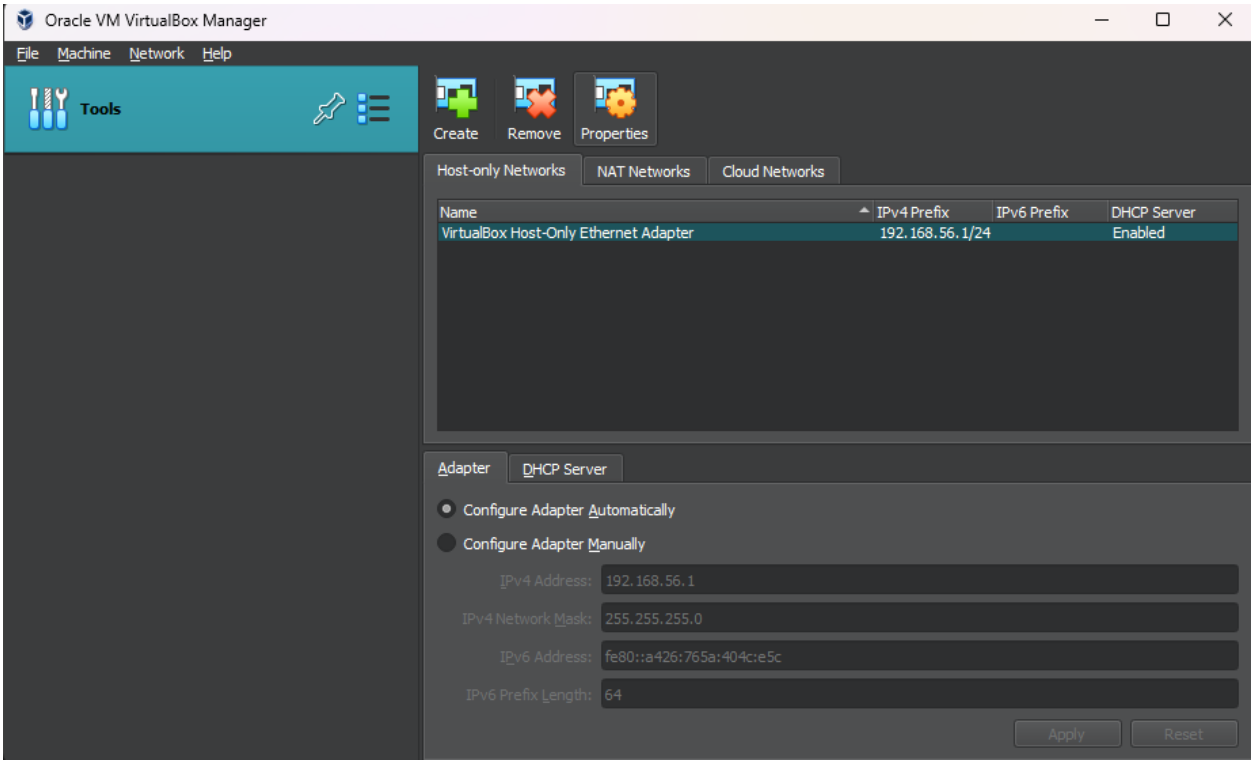
AI-Assisted Incident Triage in a Splunk SIEM Environment

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.

Installer | Pre-built VMs | ARM | Mobile | Cloud | Containers | Live | WSL

Kali Linux 2025.4 Changelog

x86_64 | Apple Silicon (ARM64)

Recommended

Installer

Complete offline installation with customization

4.4G | torrent | sum

Microsoft | Software Download | Windows | Windows Insider Preview | All Microsoft | Search | Drilon

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

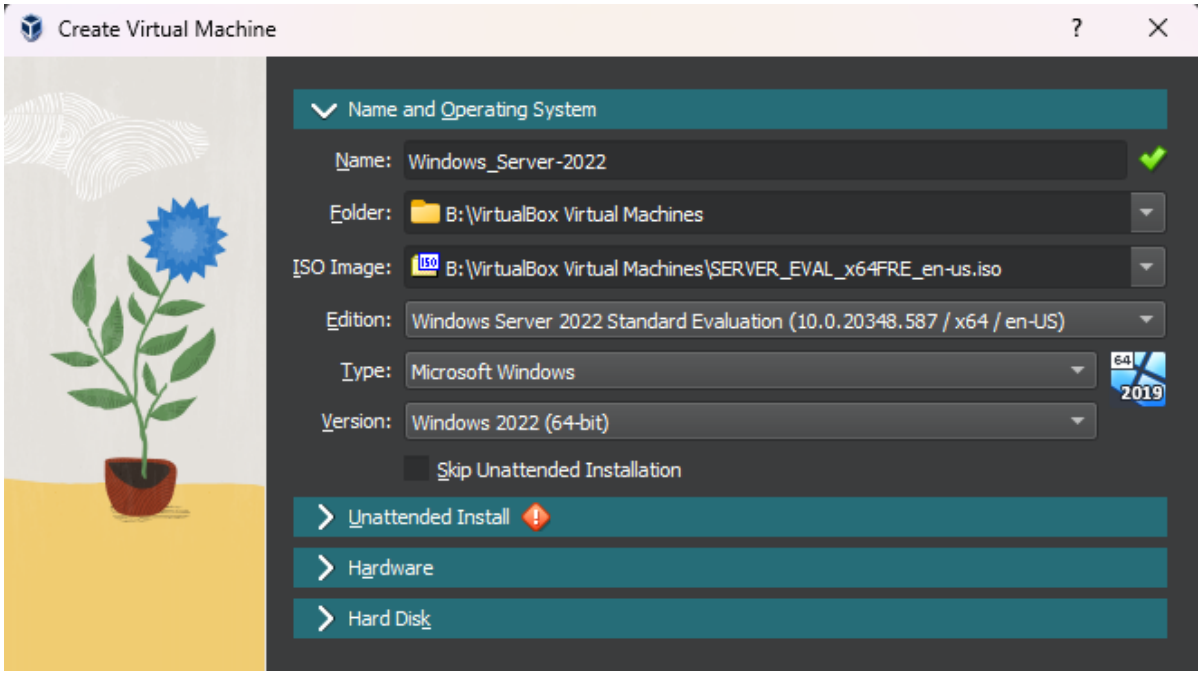
Microsoft | Evaluation Center | Windows | Windows Server | SQL Server | System Center | Microsoft Security | Additional products | All Microsoft

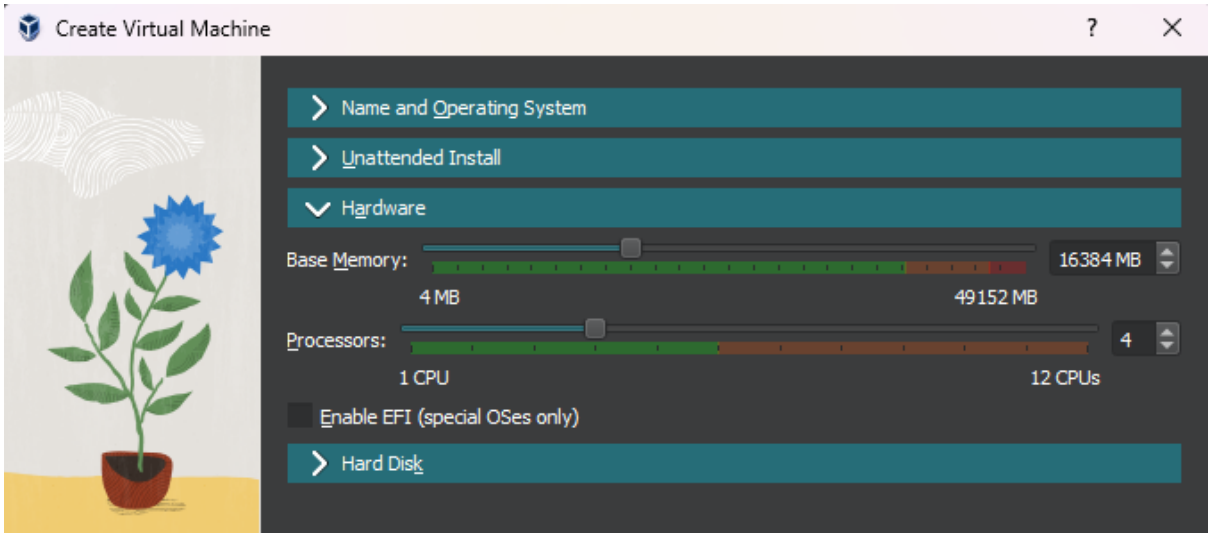
Please select your Windows Server 2022 download

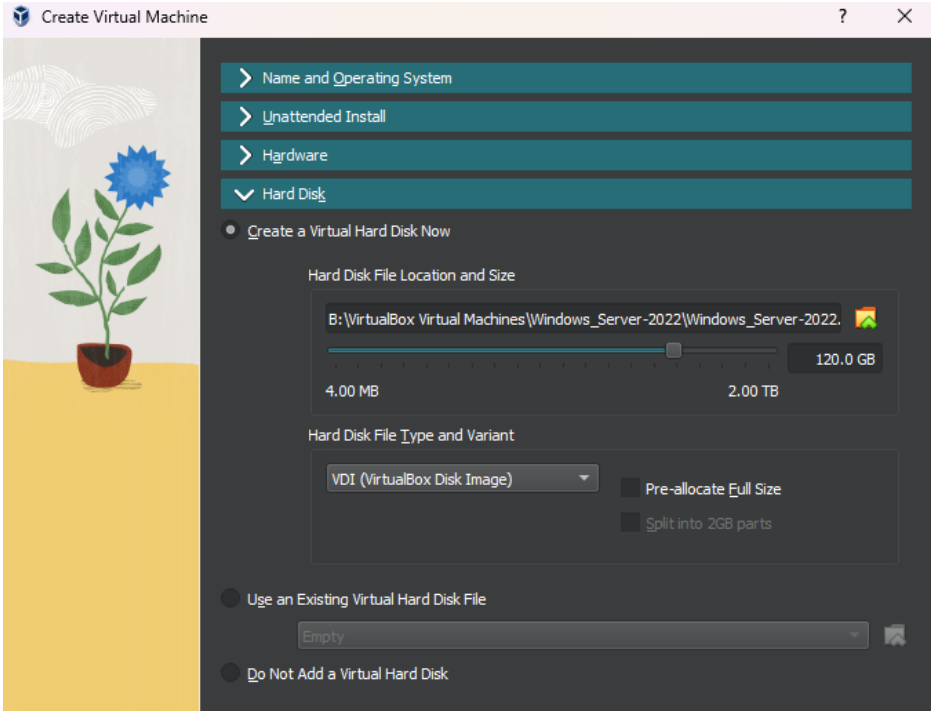
English (United States)	**ISO downloads** 64-bit edition >	**VHD download** 64-bit edition >	**Try on Azure** Learn more >	**Create a VM in Azure** Learn more >

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.

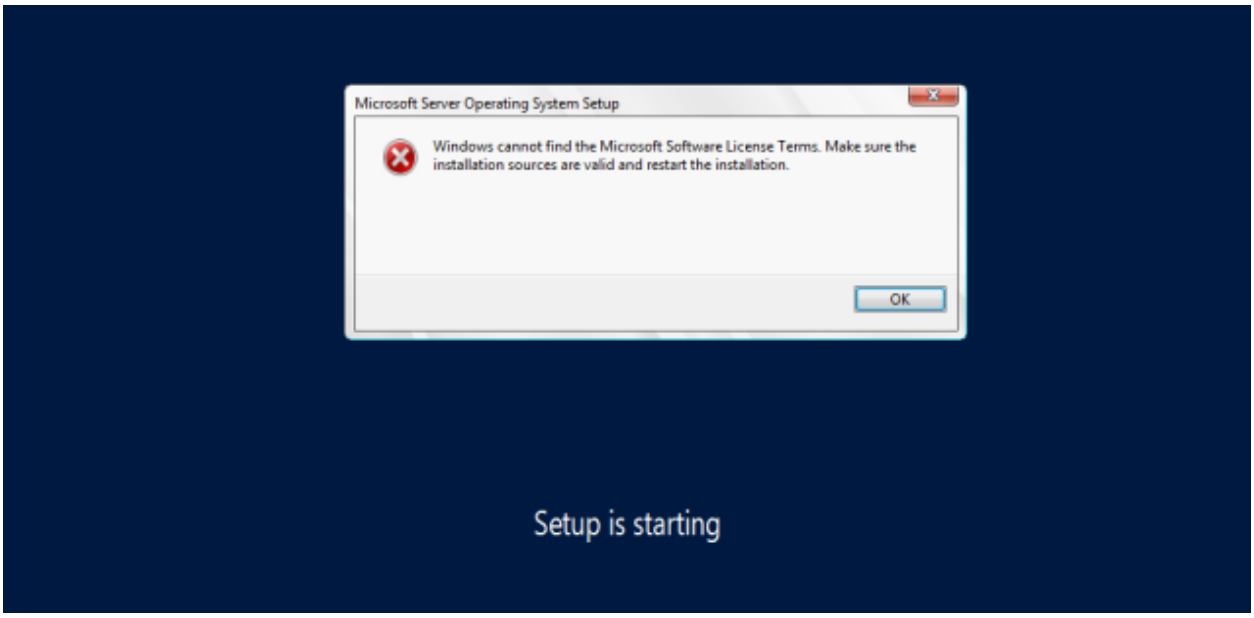
Creation of Windows Server VM



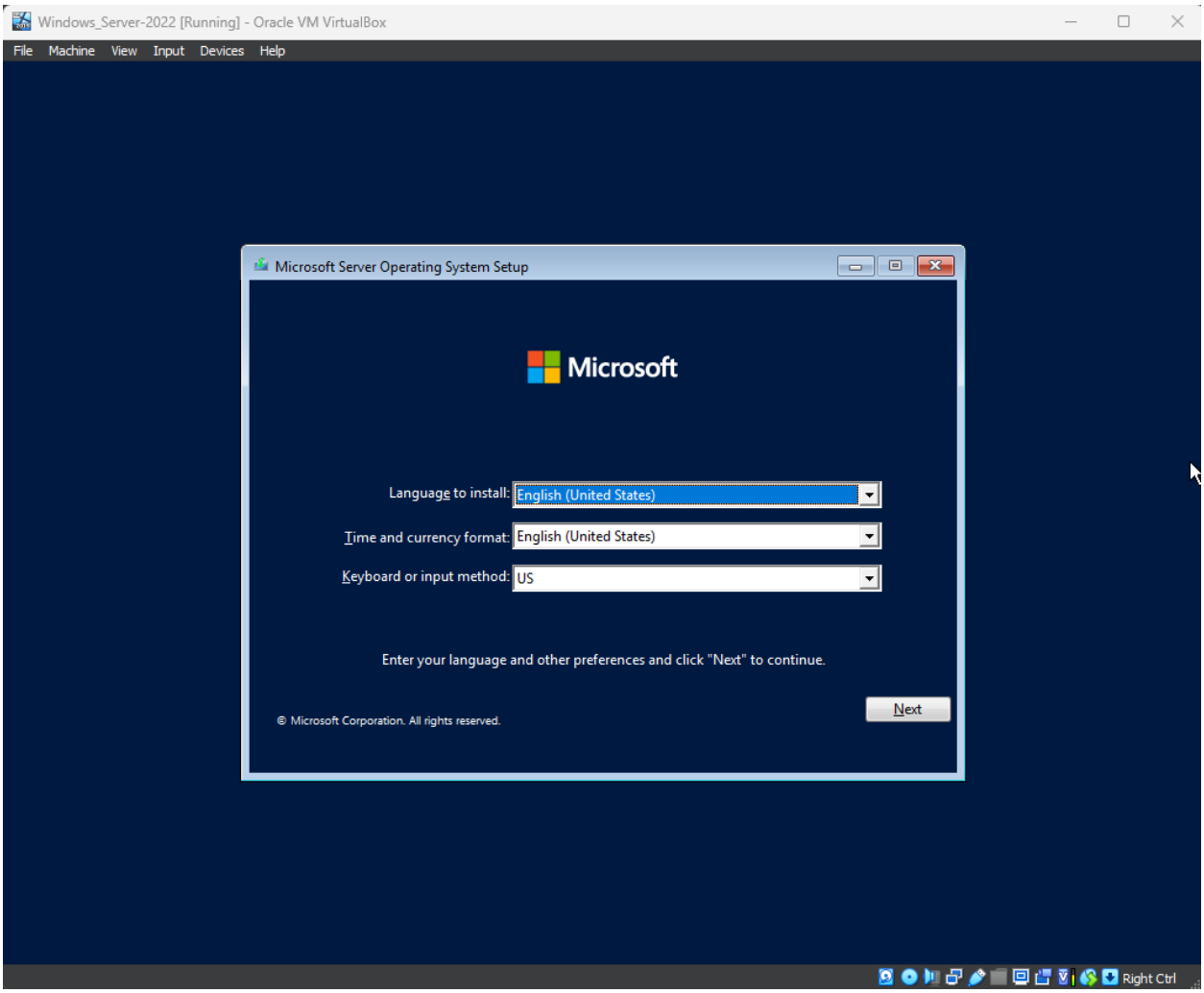




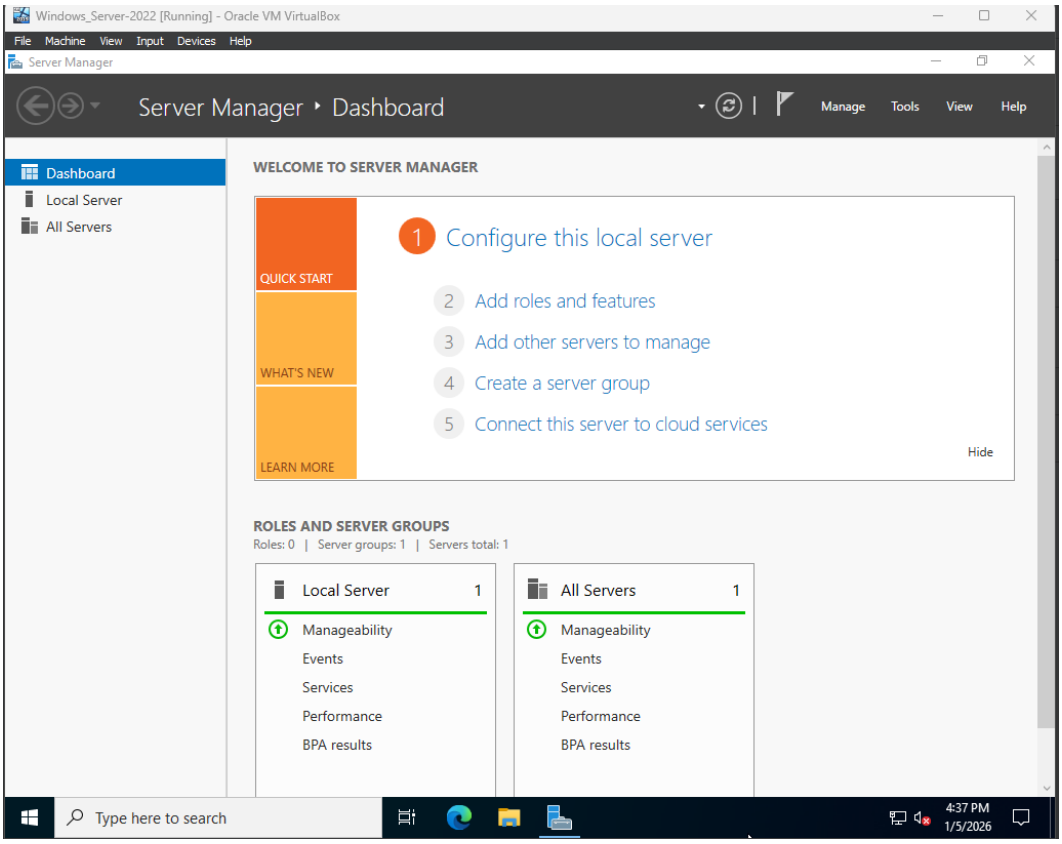
The first time I booted the server, I got this error:


Microsoft Server Operating System Setup
Windows cannot find the Microsoft Software License Terms. Make sure the installation sources are valid and restart the installation.
OK
Setup is starting

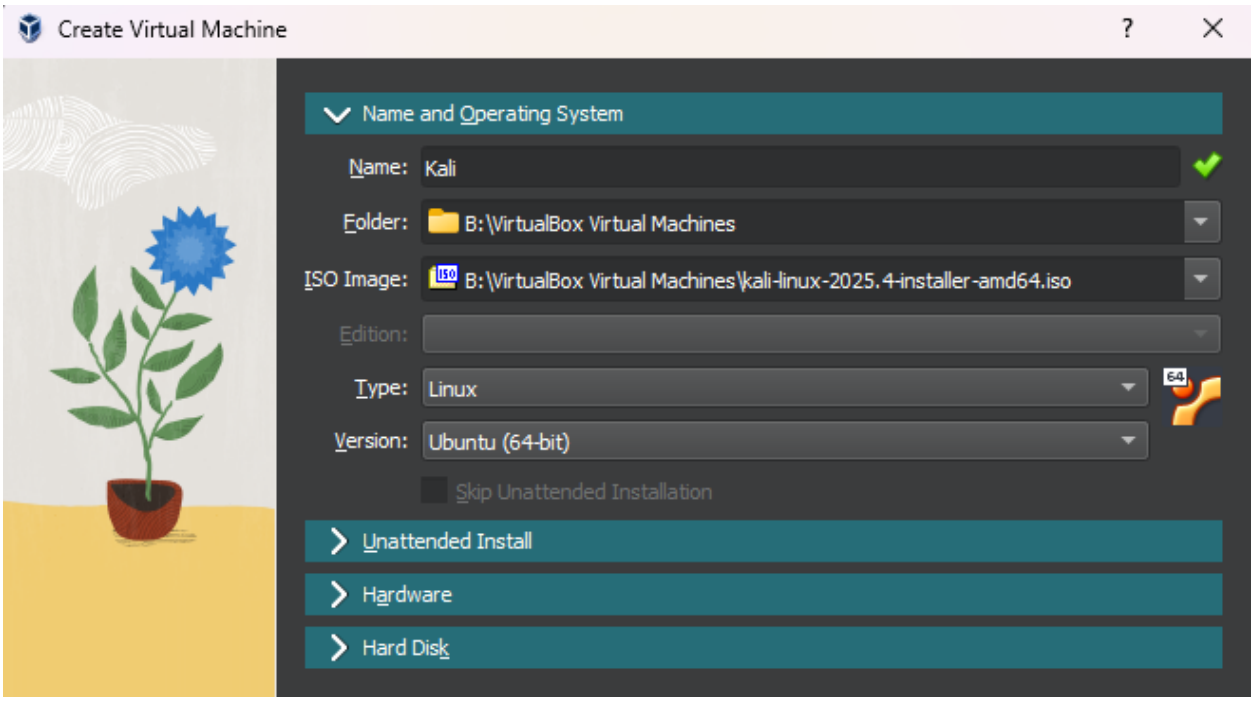
After some research, I enabled the “Skip Unattended Installation” and it booted just fine.

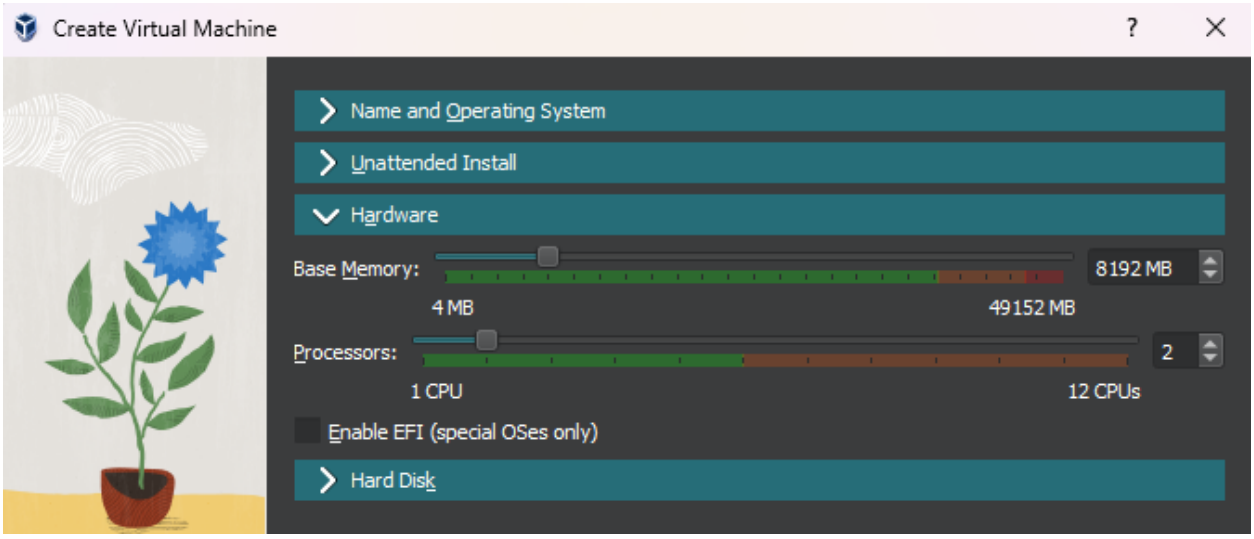


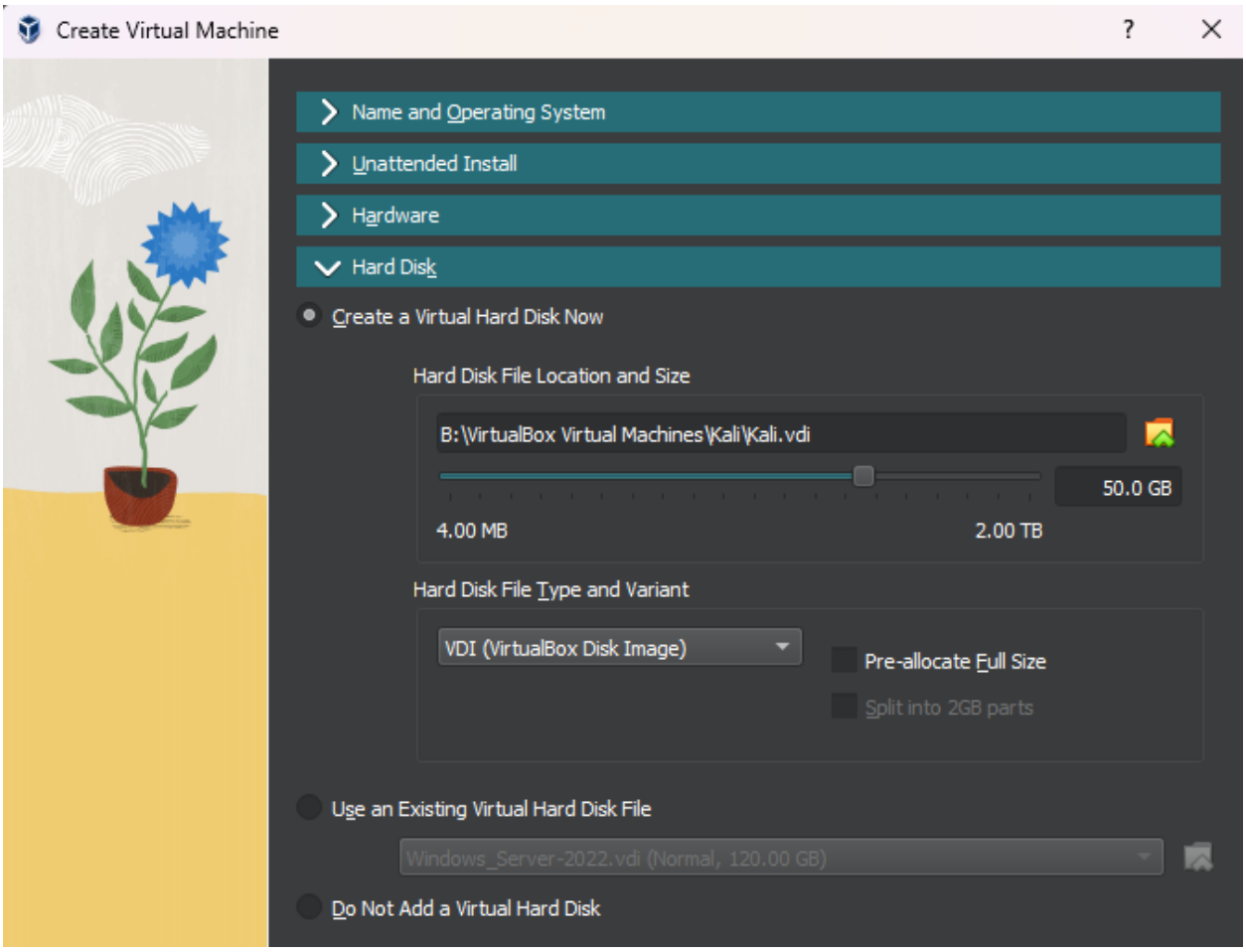
Finished installation of server:

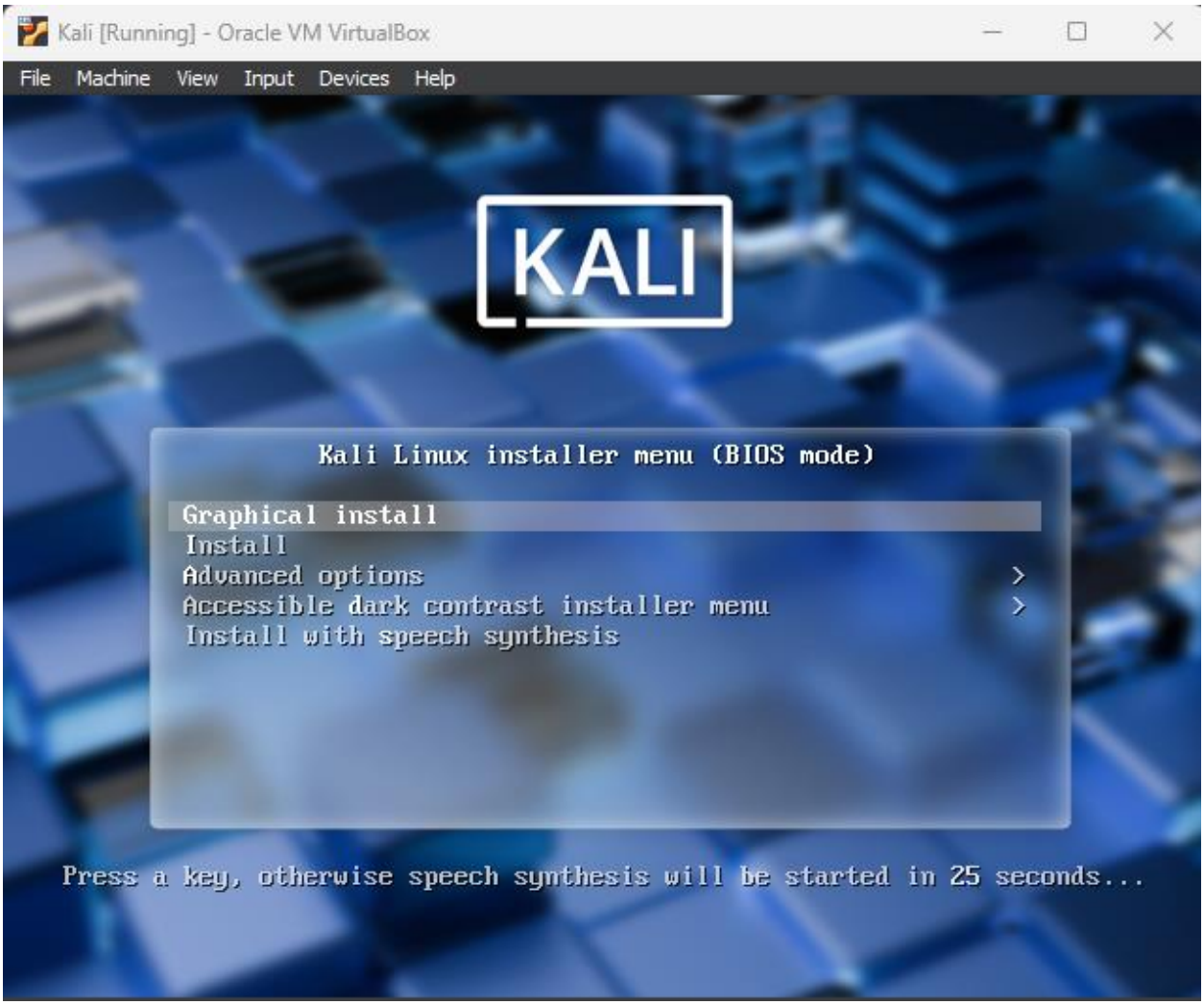


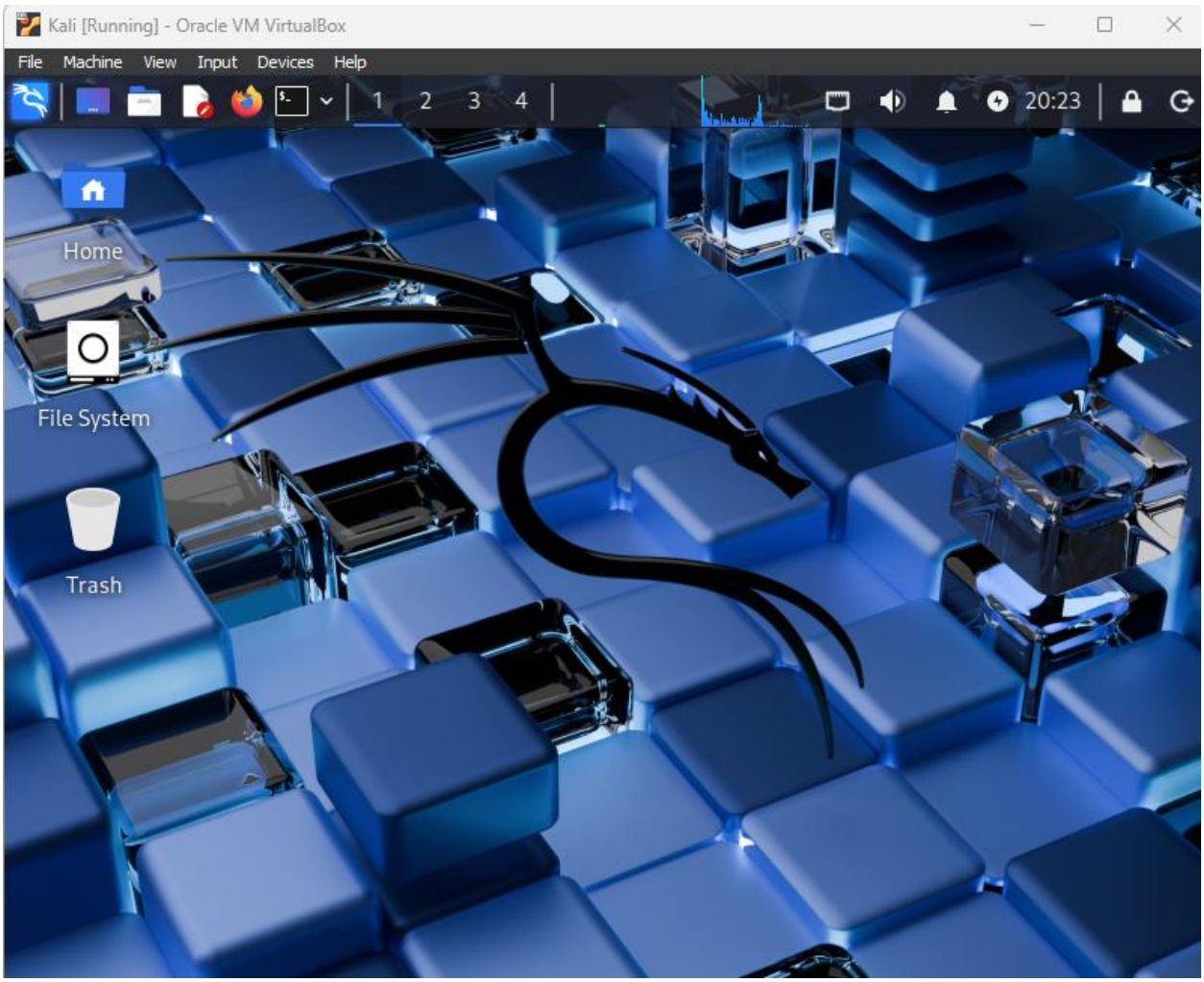
Creation of Kali Linux VM


Create Virtual Machine
Name and Operating System
Name: Kali
Folder: B:\VirtualBox Virtual Machines
ISO Image: B:\VirtualBox Virtual Machines\kali-linux-2025.4-installer-amd64.iso
Edition:
Type: Linux
Version: Ubuntu (64-bit)
Skip Unattended Installation
Unattended Install
Hardware
Hard Disk

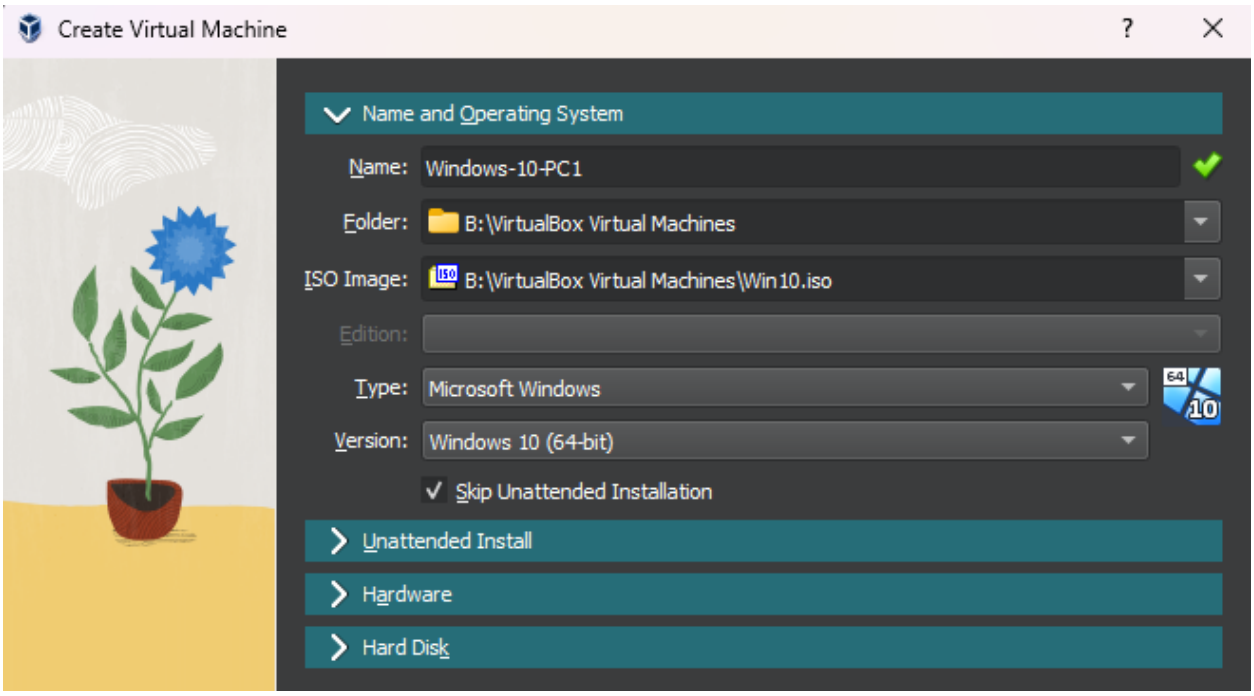

Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Base Memory: 8192 MB
4 MB
49152 MB
Processors: 2
1 CPU
12 CPUs
Enable EFI (special OSes only)
Hard Disk

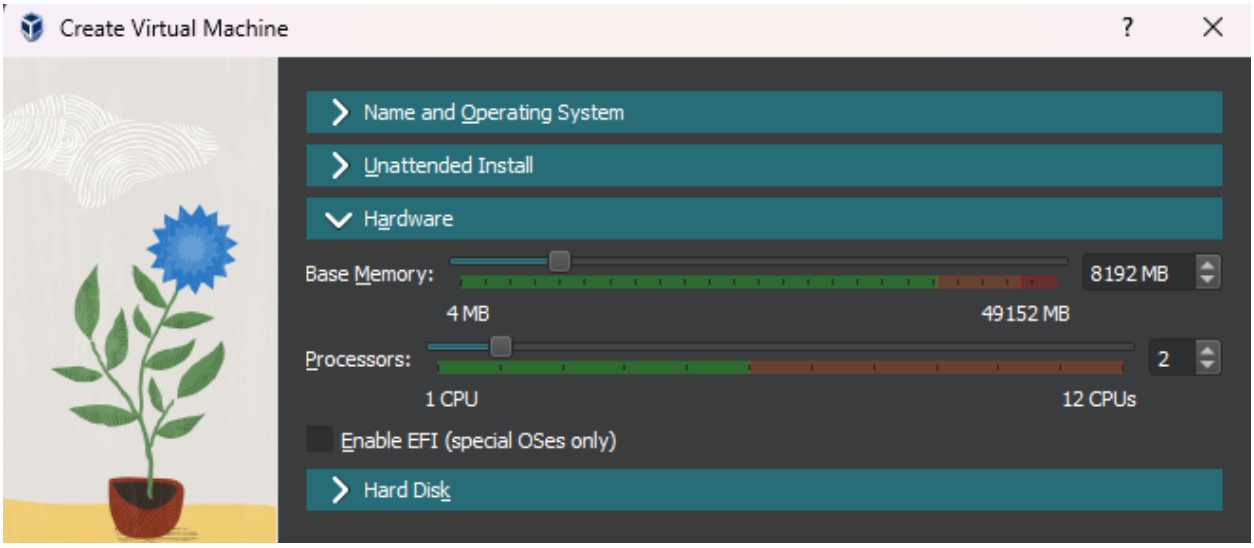

Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Hard Disk
Create a Virtual Hard Disk Now
Hard Disk File Location and Size
B:\VirtualBox Virtual Machines\Kali\Kali.vdi
50.0 GB
4.00 MB
2.00 TB
Hard Disk File Type and Variant
VDI (VirtualBox Disk Image)
Pre-allocate Full Size
Split into 2GB parts
Use an Existing Virtual Hard Disk File
Windows_Server-2022.vdi (Normal, 120.00 GB)
Do Not Add a Virtual Hard Disk

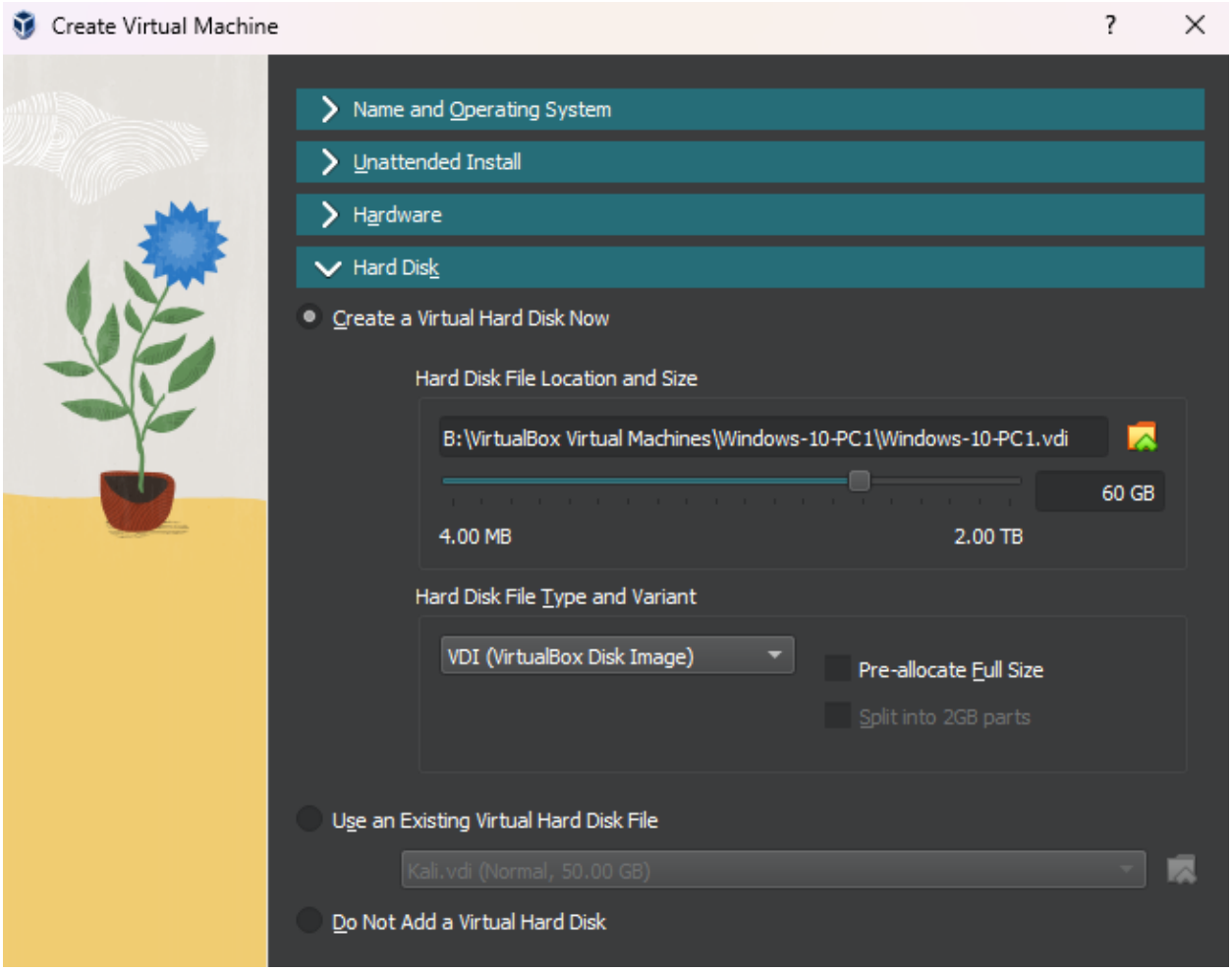

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Kali Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options
Accessible dark contrast installer menu
Install with speech synthesis
Press a key, otherwise speech synthesis will be started in 25 seconds...

