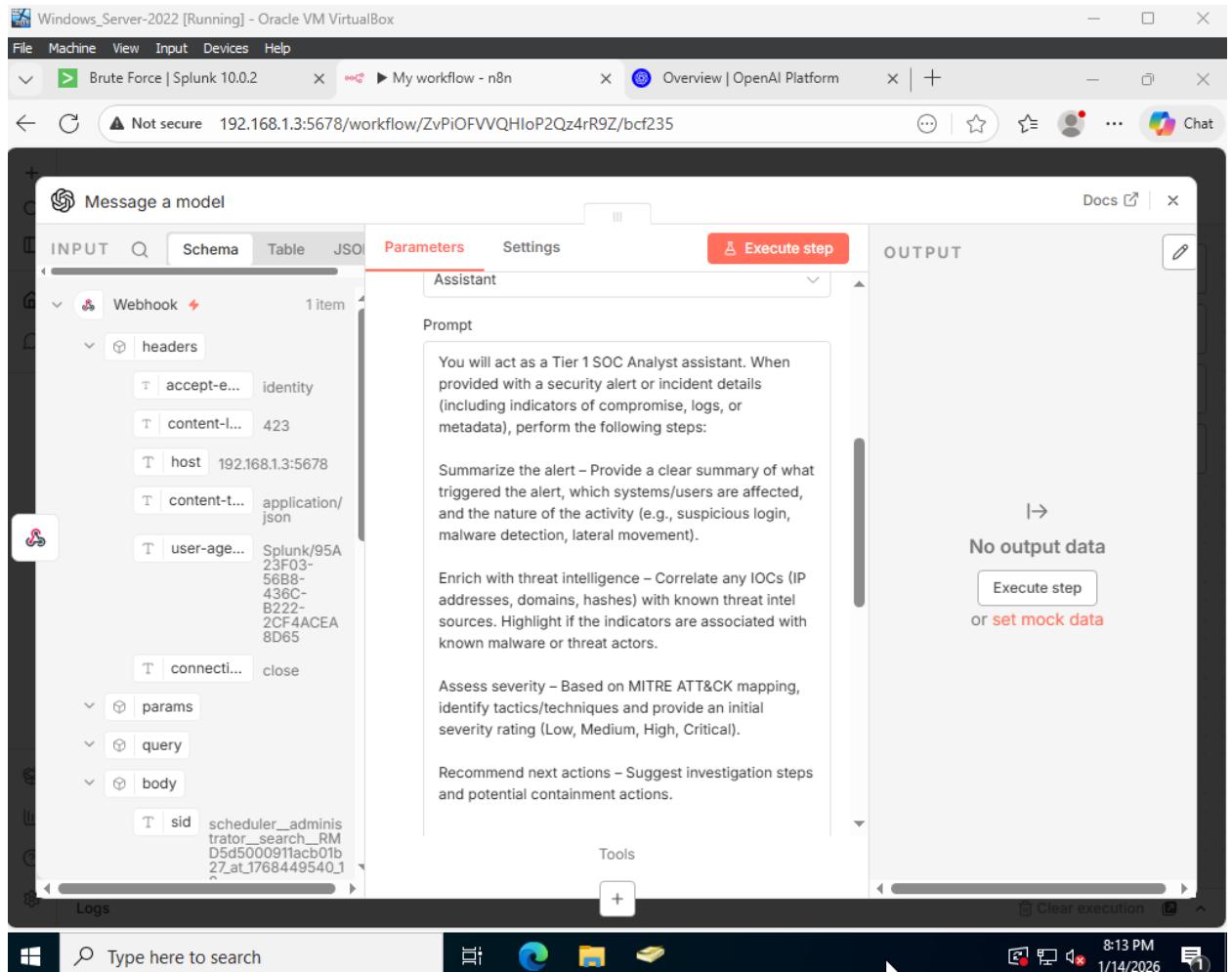
8:05 PM 1/14/2026

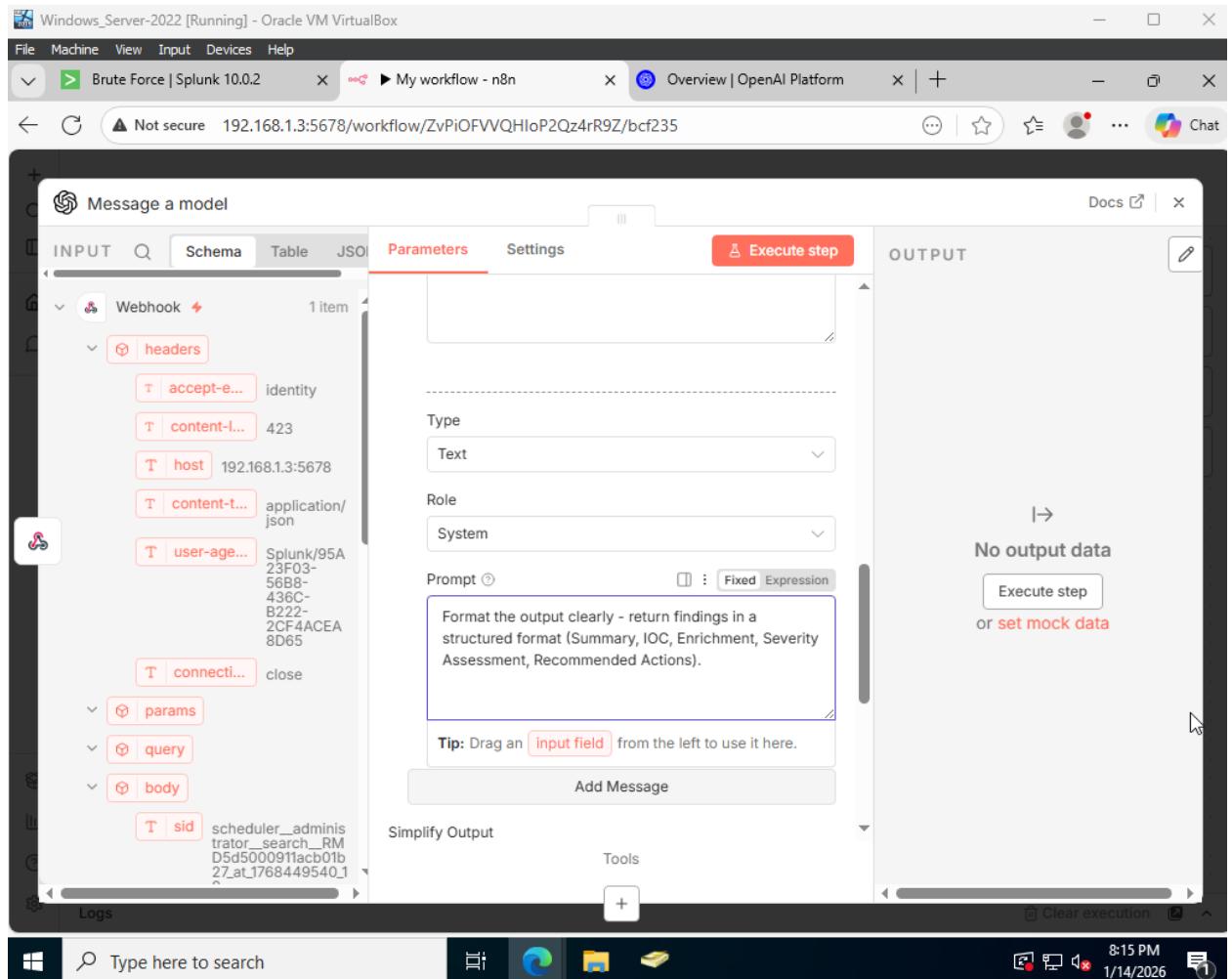


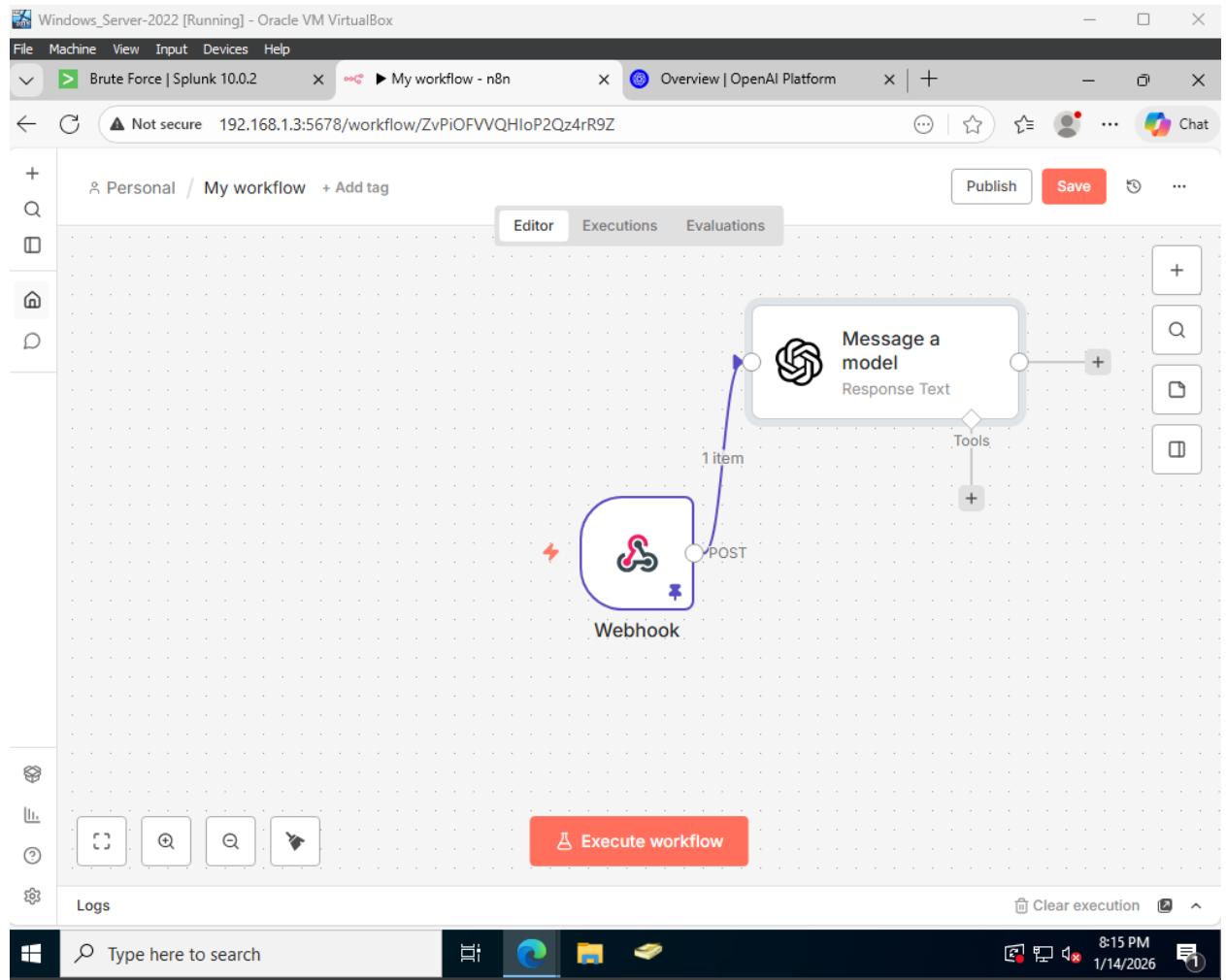
I had to purchase a few API credits to make this work.

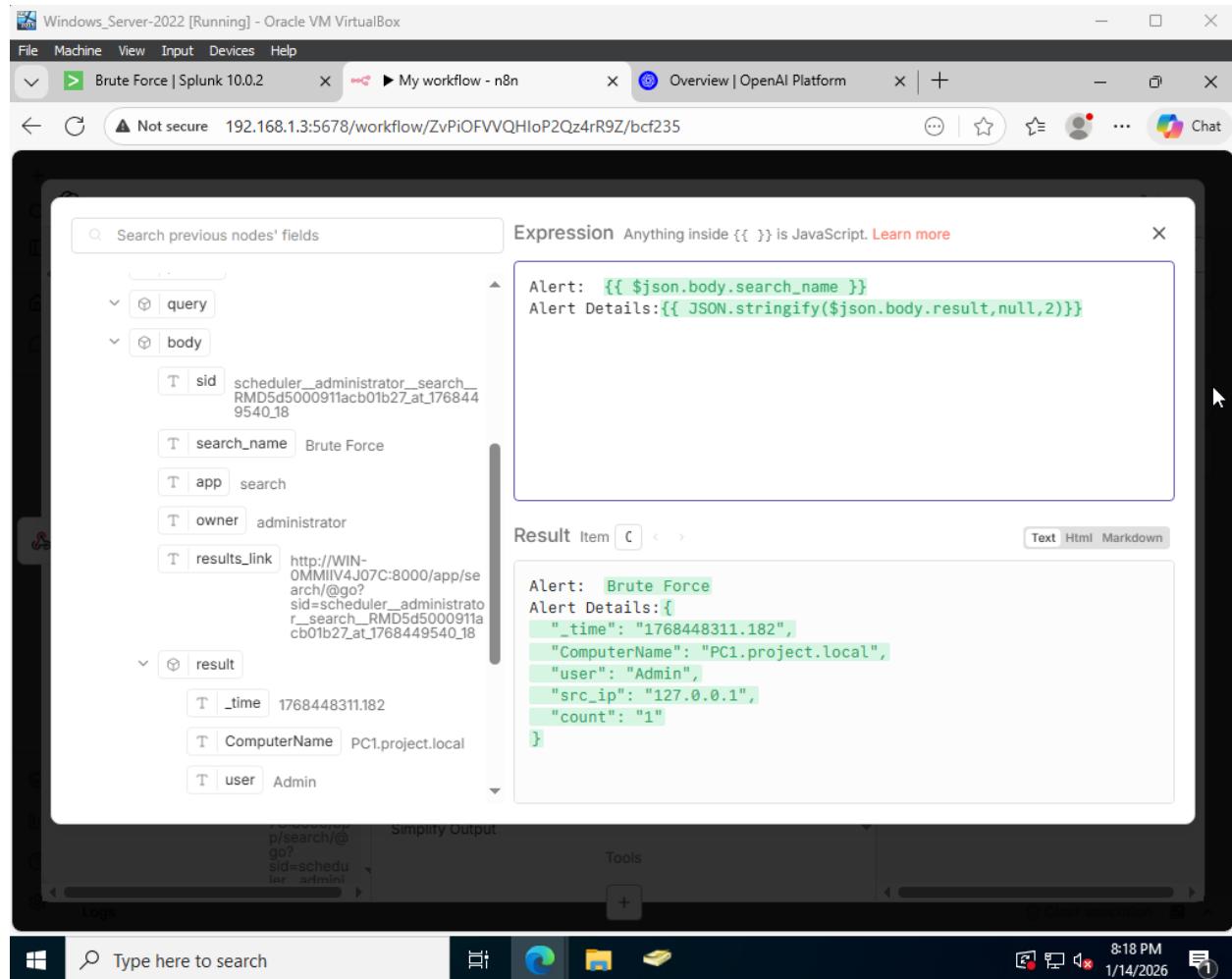


Here I set the prompt for AI to summarize the alert that was ingested.