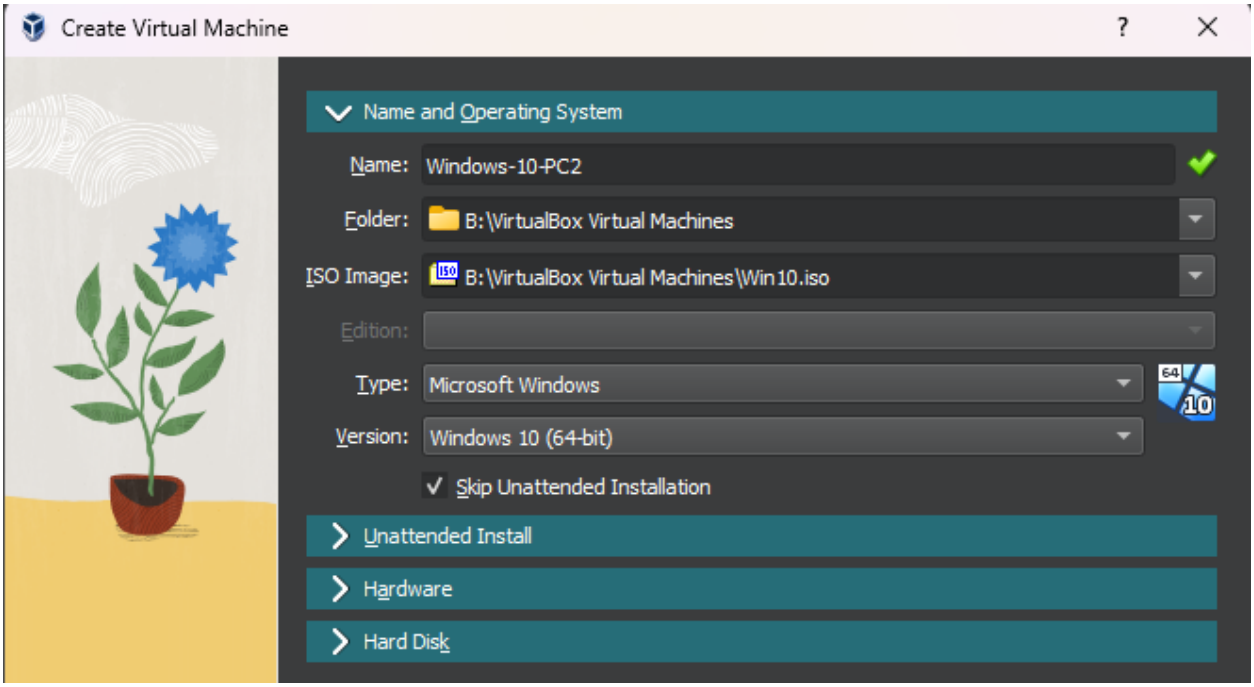


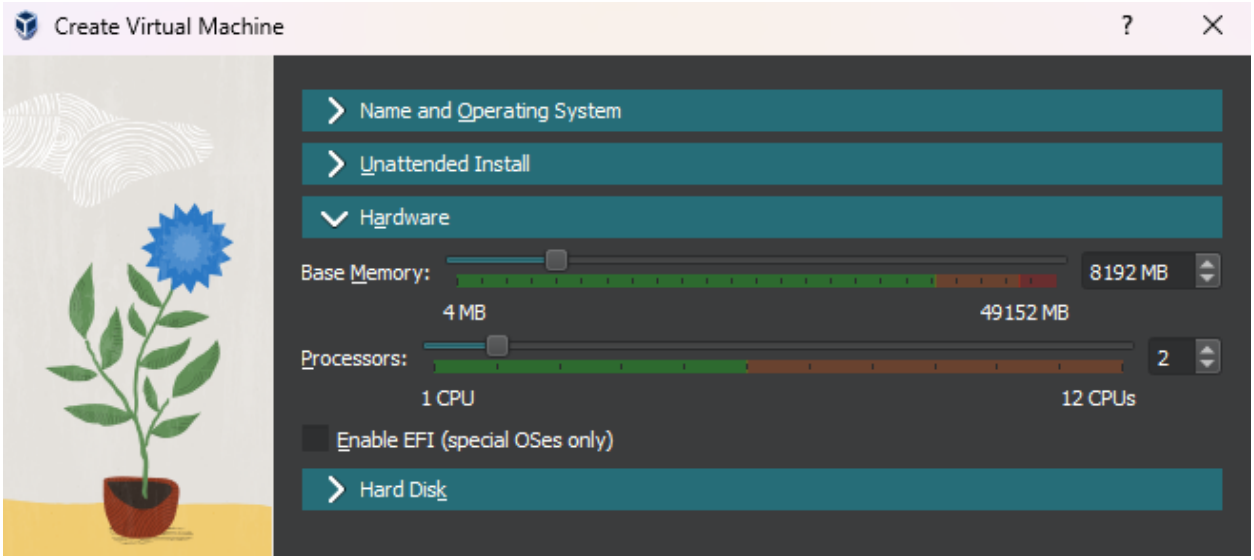
Creation of two Windows 10 Machines

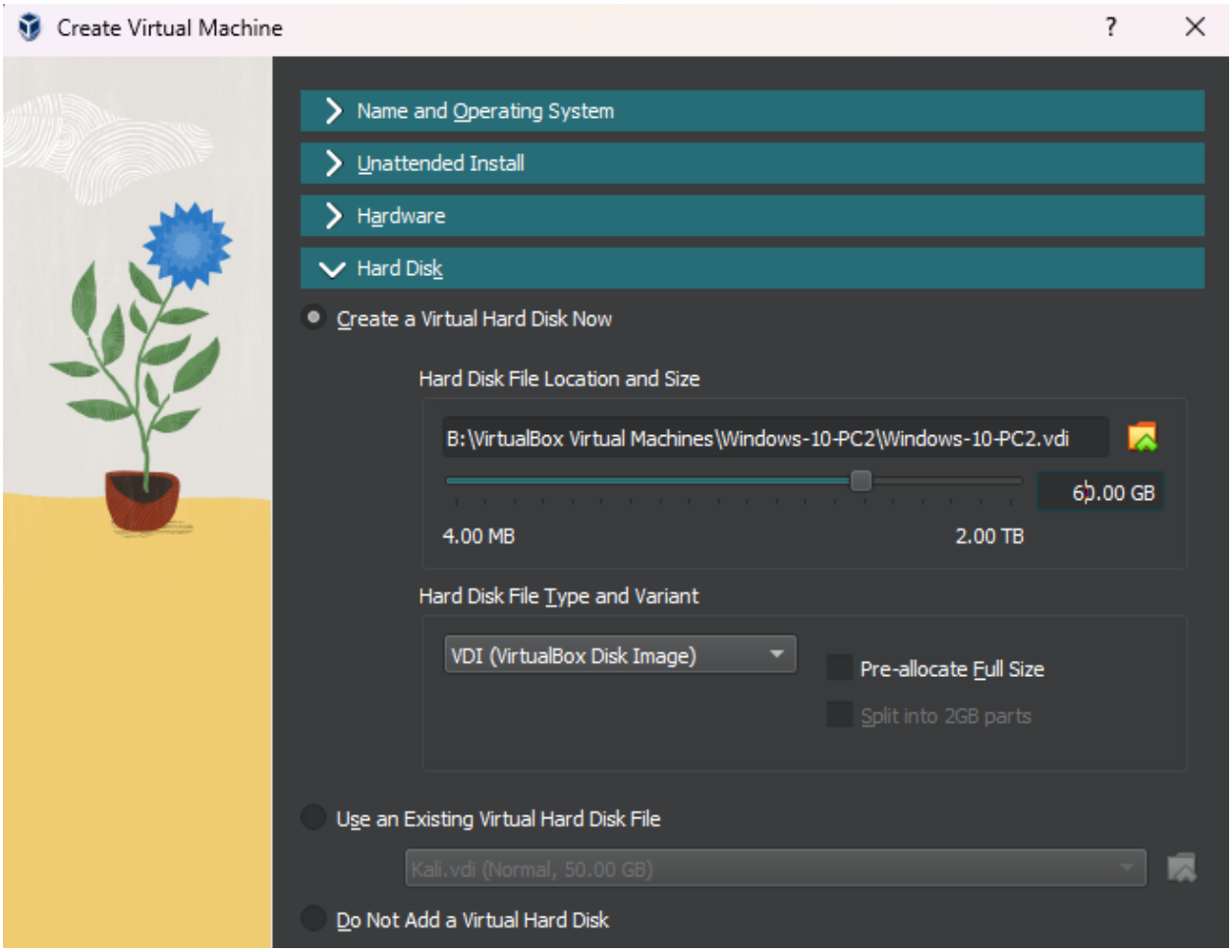

Create Virtual Machine
Name and Operating System
Name: Windows-10-PC1
Folder: B:\VirtualBox Virtual Machines
ISO Image: B:\VirtualBox Virtual Machines\Win10.iso
Edition:
Type: Microsoft Windows
Version: Windows 10 (64-bit)
Skip Unattended Installation
Unattended Install
Hardware
Hard Disk


Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Base Memory:
8192 MB
4 MB
49152 MB
Processors:
2
1 CPU
12 CPUs
Enable EFI (special OSes only)
Hard Disk

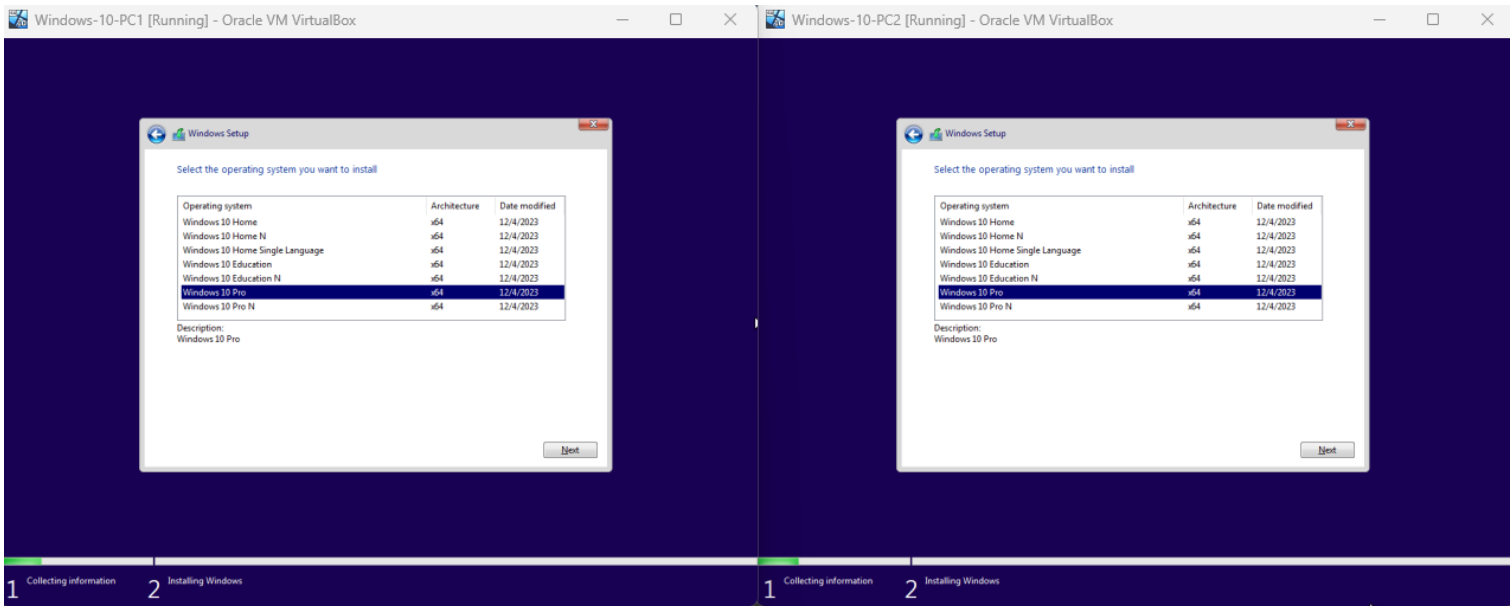

Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Hard Disk
Create a Virtual Hard Disk Now
Hard Disk File Location and Size
B:\VirtualBox Virtual Machines\Windows-10-PC1\Windows-10-PC1.vdi
60 GB
4.00 MB
2.00 TB
Hard Disk File Type and Variant
VDI (VirtualBox Disk Image)
Pre-allocate Full Size
Split into 2GB parts
Use an Existing Virtual Hard Disk File
Kali.vdi (Normal, 50.00 GB)
Do Not Add a Virtual Hard Disk


Create Virtual Machine
Name and Operating System
Name: Windows-10-PC2
Folder: B:\VirtualBox Virtual Machines
ISO Image: B:\VirtualBox Virtual Machines\Win10.iso
Edition:
Type: Microsoft Windows
Version: Windows 10 (64-bit)
Skip Unattended Installation
Unattended Install
Hardware
Hard Disk

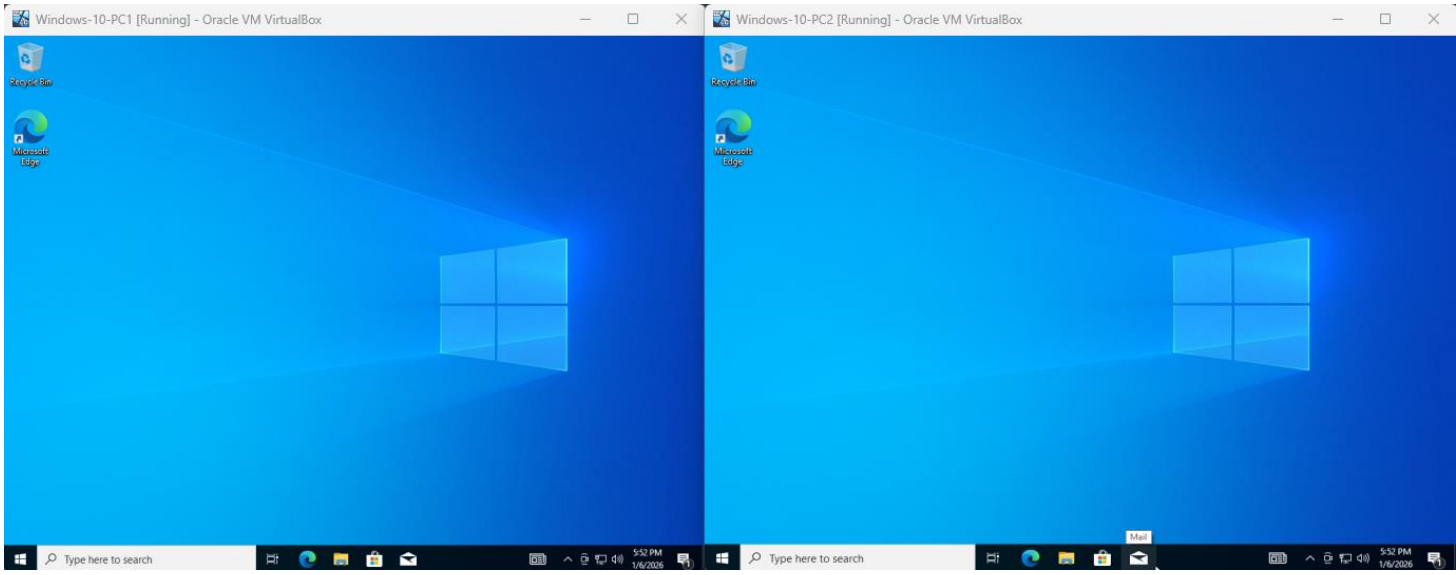




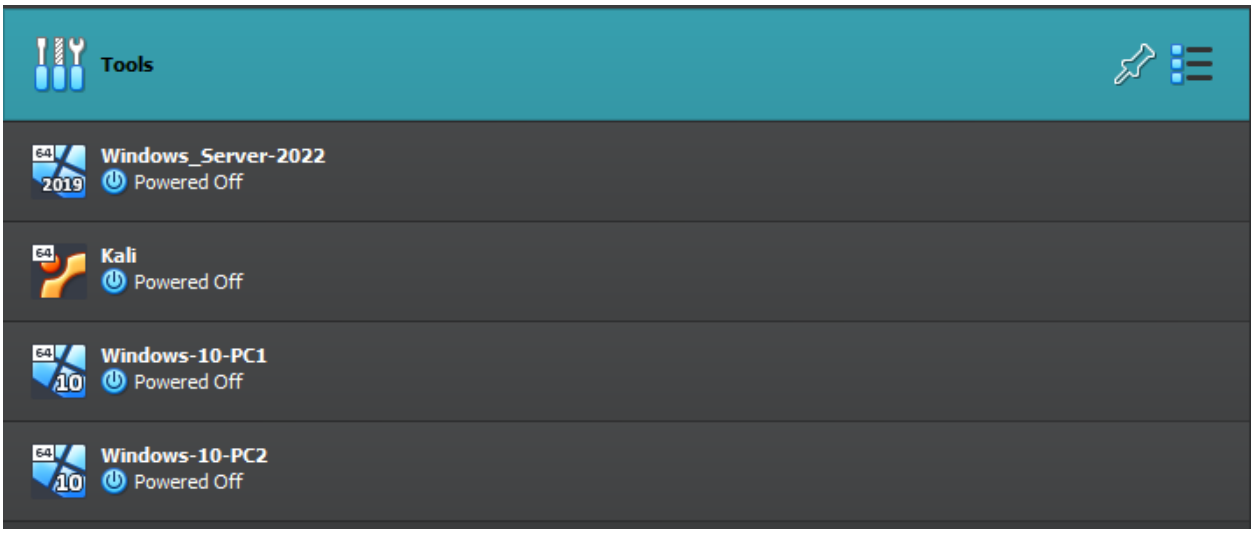
Both Windows 10 PCs successfully booted and are installing Windows 10 Pro Edition.



Both Windows 10 PCs are successfully running.



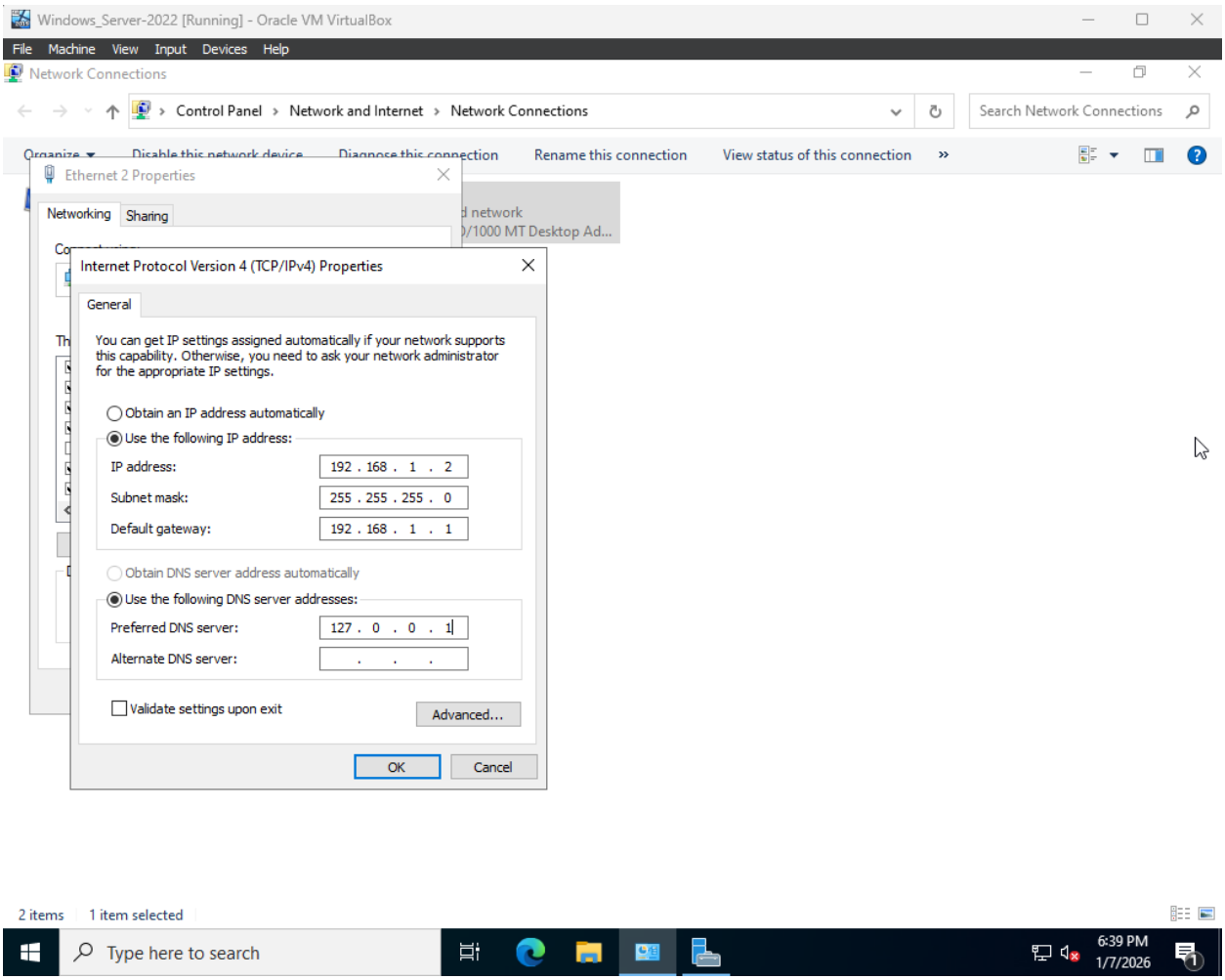
All VMs Have Been Created



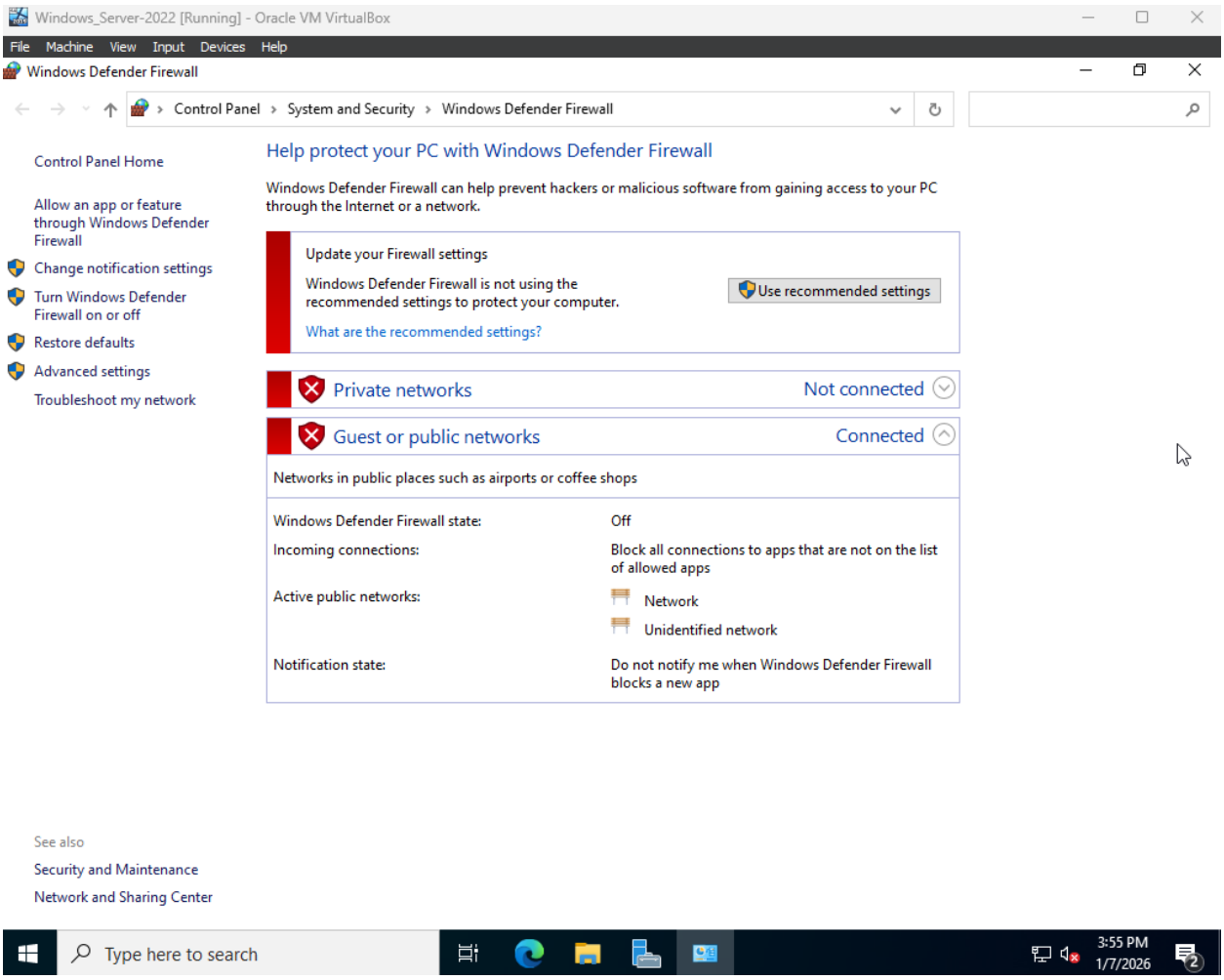
Active Directory Domain Services Promotion

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.

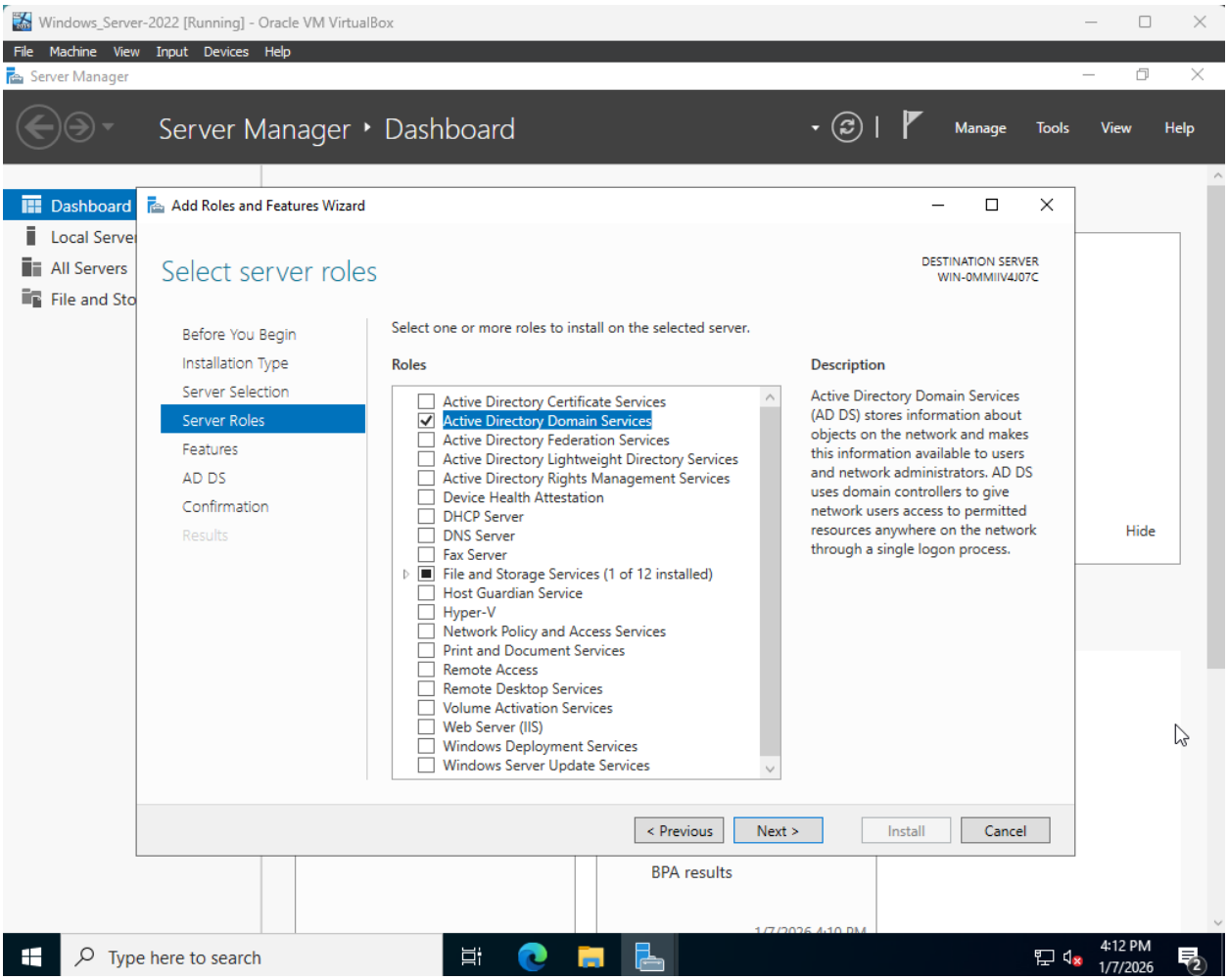
Statically assign the IP address and set the DNS IP to point at itself.



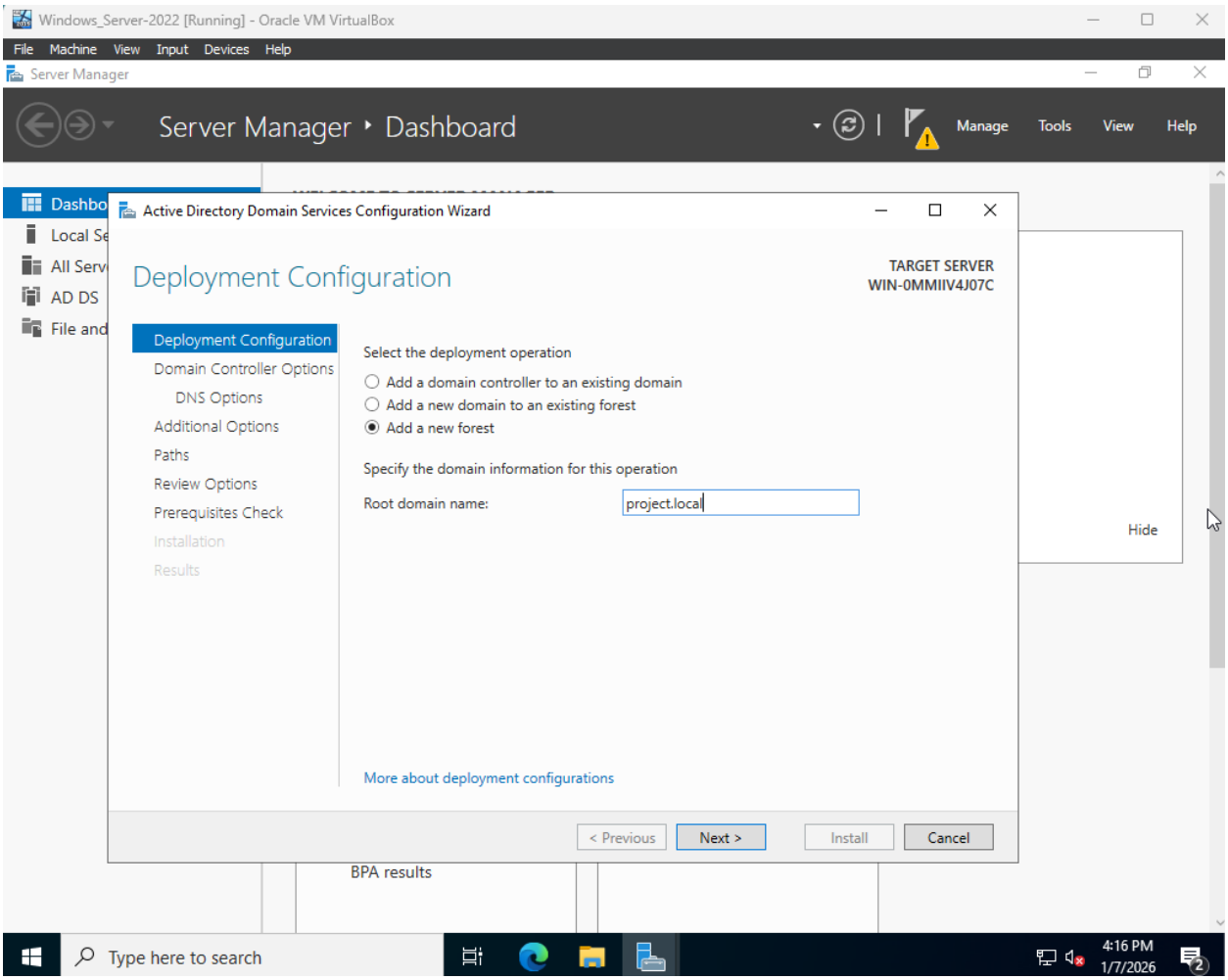
Disable Windows Defender Firewall to allow ICMP requests and to leave the system intentionally vulnerable.



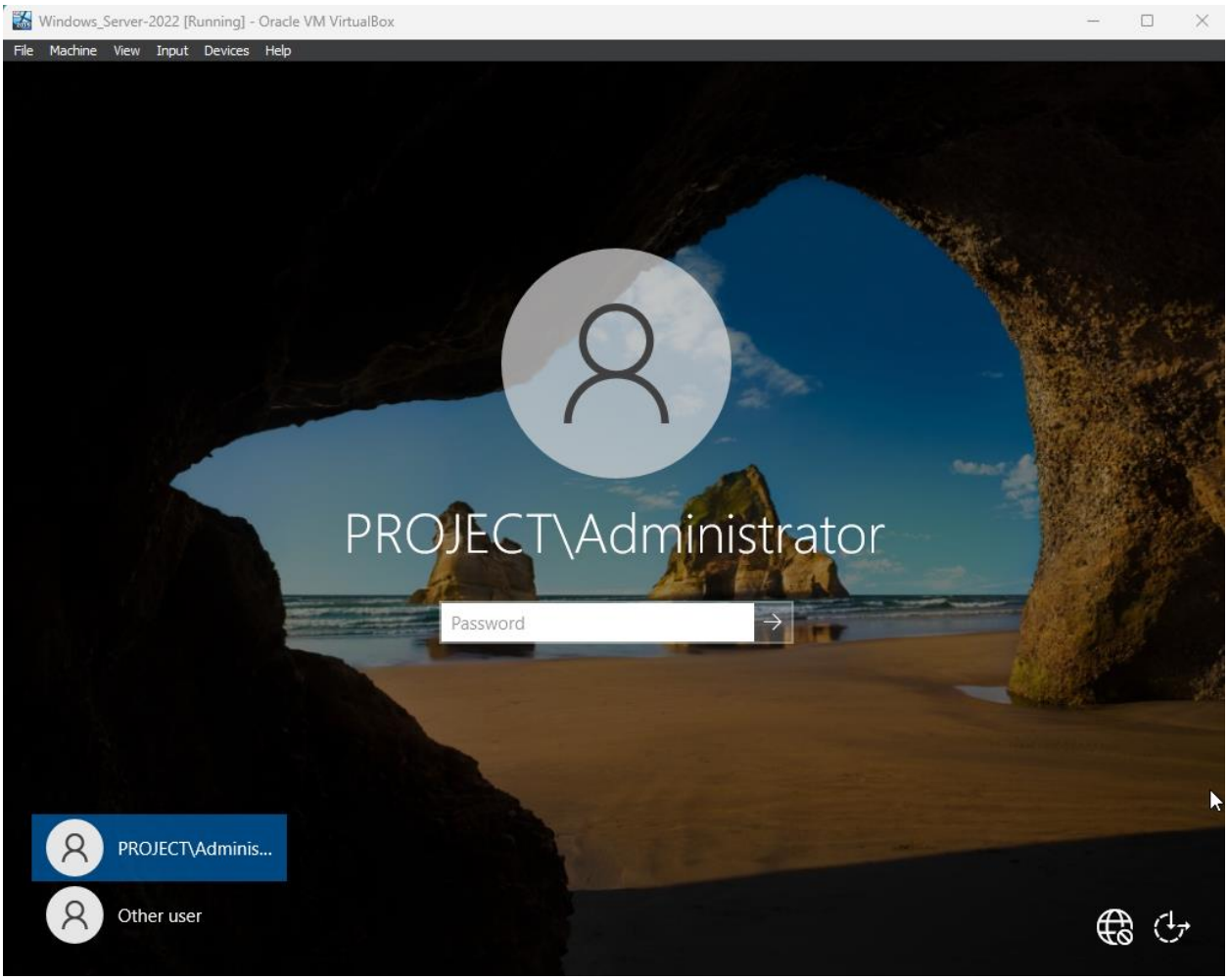
Installing the AD DS service to promote the server to a domain controller.



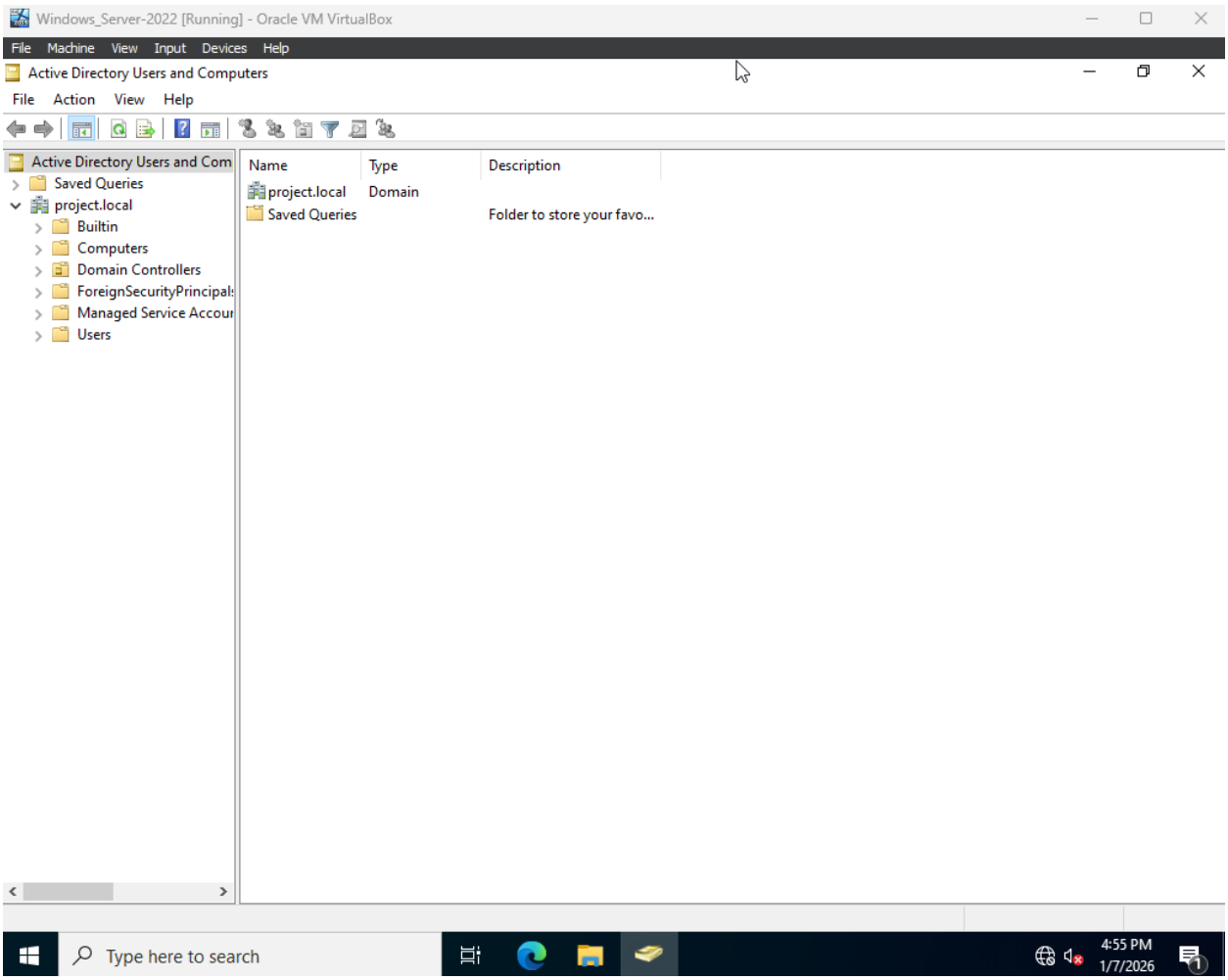
In the process of promoting the server to DC.



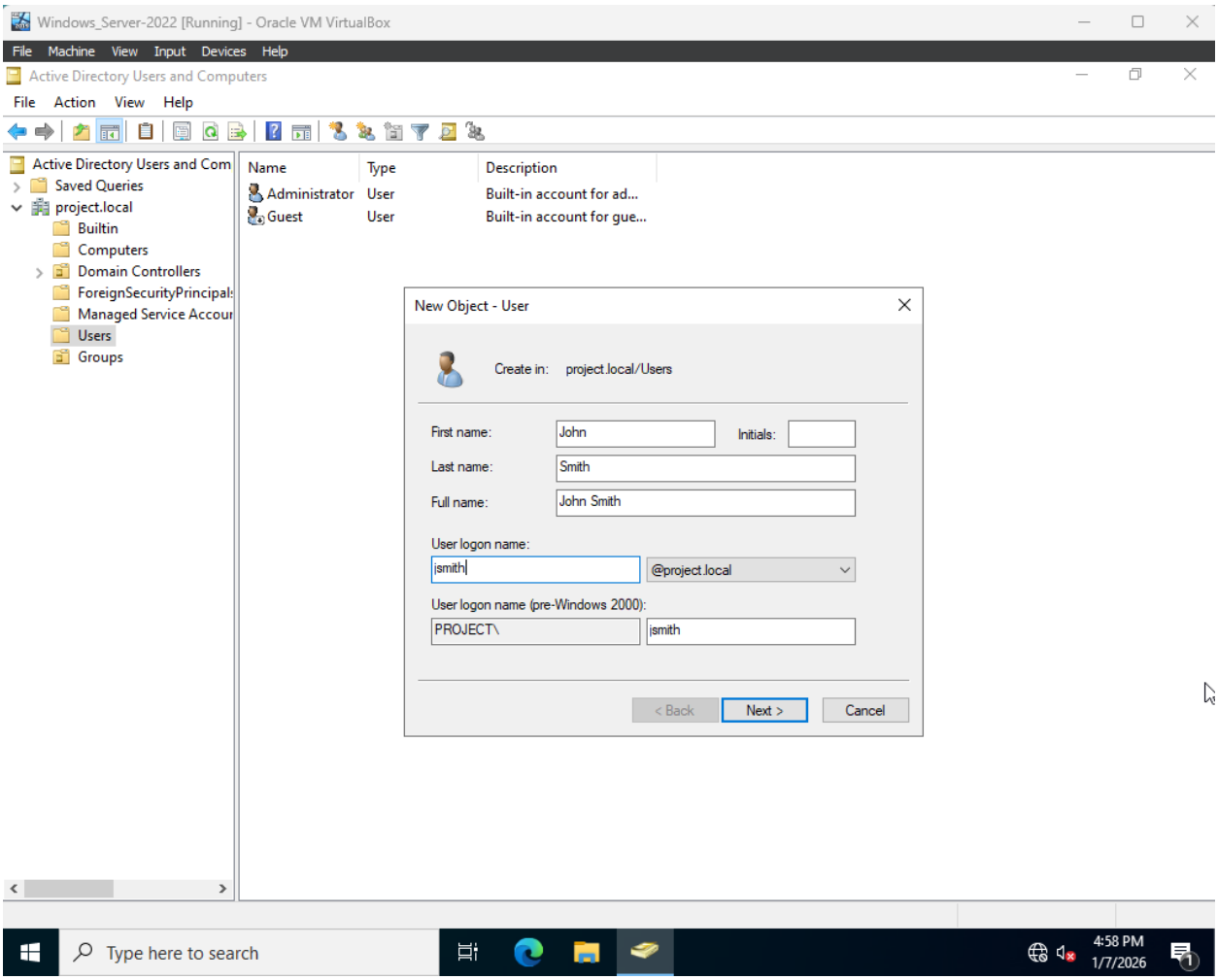
After the automatic reboot that followed the installation, you can see the server is now a domain controller.