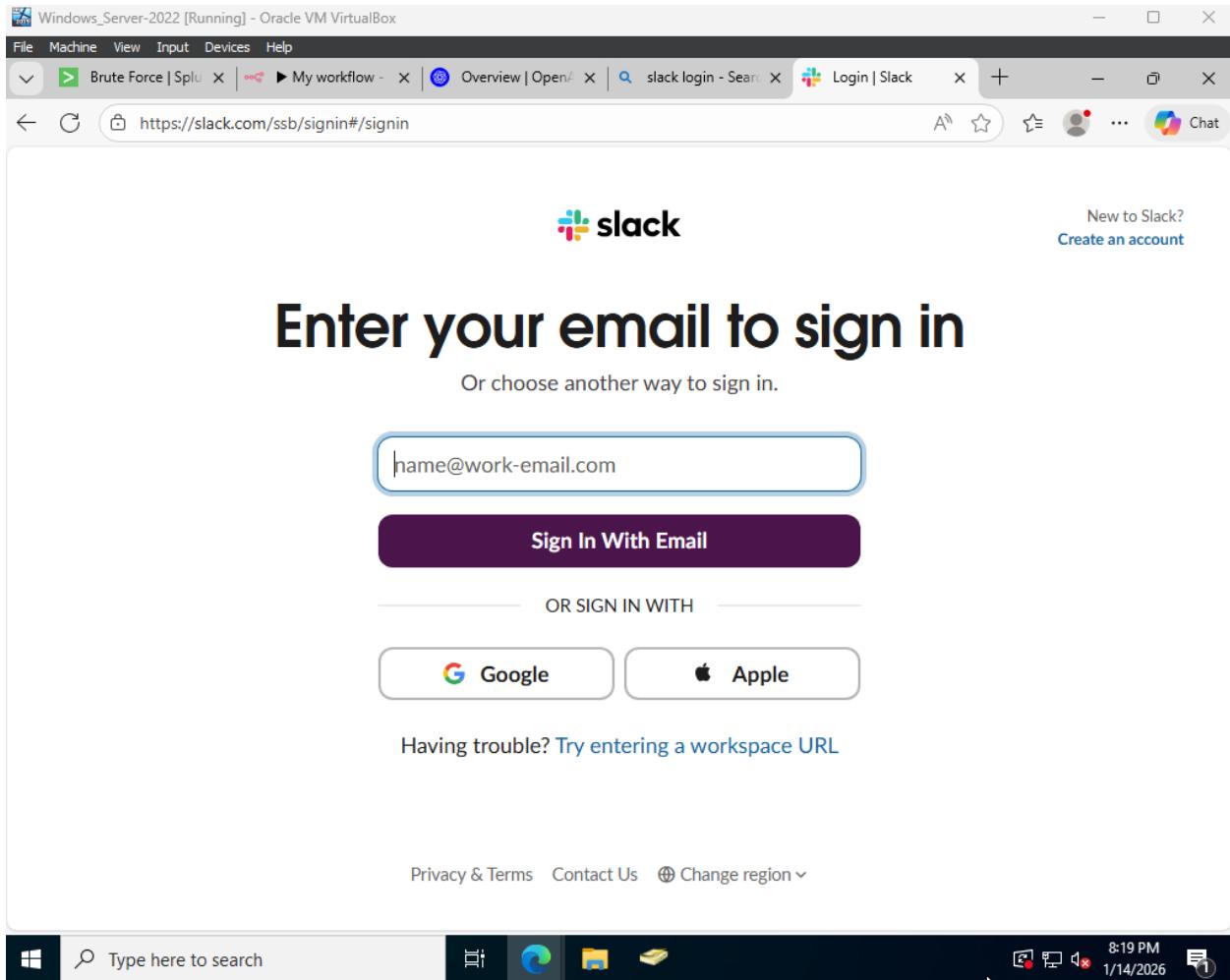




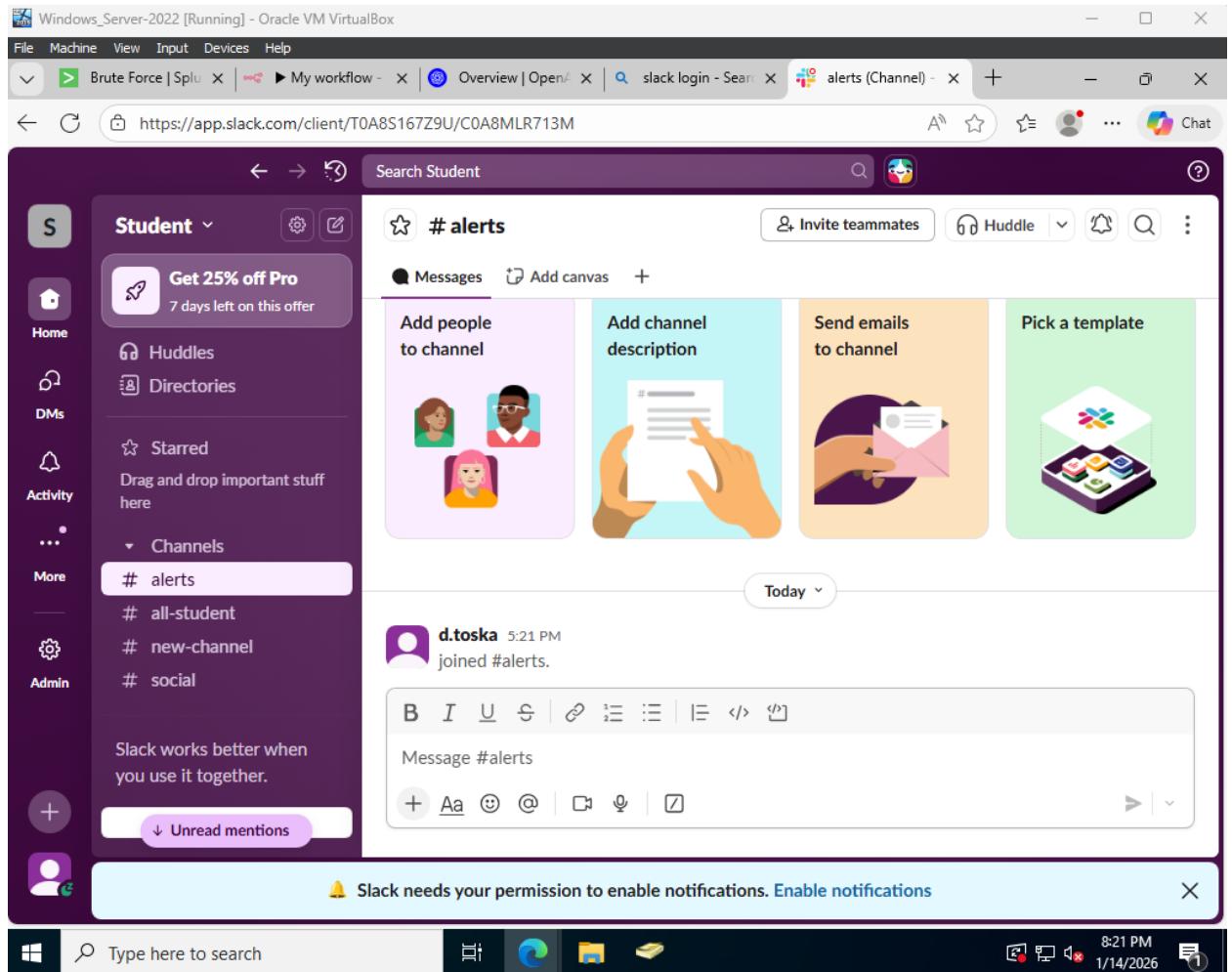




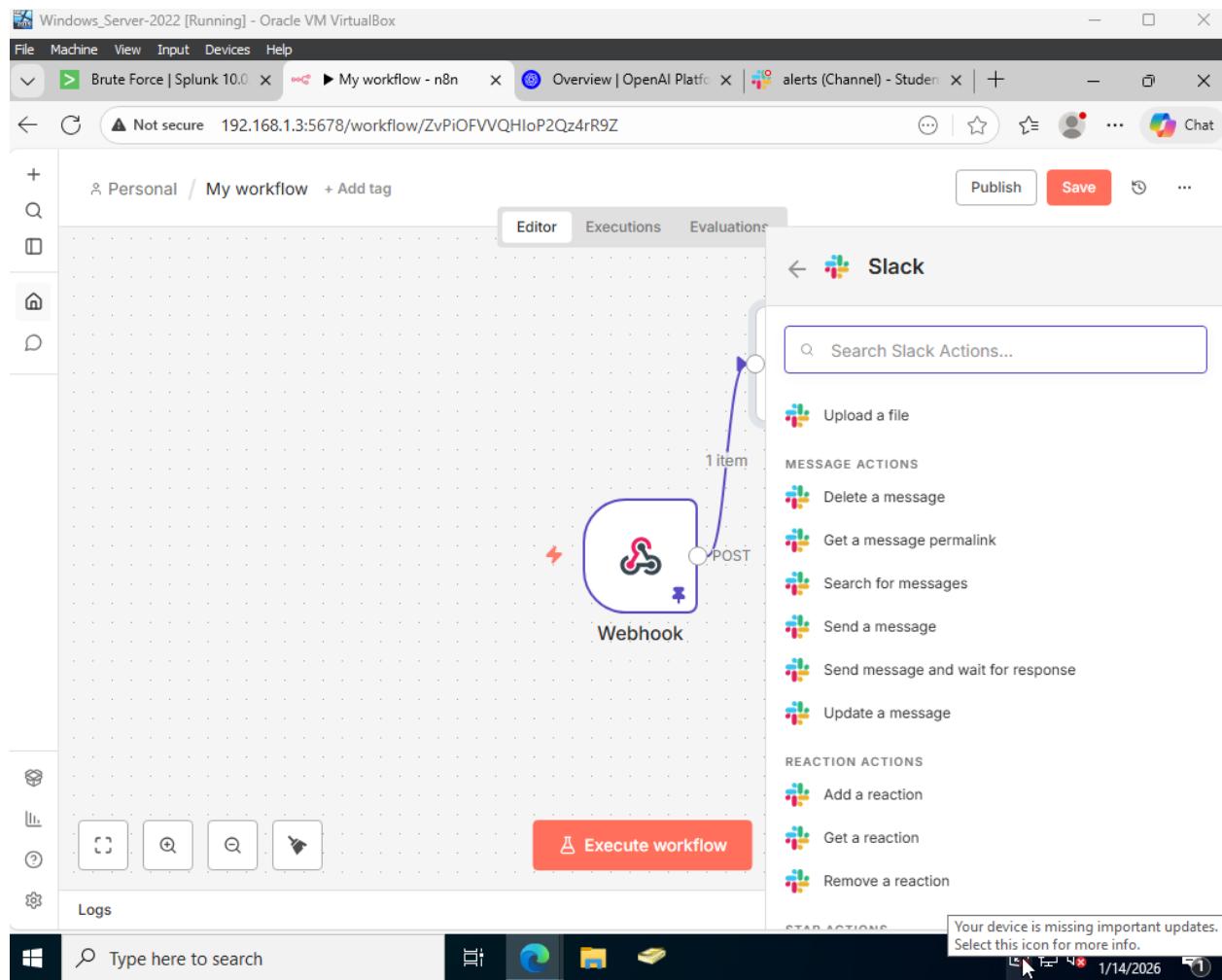
I will be using Slack to receive the alerts that n8n will produce.



I created a new channel called Alerts that will be used by n8n to produce the output.



These next few steps were done for creating the Slack node in n8n:



Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Brute Force | X My workfl | X Slack creden X Slack API: Ap X Overview | C X alerts (Chann X +

https://api.slack.com/apps

slack api Documentation Tutorials Your Apps

Your Apps

Use our APIs to build an app or service that integrates with Slack. Create a public or private app to interact with your workspace.

Name app & choose workspace

App Name: Alerts

Don't worry - you'll be able to change this later.

Pick a workspace to develop your app in:

Student

Keep in mind that you can't change this app's workspace later. If you leave the workspace, you won't be able to manage any apps you've built for it. The workspace will control the app even if you leave the workspace.

[Sign into a different workspace](#)

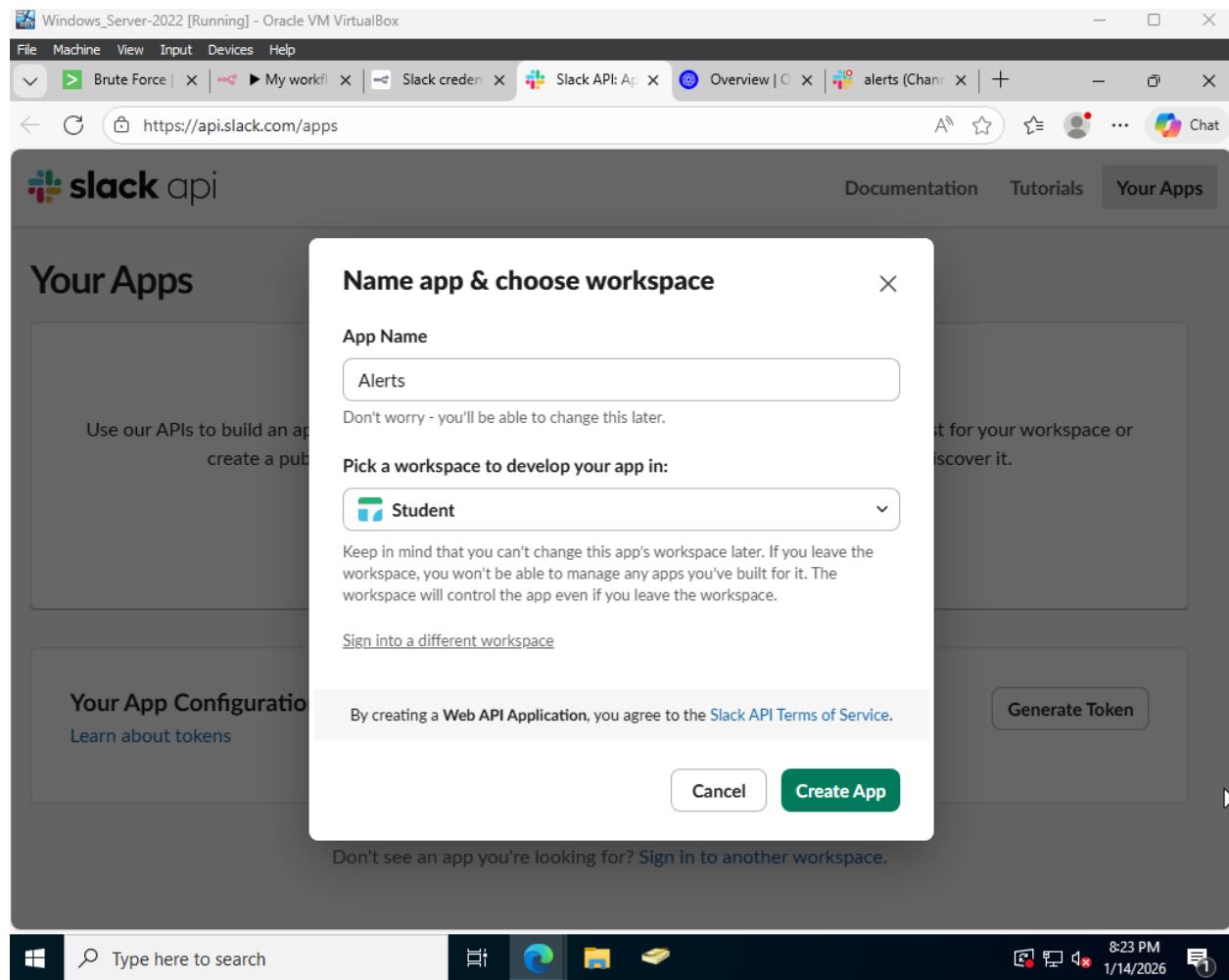
By creating a **Web API Application**, you agree to the [Slack API Terms of Service](#).

[Cancel](#) [Create App](#)

Don't see an app you're looking for? [Sign in to another workspace](#).

Type here to search

8:23 PM 1/14/2026



Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Brute Force | My work | Slack creden... | Slack API: Ap... | Overview | alerts (Chann...

https://api.slack.com/apps/A0A8U2L3Z5G?created=1

Alerts Basic Information

Settings

Basic Information

- Collaborators
- Socket Mode
- Install App
- Manage Distribution

Features

- App Home
- Agents & AI Apps...
- Work Object Previe...
- Workflow Steps...
- Org Level Apps
- Incoming Webhooks
- Interactivity & Shor...
- Slash Commands
- Steps from Apps LEGACY
- OAuth & Permissions
- Event Subscriptions

App Credentials

These credentials allow your app to access the Slack API. They are secret. Please don't share your app credentials with anyone, include them in public code repositories, or store them in insecure ways.

App ID AOA8U2L3Z5G **Date of App Creation** January 14, 2026

Client ID 10298040271334.10300088135186

Client Secret Show Regenerate

You'll need to send this secret along with your client ID when making your `oauth.v2.access` request.

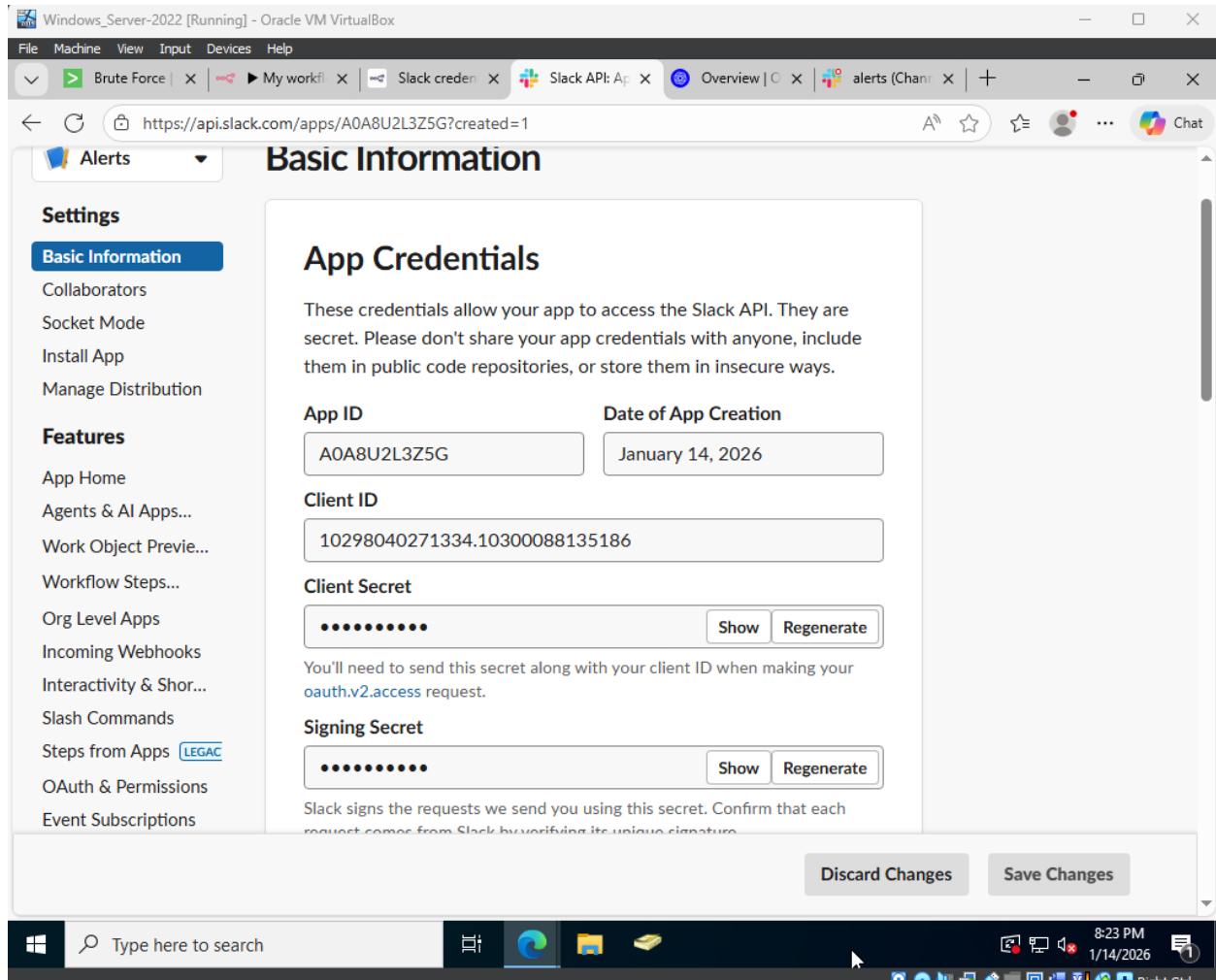
Signing Secret Show Regenerate

Slack signs the requests we send you using this secret. Confirm that each request comes from Slack by verifying its unique signature.

Discard Changes Save Changes

Type here to search

8:23 PM 1/14/2026



Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Brute Force | X My workfl | Slack creden | Slack API: Ap | Overview | C | alerts (Chann | +

https://api.slack.com/apps/A0A8U2L3Z5G/oauth?

A Slack app's capabilities and permissions are governed by the [scopes](#) it requests.

Bot Token Scopes

Scopes that govern what your app can access.

OAuth Scope	Description
canvases:write	"Alerts" will be able to create, edit and remove canvases.
channels:read	View basic information about public channels in a workspace
files:read	View files shared in channels and conversations that "Alerts" has been added to
files:write	Upload, edit, and delete files as "Alerts"
groups:read	View basic information about private channels that "Alerts" has been added to

Type here to search

8:30 PM 1/14/2026

Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Brute For My wo Slack cre Slack API Slack API Overview alerts (C Chat

https://api.slack.com/apps/A0A8U2L3Z5G/oauth?success=1

slack api Documentation Tutorials Your Apps

Install App automatically expire after they're issued within your app code. [View documentation](#)

Manage Distribution

Features

- App Home
- Agents & AI Apps...
- Work Object Previe...
- Workflow Steps...
- Org Level Apps
- Incoming Webhooks
- Interactivity & Shor...
- Slash Commands
- Steps from Apps LEGACY