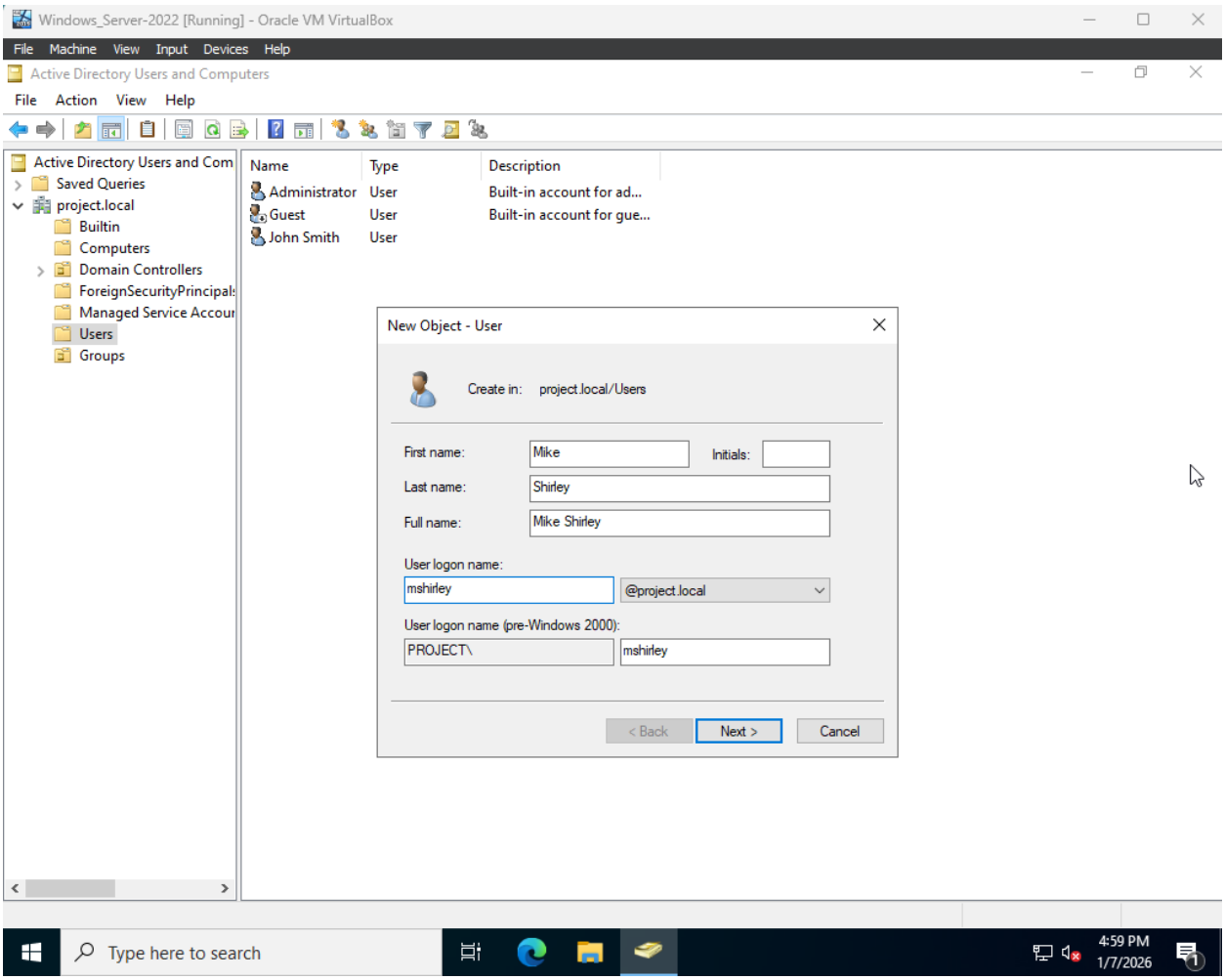


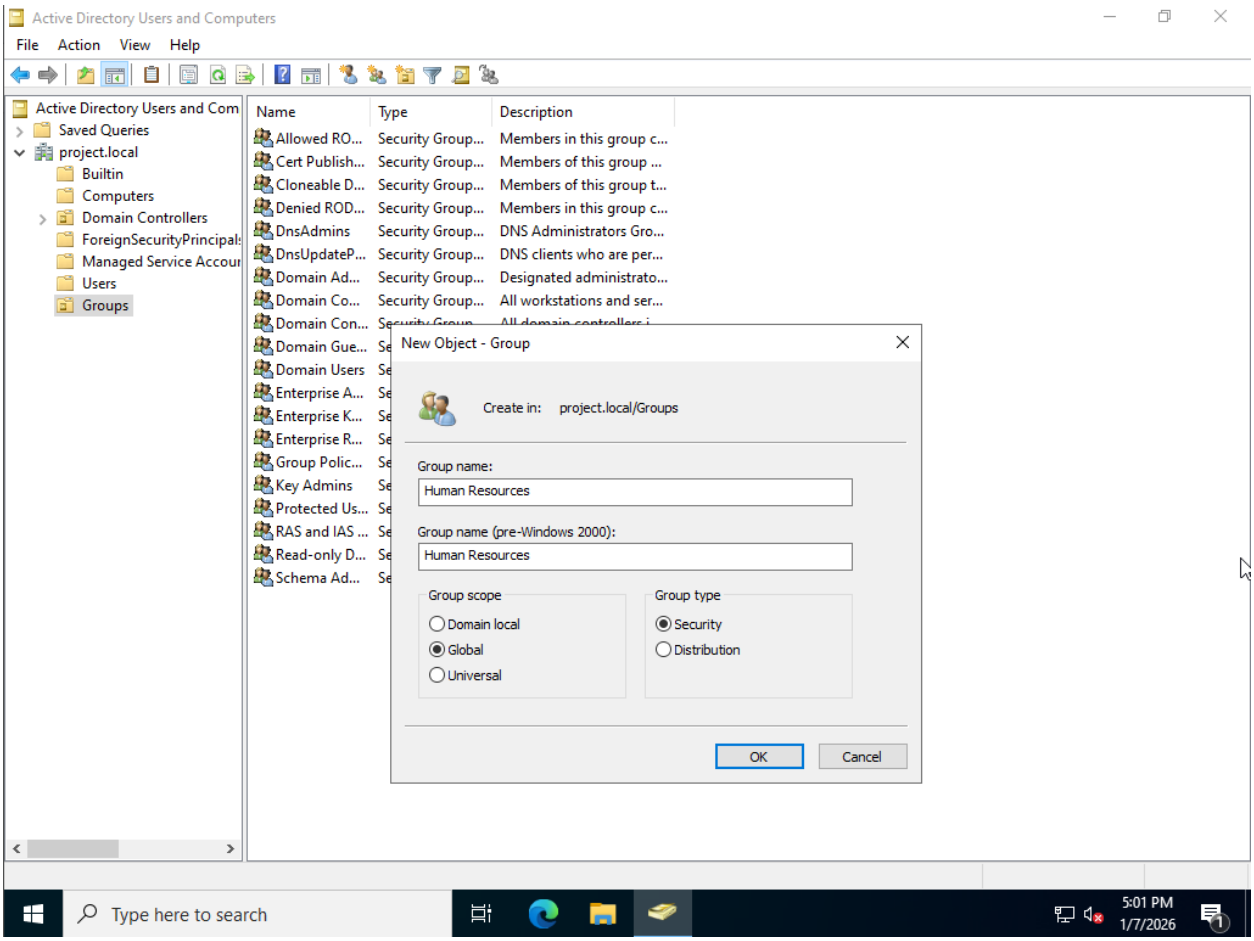
In the Active Directory application.

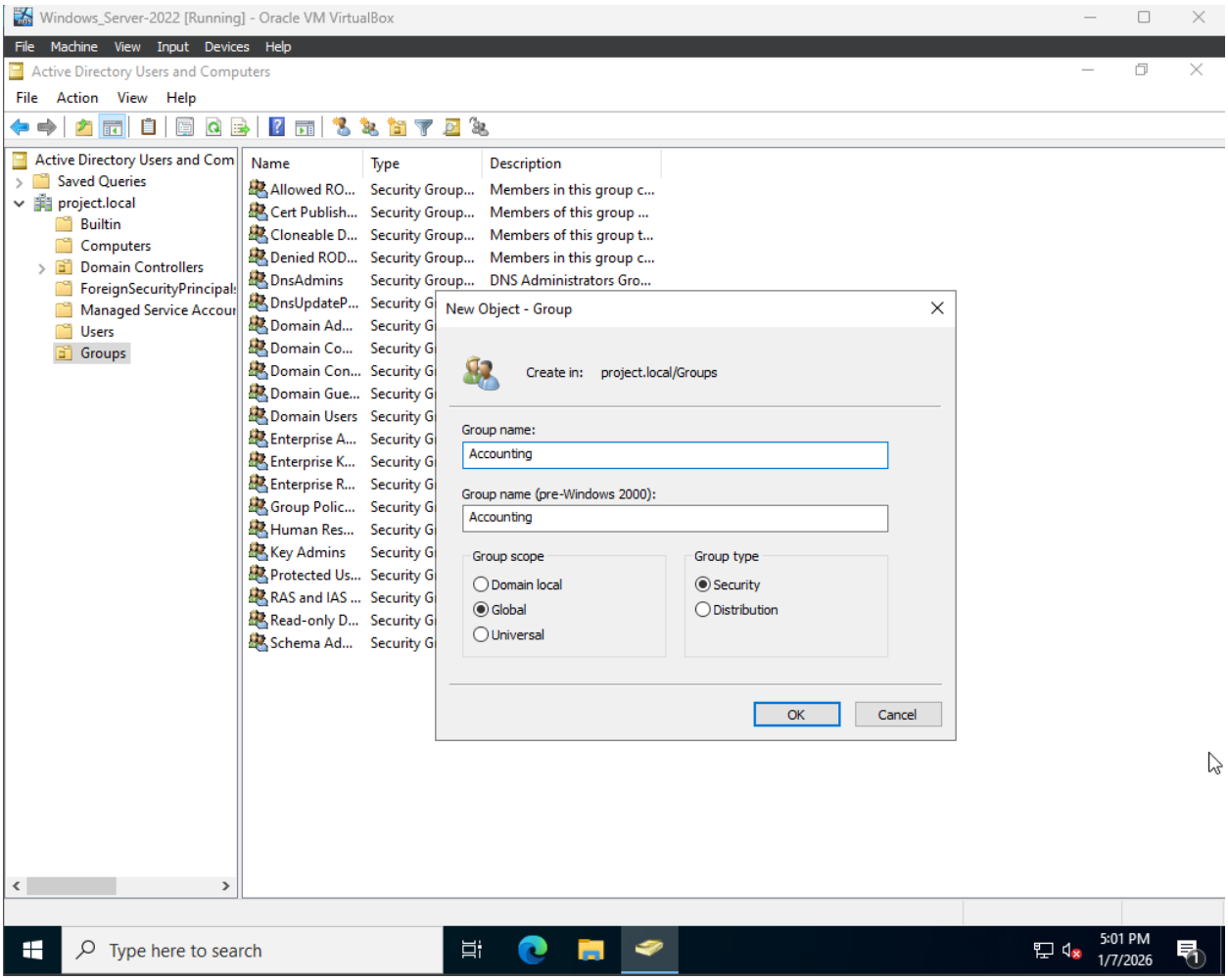


Creating two domain users and two groups for realism purposes.


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
ForeignSecurityPrincipals
Managed Service Accour
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:
jsmith
@project.local
User logon name (pre-Windows 2000):
PROJECT\
jsmith
< 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 Accour
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


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 Accour
Users
Groups
Name Type Description
Allowed RO... Security Group... Members in this group c...
Cert Publish... Security Group... Members of this group ...
Cloneable D... Security Group... Members of this group t...
Denied ROD... Security Group... Members in this group c...
DnsAdmins Security Group... DNS Administrators Gro...
DnsUpdateP... Security Group... DNS clients who are per...
Domain Ad... Security Group... Designated administrato...
Domain Co... Security Group... All workstations and ser...
Domain Con...
Domain Gue...
Domain Users
Enterprise A...
Enterprise K...
Enterprise R...
Group Polic...
Key Admins
Protected Us...
RAS and IAS ...
Read-only D...
Schema Ad...
New Object - Group
Create in: project.local/Groups
Group name:
Human Resources
Group name (pre-Windows 2000):
Human Resources
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
OK
Cancel
Type here to search
5:01 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 10 virtual machines to provide consistent network communication. Assigning fixed addresses makes it easier to reference systems, configure Splunk forwarders, and reproduce security scenarios without

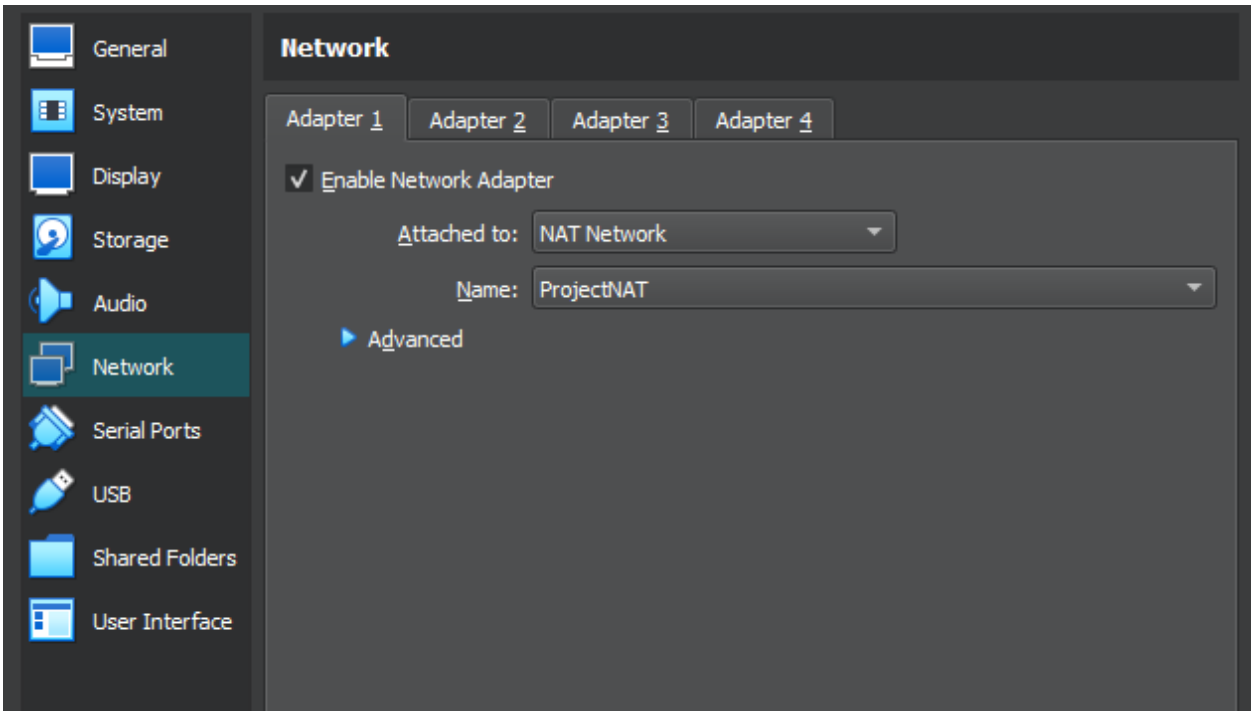
relying on changing DHCP leases. This also allows alerts and logs in Splunk to clearly map to specific hosts throughout the project.

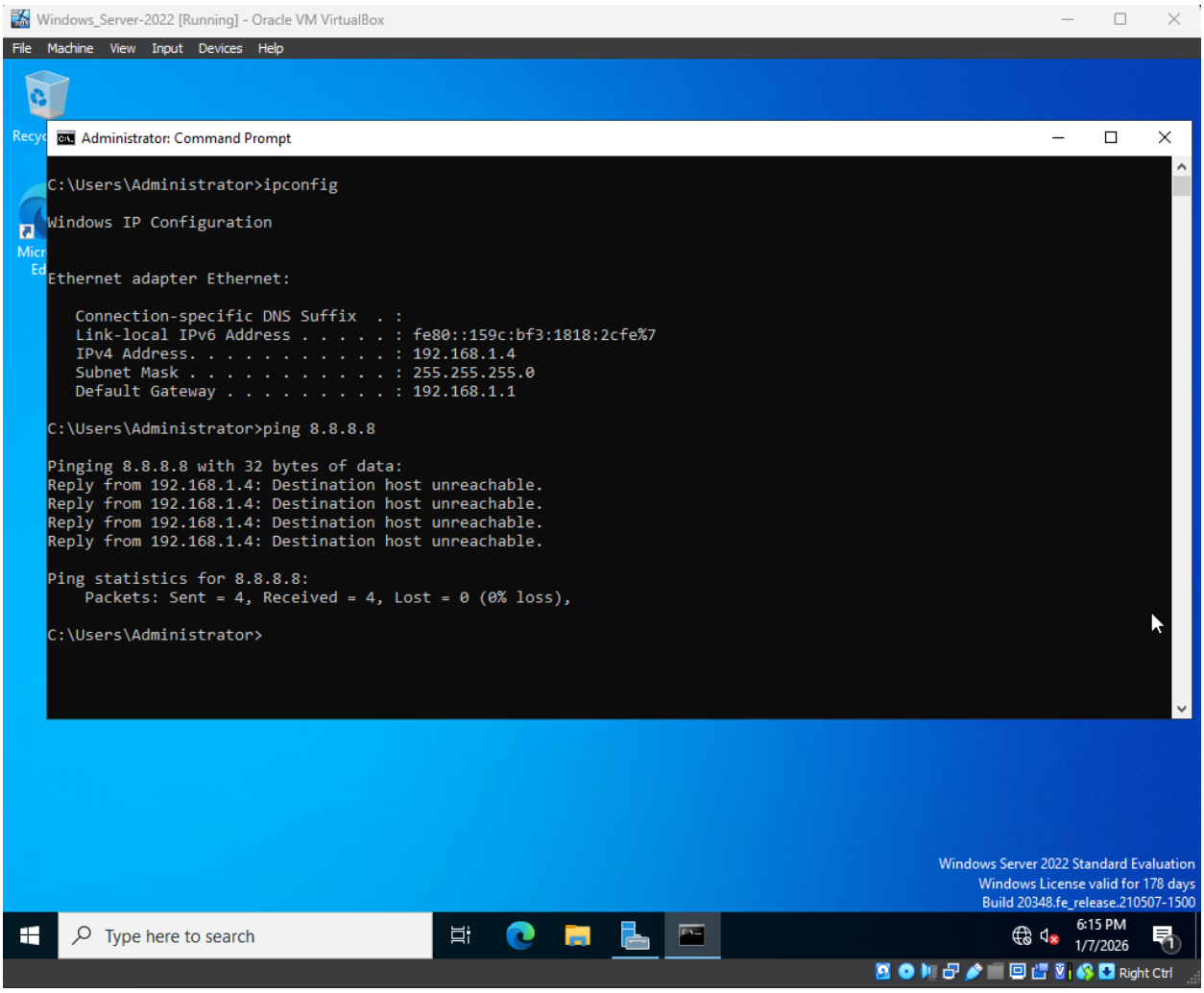
The Windows Server 2022 virtual machine will be promoted to a Domain Controller using Active Directory Domain Services. This creates a realistic enterprise environment where authentication, group membership, and administrative actions occur within a Windows domain. Operating the endpoints as domain-joined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

For the Windows 10 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.

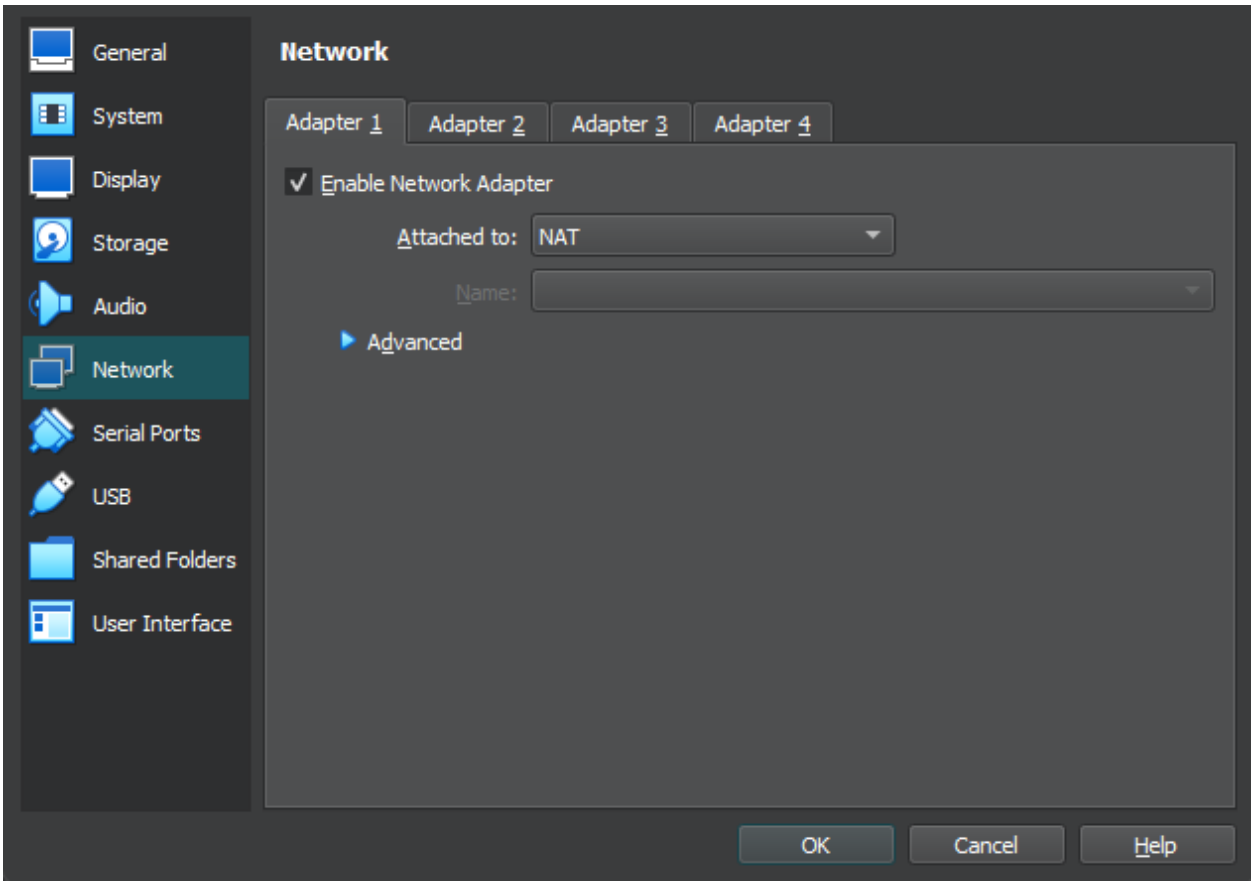
Create One Shared NAT Network

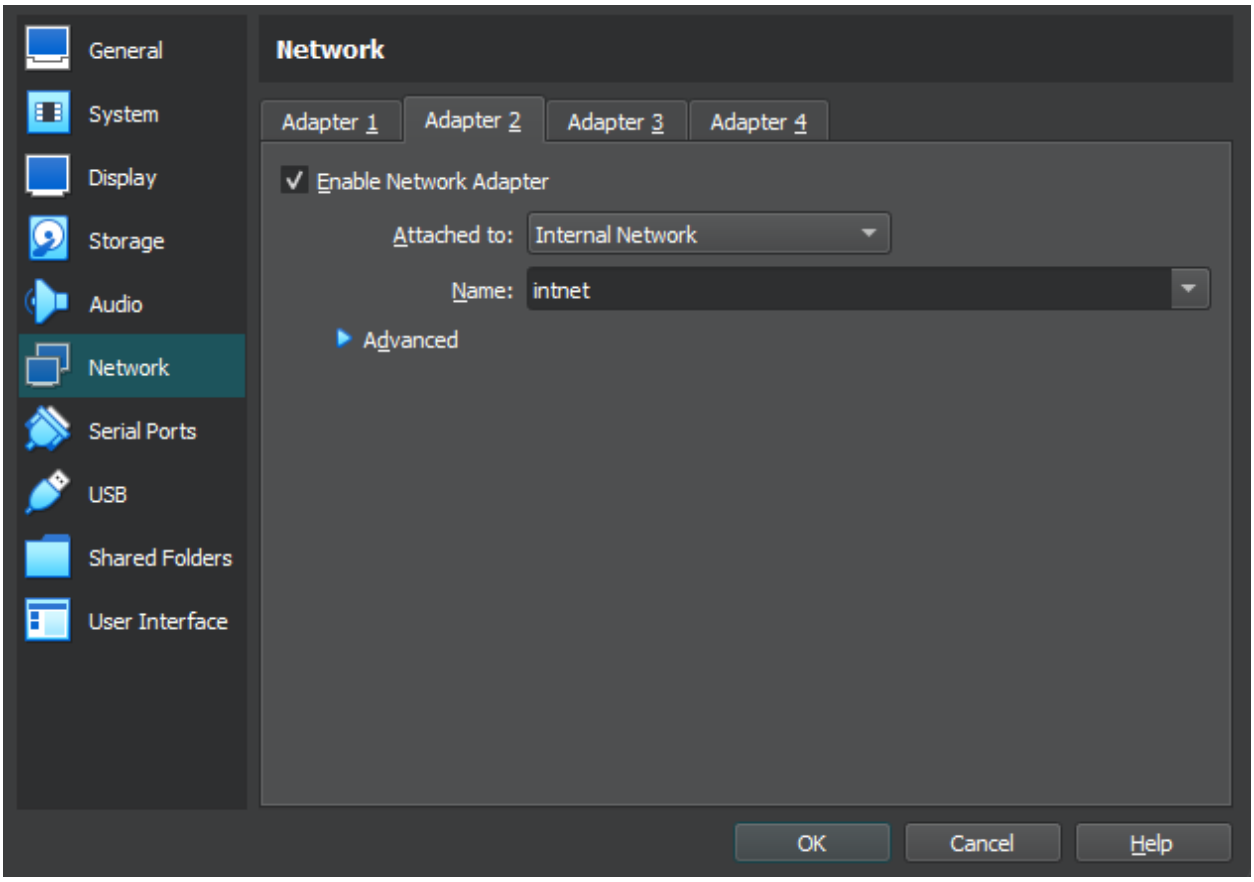
Now that the NAT network has been created, it will need to be added to each VMs network adapter in the settings while all of them are powered off.


General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
NAT Network
Name:
ProjectNAT
Advanced



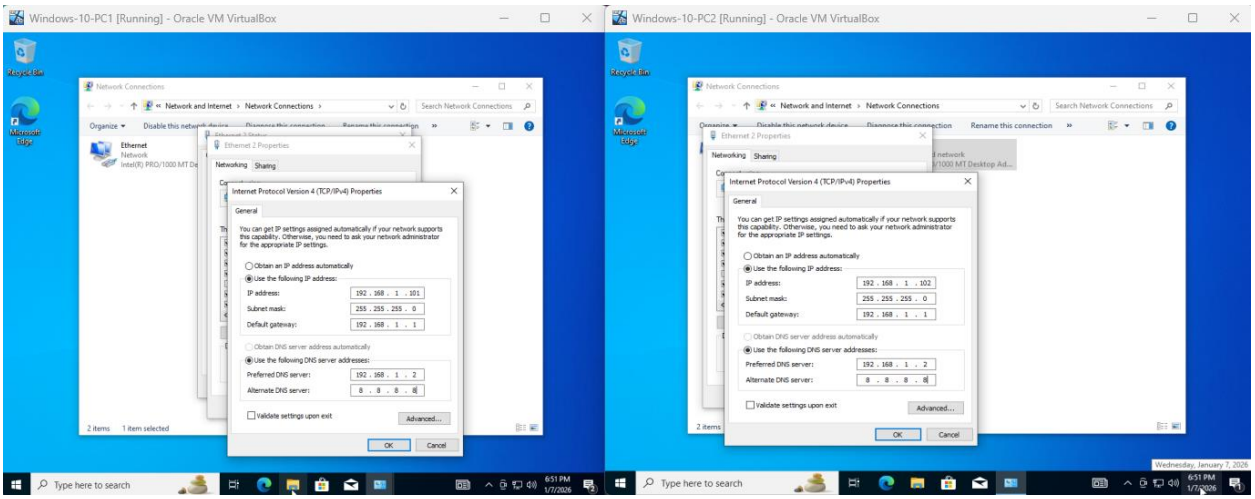
After powering the server to test this connection, I realized the NAT Network was not working properly. Although the systems were able to obtain IP addresses, internet connectivity could not be established even after spending significant time troubleshooting the configuration (See the screenshot above). 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.


General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
NAT
Name:
Advanced
OK
Cancel
Help

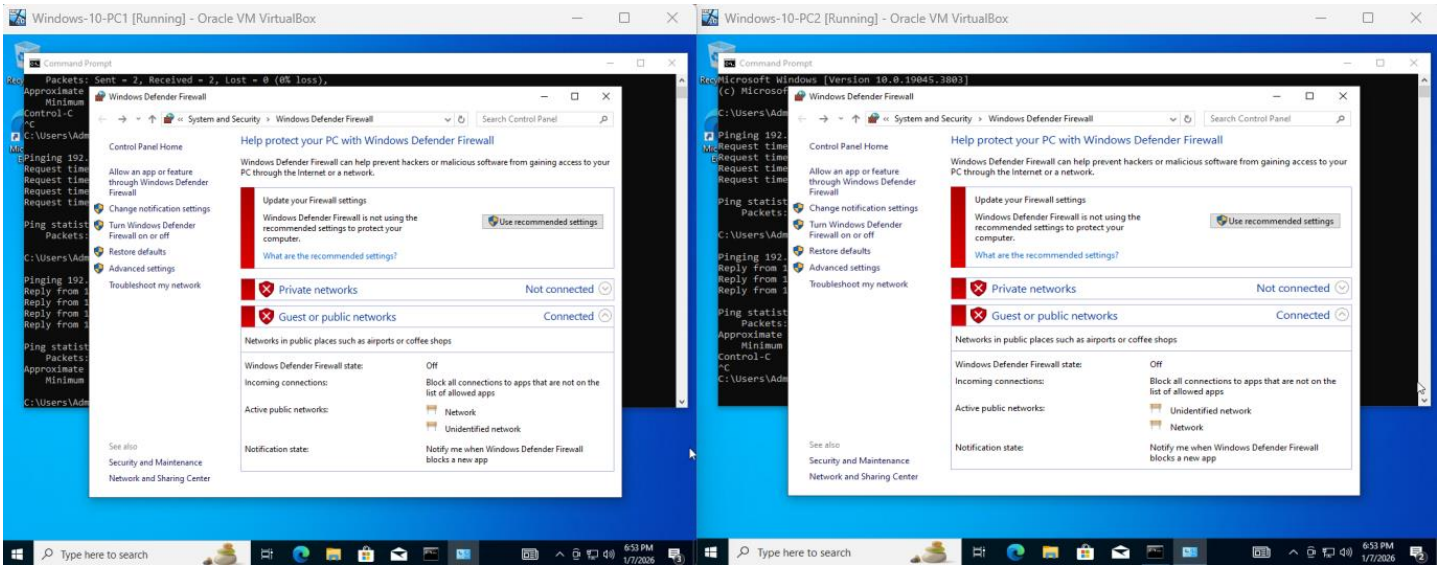


Statically Assigning IP Addresses

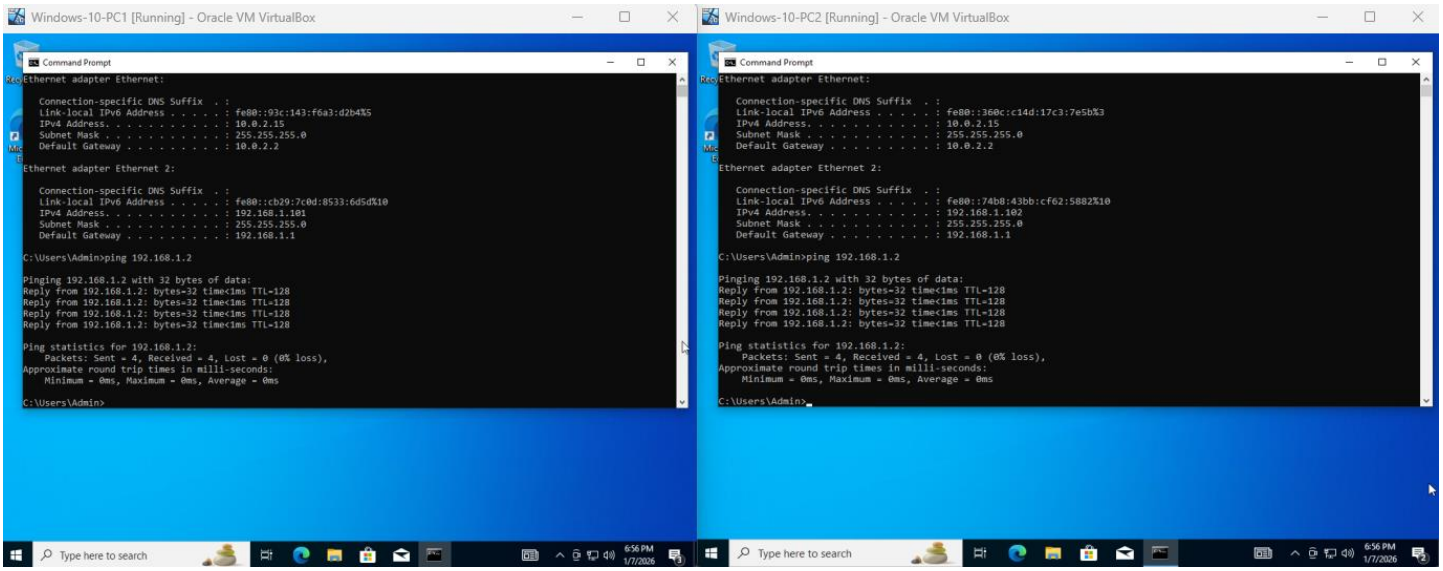
Now, I will assign static IP addresses to the Kali and both Windows VMs (Server was already done earlier). Using static addressing ensures consistent communication between the domain controller, endpoints, and attack system, and prevents issues caused by changing IP addresses. This is especially important 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.

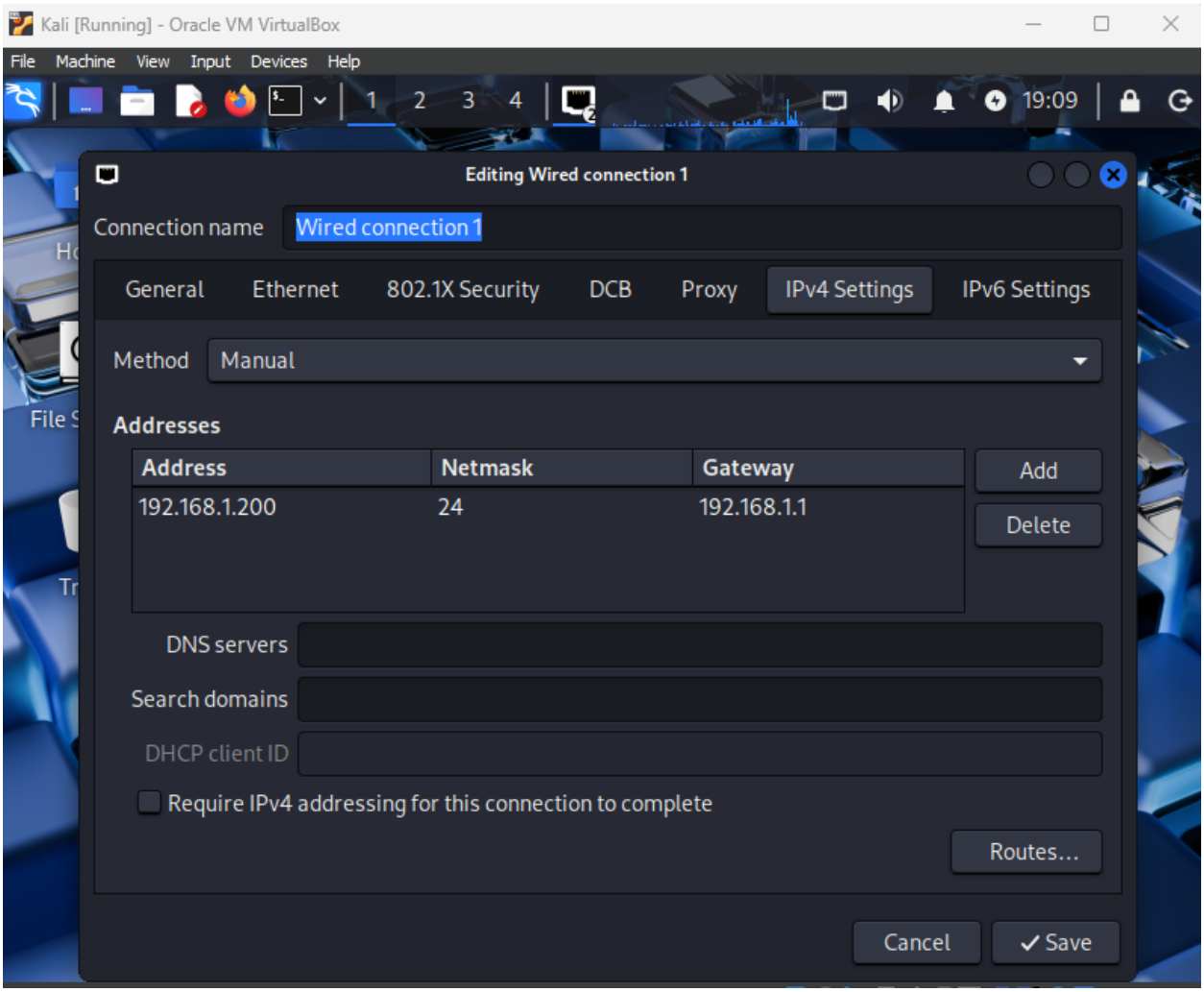


Turned off Windows Defender to allow incoming ICMP requests. This is needed for the “ping” command to work. This was also done to leave the system intentionally vulnerable for the Kali machine later.

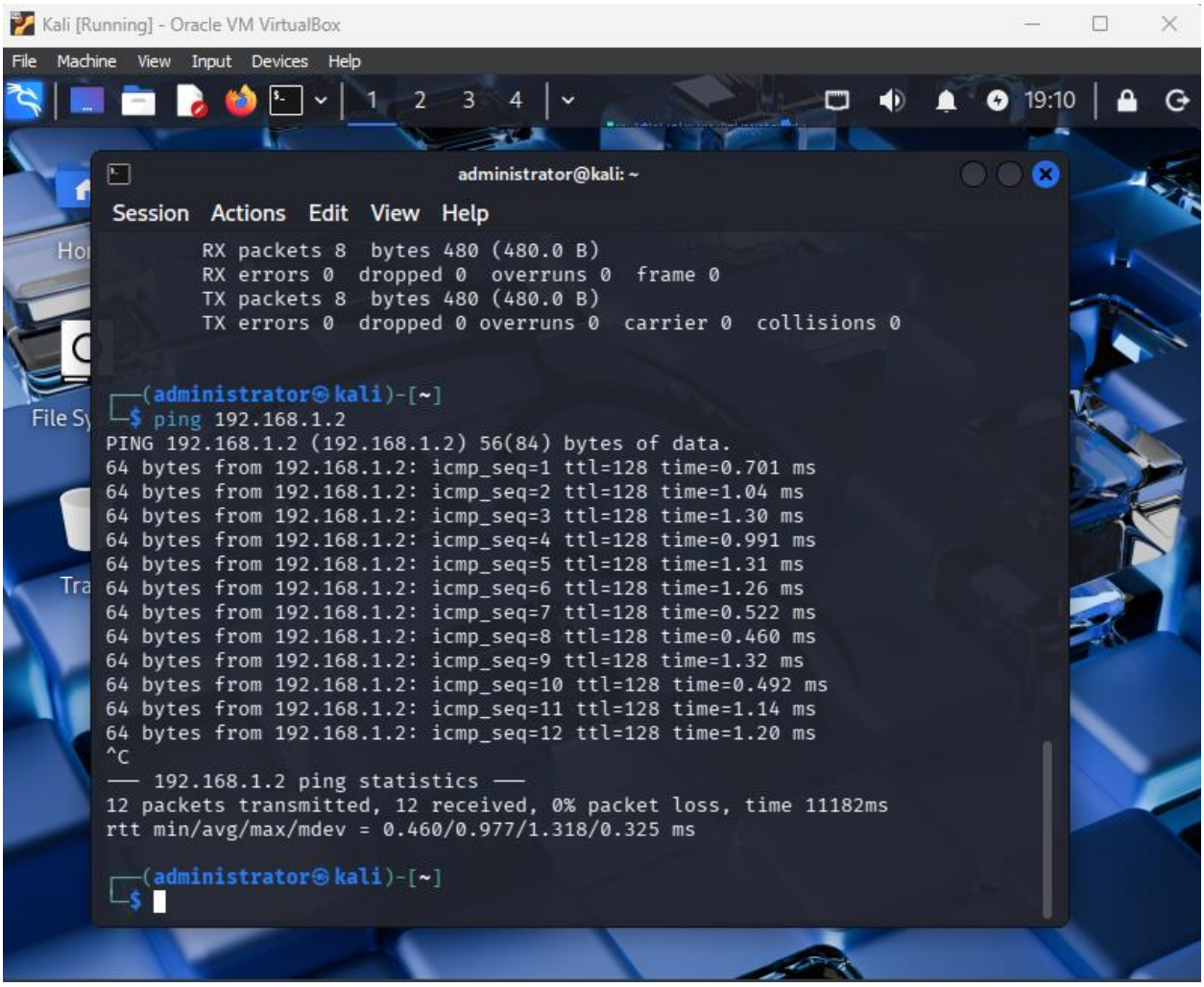


Successful ping between the computers and the server. An internal network has been established between these devices.


Windows-10-PC1 [Running] - Oracle VM VirtualBox
Command Prompt
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::93c:143:f6a3:d2b4%5
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
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
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>
Type here to search
Windows-10-PC2 [Running] - Oracle VM VirtualBox
Command Prompt
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::360c:c14d:17c3:7e5b%3
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
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
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>
Type here to search

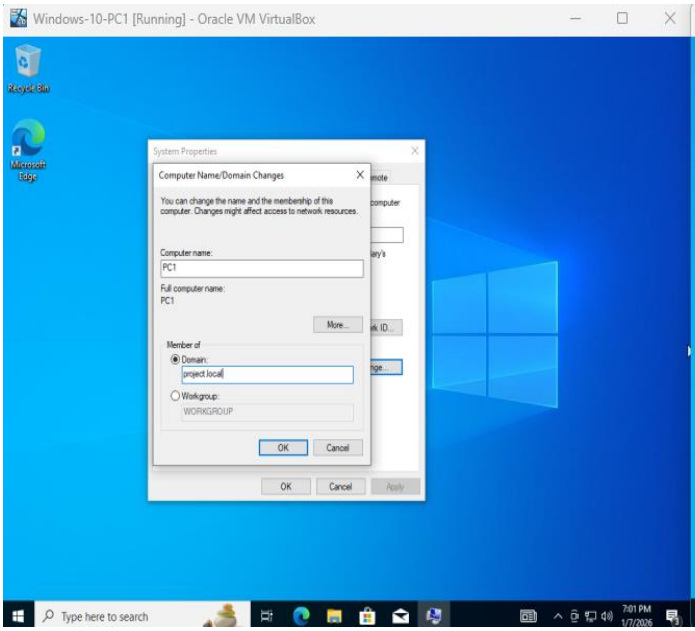

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:09
Editing Wired connection 1
Connection name
Wired connection 1
General
Ethernet
802.1X Security
DCB
Proxy
IPv4 Settings
IPv6 Settings
Method
Manual
Addresses
Address
Netmask
Gateway
192.168.1.200
24
192.168.1.1
Add
Delete
DNS servers
Search domains
DHCP client ID
Require IPv4 addressing for this connection to complete
Routes...
Cancel
Save

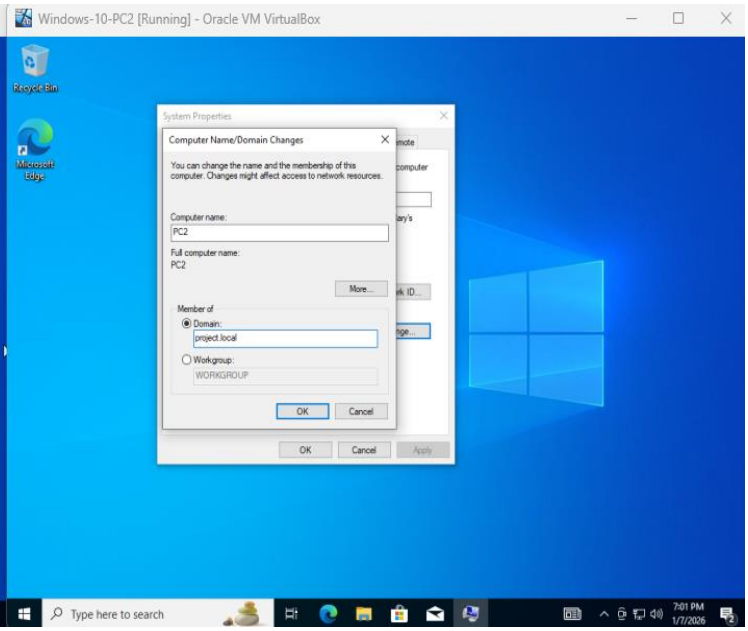
Kali machine can ping the server. This means that all devices are able to communicate with each other now.

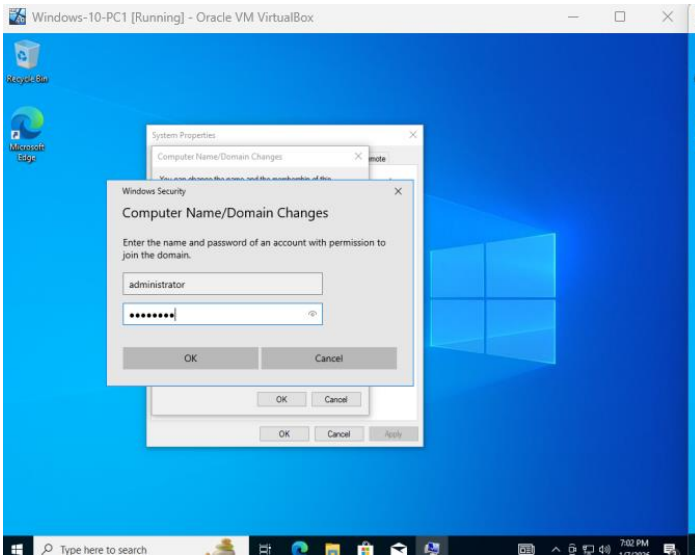


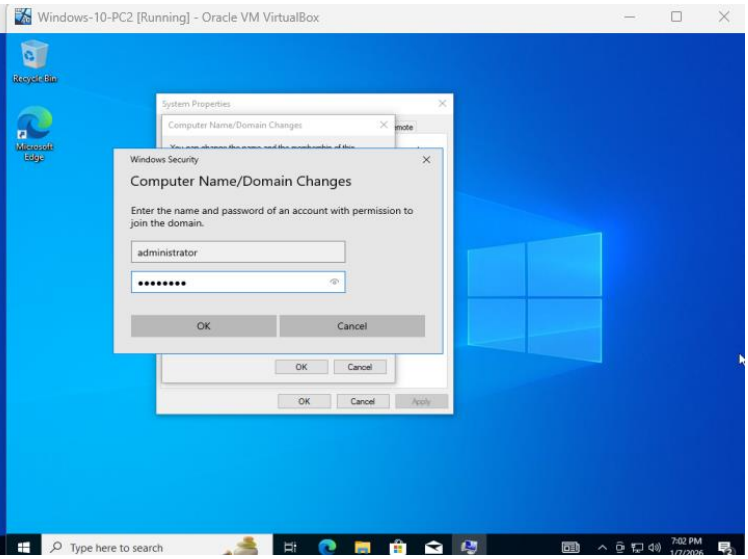
Domain Joining Windows Endpoints

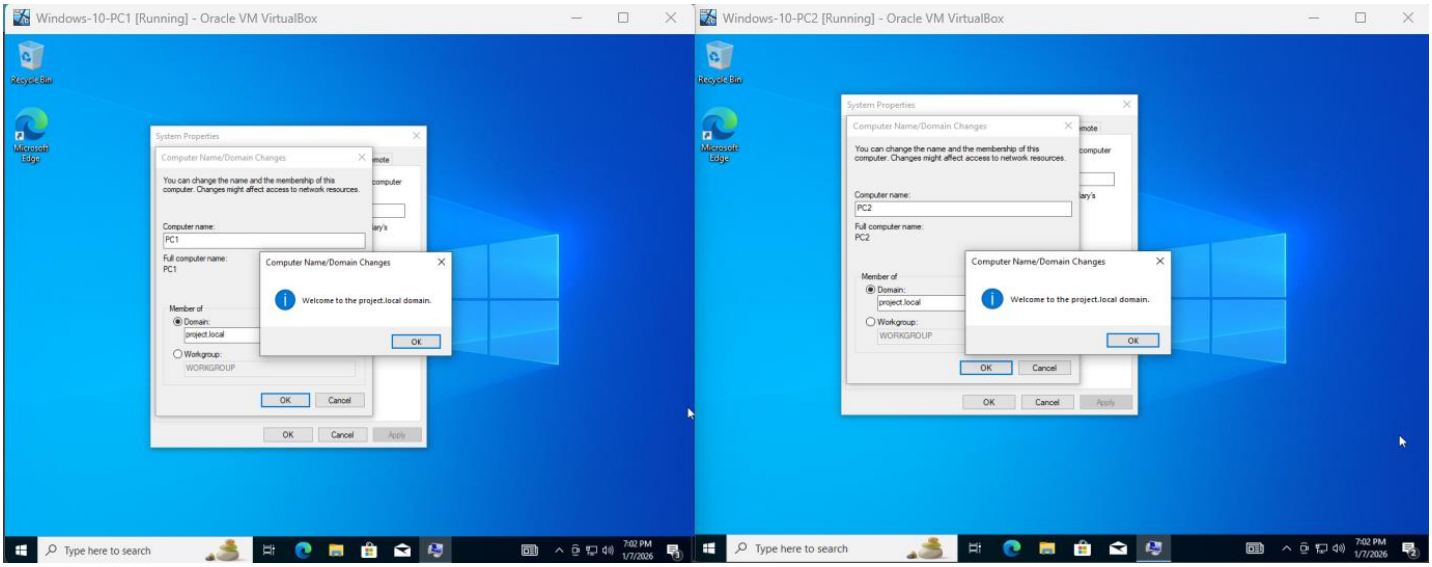
With the domain controller and network configuration in place, the two Windows 10 endpoint virtual machines will now be joined to the Active Directory domain. Joining the endpoints to the domain allows user authentication, group policies, and domain-based activity to be centrally managed by the server. This step completes the core enterprise setup and enables the generation of realistic authentication and endpoint security events for later analysis in Splunk.


Windows-10-PC1 [Running] - Oracle VM VirtualBox
Recycle Bin
Microsoft Edge
System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
PC1
Full computer name:
PC1
More...
Member of
Domain:
project.local
Workgroup:
WORKGROUP
OK
Cancel
Apply
Type here to search
7:01 PM
1/7/2026

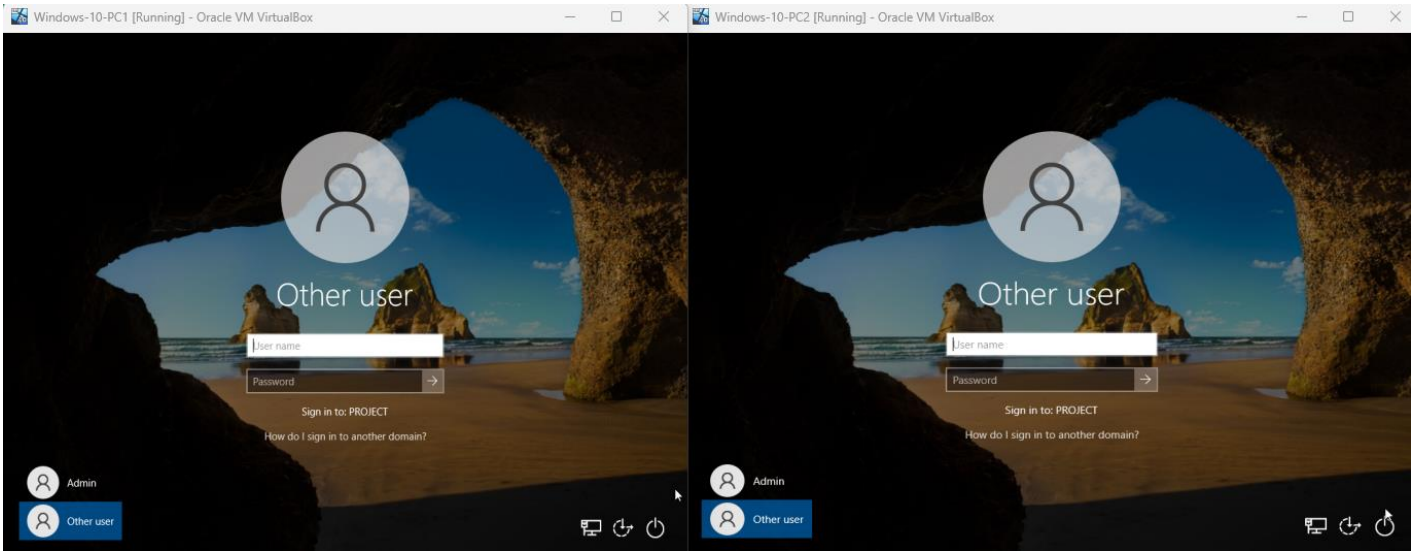

Windows-10-PC2 [Running] - Oracle VM VirtualBox
Recycle Bin
Microsoft Edge
System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
PC2
Full computer name:
PC2
More...
Member of
Domain:
project.local
Workgroup:
WORKGROUP
OK
Cancel
Apply
Type here to search
7:01 PM
1/7/2026


Windows-10-PC1 [Running] - Oracle VM VirtualBox
Recycle Bin
Microsoft Edge
System Properties
Computer Name/Domain Changes
Windows Security
Computer Name/Domain Changes
Enter the name and password of an account with permission to join the domain.
administrator
OK
Cancel
Apply
Type here to search
7:02 PM


Windows-10-PC2 [Running] - Oracle VM VirtualBox
Recycle Bin
Microsoft Edge
System Properties
Computer Name/Domain Changes
Windows Security
Computer Name/Domain Changes
Enter the name and password of an account with permission to join the domain.
administrator
OK
Cancel
Apply
Type here to search
7:02 PM



Both PCs are now domain joined.

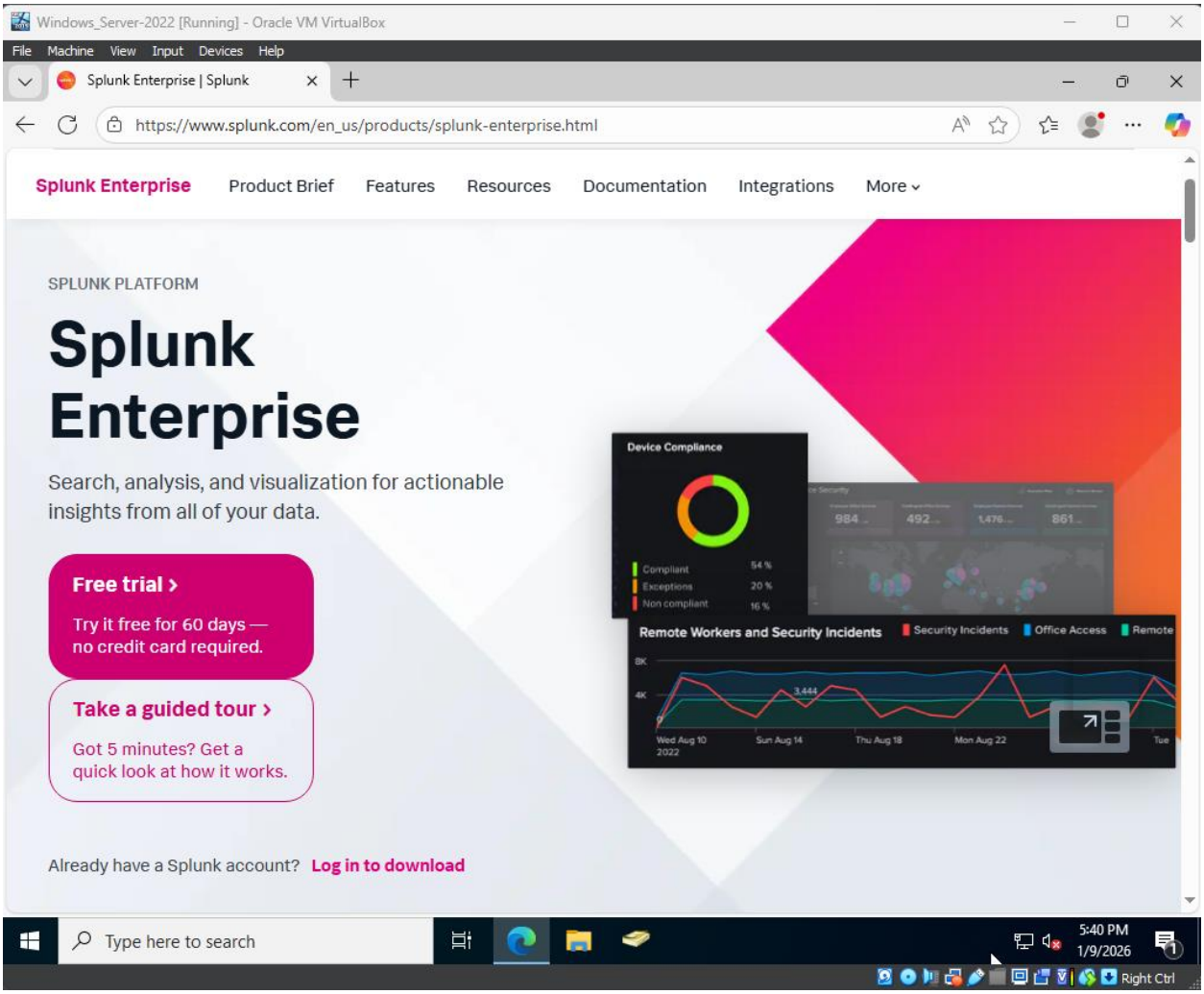


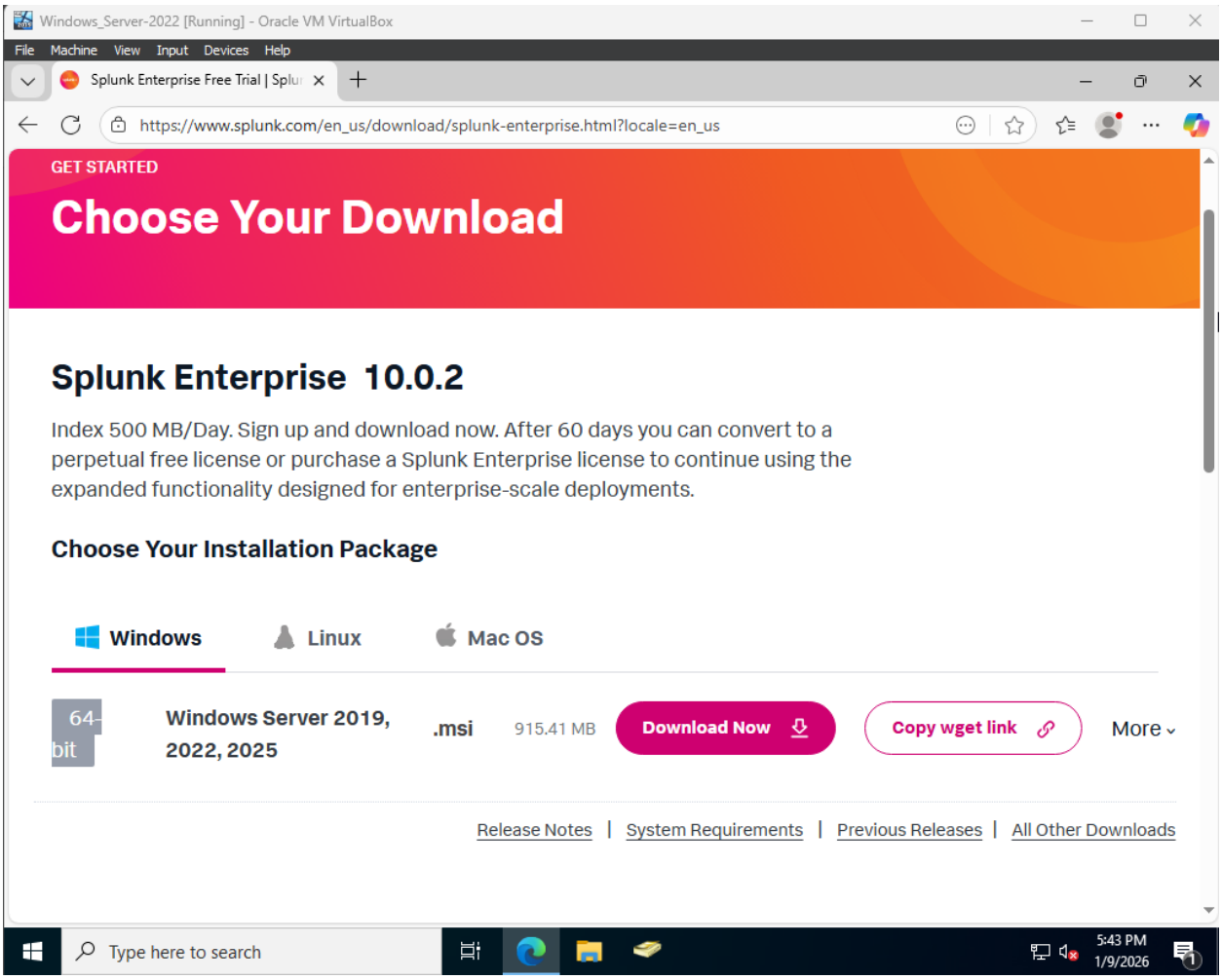
At this stage, the Active Directory domain has been successfully created, establishing a centralized authentication and management system that represents a small enterprise network. The Windows endpoints are domain-joined and generate realistic user and administrative activity within the environment. 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.

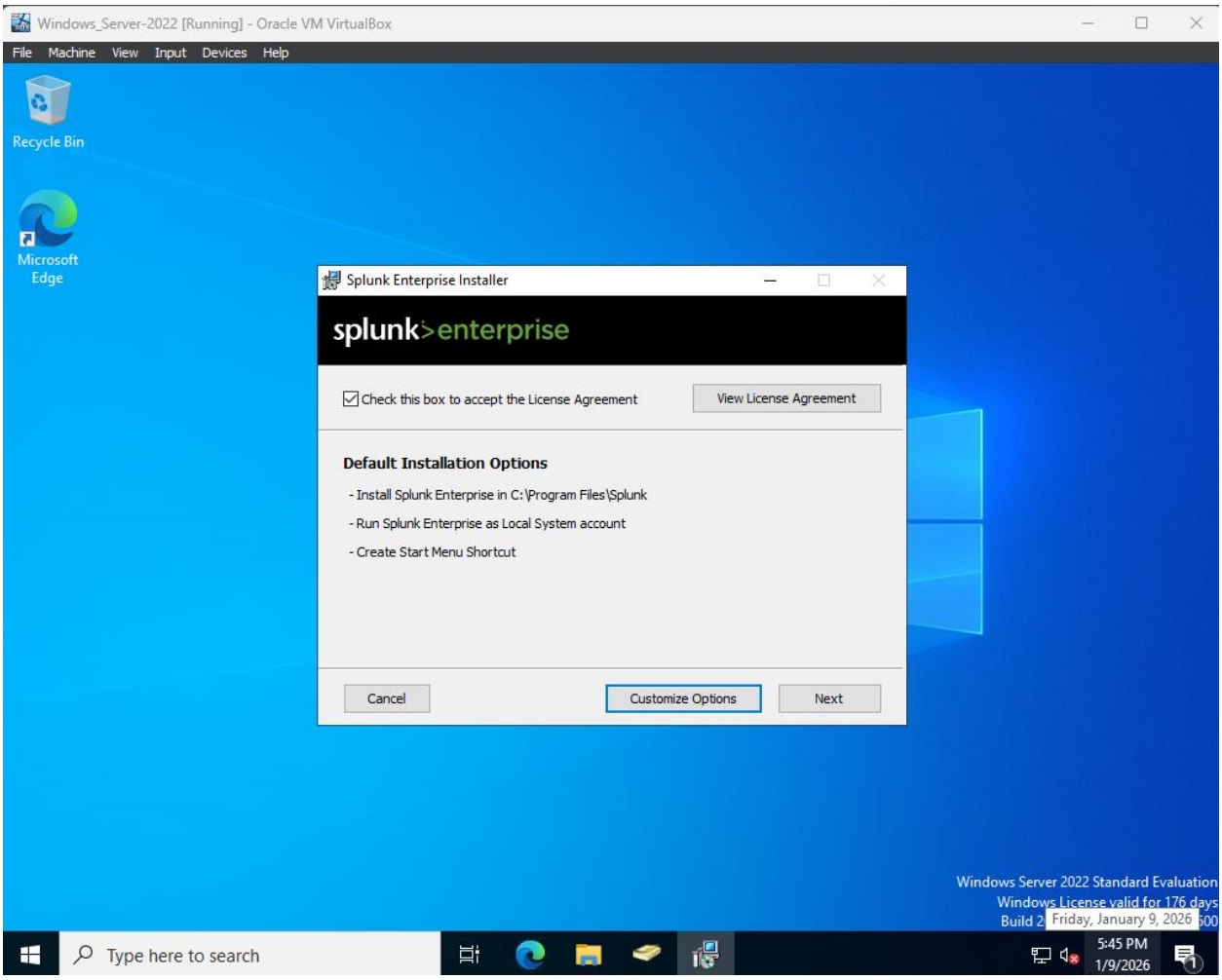
Splunk Installation and Setup

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.

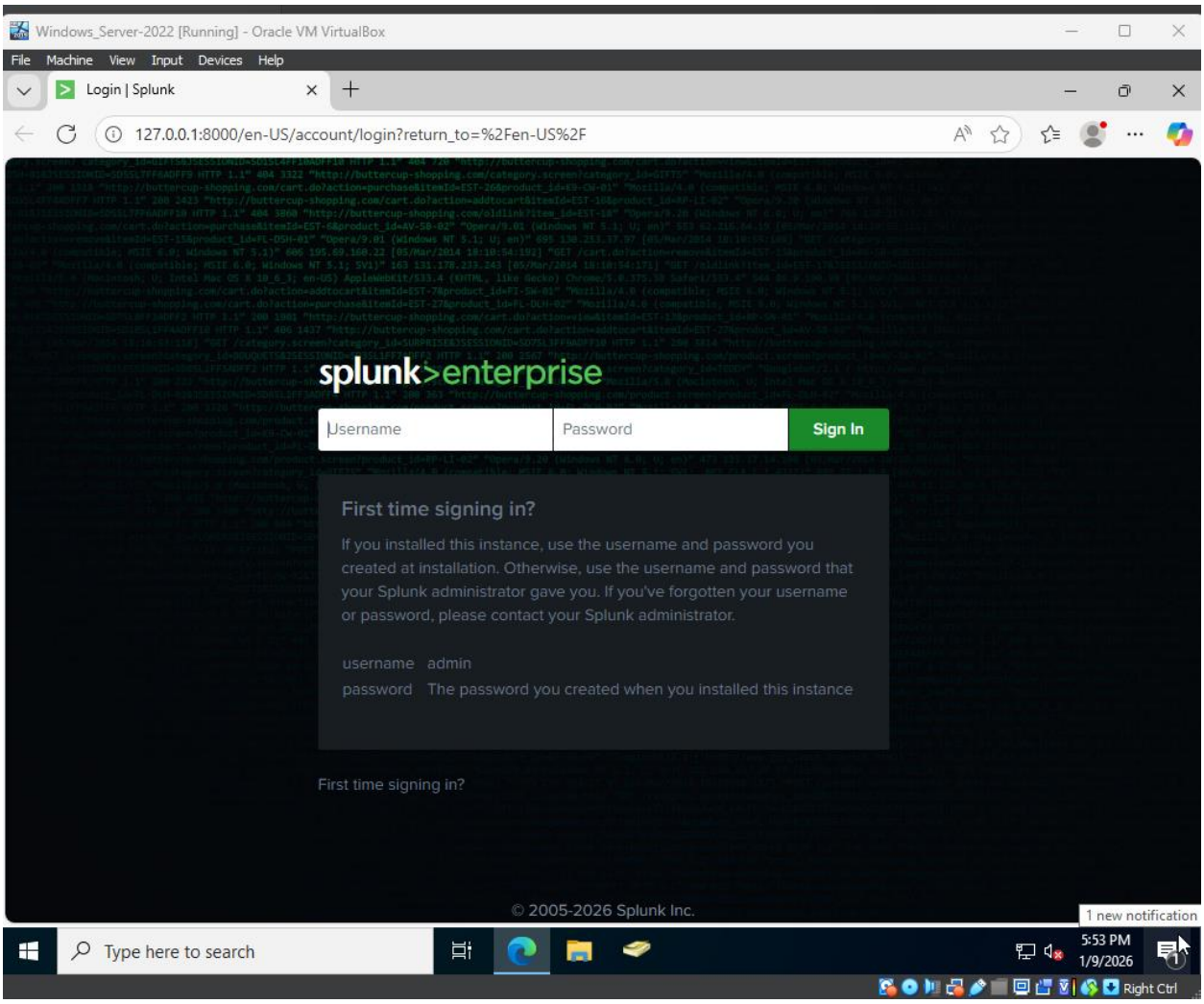
I will be using the free trial.



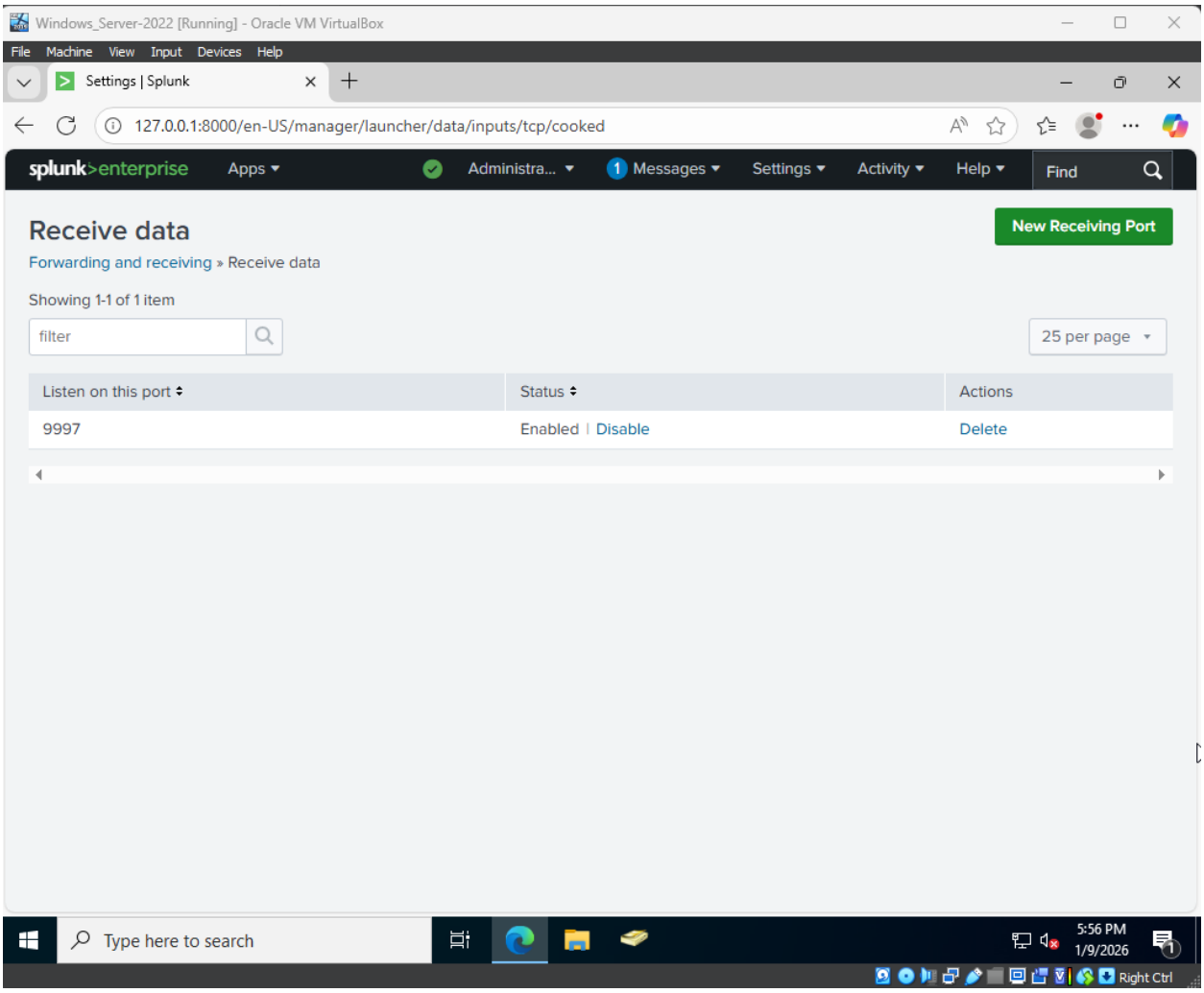

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Splunk Enterprise Free Trial | Splu
https://www.splunk.com/en_us/download/splunk-enterprise.html?locale=en_us
GET STARTED
Choose Your Download
Splunk Enterprise 10.0.2
Index 500 MB/Day. Sign up and download now. 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



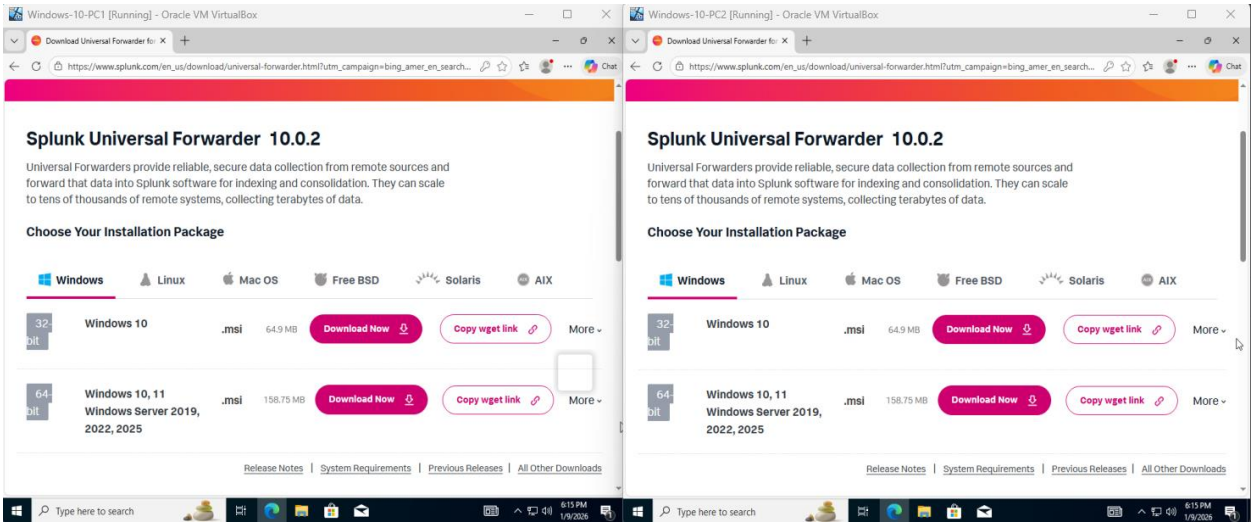
The web UI of Splunk Enterprise after installation.

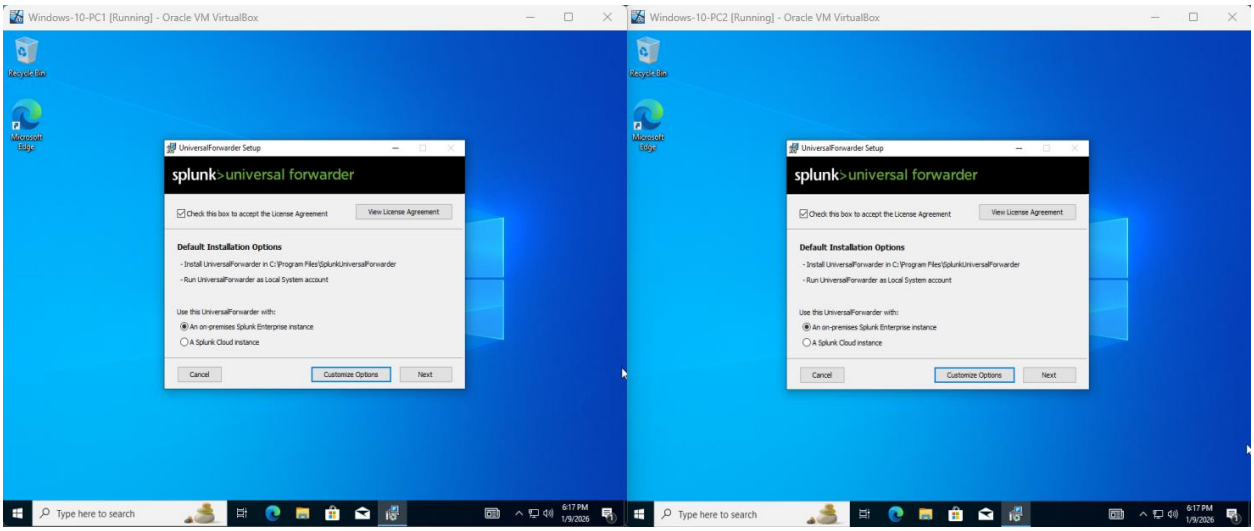


Once I logged, I navigated to the settings page. From there I went into forwarding and receiving in order to add a receiving port. This is needed to add the Windows 10 PCs.

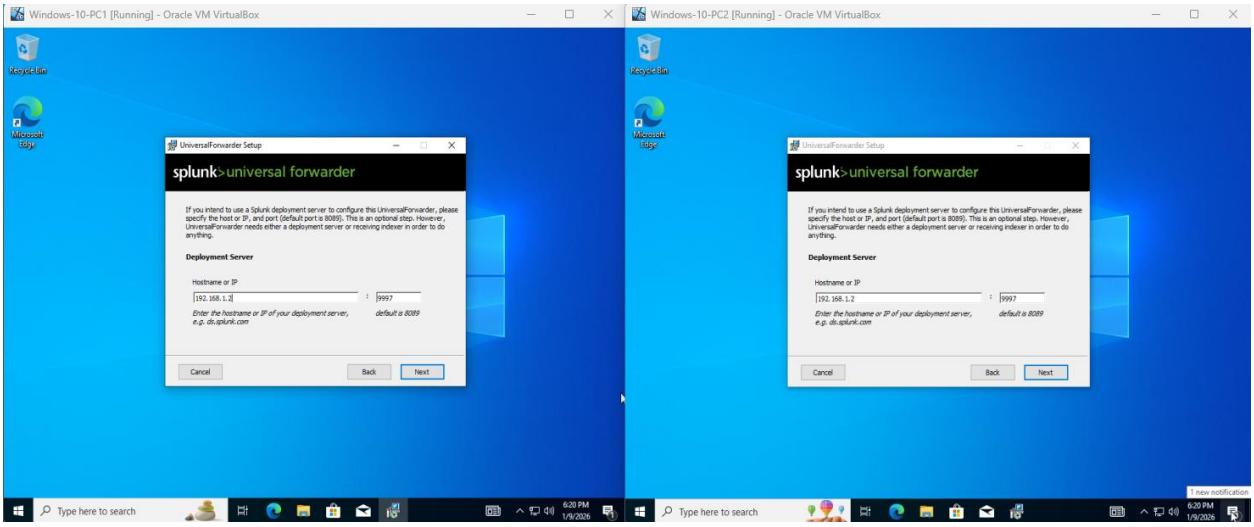


Installing the Splunk Universal Forwarder on the two Windows 10 PCs.

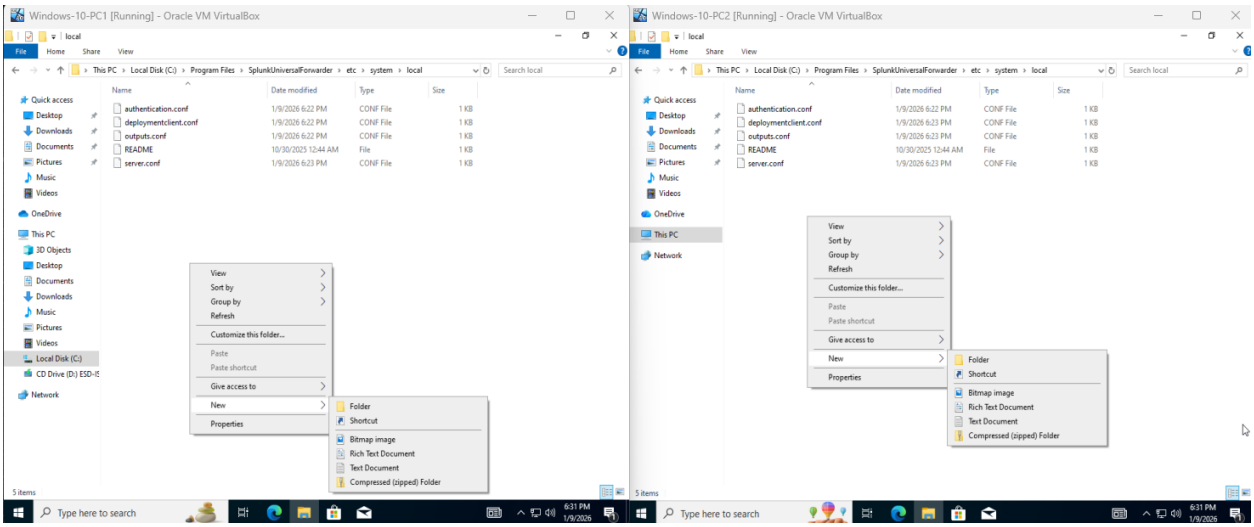




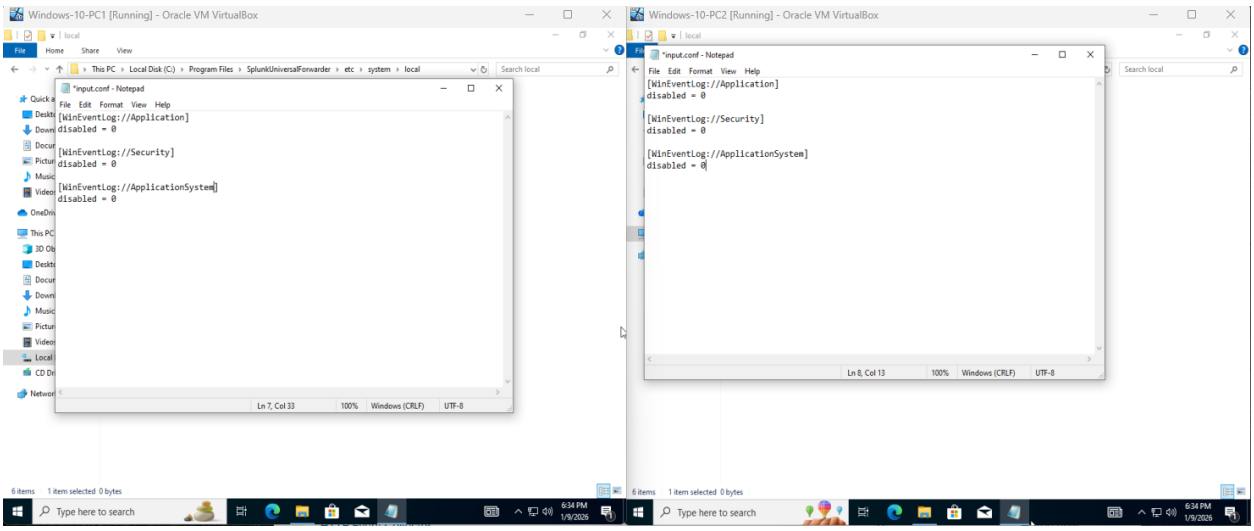
Added the private IP of the server along with the port we configured to receive.



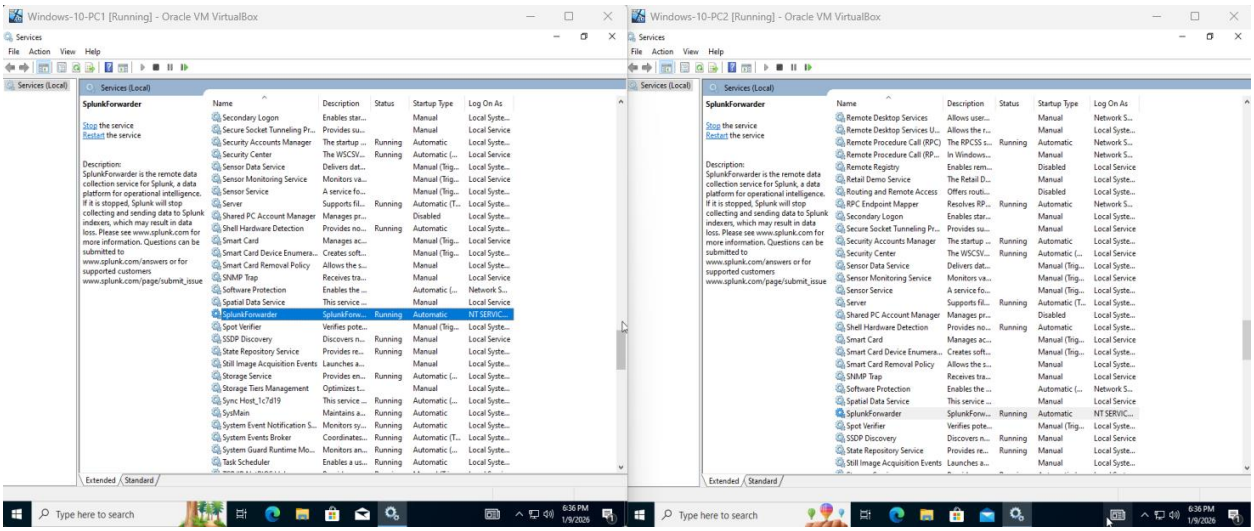
After the install, I will need to create a new text file in the SplunkUniversalForwarder folder that is now in the C drive. This text file will be called inputs.conf.



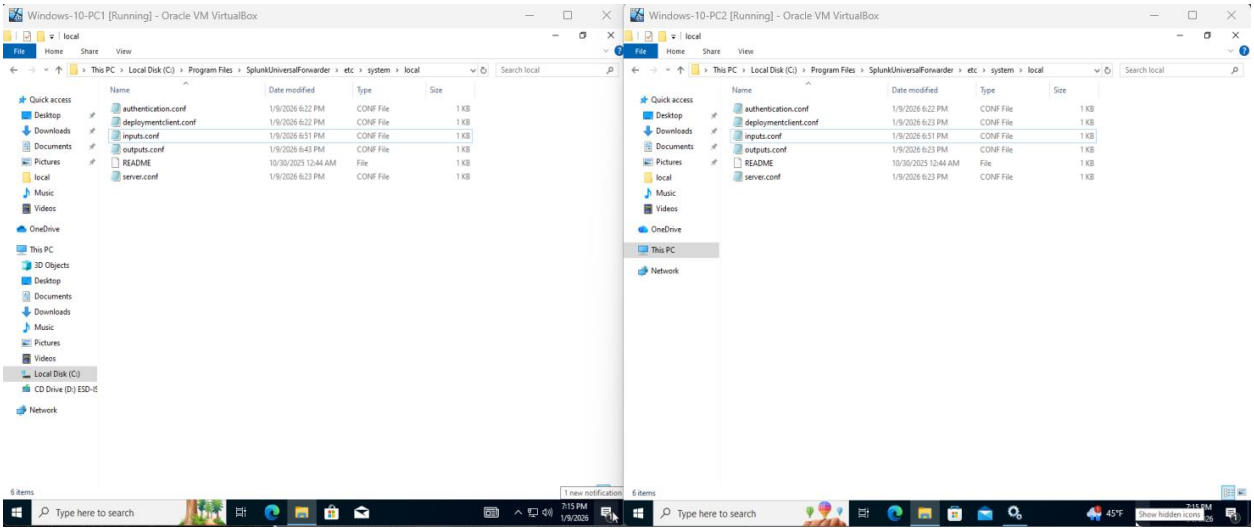
I include this bit of writing in the text files and save them.



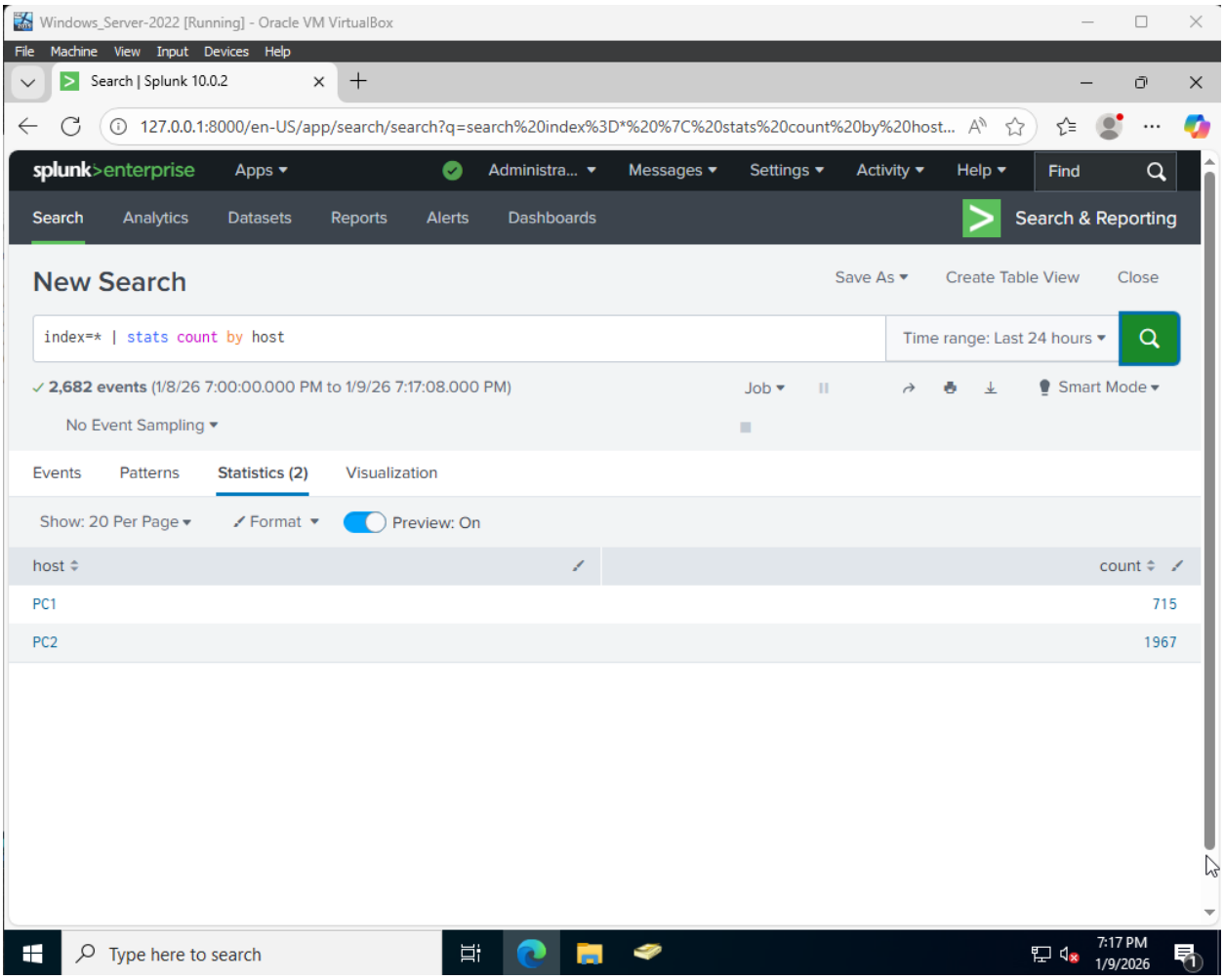
In the services application, I had to restart the SplunkForwarder service.