OAuth & Permissions

- Event Subscriptions
- User ID Translation
- App Manifest NEW
- Beta Features

Submit to Slack Marketplace

Review & Submit

Bot User OAuth Token

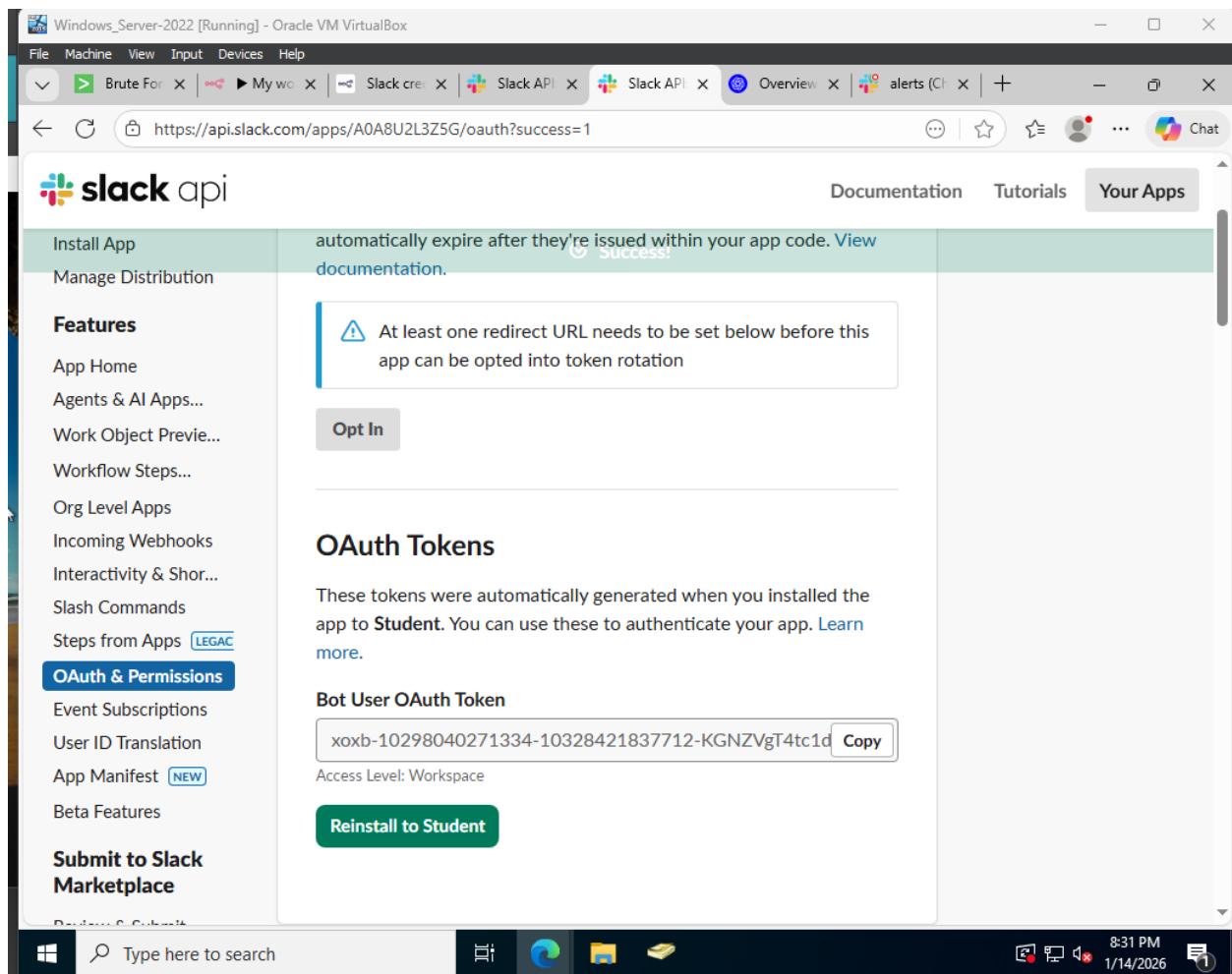
xoxb-10298040271334-10328421837712-KGNZVgT4tc1d [Copy](#)

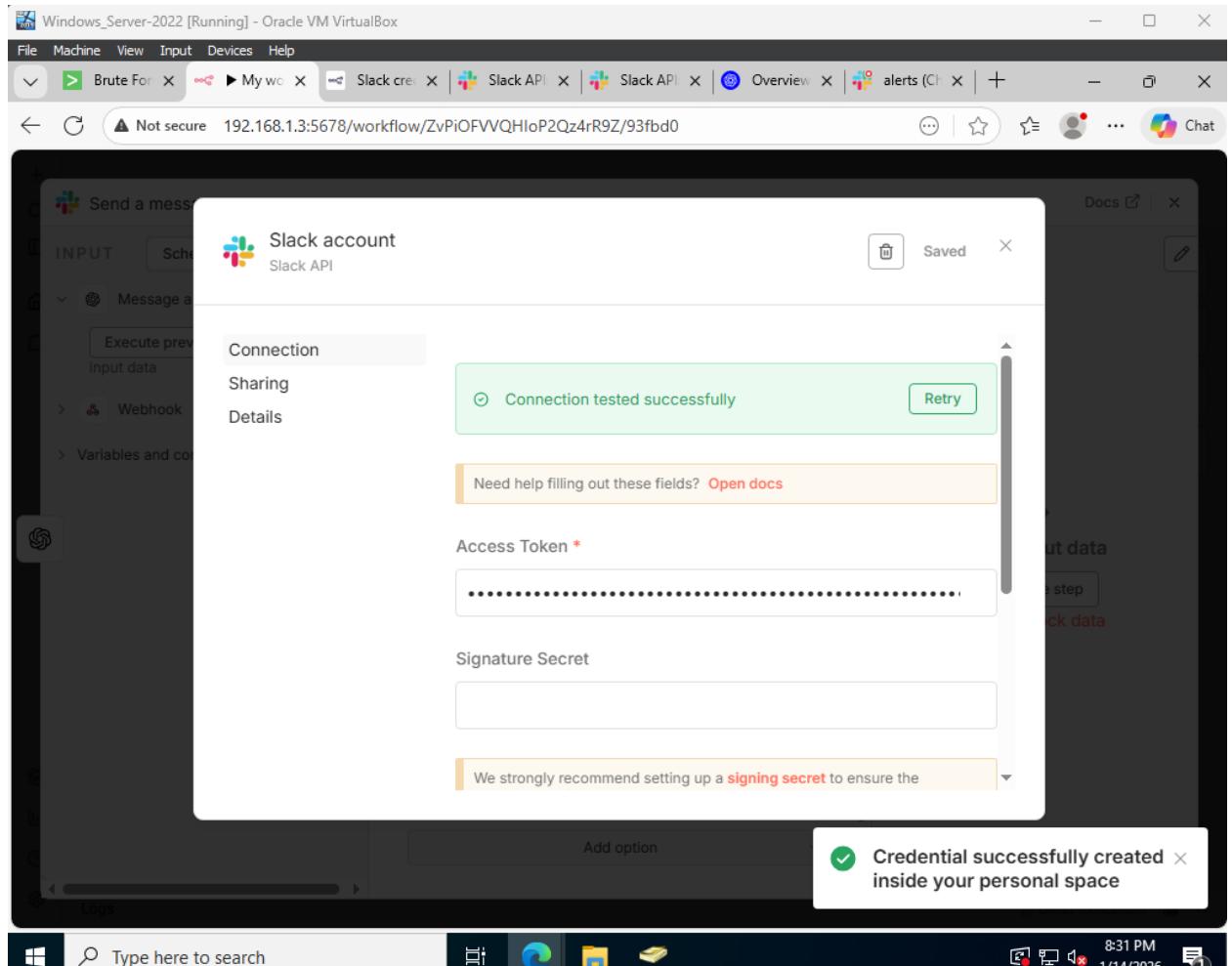
Access Level: Workspace

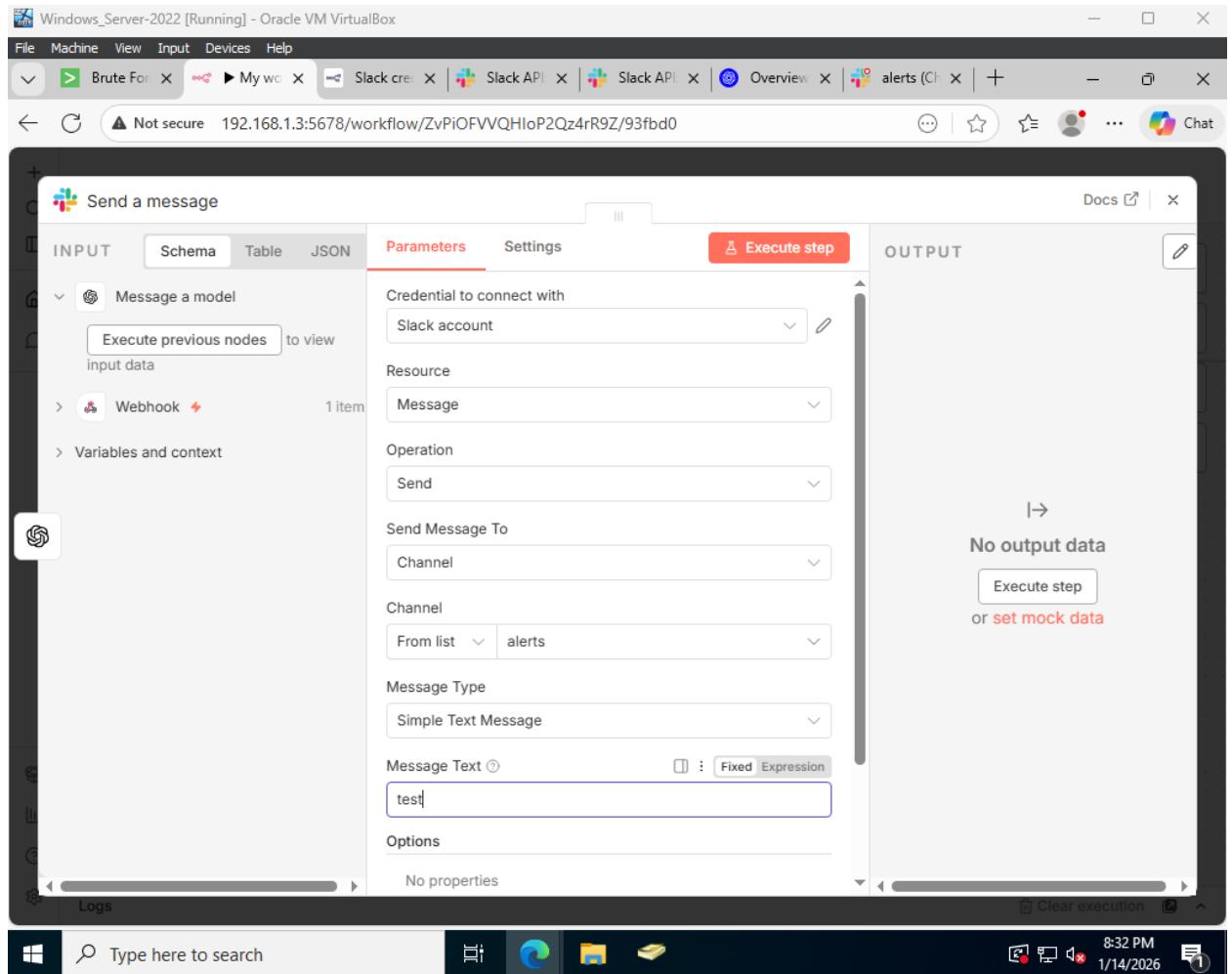
[Reinstall to Student](#)