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.

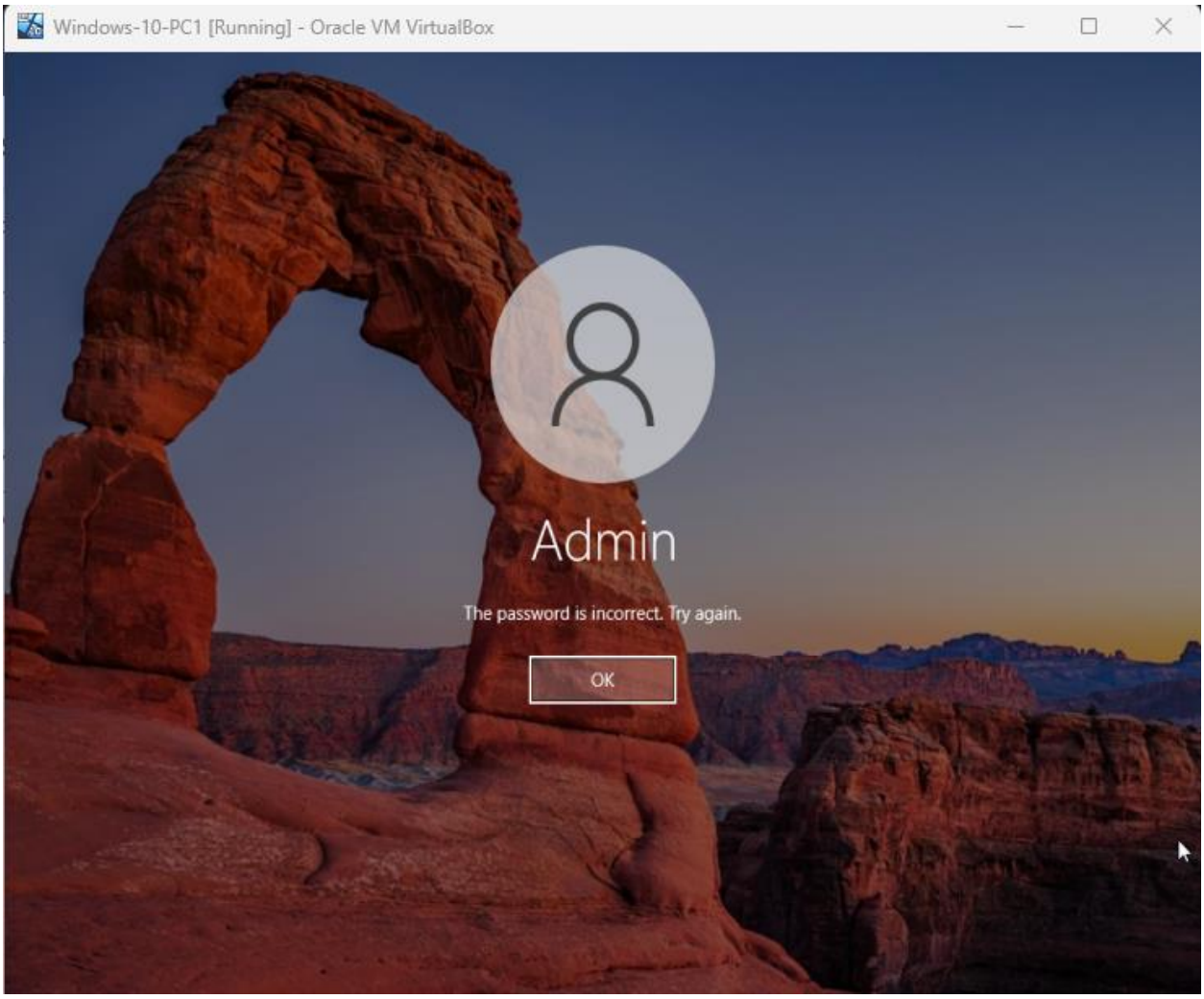


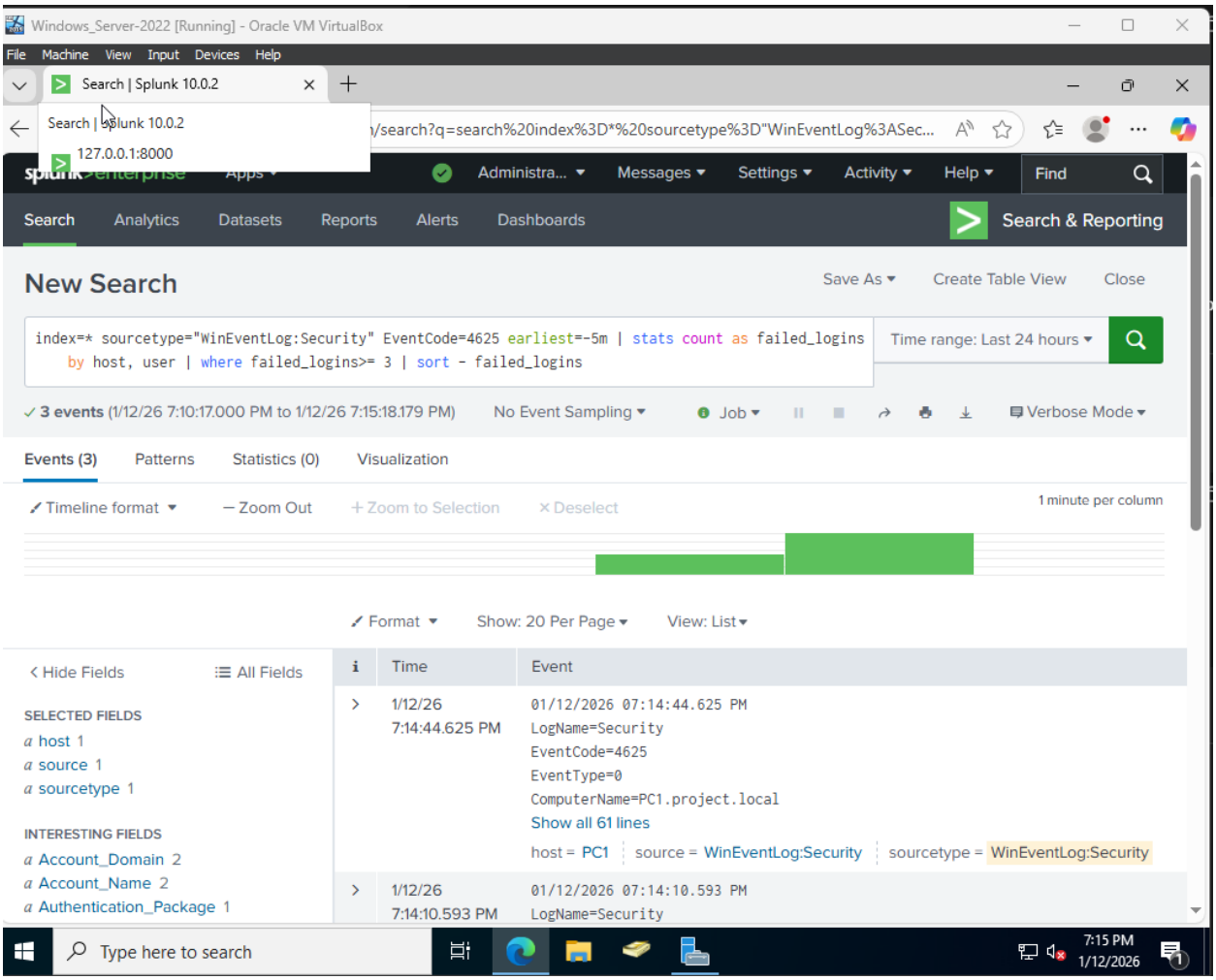
As you can see, the two PCs are now seen in the portal with all of their logs.

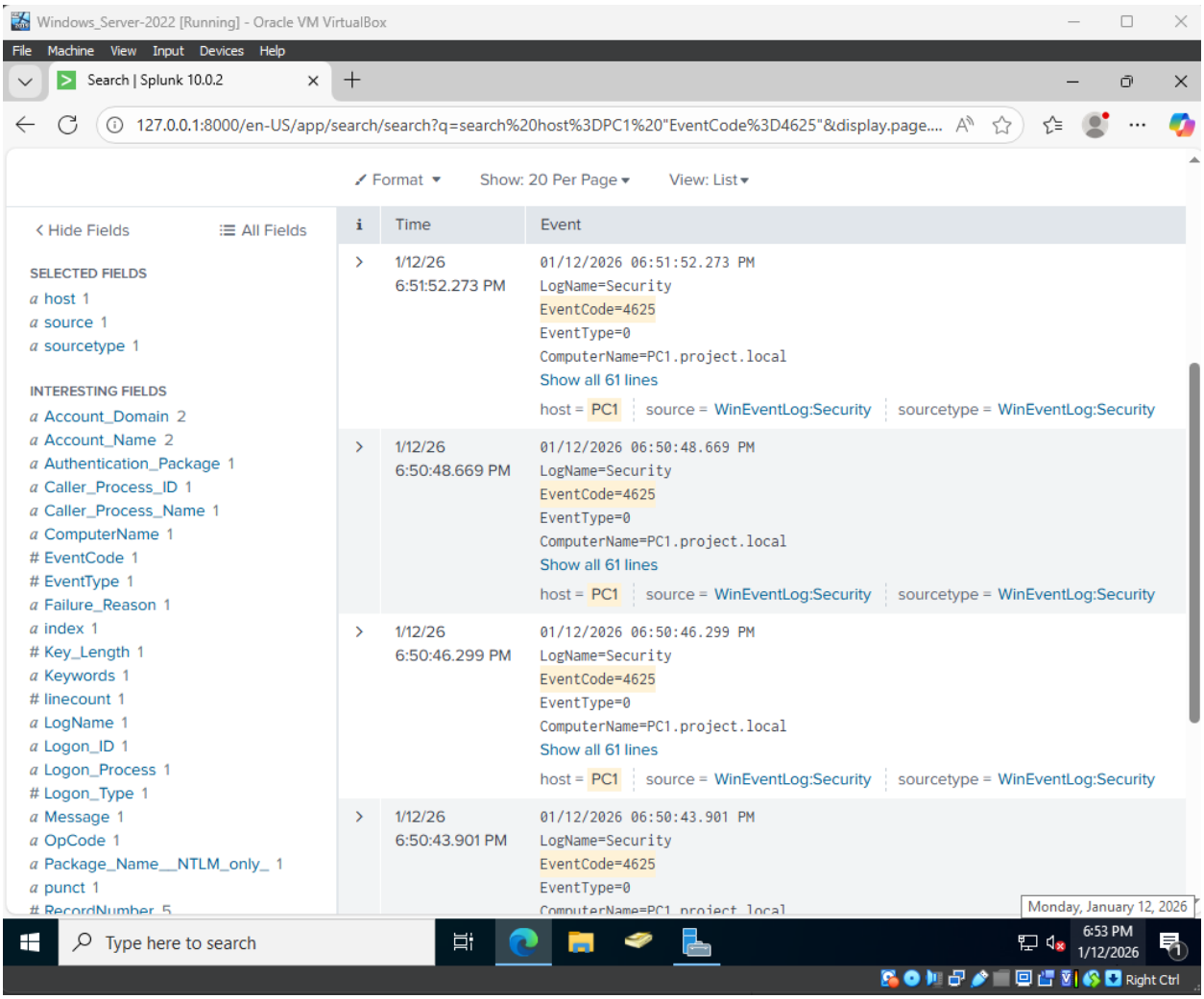


Setting Up SPL

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-10-PC1 [Running] - Oracle VM VirtualBox
Admin
The password is incorrect. Try again.
OK

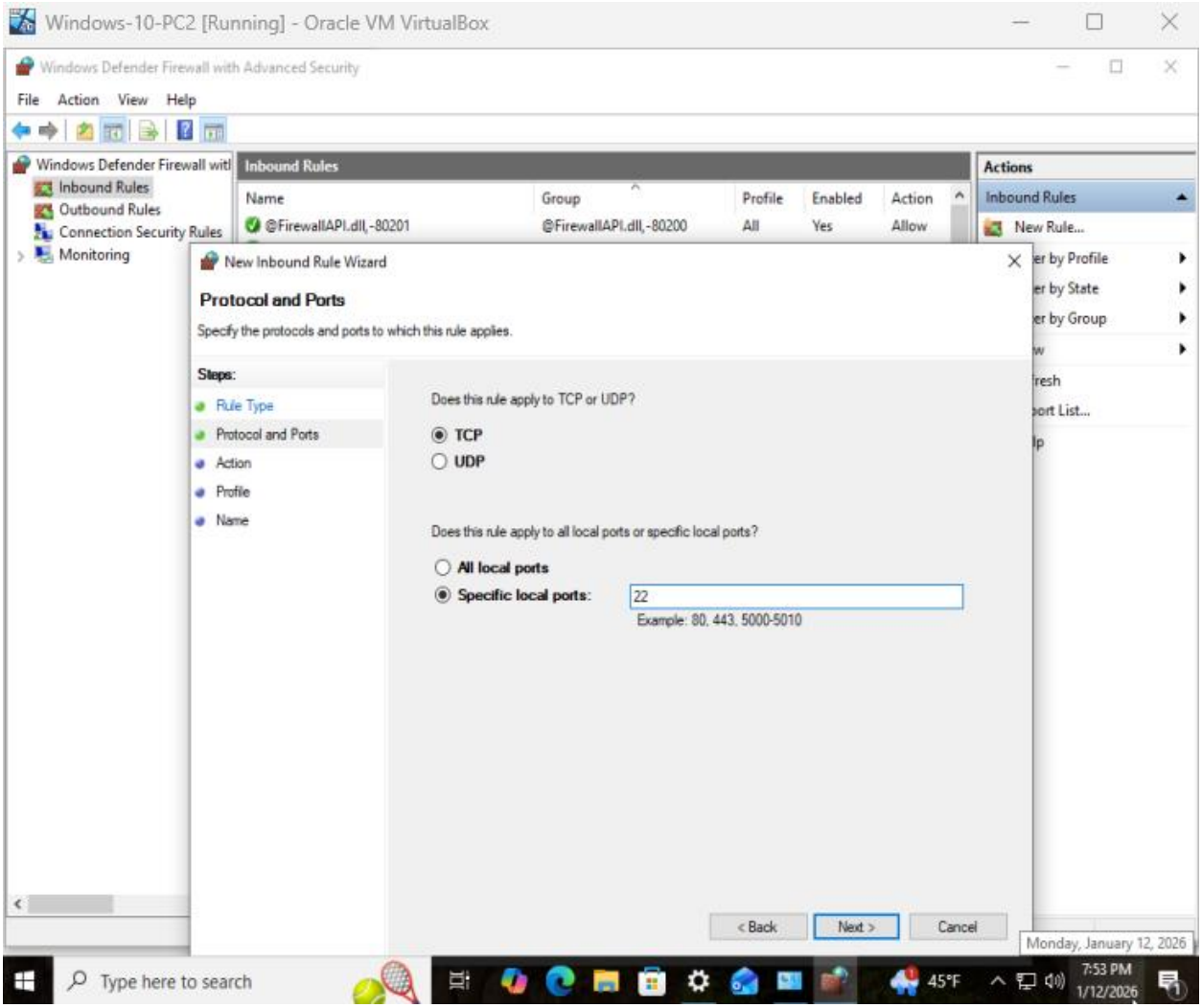

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Search | Splunk 10.0.2
127.0.0.1:8000
Administra... Messages Settings Activity Help Find
Search Analytics Datasets Reports Alerts Dashboards
Search & Reporting
New Search
Save As Create Table View Close
index=* 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
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
host 1
source 1
sourcetype 1
INTERESTING FIELDS
Account_Domain 2
Account_Name 2
Authentication_Package 1
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



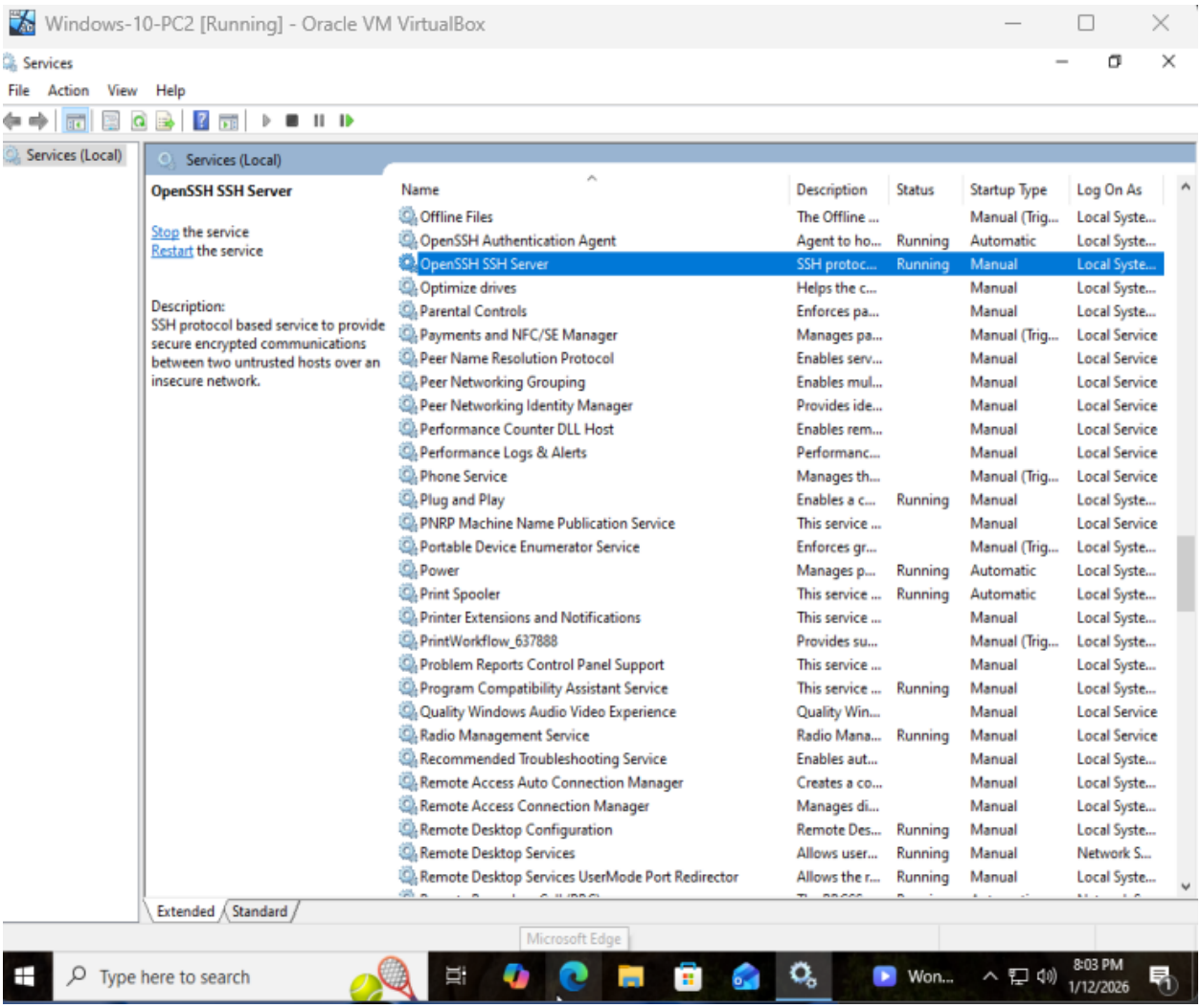
As you can see, the failed log in attempts have been sent over to the server.

Using Kali to Brute Force into the System and Create Logs

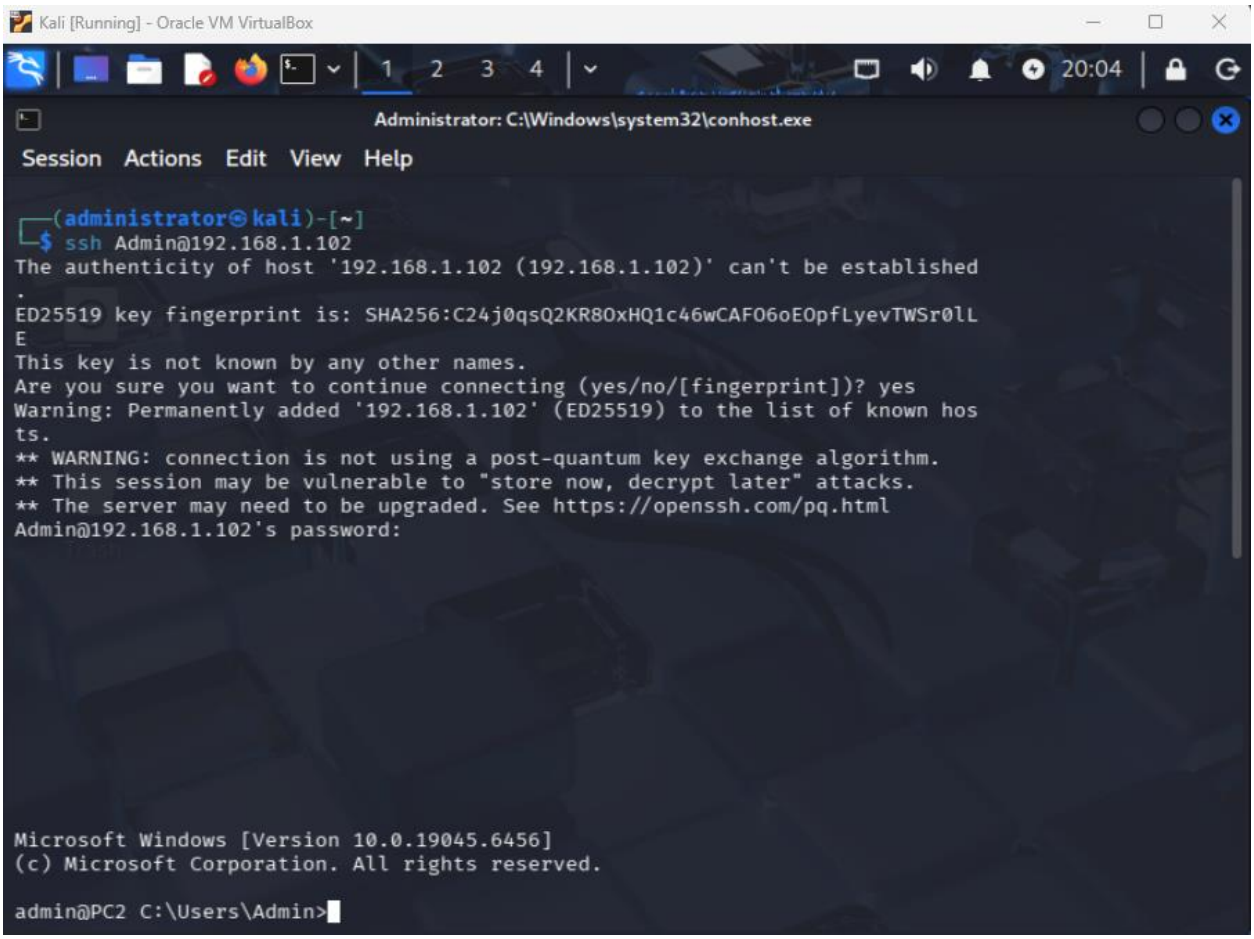
Enabling port 22 for SSH to allow for vulnerabilities. Kali will attack using SSH.



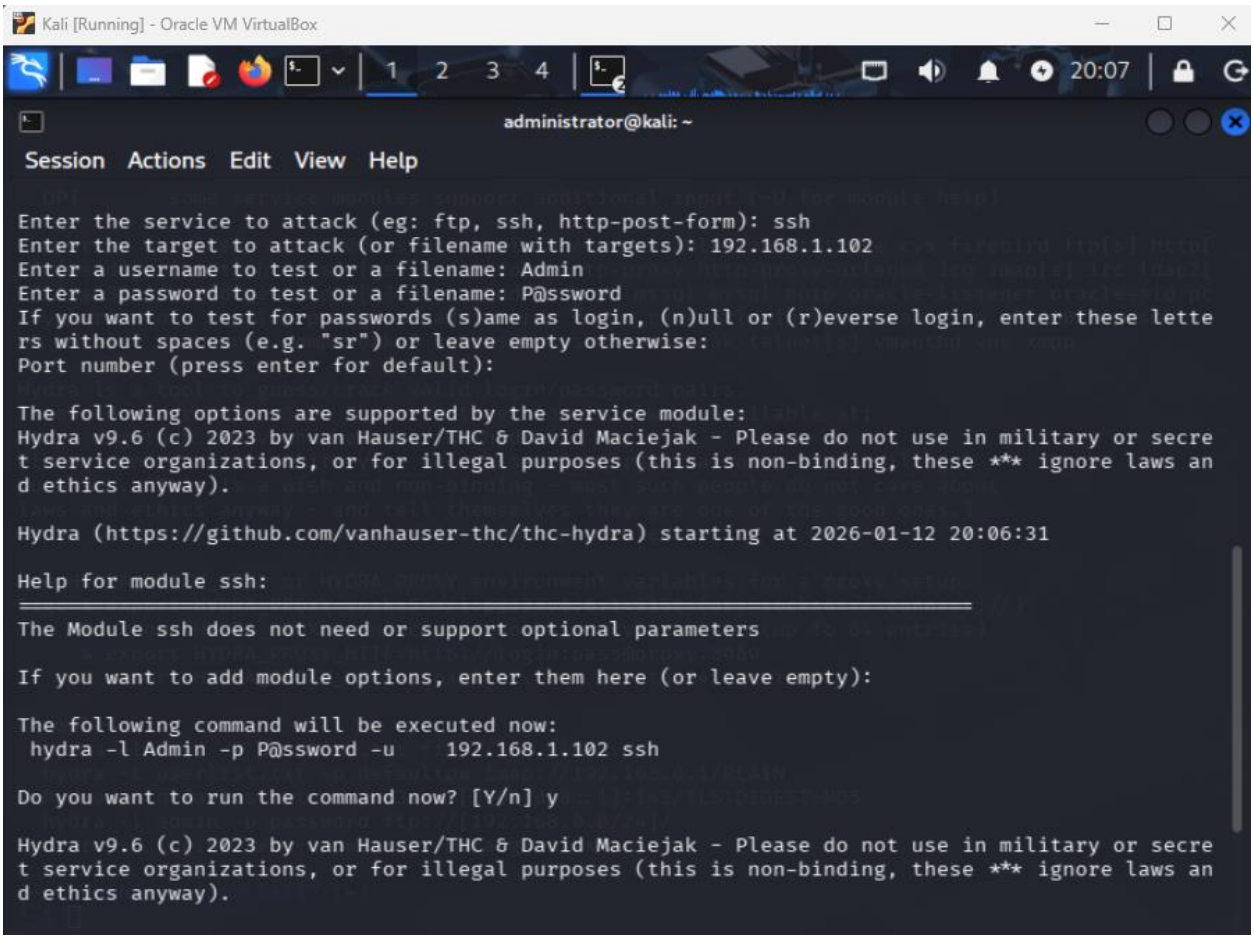
Starting up the SSH Server service to allow for SSH connections.

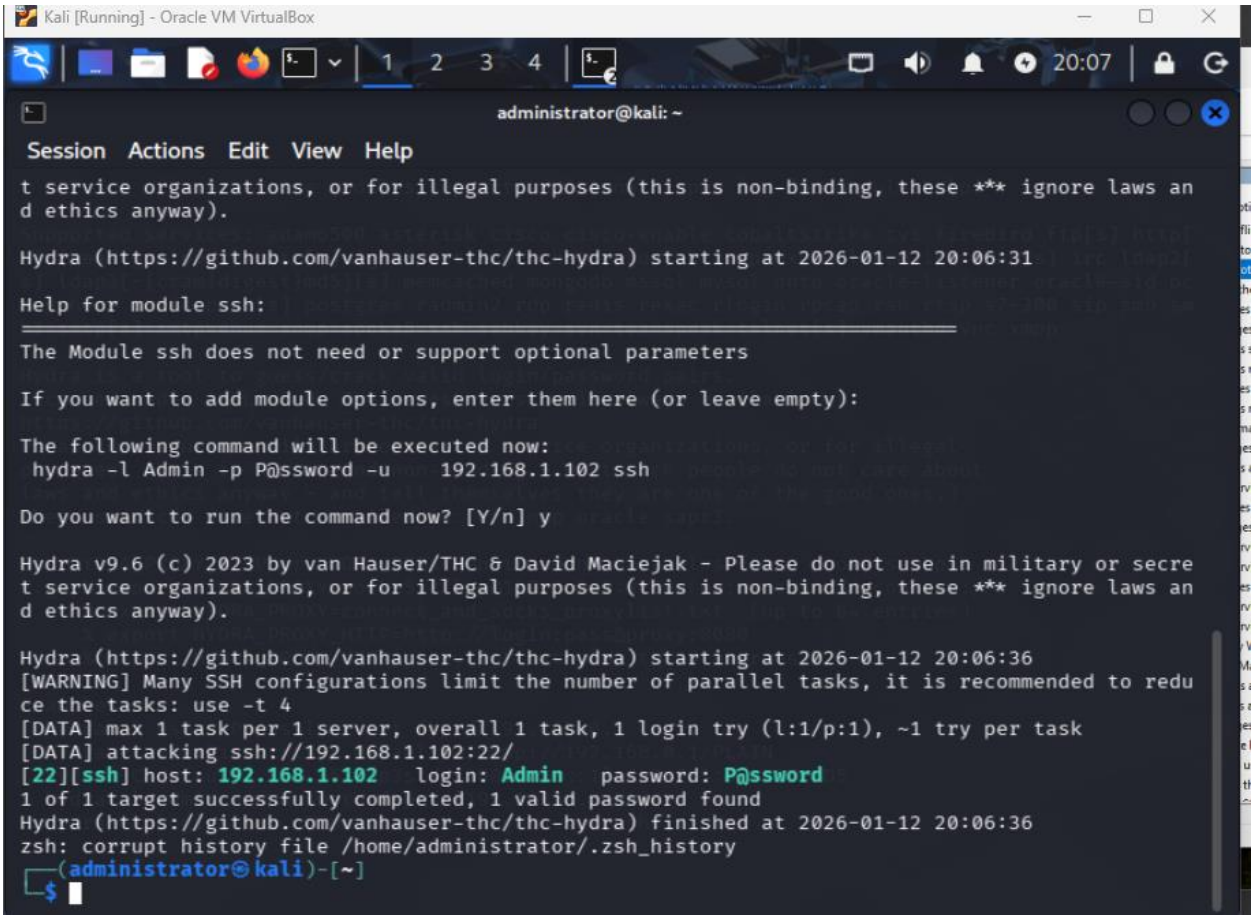


Testing the SSH and seeing that does indeed work.

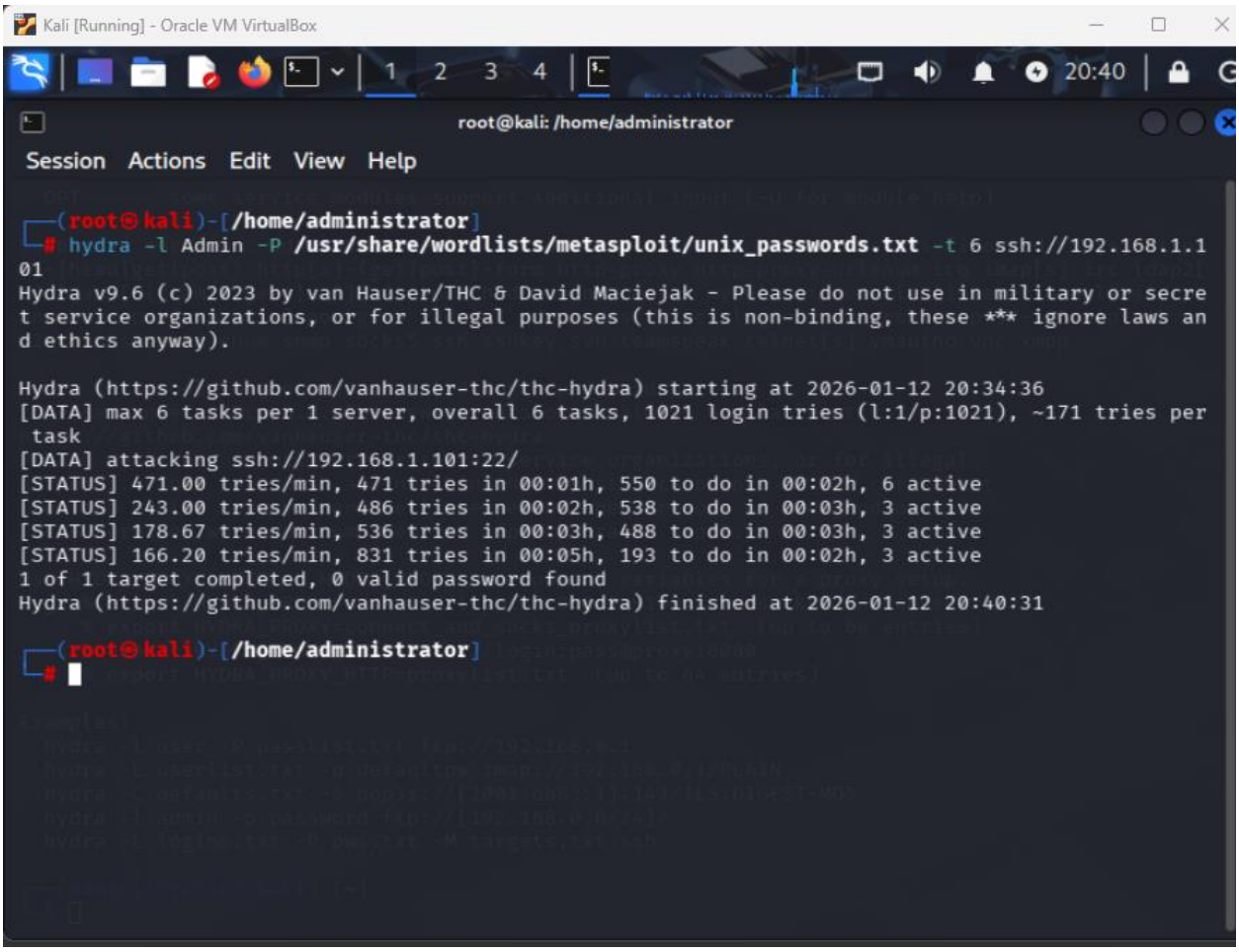


Using a basic Hydra tool command to attempt the SSH connection.

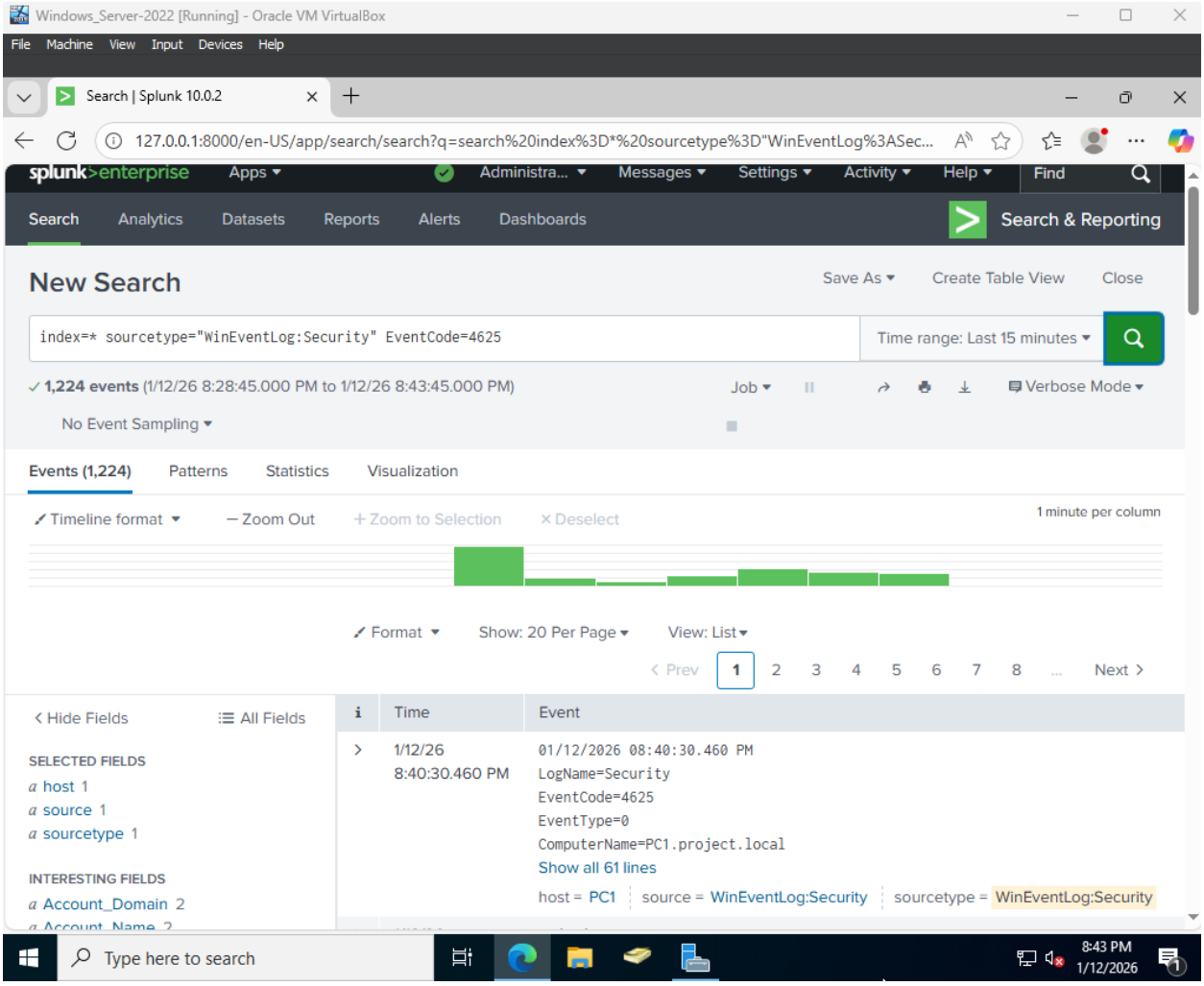

Kali [Running] - Oracle VM VirtualBox
1 2 3 4
20:07
administrator@kali: ~
Session Actions Edit View Help
Enter the service to attack (eg: ftp, ssh, http-post-form): ssh
Enter the target to attack (or filename with targets): 192.168.1.102
Enter a username to test or a filename: Admin
Enter a password 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).



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.



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.

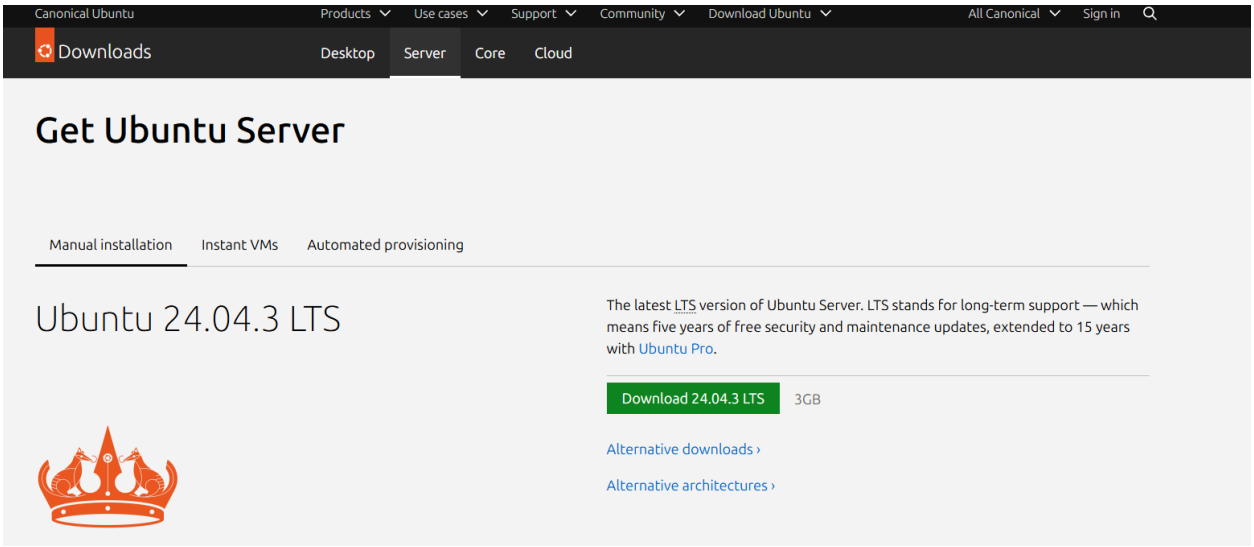


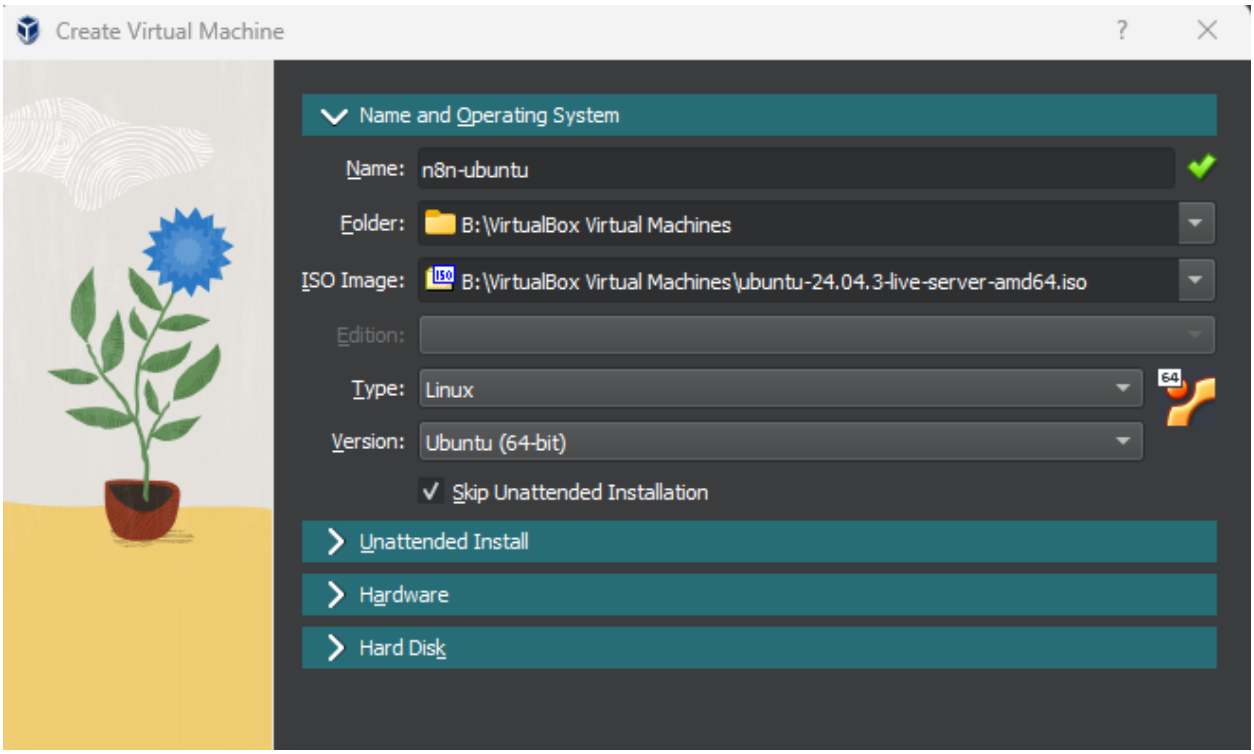
n8n and AI Integration Setup

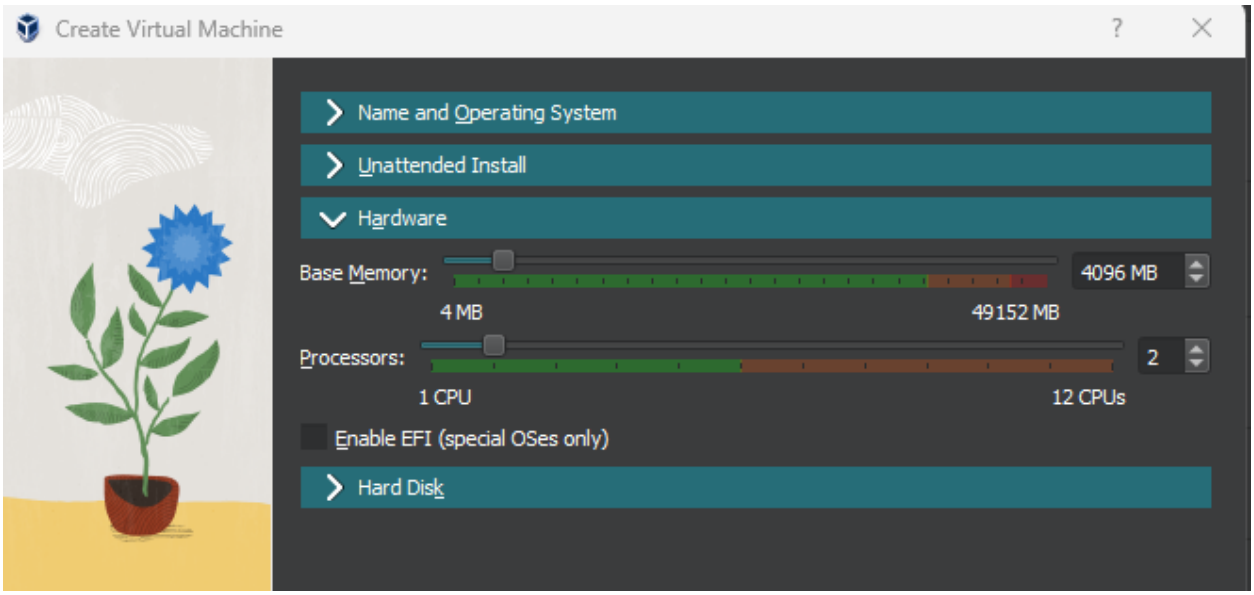
n8n is an open-source workflow automation tool that allows different systems and services to be connected using a visual, low-code interface. In this lab, n8n is used as the automation layer between Splunk and AI. Security events and logs generated from Kali attacks and collected by Splunk can be passed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

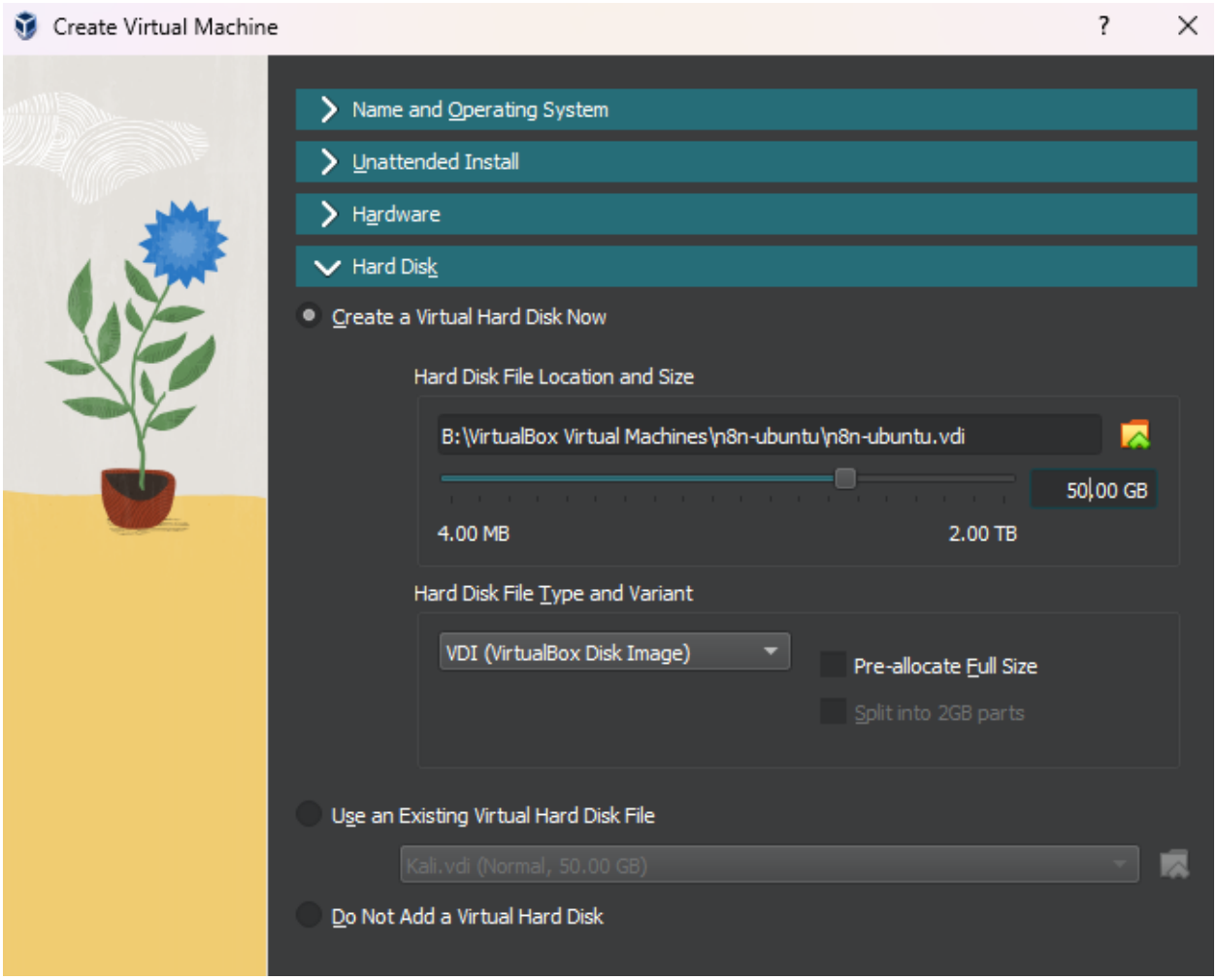
To support this, an Ubuntu virtual machine will be created to host n8n and manage the automation workflows. As the AI component, ChatGPT is integrated into n8n to analyze Splunk log data, summarize events, and provide context on potential security threats. This allows raw log data to be transformed into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

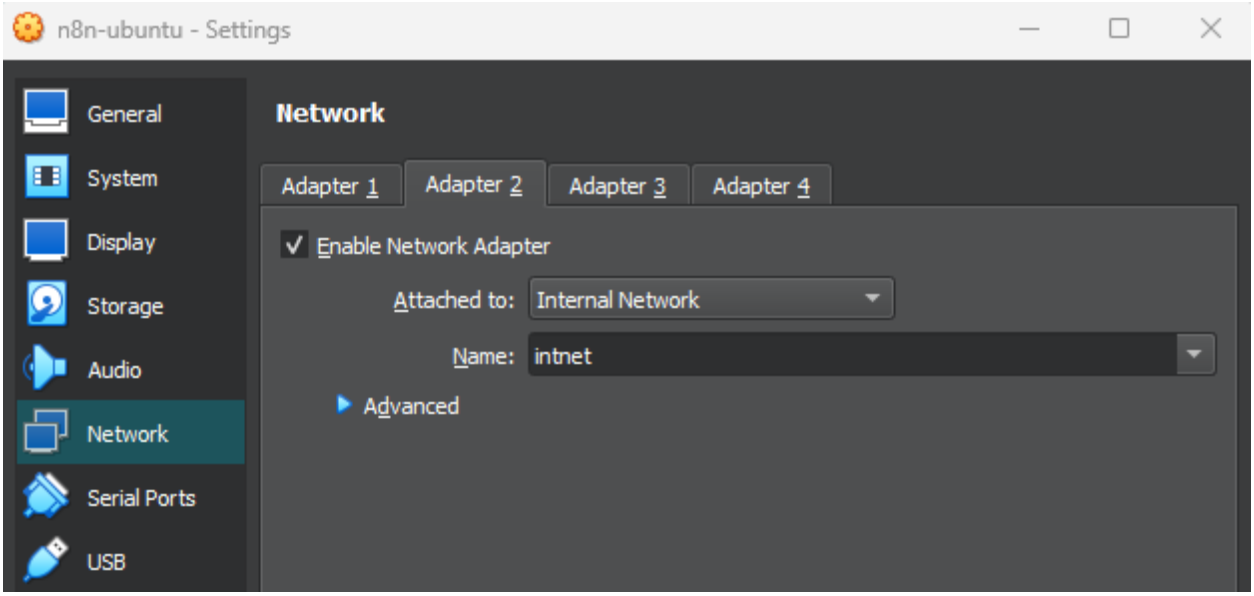
real enterprise environment. The combination of Splunk for detection, n8n for automation, and ChatGPT for analysis demonstrates a modern security monitoring and response workflow.

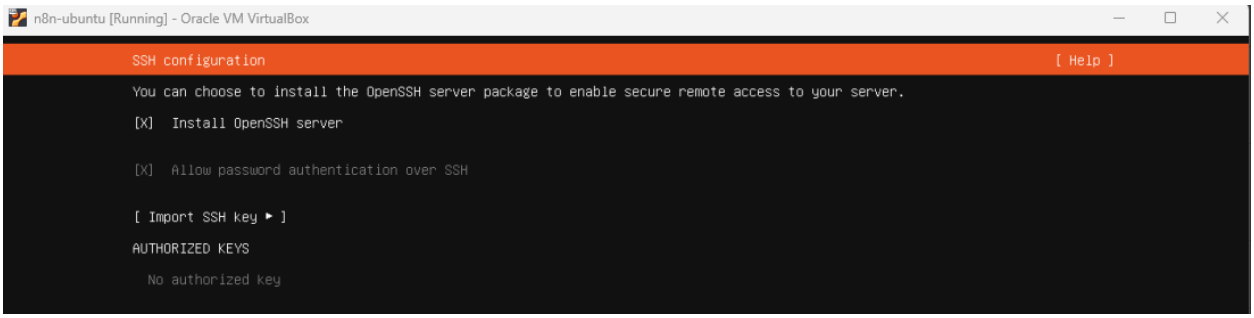


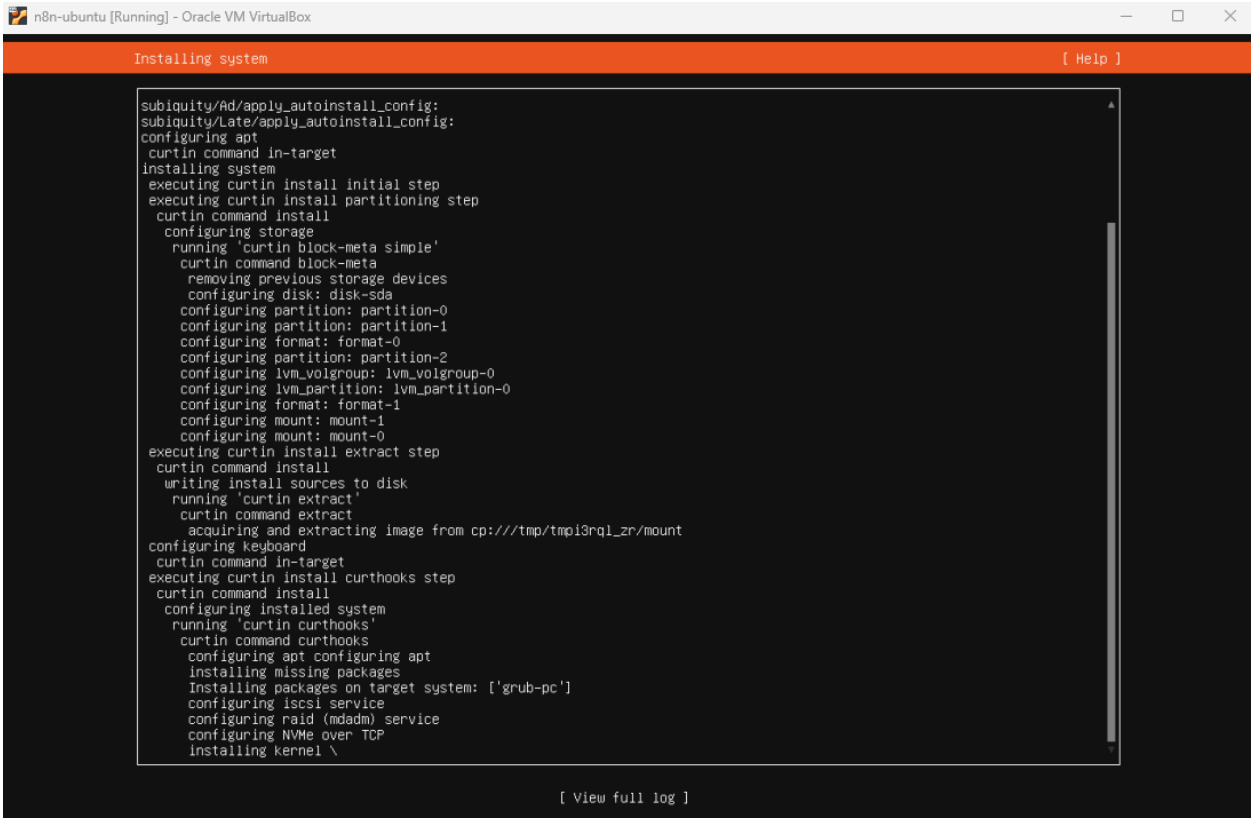


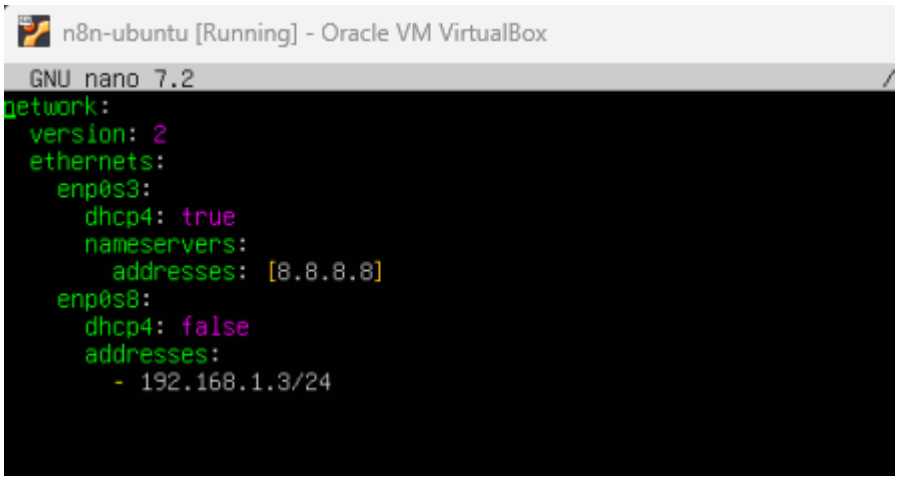

Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Base Memory:
4096 MB
4 MB
49152 MB
Processors:
2
1 CPU
12 CPUs
Enable EFI (special OSes only)
Hard Disk


Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Hard Disk
Create a Virtual Hard Disk Now
Hard Disk File Location and Size
B:\VirtualBox Virtual Machines\n8n-ubuntu\n8n-ubuntu.vdi
50,00 GB
4.00 MB
2.00 TB
Hard Disk File Type and Variant
VDI (VirtualBox Disk Image)
Pre-allocate Full Size
Split into 2GB parts
Use an Existing Virtual Hard Disk File
Kali.vdi (Normal, 50.00 GB)
Do Not Add a Virtual Hard Disk


n8n-ubuntu - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
intnet
Advanced


n8n-ubuntu [Running] - Oracle VM VirtualBox
SSH configuration
[Help]
You can choose to install the OpenSSH server package to enable secure remote access to your server.
[X] Install OpenSSH server
[X] Allow password authentication over SSH
[Import SSH key ►]
AUTHORIZED KEYS
No authorized key


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_volgroup: lvm_volgroup-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
```

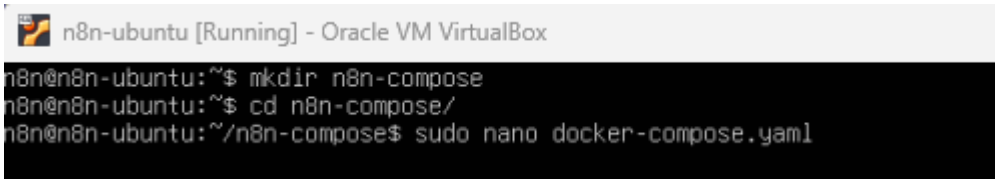
Now that the Ubuntu machine is running and connected to the internal network, n8n will need to be installed.

n8n-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_28.2.2-0ubuntu1~24.04.1_amd64.deb ...
Unpacking docker.io (28.2.2-0ubuntu1~24.04.1) ...
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 (28.2.2-0ubuntu1~24.04.1) ...
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 [Running] - Oracle VM VirtualBox

```
et:7 http://us.archive.ubuntu.com/ubuntu noble/universe amd64 python3-compose all 1.29.2-6ubuntu1 [84.6 kB]
et:8 http://us.archive.ubuntu.com/ubuntu noble/universe amd64 docker-compose all 1.29.2-6ubuntu1 [14.0 kB]
etched 297 kB in 0s (2,976 kB/s)
electing previously unselected package python3-websocket.
(Reading database ... 87792 files and directories currently installed.)
reparing to unpack .../0-python3-websocket_1.7.0-1_all.deb ...
npacking python3-websocket (1.7.0-1) ...
electing previously unselected package python3-docker.
reparing to unpack .../1-python3-docker_5.0.3-1ubuntu1.1_all.deb ...
npacking python3-docker (5.0.3-1ubuntu1.1) ...
electing previously unselected package python3-dockerpty.
reparing to unpack .../2-python3-dockerpty_0.4.1-5_all.deb ...
npacking python3-dockerpty (0.4.1-5) ...
electing previously unselected package python3-docopt.
reparing to unpack .../3-python3-docopt_0.6.2-6_all.deb ...
npacking python3-docopt (0.6.2-6) ...
electing previously unselected package python3-dotenv.
reparing to unpack .../4-python3-dotenv_1.0.1-1_all.deb ...
npacking python3-dotenv (1.0.1-1) ...
electing previously unselected package python3-texttable.
reparing to unpack .../5-python3-texttable_1.6.7-1_all.deb ...
npacking python3-texttable (1.6.7-1) ...
electing previously unselected package python3-compose.
reparing to unpack .../6-python3-compose_1.29.2-6ubuntu1_all.deb ...
npacking python3-compose (1.29.2-6ubuntu1) ...
electing previously unselected package docker-compose.
reparing to unpack .../7-docker-compose_1.29.2-6ubuntu1_all.deb ...
npacking docker-compose (1.29.2-6ubuntu1) ...
etting up python3-dotenv (1.0.1-1) ...
etting up python3-texttable (1.6.7-1) ...
etting up python3-docopt (0.6.2-6) ...
etting up python3-websocket (1.7.0-1) ...
etting up python3-dockerpty (0.4.1-5) ...
etting up python3-docker (5.0.3-1ubuntu1.1) ...
etting up python3-compose (1.29.2-6ubuntu1) ...
etting up docker-compose (1.29.2-6ubuntu1) ...
rocessing triggers for man-db (2.12.0-4build2) ...
canning processes...
canning linux images...

unning kernel seems to be up-to-date.

o services need to be restarted.

o containers need to be restarted.

o user sessions are running outdated binaries.

o VM guests are running outdated hypervisor (qemu) binaries on this host.
8n@n8n-ubuntu:~$
```

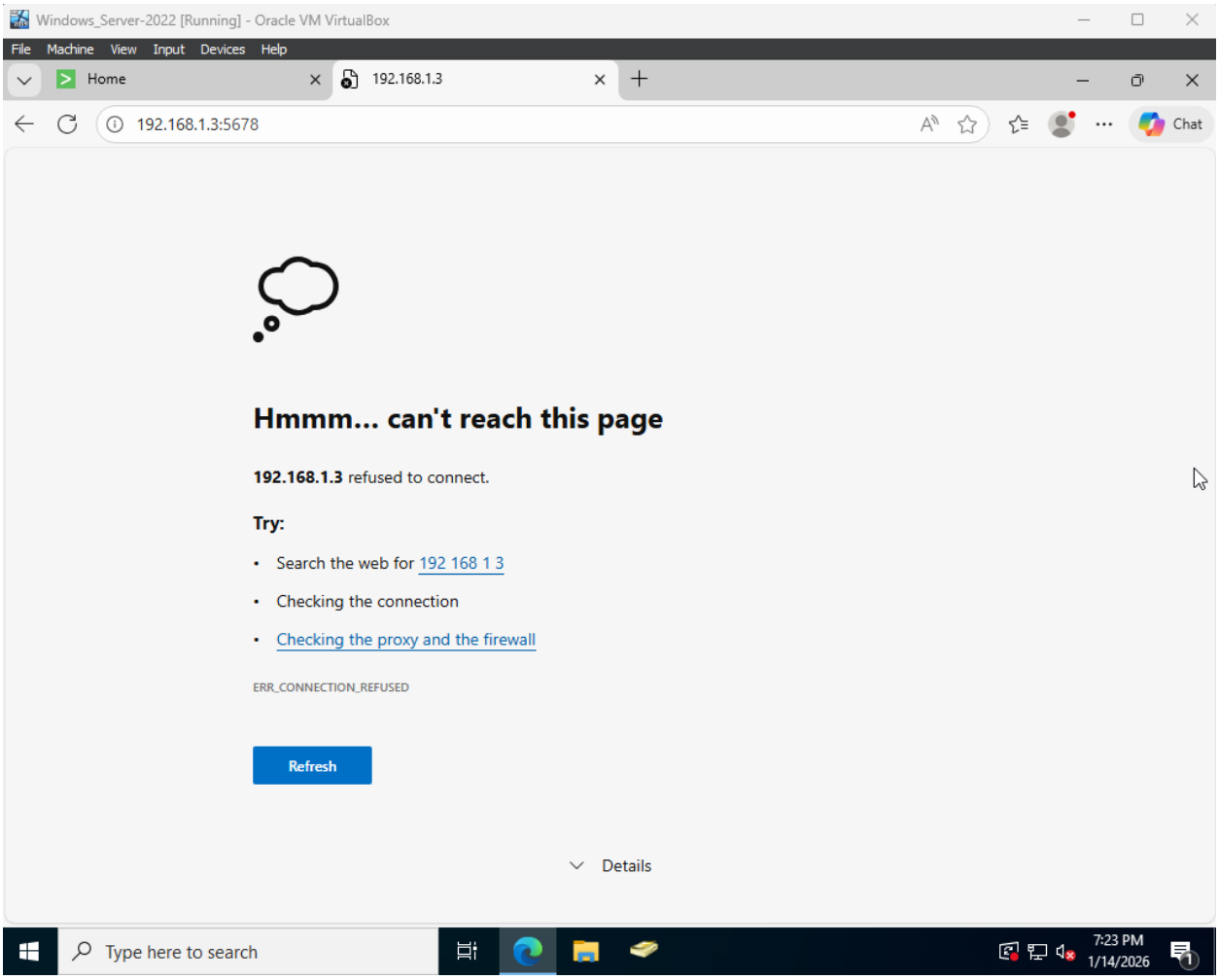


n8n-ubuntu [Running] - Oracle VM VirtualBox

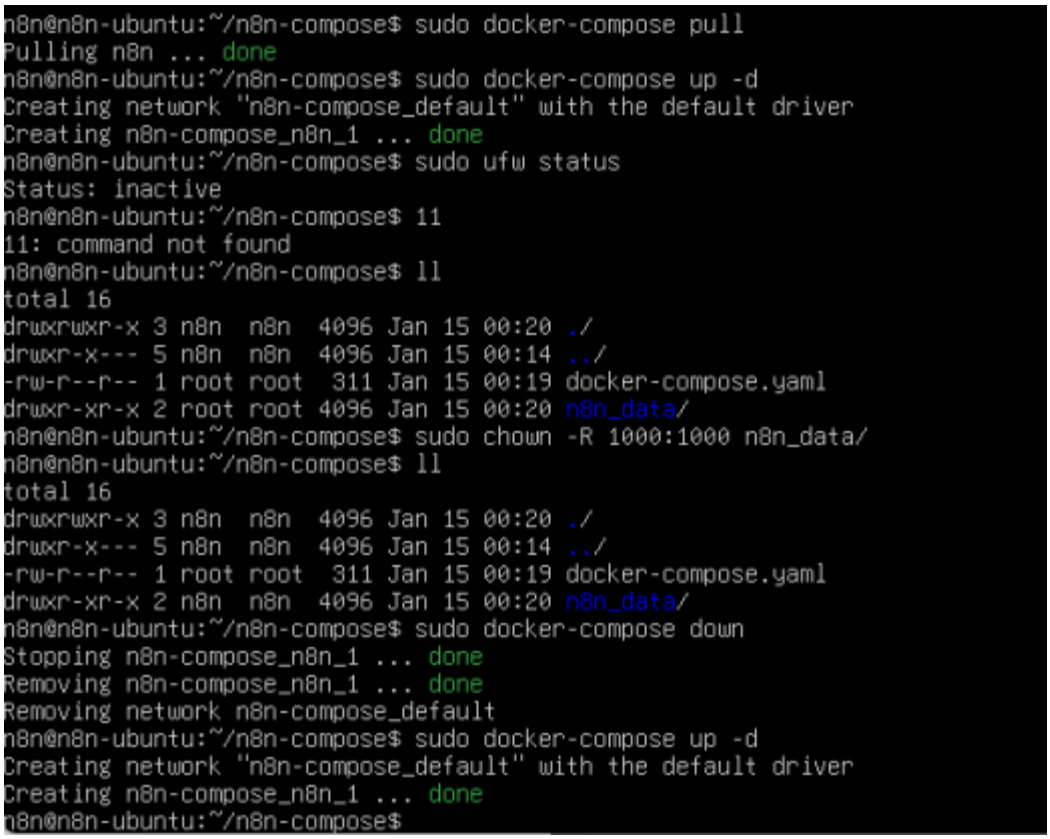
```
  GNU nano 7.2                                                docker-compose.yaml
services:
  n8n:
    image: n8nio/n8n:latest
    restart: always
    ports:
      - "5678:5678"
    environment:
      - N8N_HOST=192.168.1.3
      - N8N_PORT=5678
      - N8N_PROTOCOL=http
      - N8N_SECURE_COOKIE-false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

```
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$
```

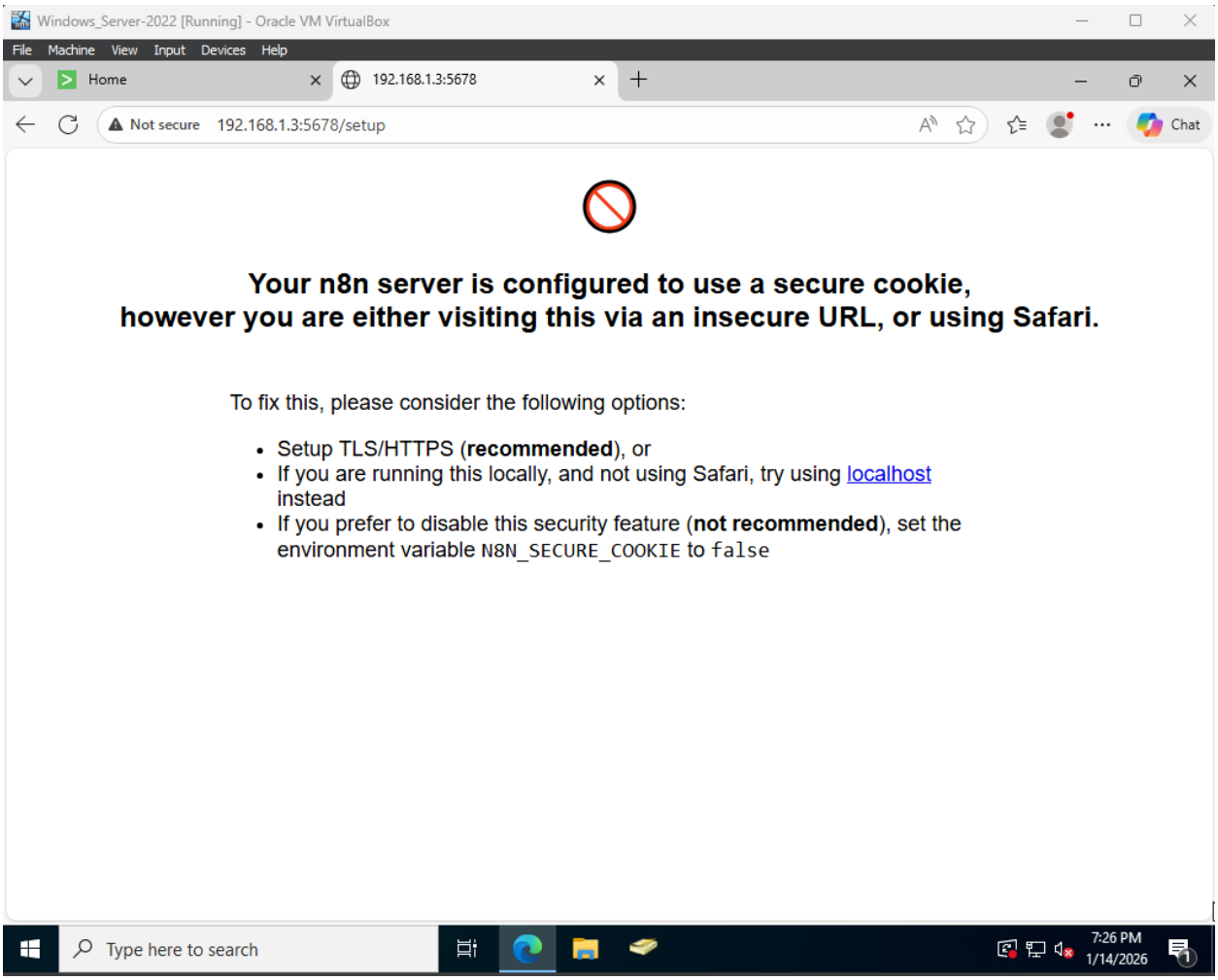
Now that the n8n is installed and running, I will access it through the server.

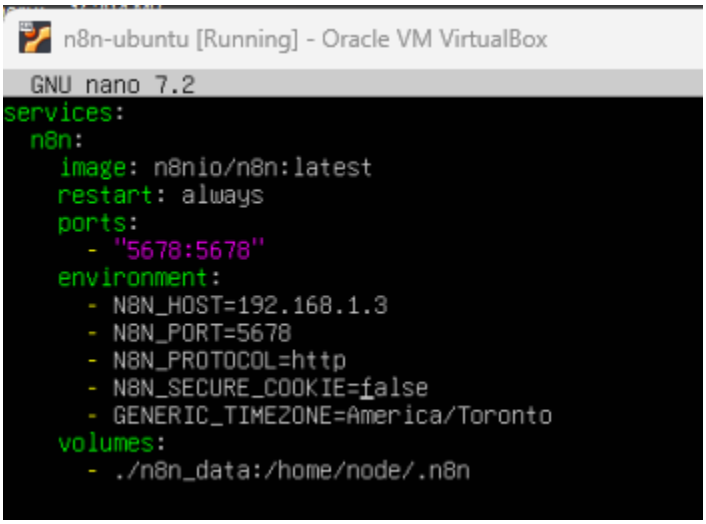


As you can see, I ran into an issue when attempting to access the servers' n8n service.

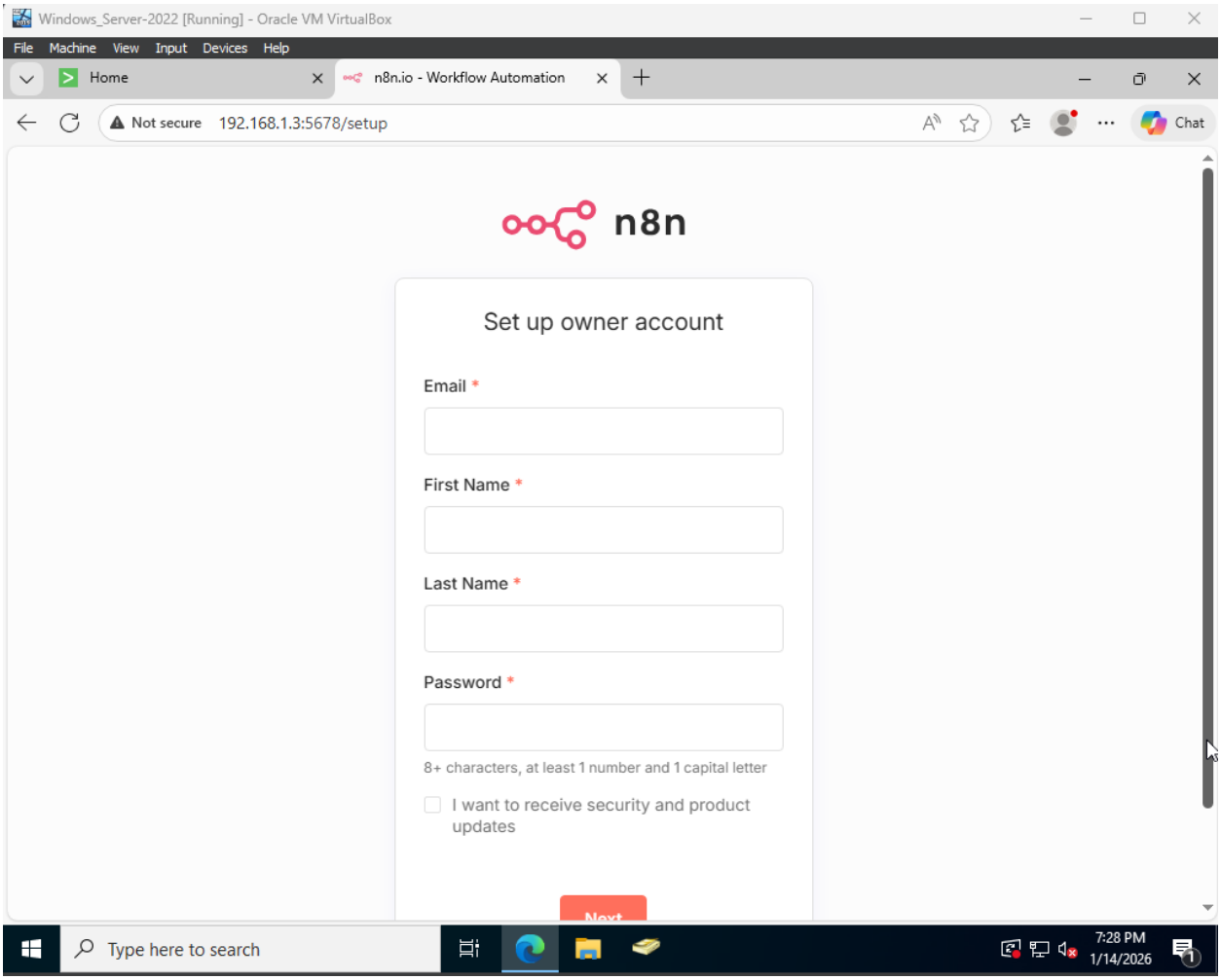


I was able to fix the issue, but then I ran into a different one.

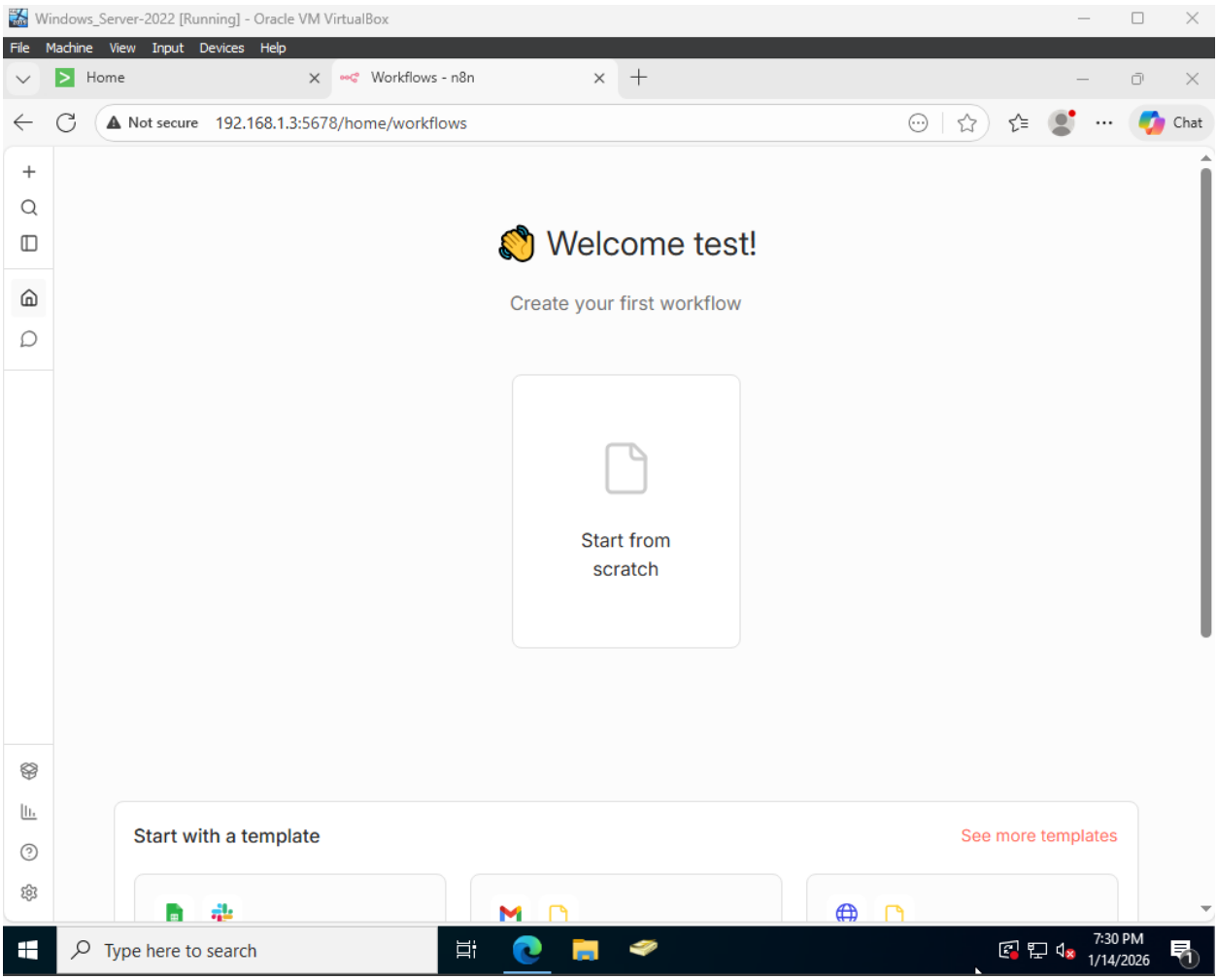




I found that I had accidentally entered a – sign instead of an = sign int the .yaml file.

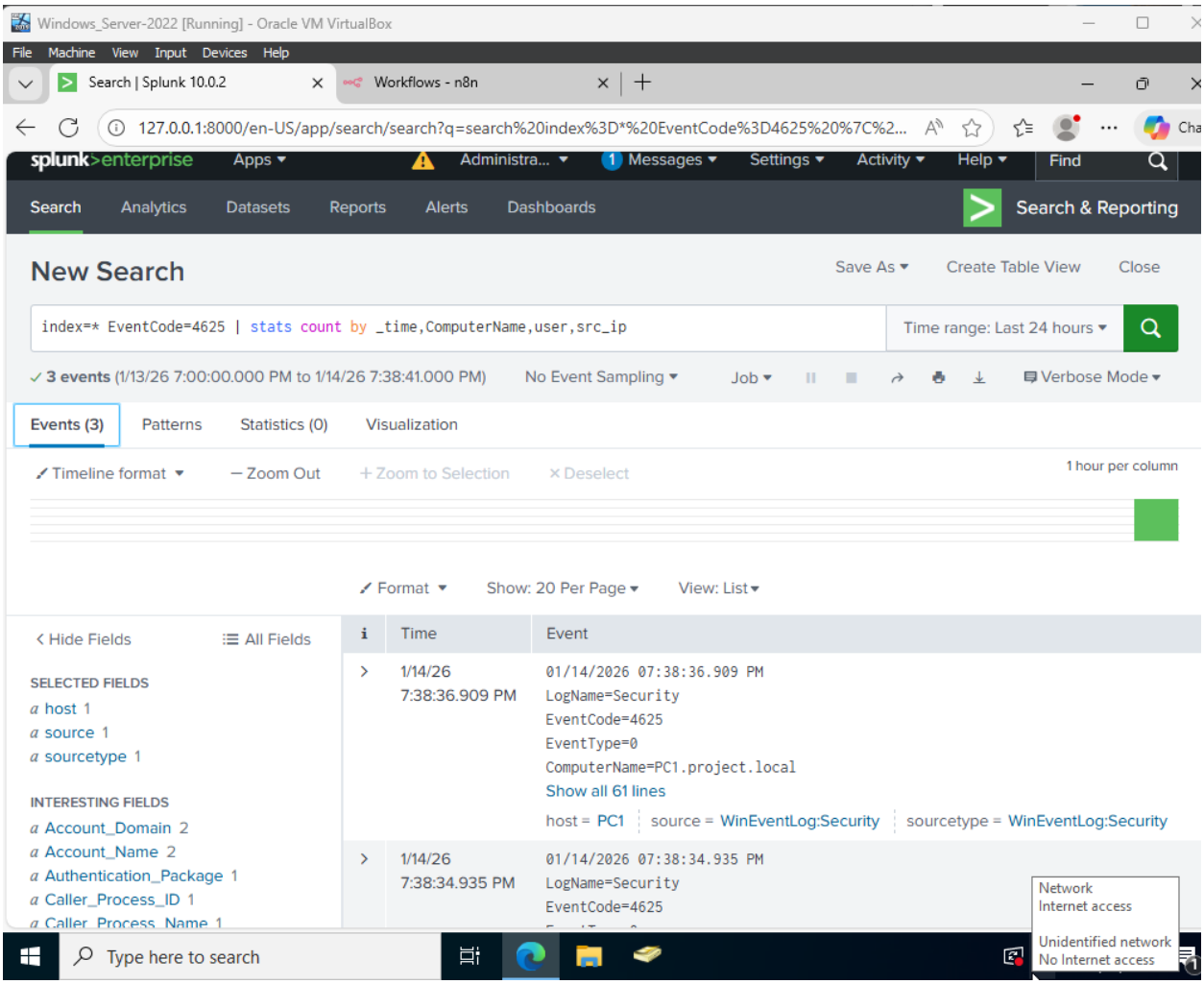


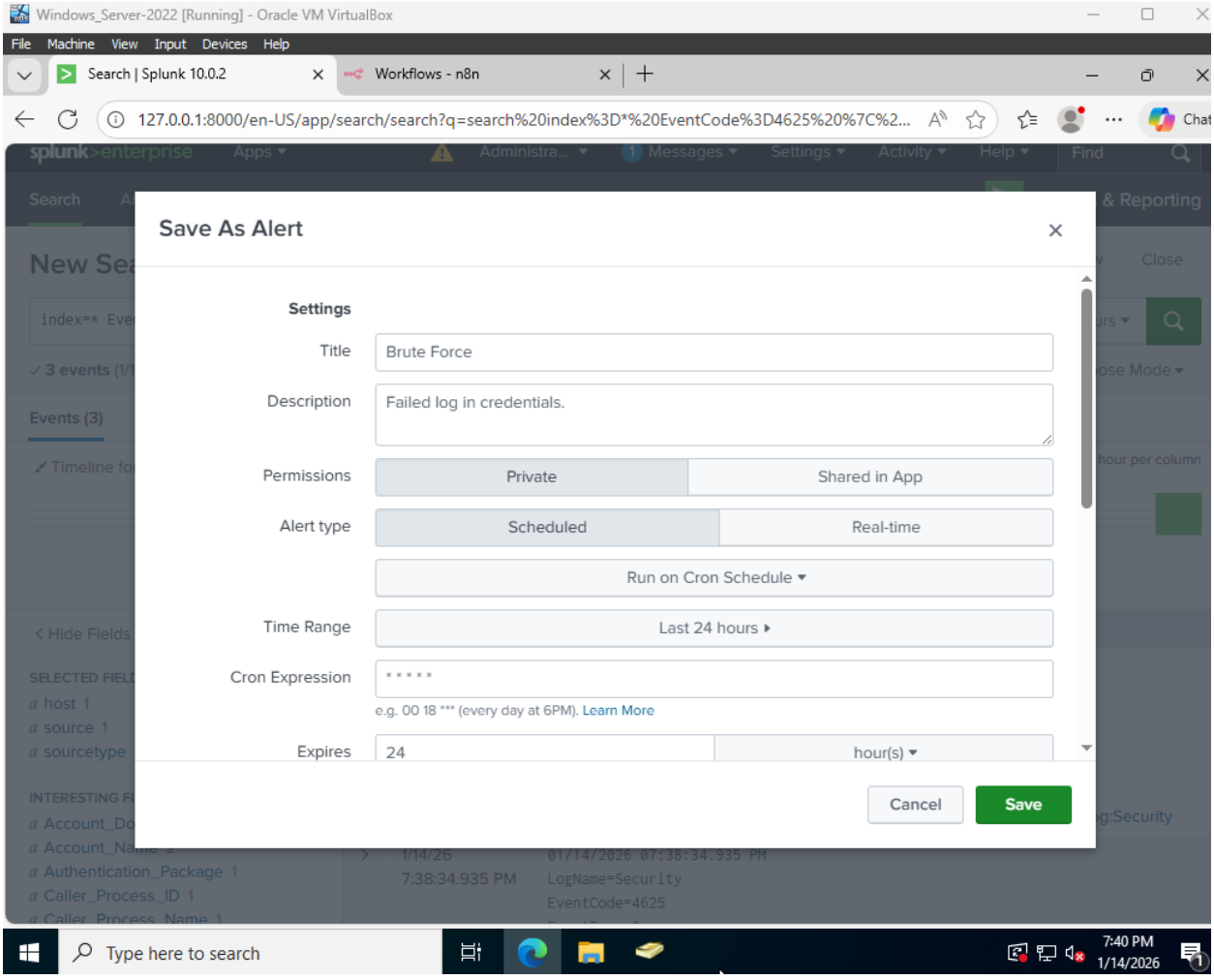
The service is now running and I can continue the setup.