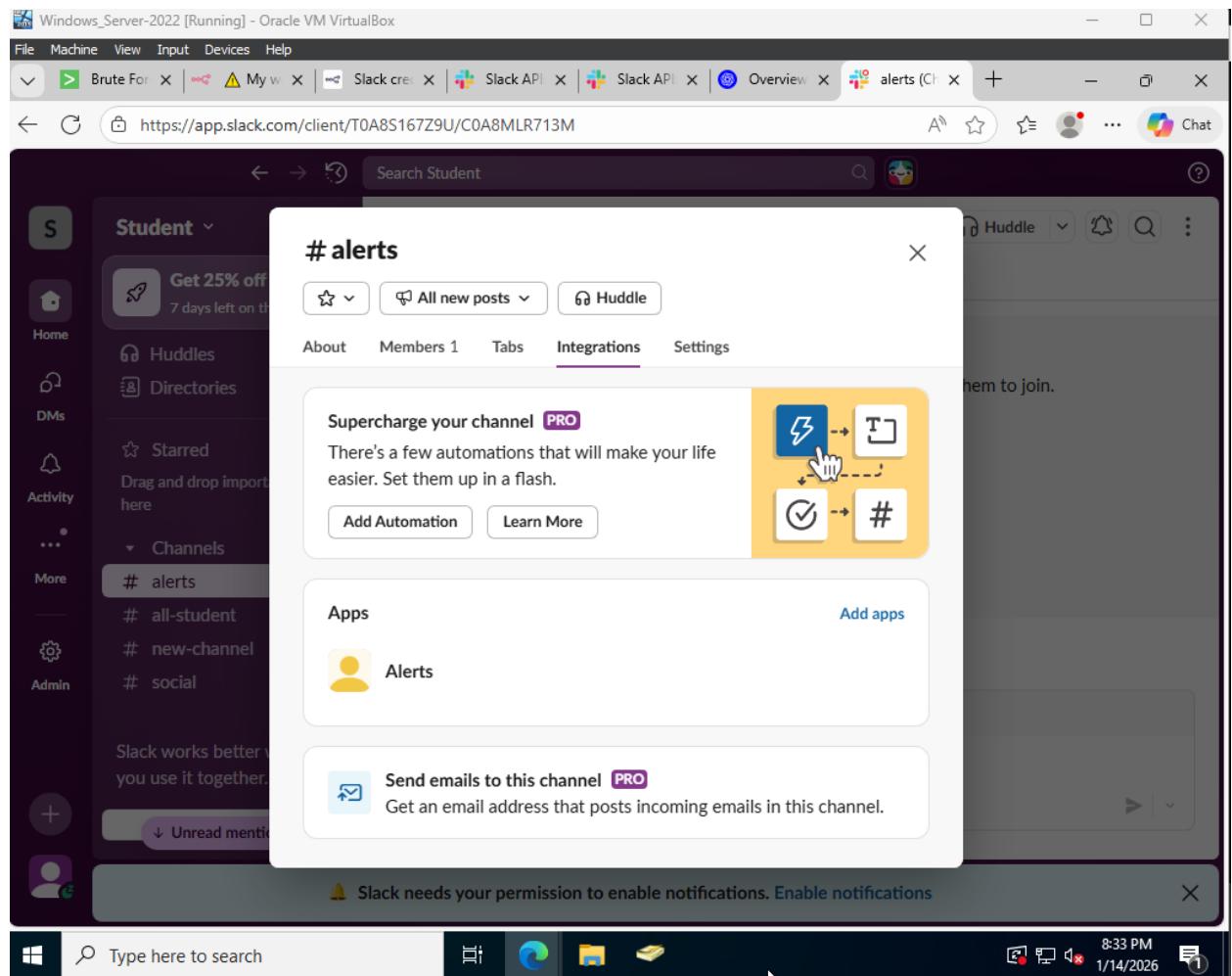
Type here to search

8:31 PM 1/14/2026









Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Brute Force | Splunk | My workflow - Slack API: Application | Overview | Open | alerts (Channel) - +

Not secure 192.168.1.3:5678/workflow/ZvPiOFVQHloP2Qz4rR9Z/93fb0

Send a message

INPUT Schema Table JSON Parameters Settings Execute step

Credential to connect with: Slack account

Resource: Message

Operation: Send

Send Message To: Channel

Channel: From list: alerts

Message Type: Simple Text Message

Message Text: test

Options: No properties

OUTPUT Schema Table

1 item

ok	channel	message
true	COA8MLR713M	user : U0A9NCD type : message ts : 1768441217.5 bot_id : B0A8MM app_id : A0A8U text : test\n_Auto <http://192.168. Qz4rR9Z?utm_& internal&pa mpaign=n8n- base.slack.c7 283661229f9a team : T0A8S16; bot_profile id : B0A8MM app_id : A0A8U user_id : U0A name : Alerts icons image_36 :

Logs

Clear execution

The screenshot shows a workflow editor interface with a central step configuration panel. On the left, the input is displayed as a Slack message object with fields like id, type (message), status (completed), and content (containing a summary and a link). On the right, the output is shown as a table with one item, indicating success (ok: true), the channel (COA8MLR713M), and the message content, which includes a user ID, type, timestamp, bot ID, app ID, text, and various Slack-specific fields like team, bot_profile, and icons.

As you can see, the test alert was outputted:

Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Brute Force | Splu My workflow | Slack API: Application Overview | Open alerts (Channel) -

https://app.slack.com/client/T0A8S167Z9U/C0A8MLR713M

Search Student

Student

Get 25% off Pro
7 days left on this offer

Home DMs Activity More Admin

alerts # all-student # new-channel # social Direct messages d.toska you Apps Slackbot Alerts 1

Slack works better when you use it together.

Invite teammates

alerts

Messages Add canvas +

(198 kB)

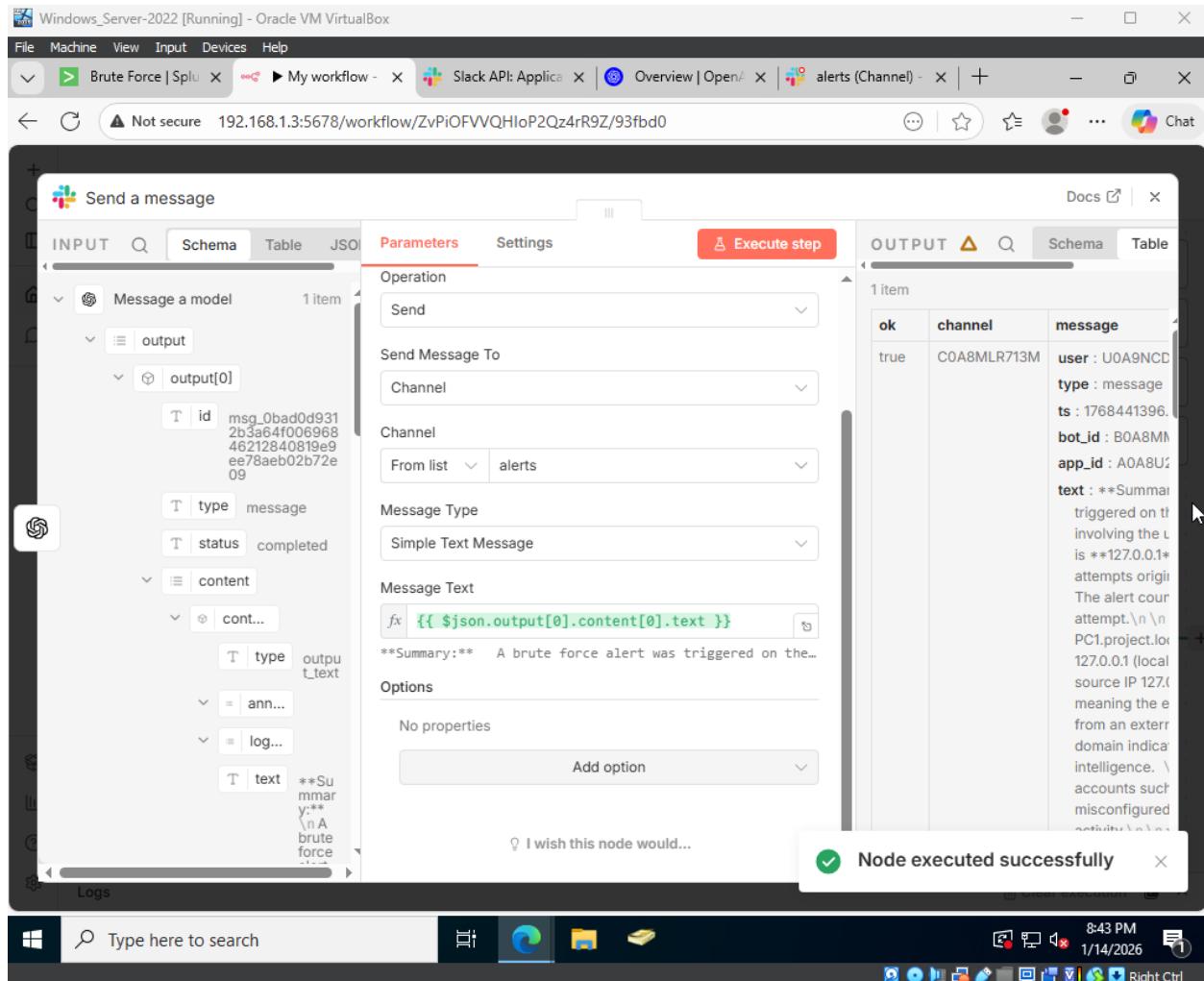


Type here to search

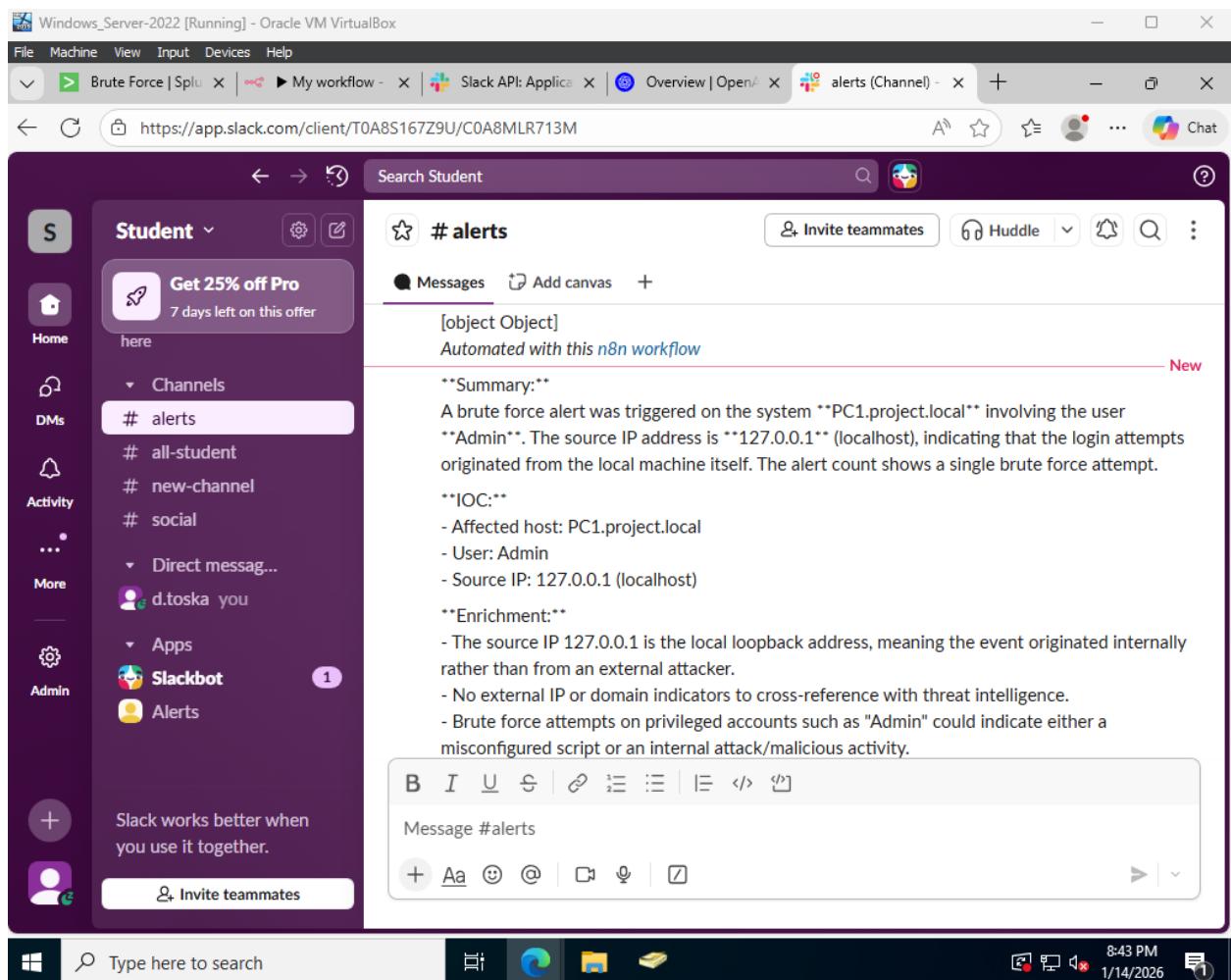


8:40 PM 1/14/2026





After swapping the test to the AI, it was able to produce the output it made.



Windows_Server-2022 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Brute Force | Splunk | My workflow | Slack API: Application | Overview | Open | alerts (Channel) -

https://app.slack.com/client/T0A8S167Z9U/C0A8MLR713M

Search Student

Student

Get 25% off Pro
here

Channels

- # alerts
- # all-student
- # new-channel
- # social

Direct messages

- d.toska you

Apps

- Slackbot
- Alerts

Slack works better when you use it together.

Invite teammates

alerts

Messages Add canvas +

rather than from an external attacker.

- No external IP or domain indicators to cross-reference with threat intelligence.
- Brute force attempts on privileged accounts such as "Admin" could indicate either a misconfigured script or an internal attack/malicious activity.

Severity Assessment:

- **MITRE ATT&CK Mapping:**
- Technique: T1110 - Brute Force
- Tactic: Initial Access / Defense Evasion

- Considering this is a local brute force attempt on a high-privileged account, initial severity is **Medium**.

- If repeated attempts or other suspicious actions are found, severity could increase.

Recommended Actions:

1. Investigate login attempts on PC1.project.local: check logs for multiple failed login attempts from the localhost.
2. Verify if the attempt was legitimate (e.g., a script, automated process, or user mistake) or malicious.
3. Check for abnormal processes or applications running under the Admin user or on the PC1

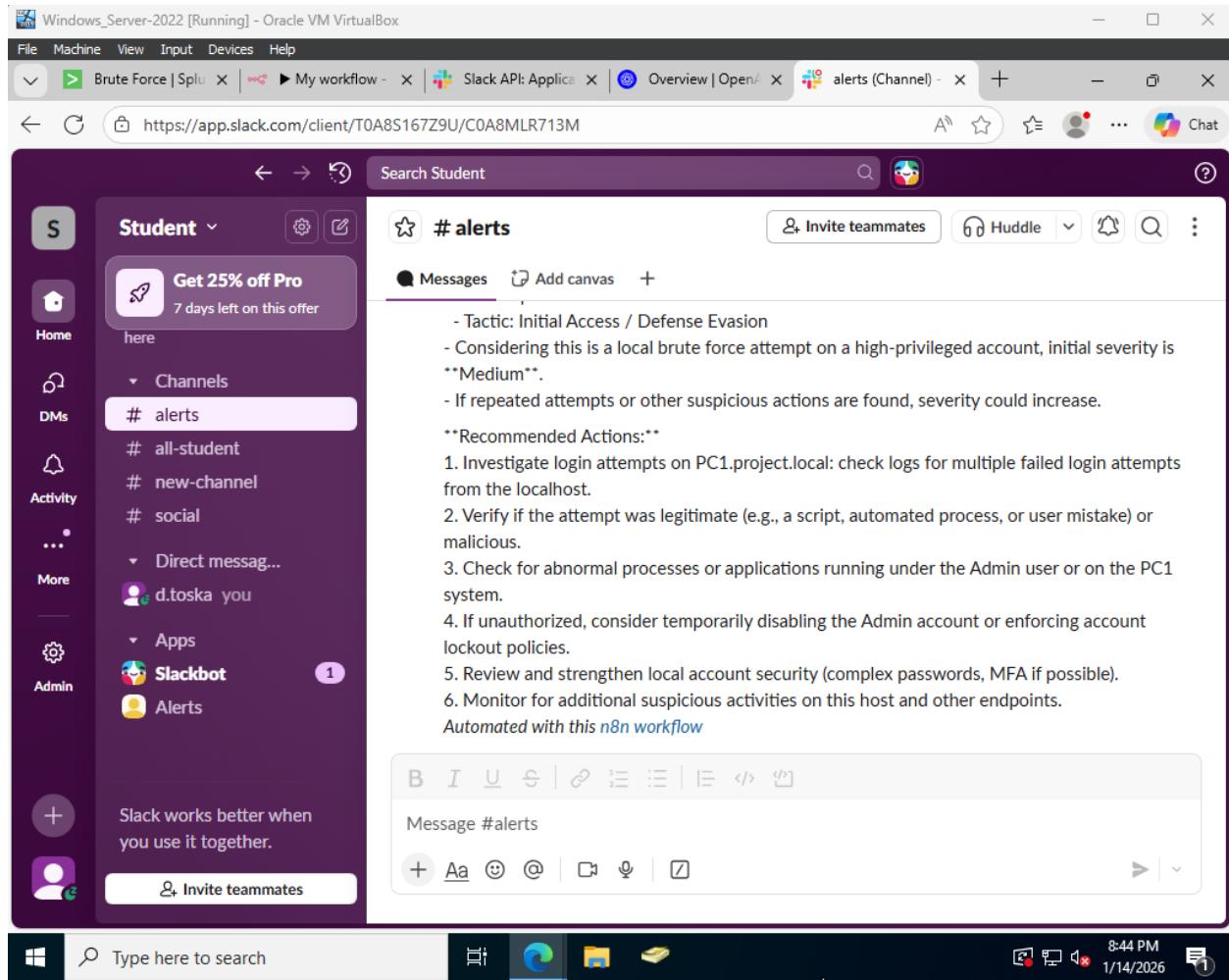
B I U S | ⌂ ⌂ ⌂ | ↵ ↵ ↵ | ↵ ↵ ↵ | ↵ ↵ ↵

Message #alerts

+ Aa ☺ @ | ↵ ↵ ↵ | ↵ ↵ ↵

8:43 PM 1/14/2026

The screenshot shows a Slack application window titled '# alerts'. The message content discusses a brute force attempt on a privileged account ('Admin') and provides a severity assessment and recommended actions. The Slack interface includes a sidebar with channels like # all-student and # social, and a bottom bar with various icons.



I will now use Hydra to create logs for the alert to trigger and send to n8n:

Kali [Running] - Oracle VM VirtualBox

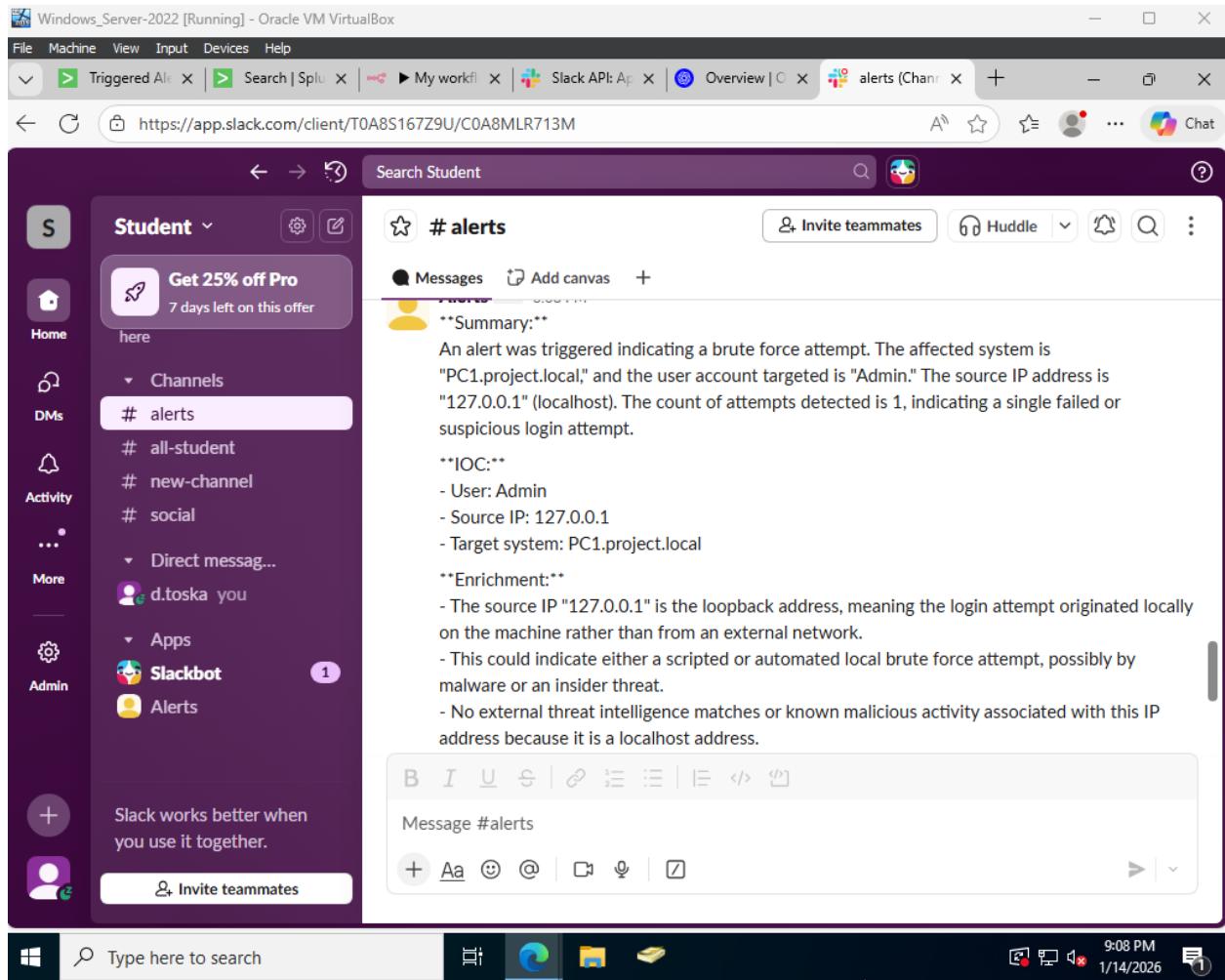
root@kali: /home/administrator

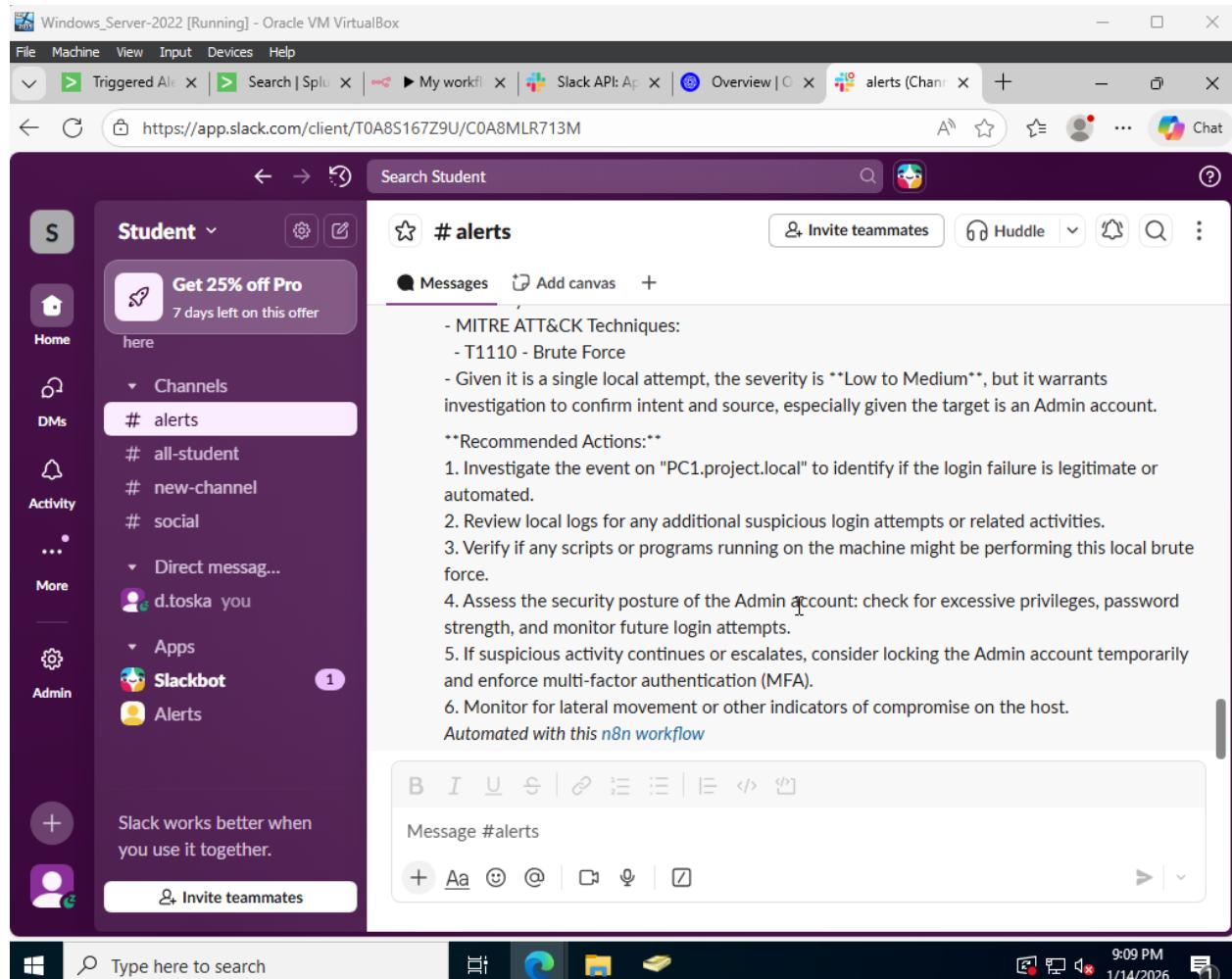
Session Actions Edit View Help

```
[root@kali ~]# hydra -l Admin -P /usr/share/wordlists/metasploit/unix_passwords.txt ssh://192.168.1.101
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-14 21:01:41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1022 login tries (l:1/p:1022), ~64 tries per task
[DATA] attacking ssh://192.168.1.101:22/
[22][ssh] host: 192.168.1.101 login: Admin password: P@ssword
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-14 21:01:43

[root@kali ~]#
```





As you can see, the logs were triggered from the Hydra attack.