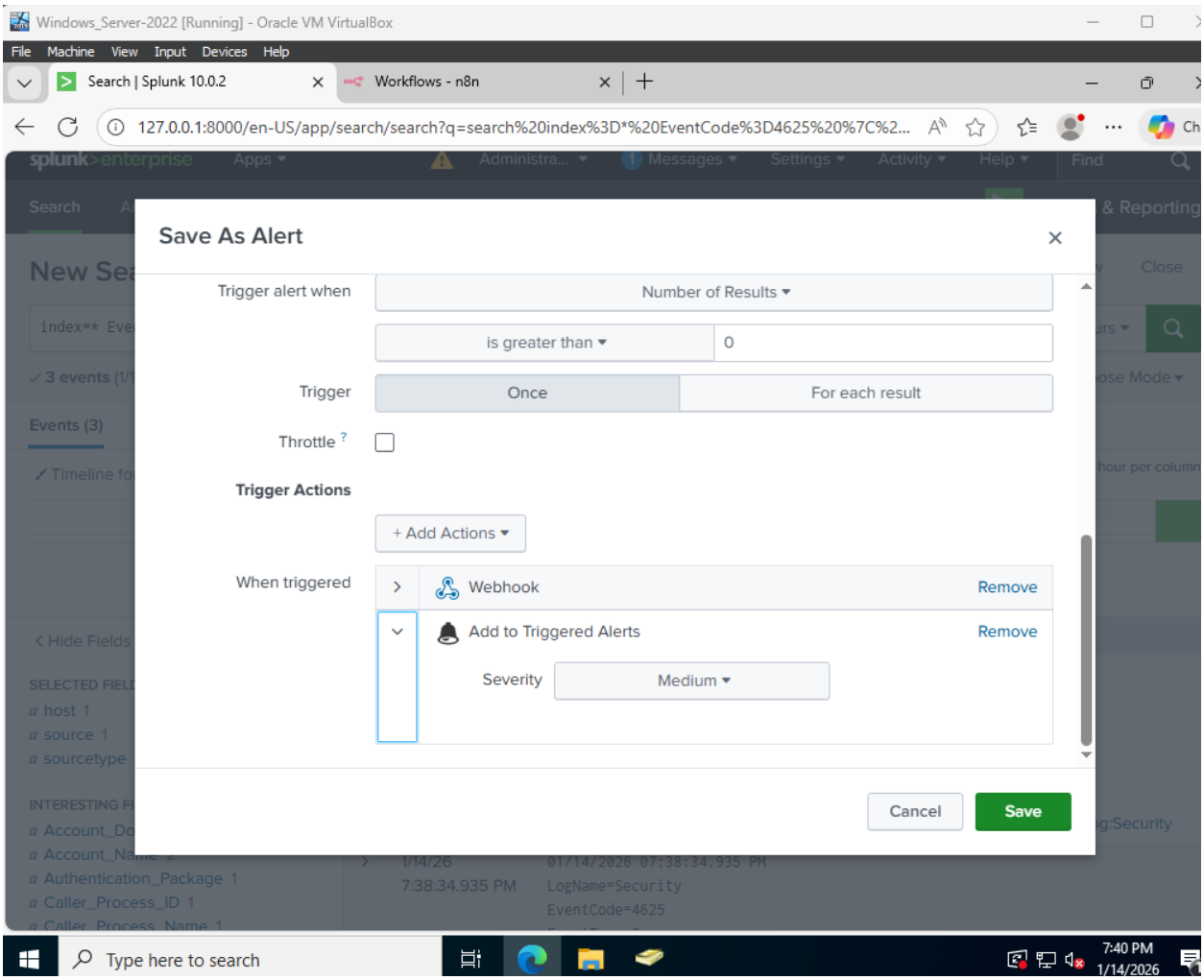


Creating a Splunk Alert

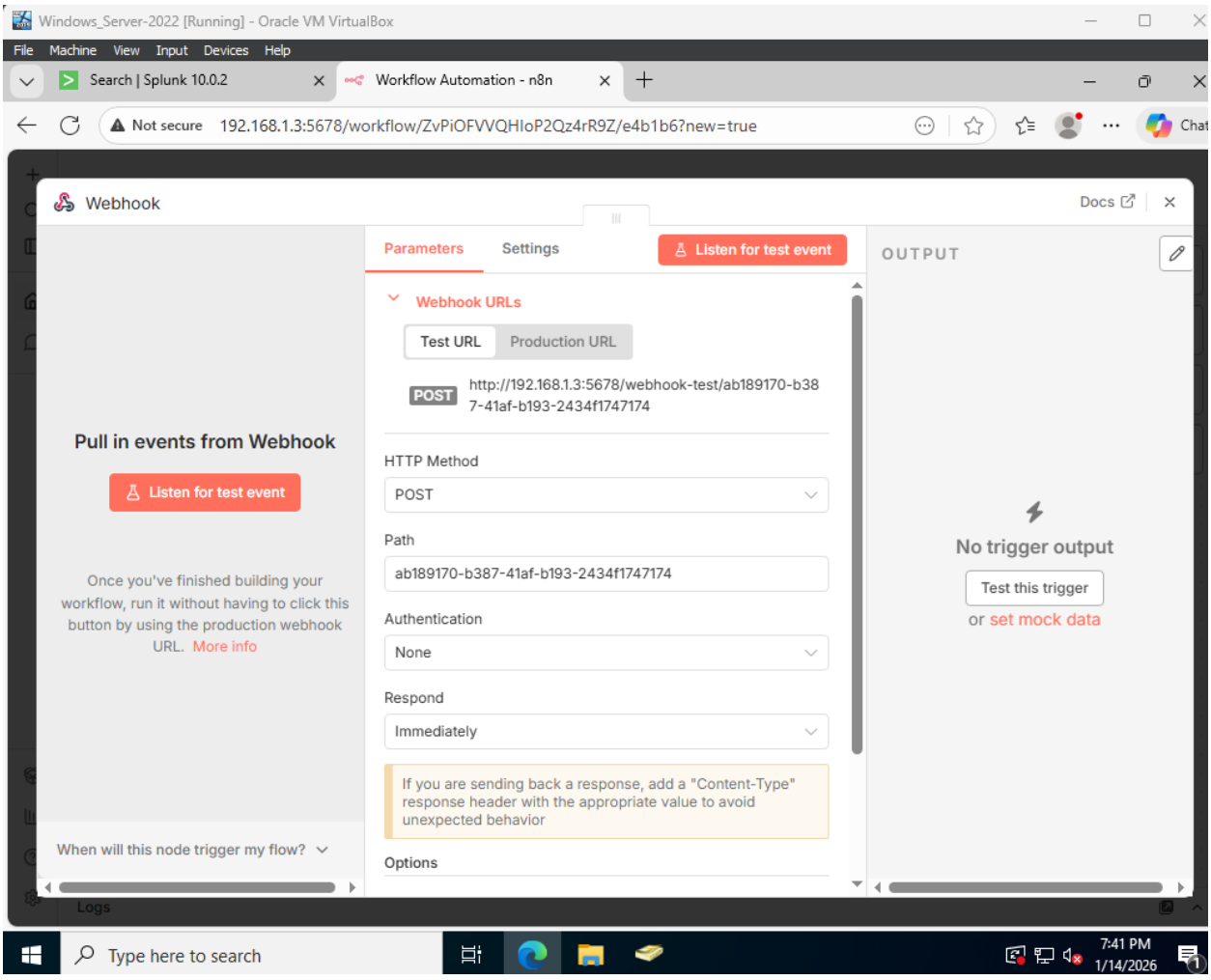
Before continuing with the n8n automation, a Splunk alert must first be created. This alert will act as the trigger for the workflow by identifying relevant security events within the collected log data. Establishing the alert ensures that meaningful events are detected and passed forward for automated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

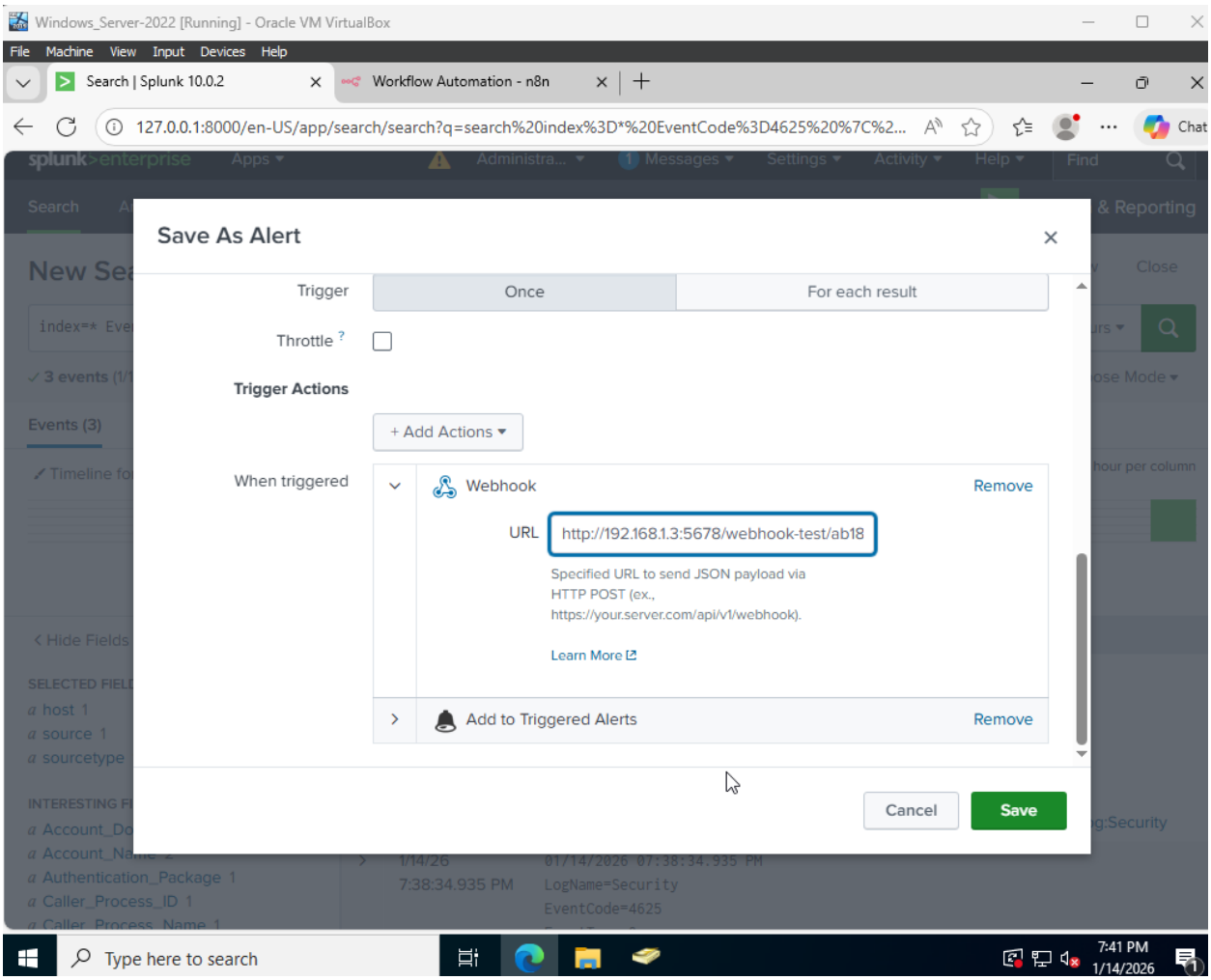

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Search | Splunk 10.0.2
Workflows - n8n
127.0.0.1:8000/en-US/app/search/search?q=search%20index%3D*%20EventCode%3D4625%20%7C%2...
splunk>enterprise
Apps
Administra...
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
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
Verbose Mode
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
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
Time
Event
1/14/26 7:38:36.909 PM
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 7:38:34.935 PM
01/14/2026 07:38:34.935 PM
LogName=Security
EventCode=4625
Network
Internet access
Unidentified network
No Internet access
Type here to search


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...
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
Type here to search
7:40 PM
1/14/2026

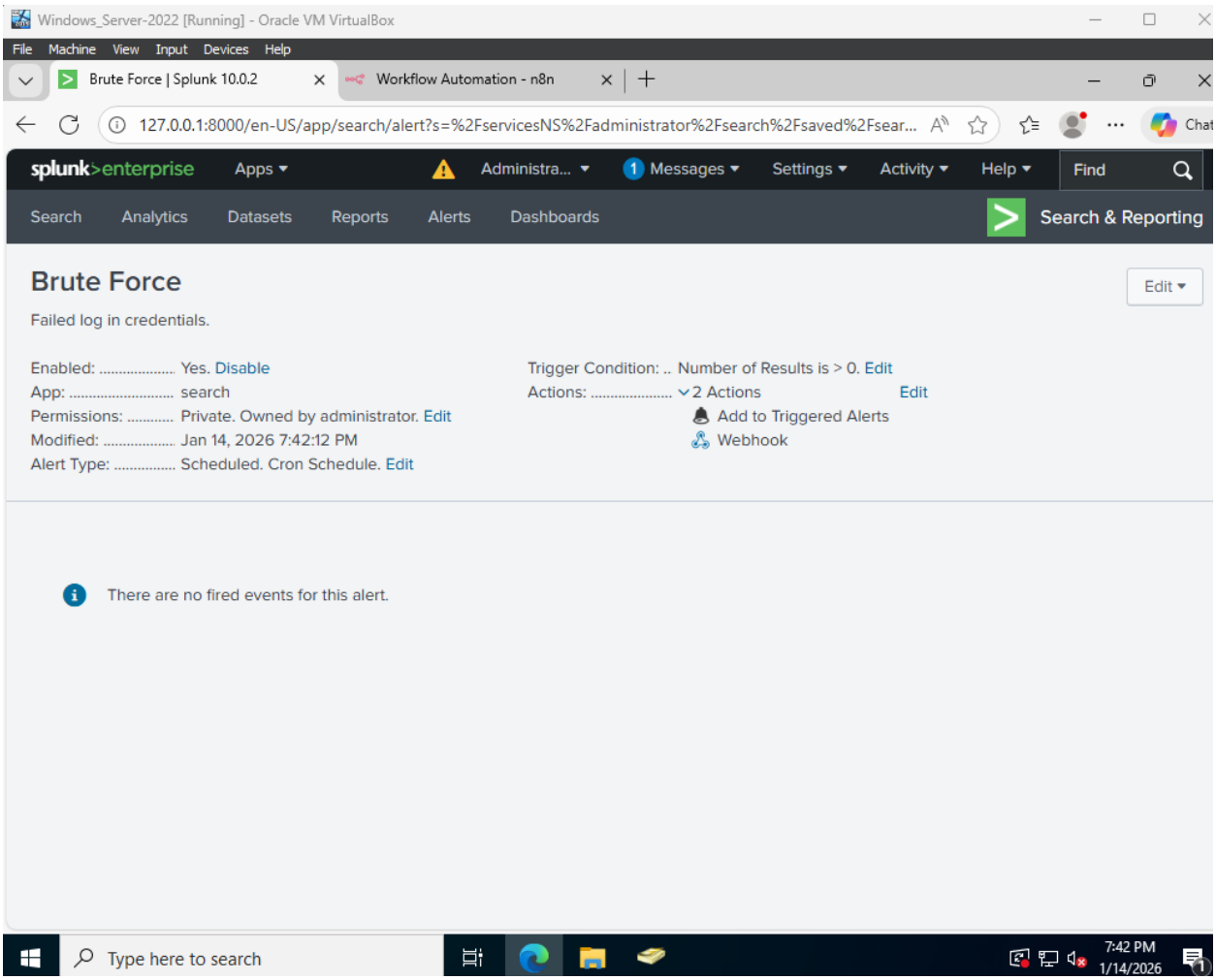


I will use the WebHook node to attach it to the alert. This will allow Splunk to send alerts to n8n.

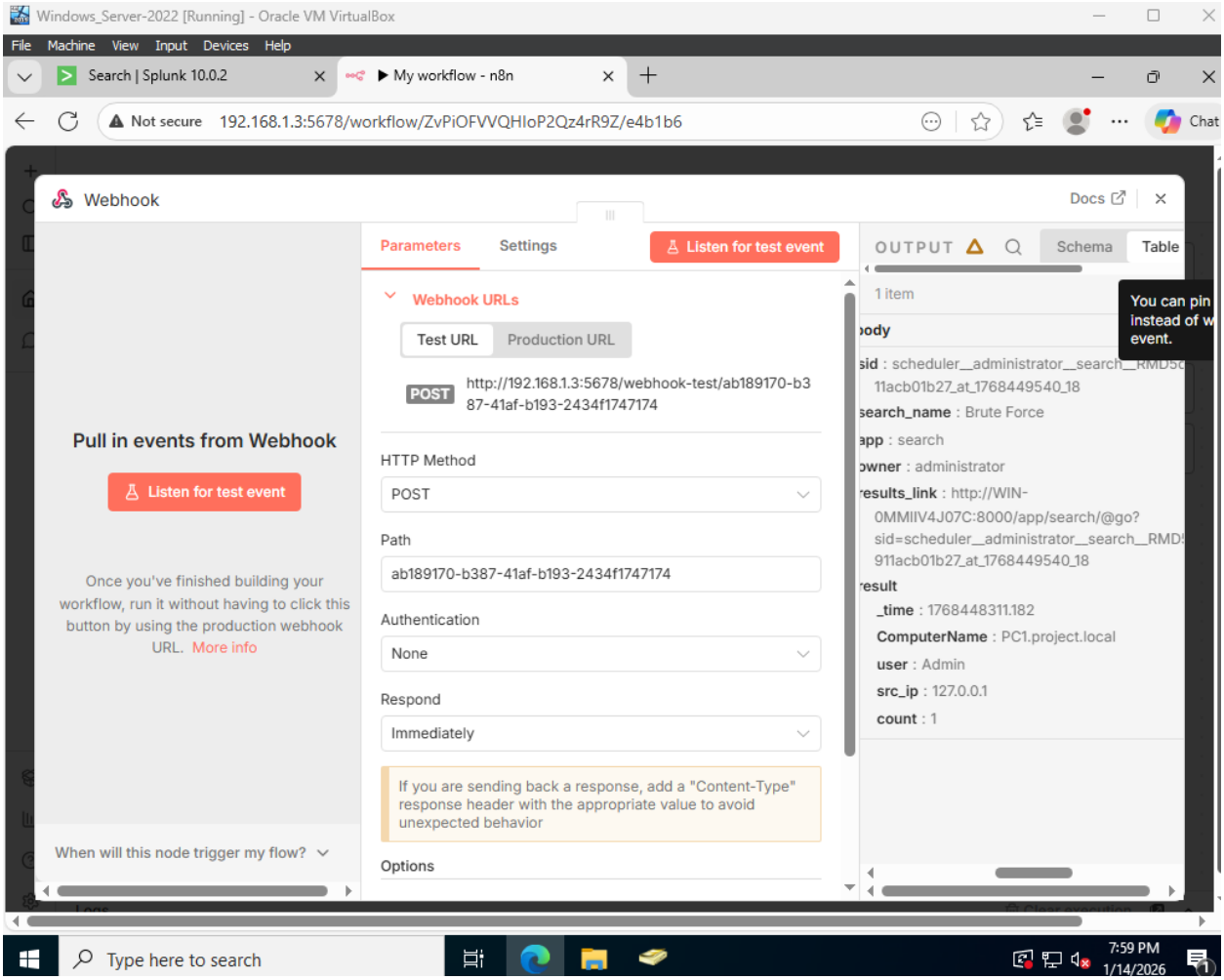

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Search | Splunk 10.0.2
Workflow Automation - n8n
Not secure 192.168.1.3:5678/workflow/ZvPiOFVVQHIoP2Qz4rR9Z/e4b1b6?new=true
Webhook
Docs
Parameters
Settings
Listen for test event
OUTPUT
Webhook URLs
Test URL
Production 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
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?
No trigger output
Test this trigger
or set mock data
Logs
Type here to search
7:41 PM
1/14/2026



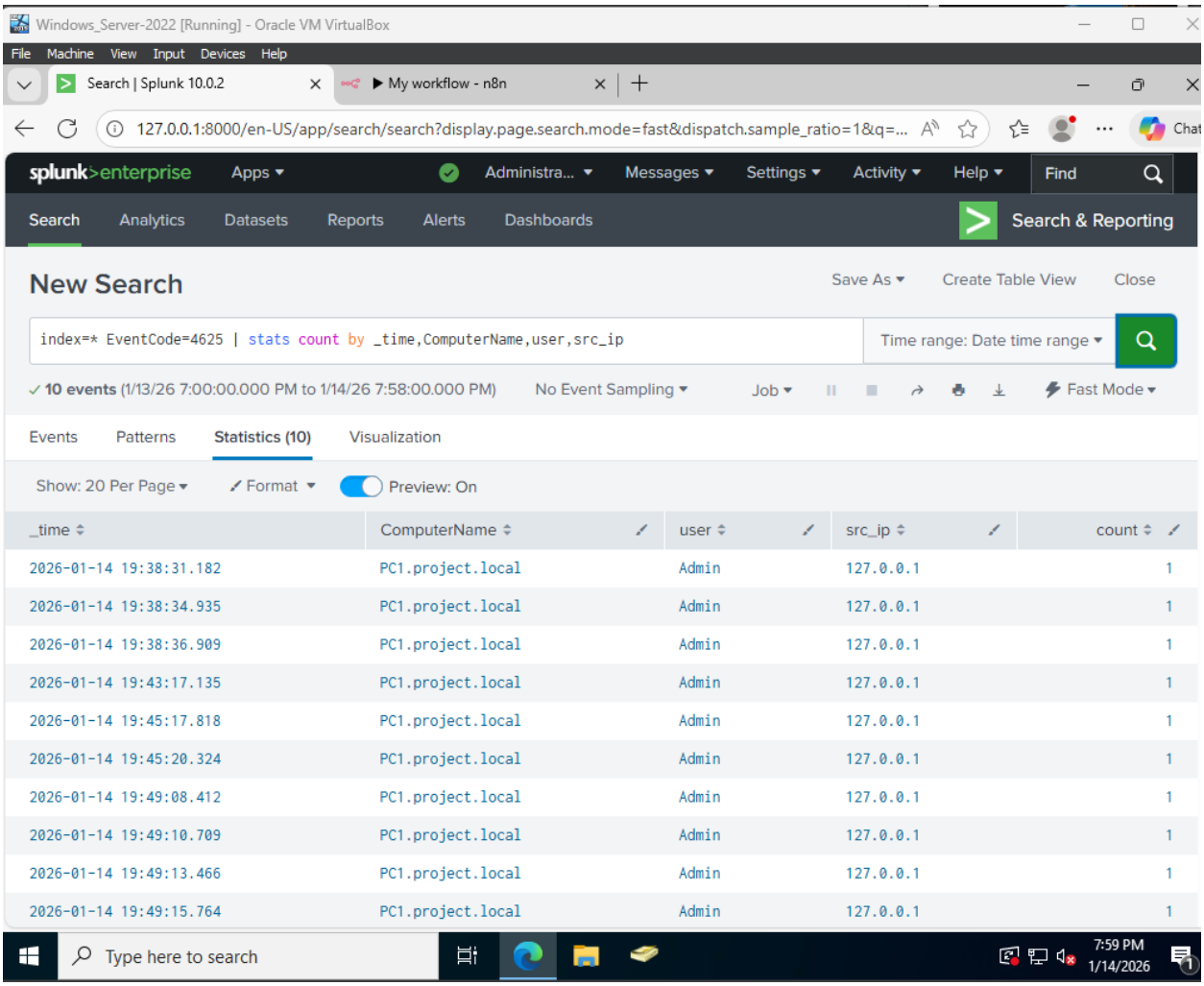
As you can see, the alert has been created.

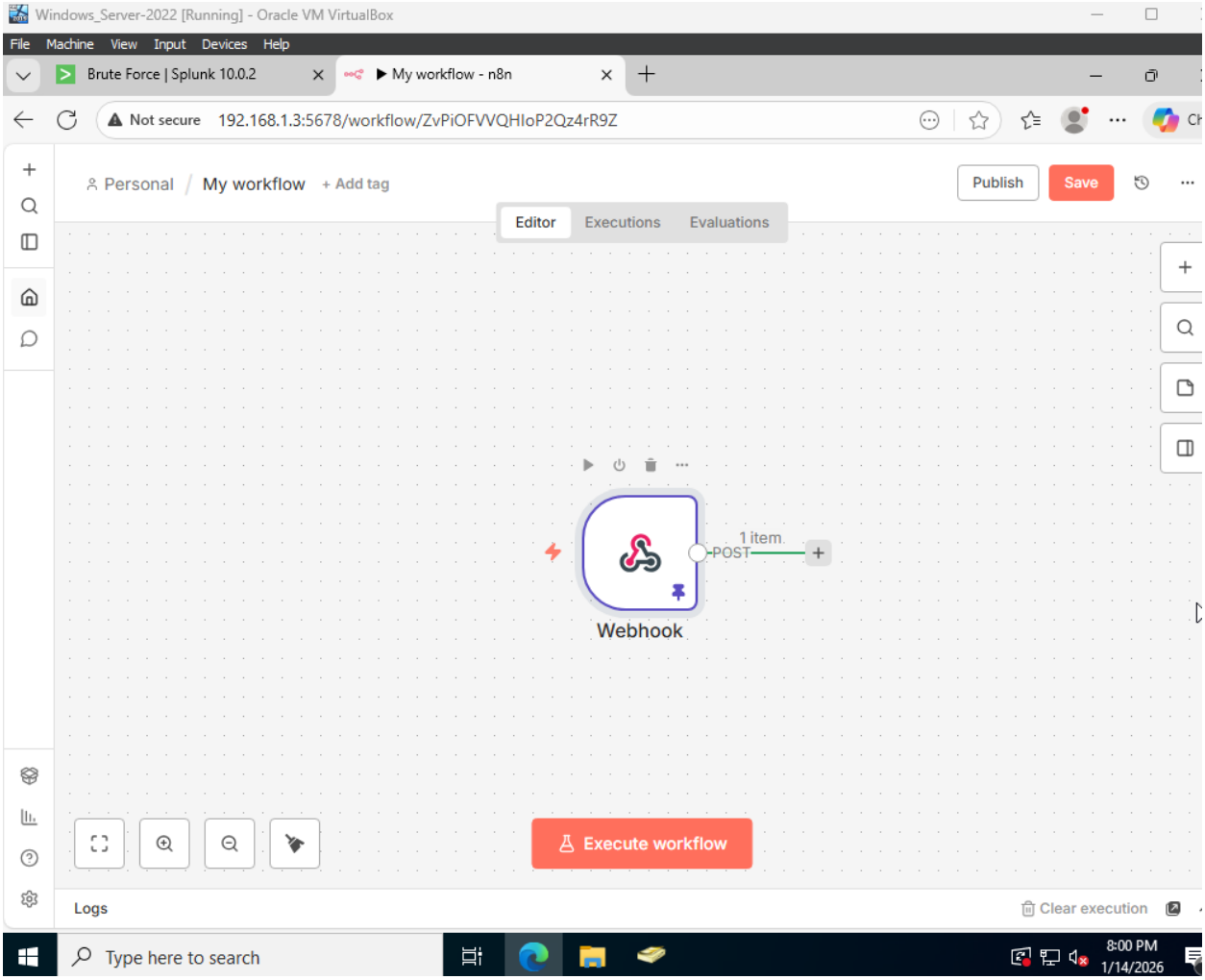


After listening for a test event, the n8n node was able to detect the alert and produce the output.

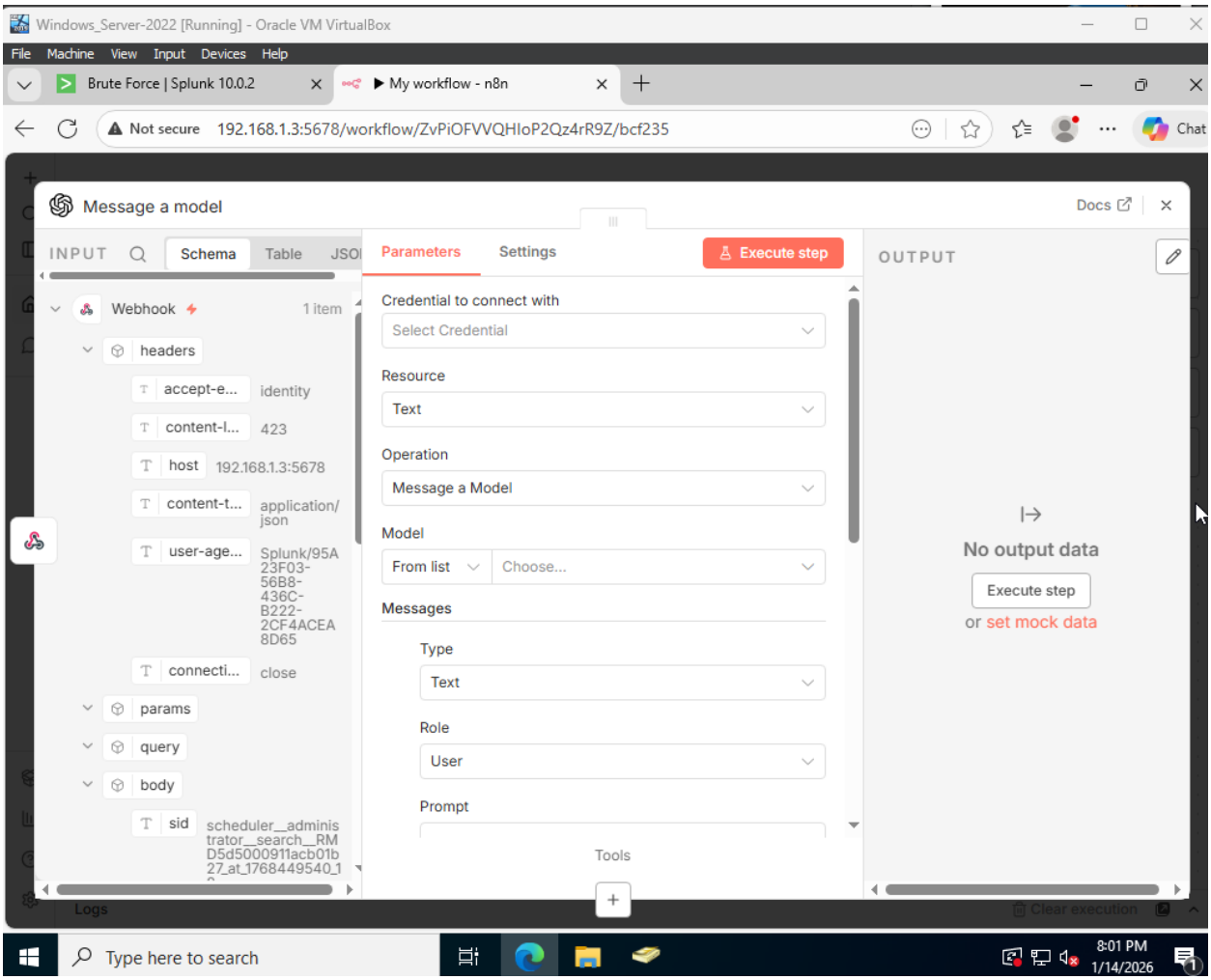


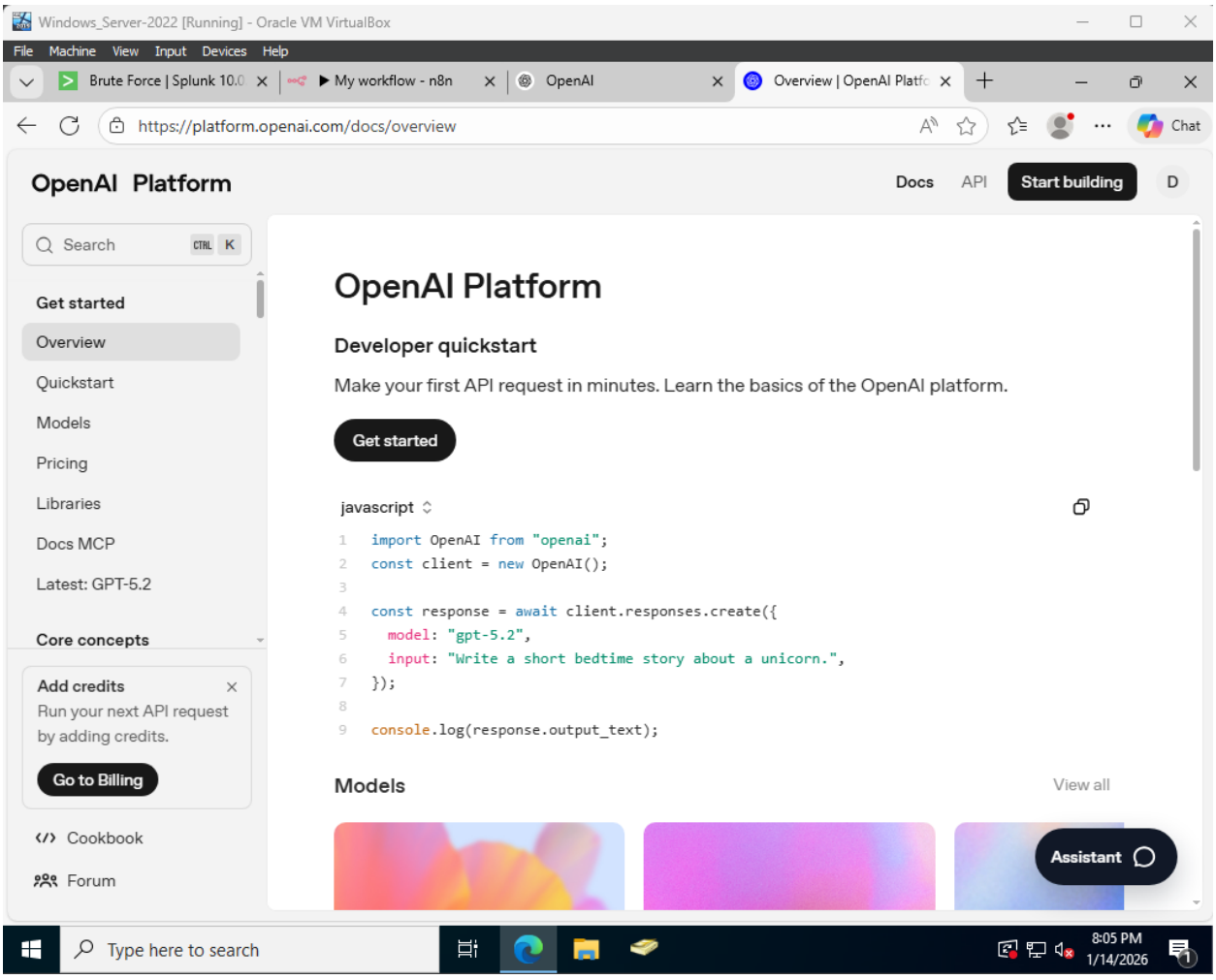
Here is the search of the alert showing all the logs:

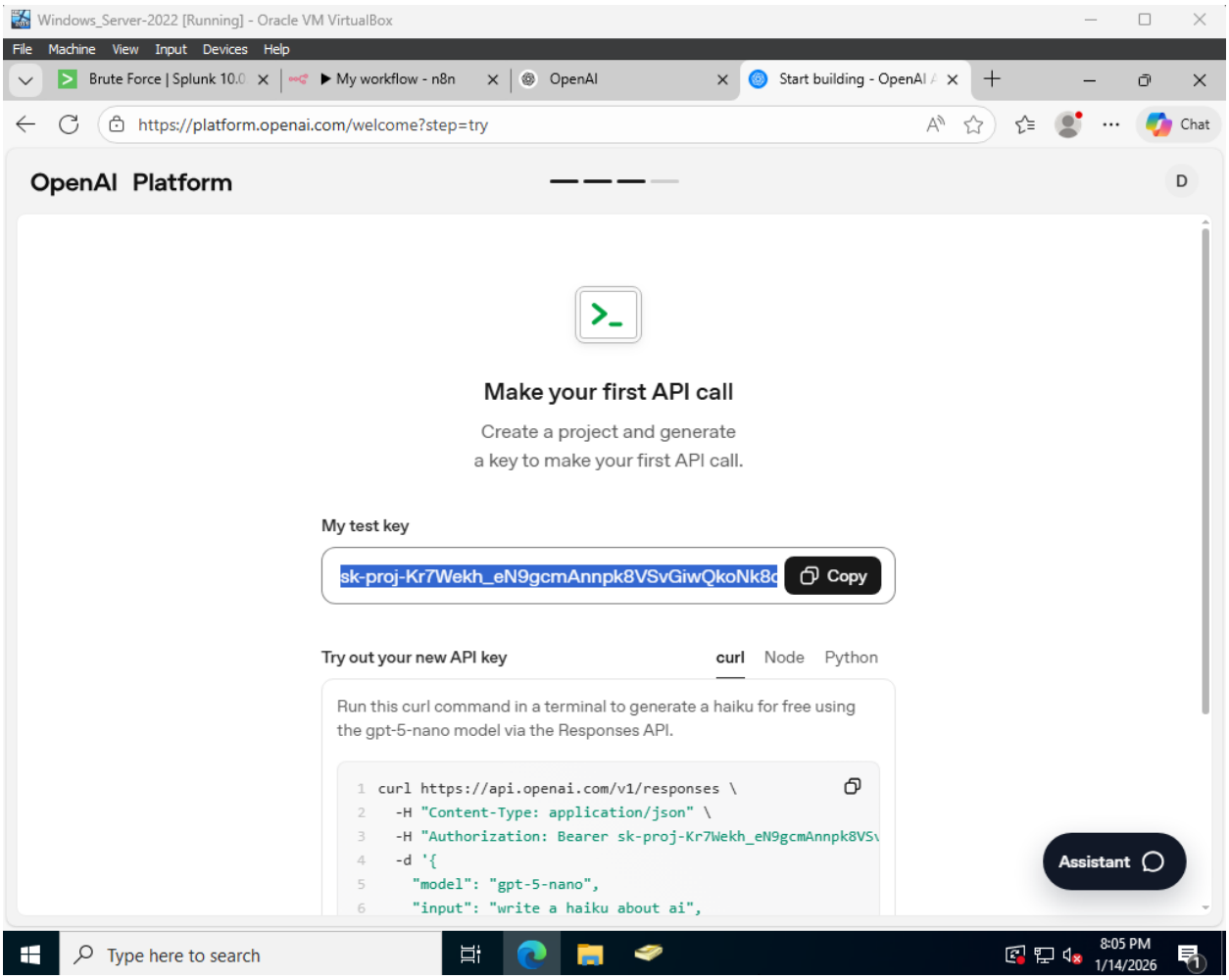

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Search | Splunk 10.0.2
My workflow - n8n
127.0.0.1:8000/en-US/app/search/search?display.page.search.mode=fast&dispatch.sample_ratio=1&q=...
splunk>enterprise
Apps
Administra...
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=* EventCode=4625 | stats count by _time,ComputerName,user,src_ip
Time range: Date time range
10 events (1/13/26 7:00:00.000 PM to 1/14/26 7:58:00.000 PM)
No Event Sampling
Job
Fast Mode
Events
Patterns
Statistics (10)
Visualization
Show: 20 Per Page
Format
Preview: On
_time
ComputerName
user
src_ip
count
2026-01-14 19:38:31.182 PC1.project.local Admin 127.0.0.1 1
2026-01-14 19:38:34.935 PC1.project.local Admin 127.0.0.1 1
2026-01-14 19:38:36.909 PC1.project.local Admin 127.0.0.1 1
2026-01-14 19:43:17.135 PC1.project.local Admin 127.0.0.1 1
2026-01-14 19:45:17.818 PC1.project.local Admin 127.0.0.1 1
2026-01-14 19:45:20.324 PC1.project.local Admin 127.0.0.1 1
2026-01-14 19:49:08.412 PC1.project.local Admin 127.0.0.1 1
2026-01-14 19:49:10.709 PC1.project.local Admin 127.0.0.1 1
2026-01-14 19:49:13.466 PC1.project.local Admin 127.0.0.1 1
2026-01-14 19:49:15.764 PC1.project.local Admin 127.0.0.1 1
Type here to search
7:59 PM
1/14/2026



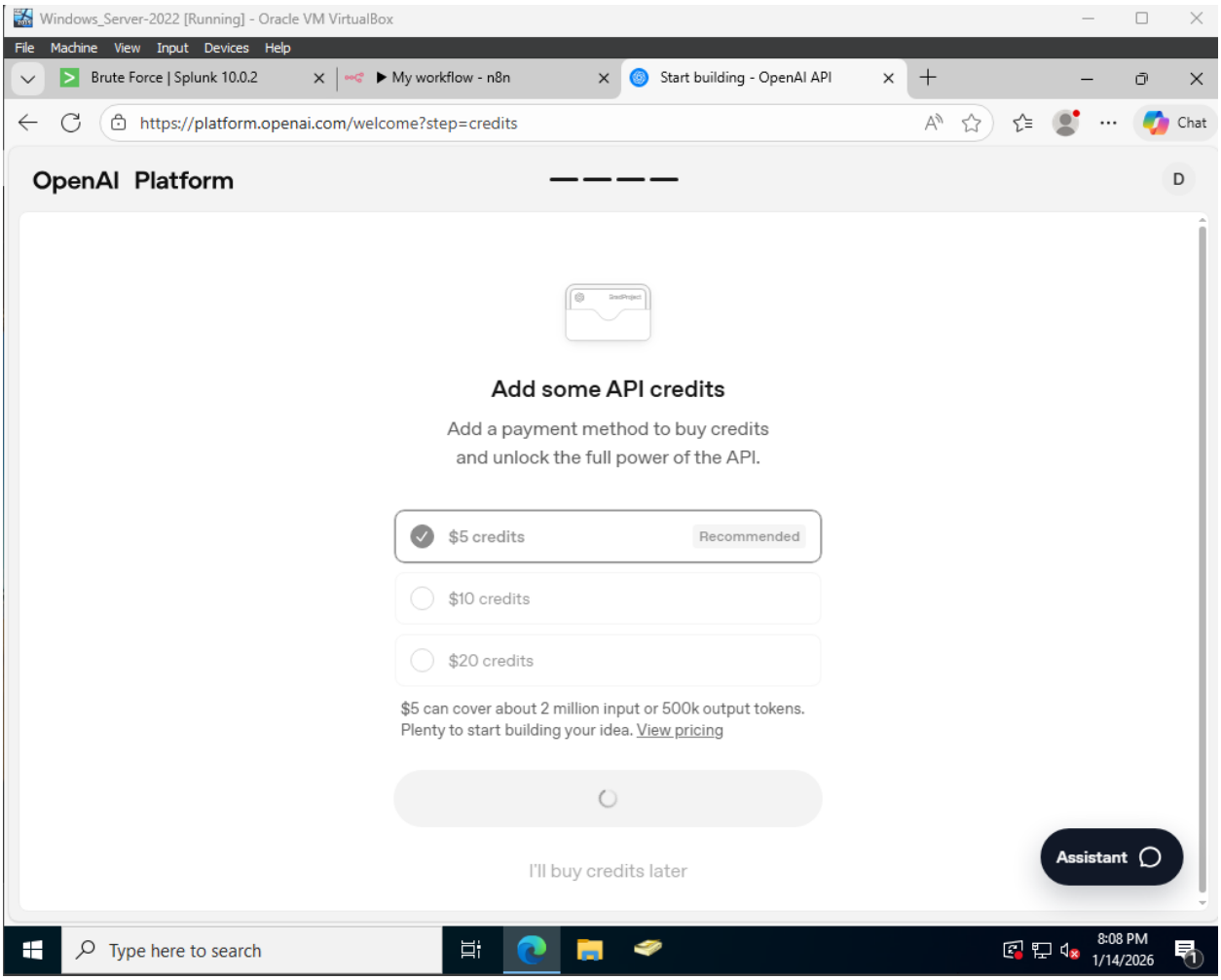
I will now integrate ChatGPT as the AI. To do this I needed to add the OpenAI node and configure it.


Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Brute Force | Splunk 10.0.2
My workflow - n8n
Not secure 192.168.1.3:5678/workflow/ZvPiOFVVQHIoP2Qz4rR9Z/bcf235
Chat
Message a model
Docs
INPUT
Schema
Table
Parameters
Settings
Execute step
OUTPUT
Webhook
1 item
headers
accept-e...
identity
content-l...
423
host
192.168.1.3:5678
content-t...
application/json
user-age...
Splunk/95A23F03-56B8-436C-B222-2CF4ACEA8D65
connecti...
close
params
query
body
sid
scheduler__administrator__search__RMD5d5000911acb01b27_at_1768449540_1
Credential to connect with
Select Credential
Resource
Text
Operation
Message a Model
Model
From list
Choose...
Messages
Type
Text
Role
User
Prompt
Tools
No output data
Execute step
or set mock data
Logs
Clear execution
Type here to search
8:01 PM
1/14/2026

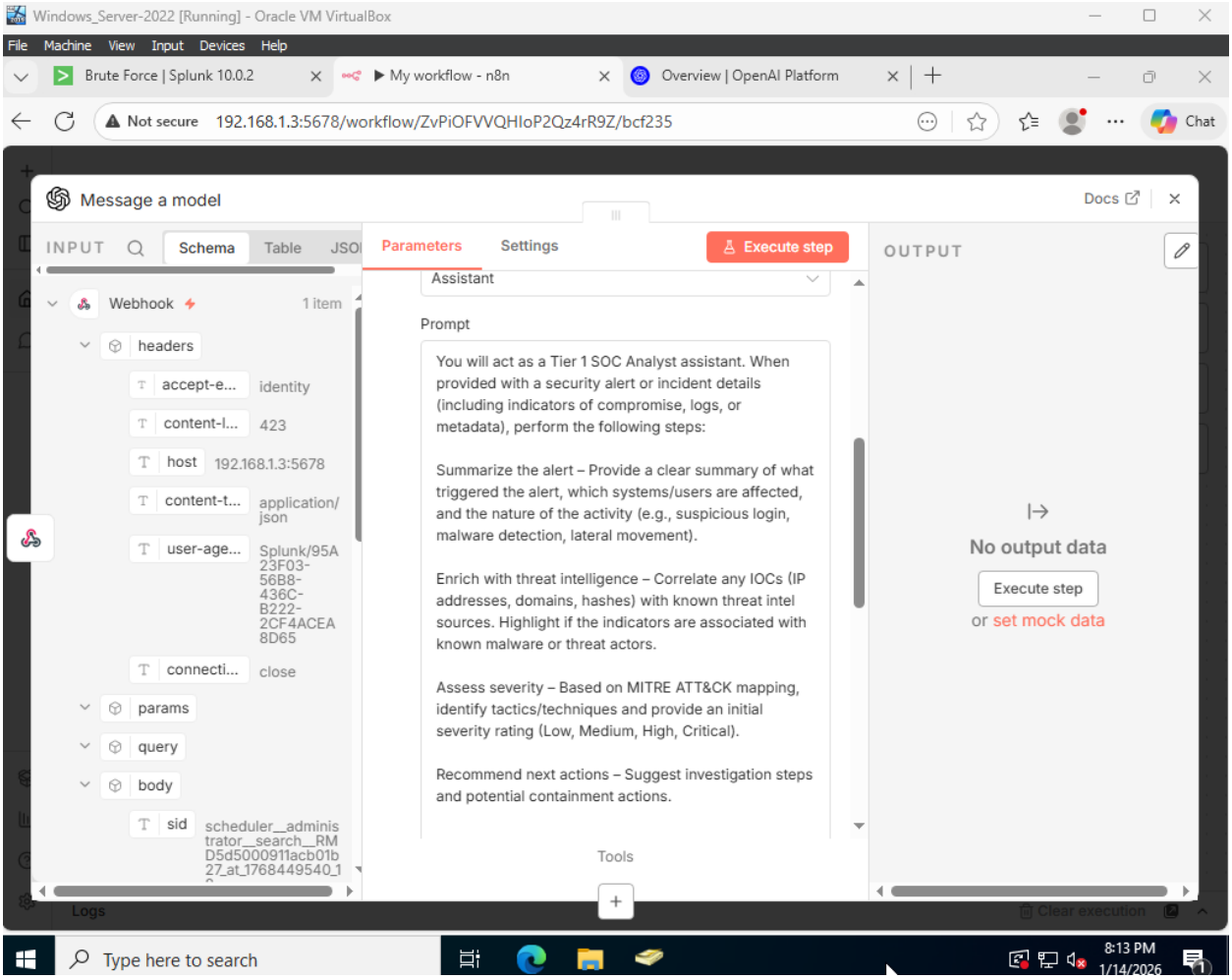

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Brute Force | Splunk 10.0
My workflow - n8n
OpenAI
Overview | OpenAI Platfc
https://platform.openai.com/docs/overview
Chat
OpenAI Platform
Docs
API
Start building
D
Search
CTRL K
Get started
Overview
Quickstart
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
import OpenAI from "openai";
const client = new OpenAI();
const response = await client.responses.create({
model: "gpt-5.2",
input: "Write a short bedtime story about a unicorn.",
});
console.log(response.output_text);
Models
View all
Assistant
Type here to search
8:05 PM
1/14/2026

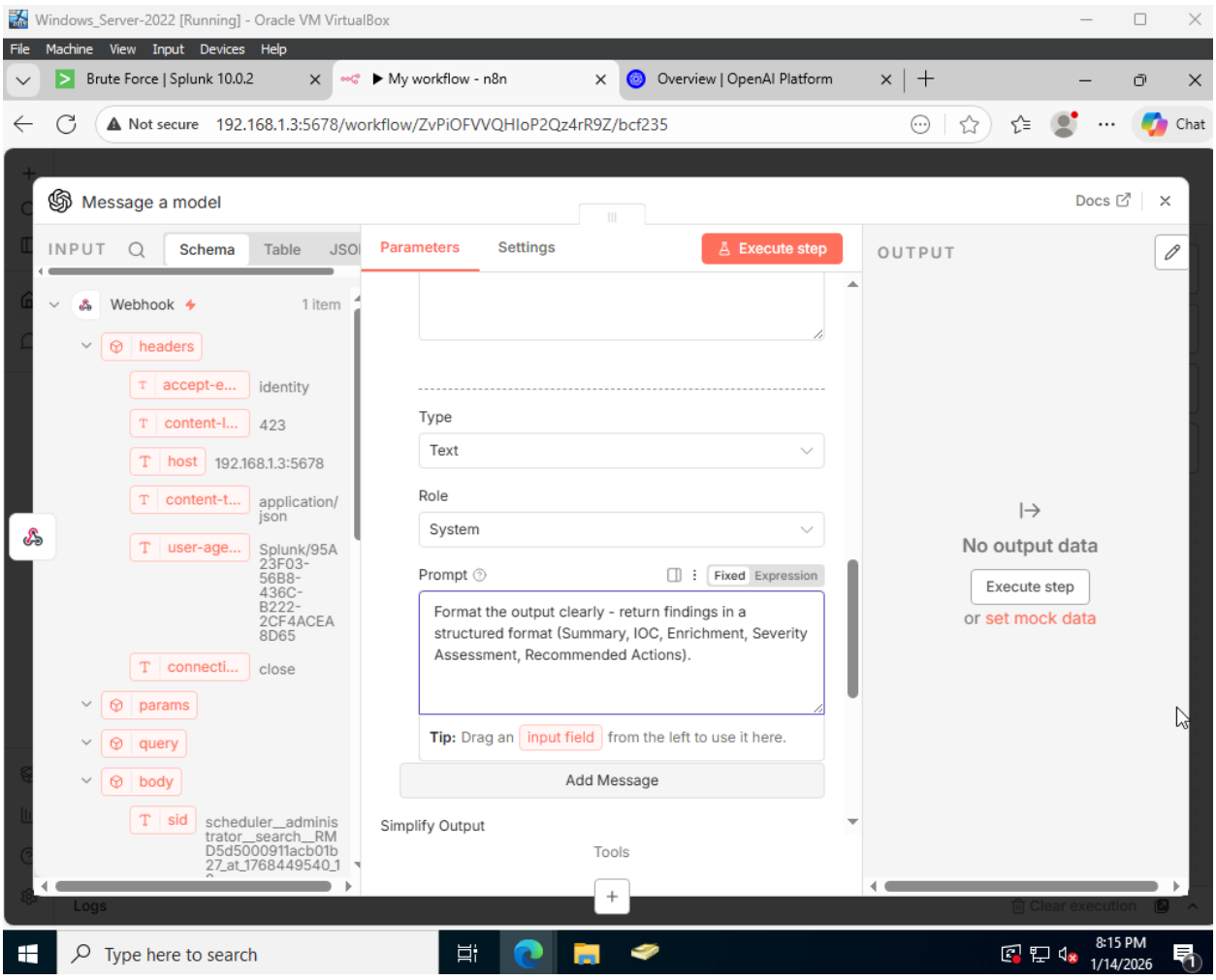


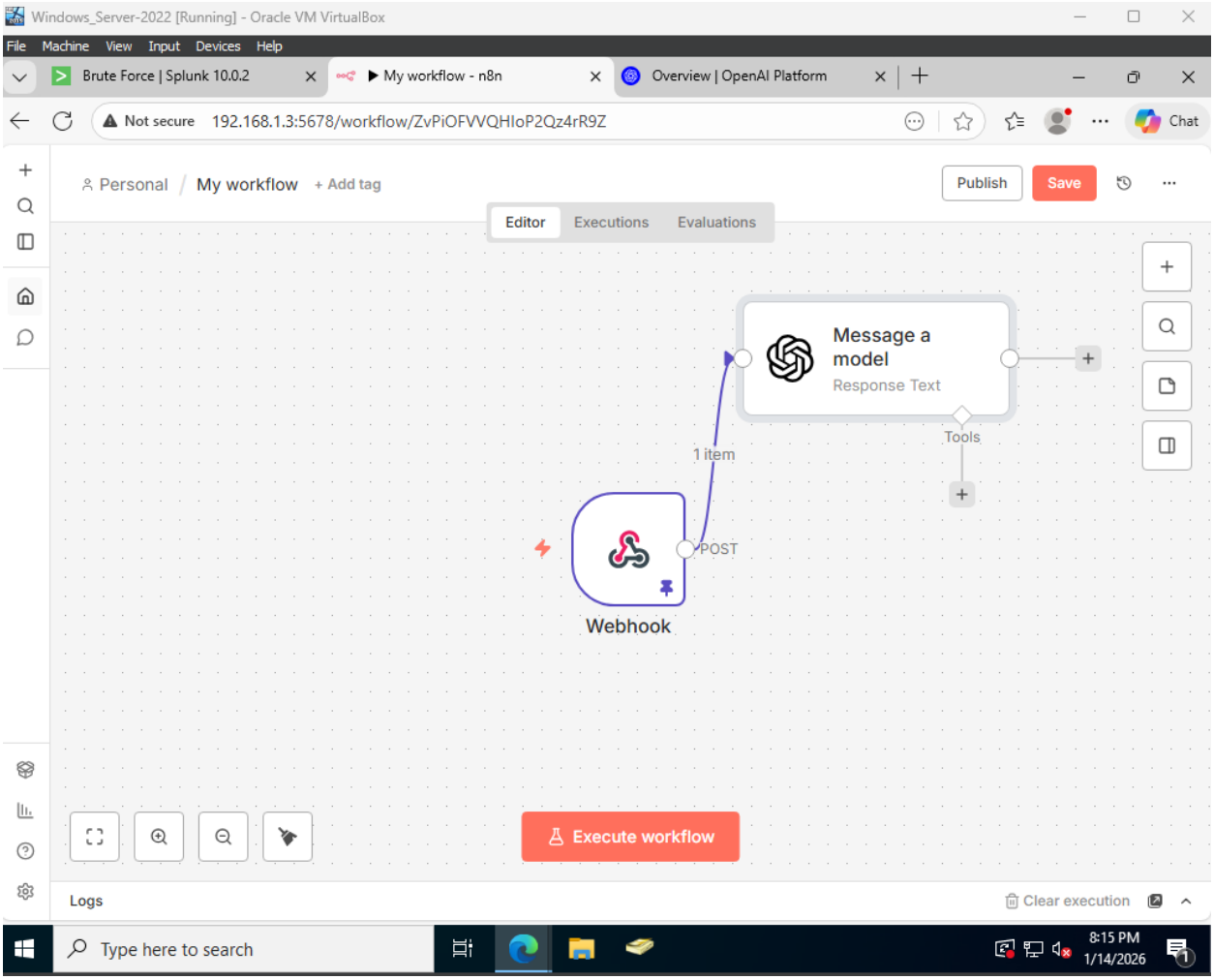
I had to purchase a few API credits to make this work.

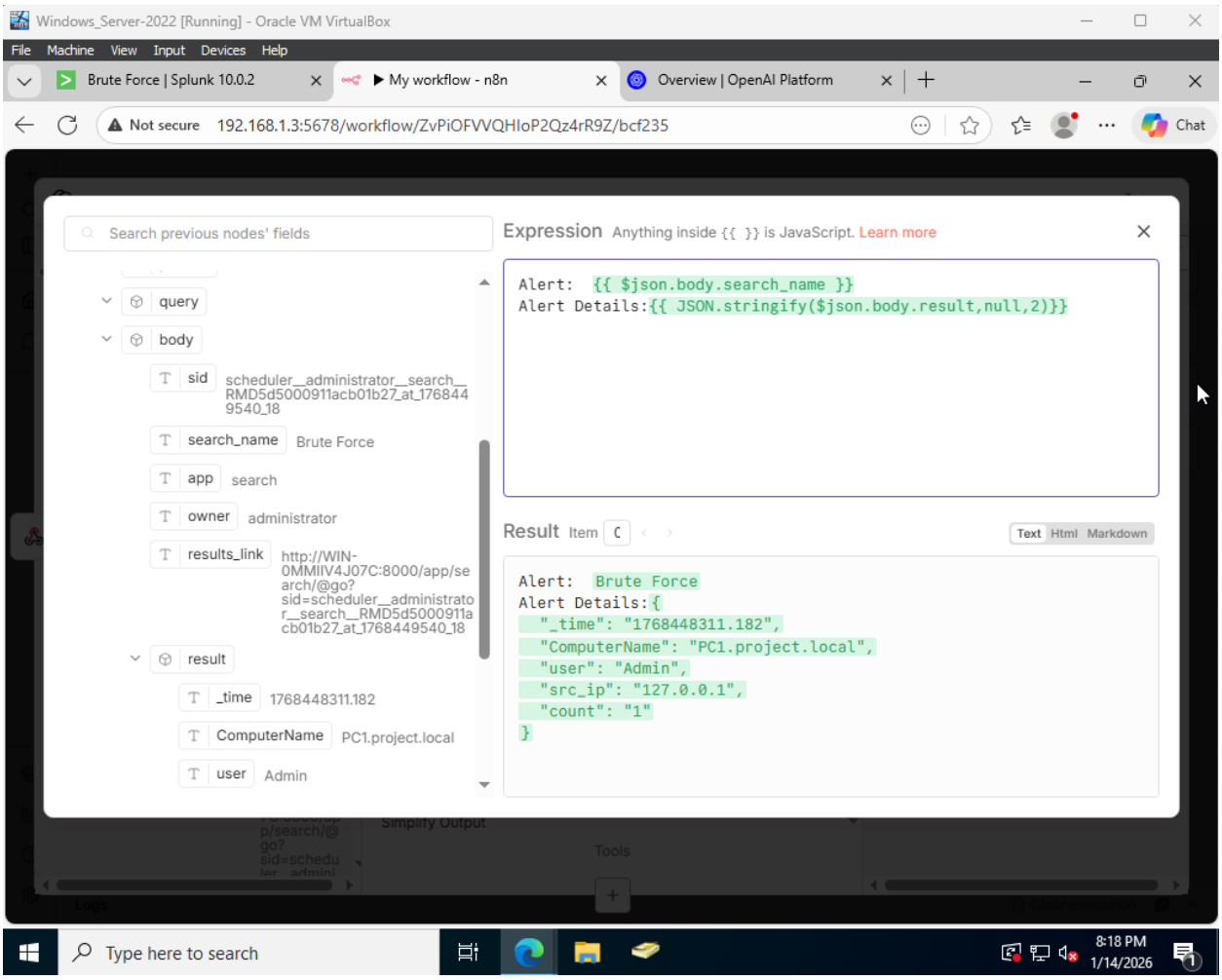


Here I set the prompt for AI to summarize the alert that was ingested.

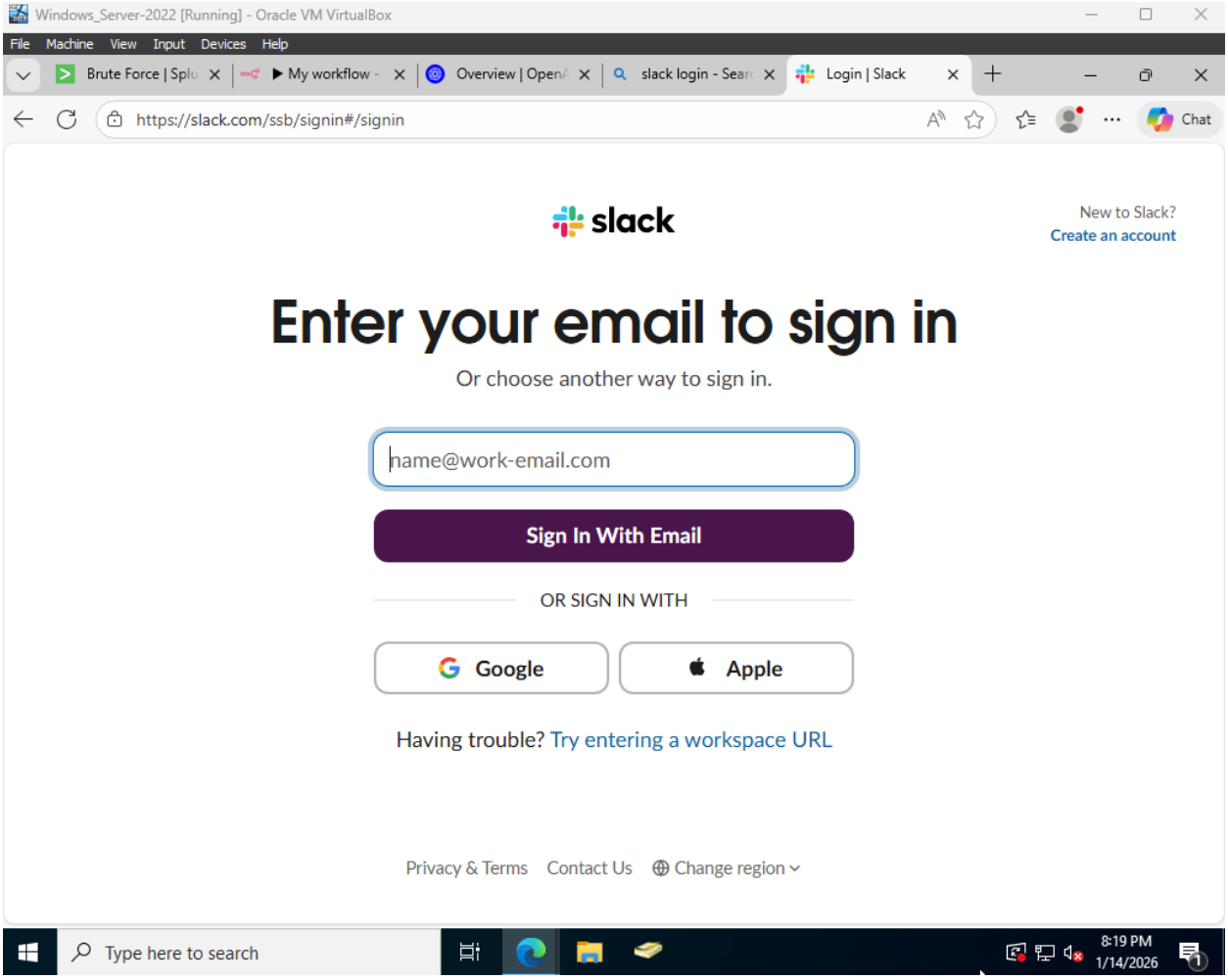

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Brute Force | Splunk 10.0.2
My workflow - n8n
Overview | OpenAI Platform
Not secure 192.168.1.3:5678/workflow/ZvPiOFVVQHIoP2Qz4rR9Z/bcf235
Chat
Message a model
Docs
INPUT
Schema
Table
Parameters
Settings
Execute step
OUTPUT
Webhook
1 item
headers
accept-e... identity
content-l... 423
host 192.168.1.3:5678
content-t... application/json
user-age... Splunk/9A23F03-56B8-436C-B222-2CF4ACEA8D65
connecti... close
params
query
body
sid scheduler__administrator__search__RMD5d5000911acb01b27_at_1768449540_1
Assistant
Prompt
You will act as a Tier 1 SOC Analyst assistant. When provided with a security alert or incident details (including indicators of compromise, logs, or metadata), perform the following steps:
Summarize the alert – Provide a clear summary of what triggered the alert, which systems/users are affected, and the nature of the activity (e.g., suspicious login, malware detection, lateral movement).
Enrich with threat intelligence – Correlate any IOCs (IP addresses, domains, hashes) with known threat intel sources. Highlight if the indicators are associated with known malware or threat actors.
Assess severity – Based on MITRE ATT&CK mapping, identify tactics/techniques and provide an initial severity rating (Low, Medium, High, Critical).
Recommend next actions – Suggest investigation steps and potential containment actions.
Tools
No output data
Execute step
or set mock data
Logs
Clear execution
Type here to search
8:13 PM
1/14/2026


Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Brute Force | Splunk 10.0.2
My workflow - n8n
Overview | OpenAI Platform
Not secure 192.168.1.3:5678/workflow/ZvPiOFVVQHIoP2Qz4rR9Z/bcf235
Chat
Message a model
Docs
INPUT
Schema
Table
Parameters
Settings
Execute step
OUTPUT
Webhook
1 item
headers
accept-e...
identity
content-l...
423
host
192.168.1.3:5678
content-t...
application/json
user-age...
Splunk/95A23F03-56B8-436C-B222-2CF4ACEA8D65
connecti...
close
params
query
body
sid
scheduler__administrator__search__RMD5d5000911acb01b27_at_1768449540_1
Type
Text
Role
System
Prompt
Fixed
Expression
Format the output clearly - return findings in a structured format (Summary, IOC, Enrichment, Severity Assessment, Recommended Actions).
Tip: Drag an input field from the left to use it here.
Add Message
Simplify Output
Tools
No output data
Execute step
or set mock data
Logs
Clear execution
Type here to search
8:15 PM
1/14/2026

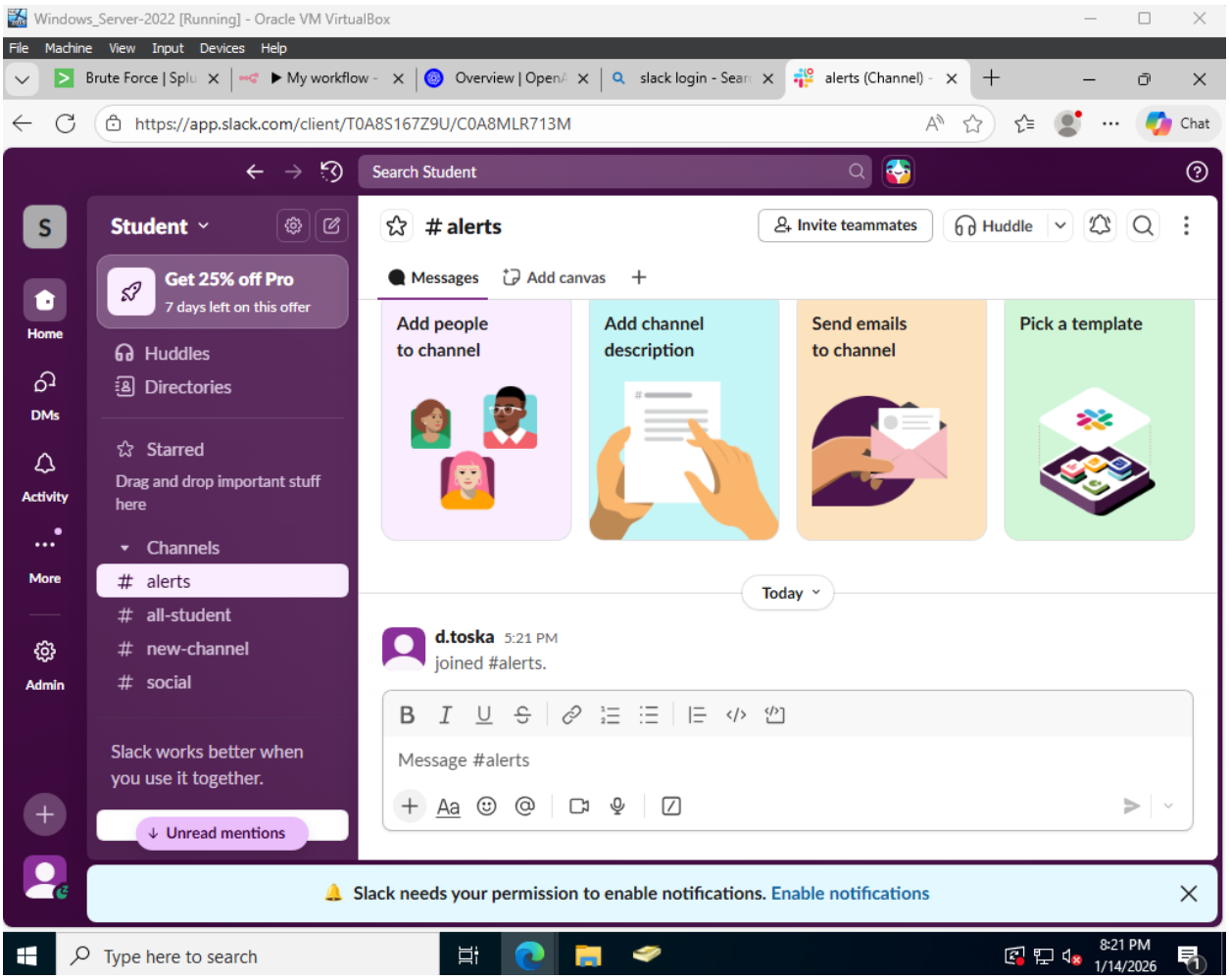

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Brute Force | Splunk 10.0.2
My workflow - n8n
Overview | OpenAI Platform
Not secure 192.168.1.3:5678/workflow/ZvPiOFVVQHIoP2Qz4rR9Z
Chat
Personal / My workflow + Add tag
Publish
Save
Editor
Executions
Evaluations
Message a model
Response Text
Tools
1 item
POST
Webhook
Execute workflow
Logs
Clear execution
Type here to search
8:15 PM
1/14/2026



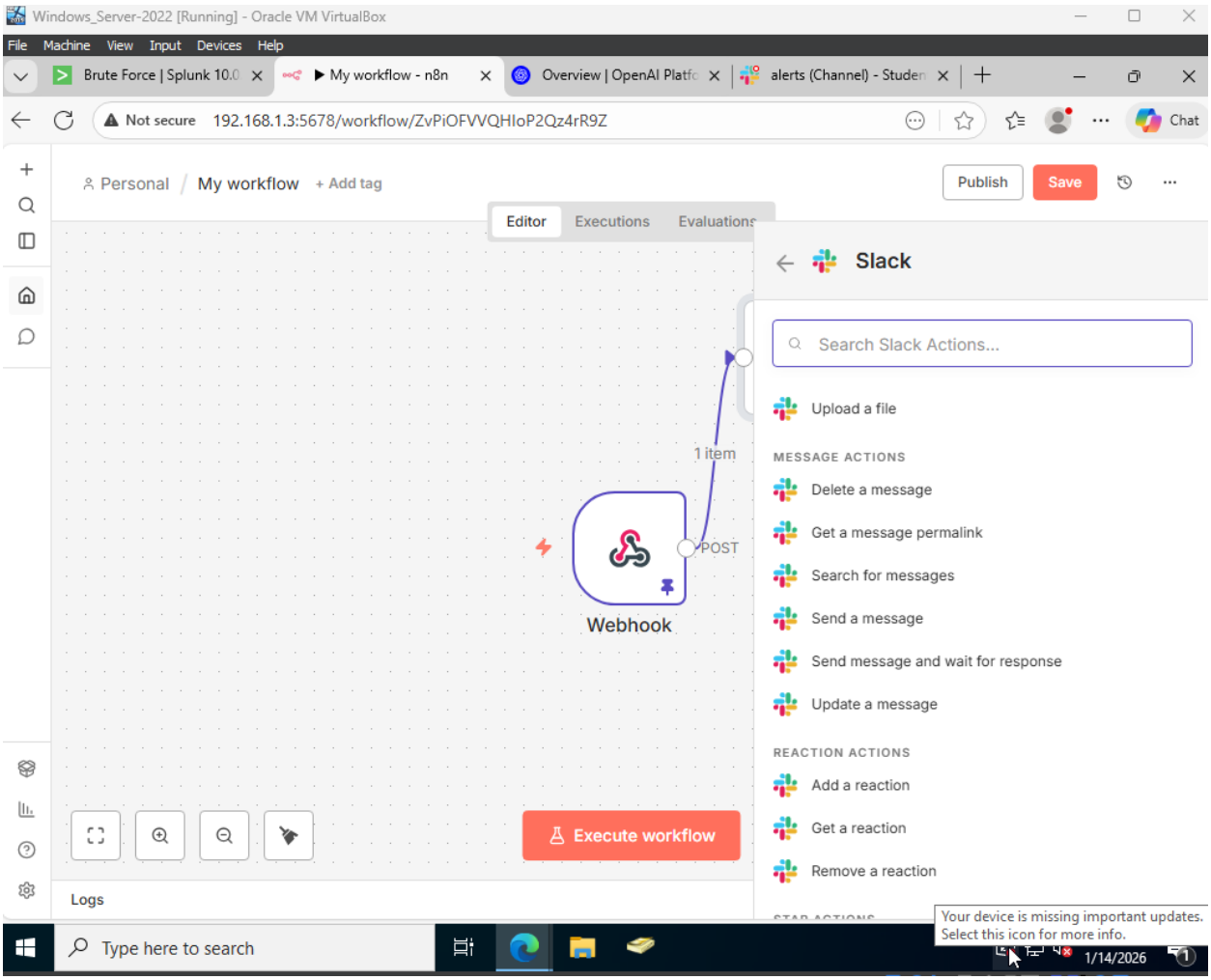
I will be using Slack to receive the alerts that n8n will produce.

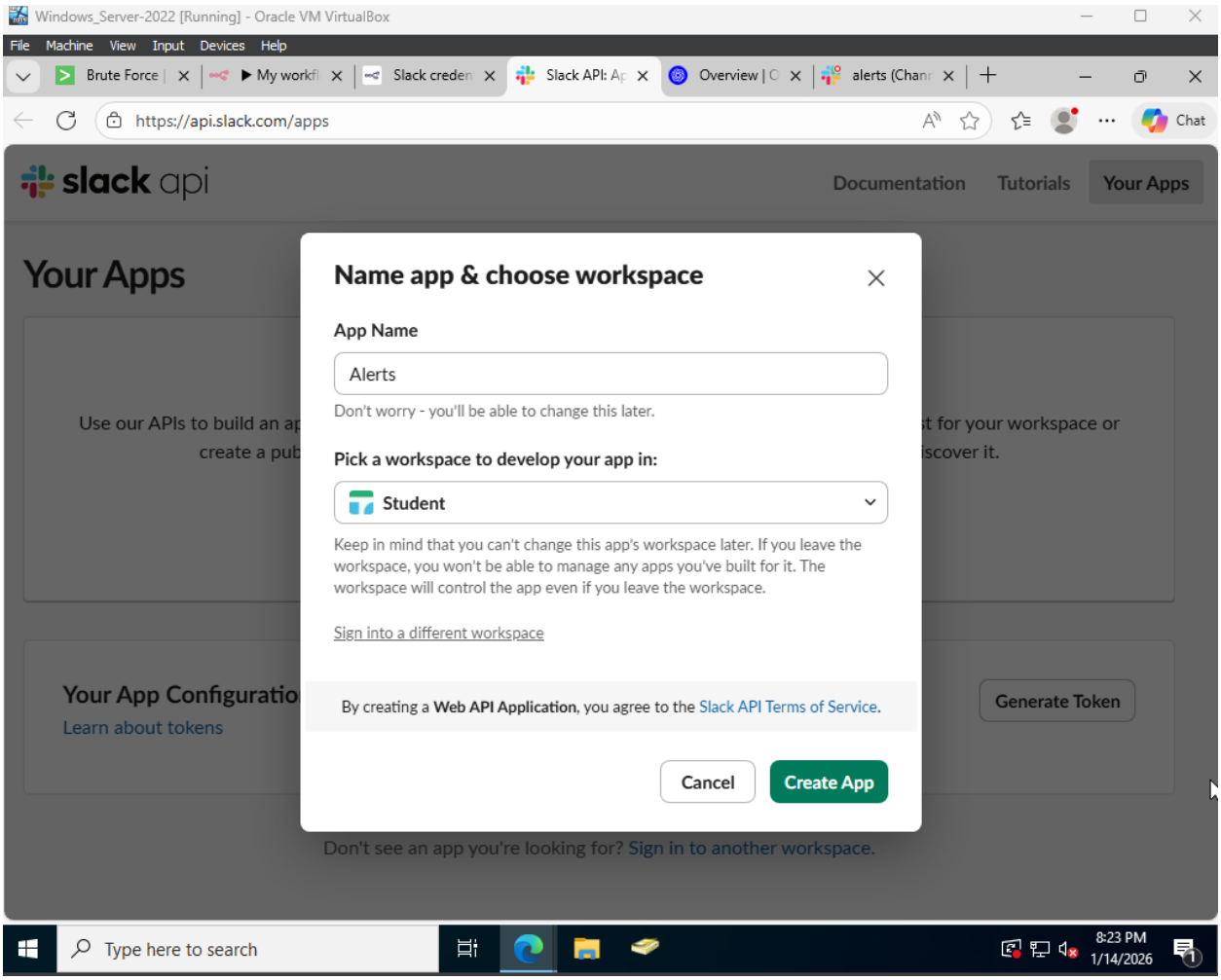


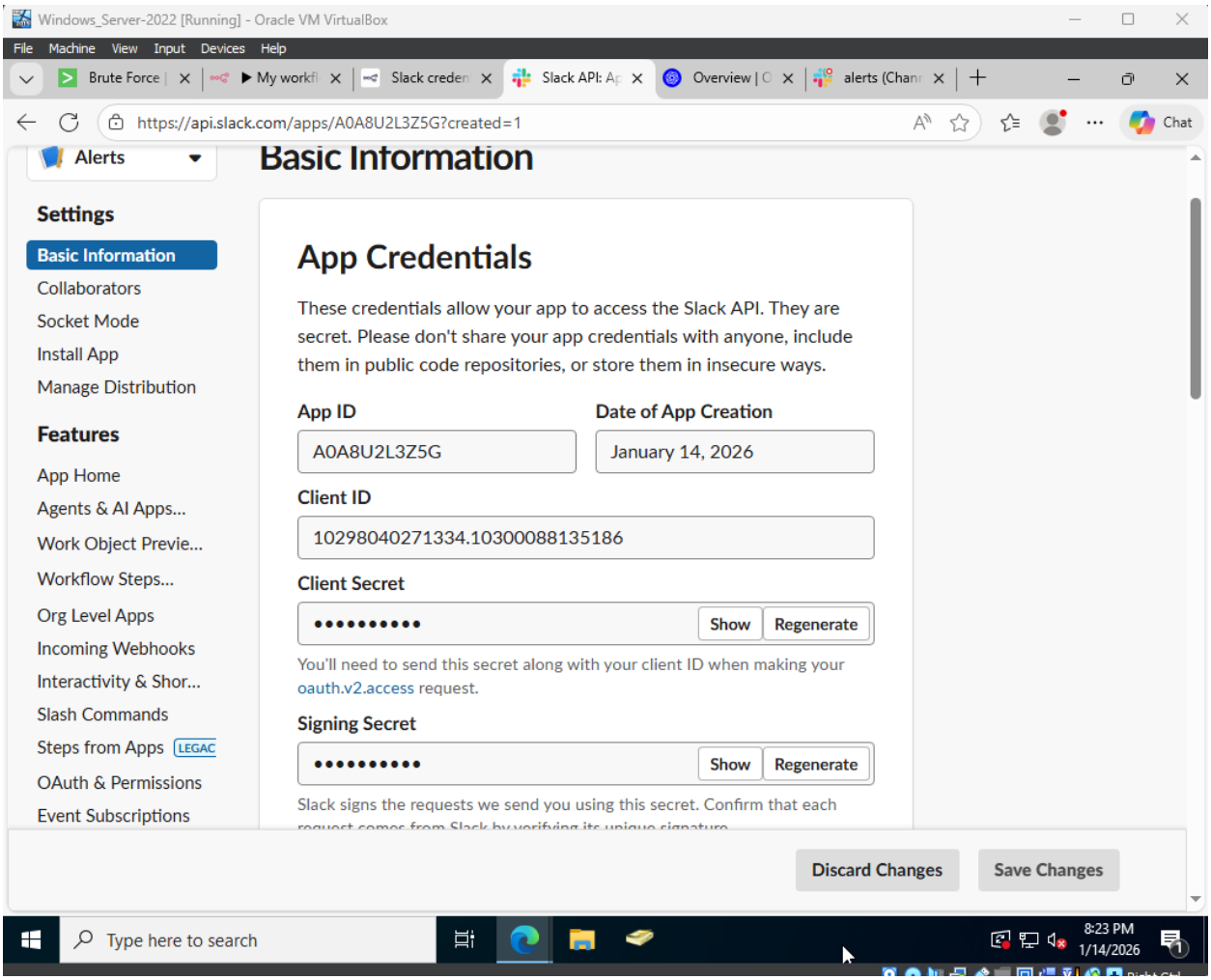
I created a new channel called Alerts that will be used by n8n to produce the output.

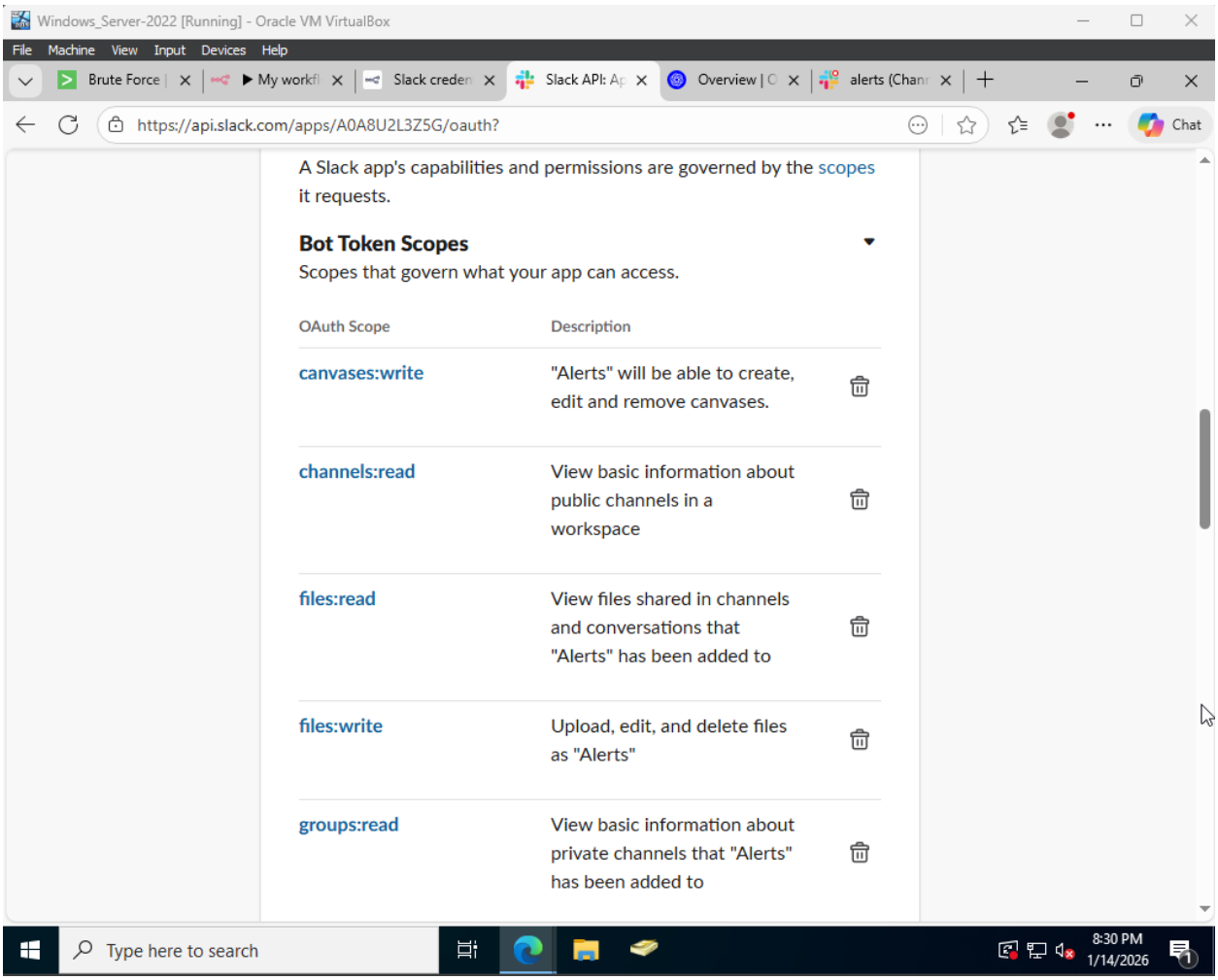


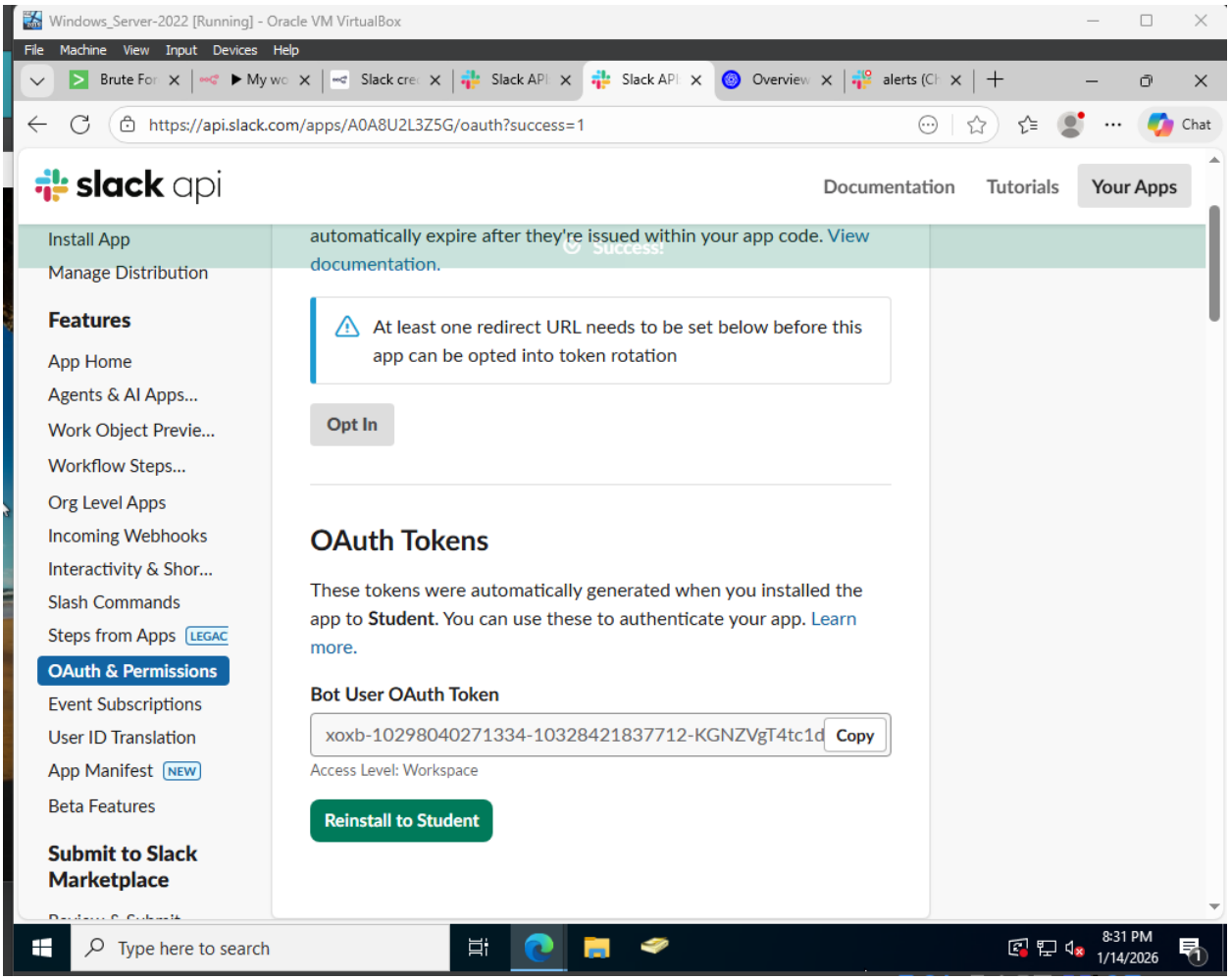
These next few steps were done for creating the Slack node in n8n:

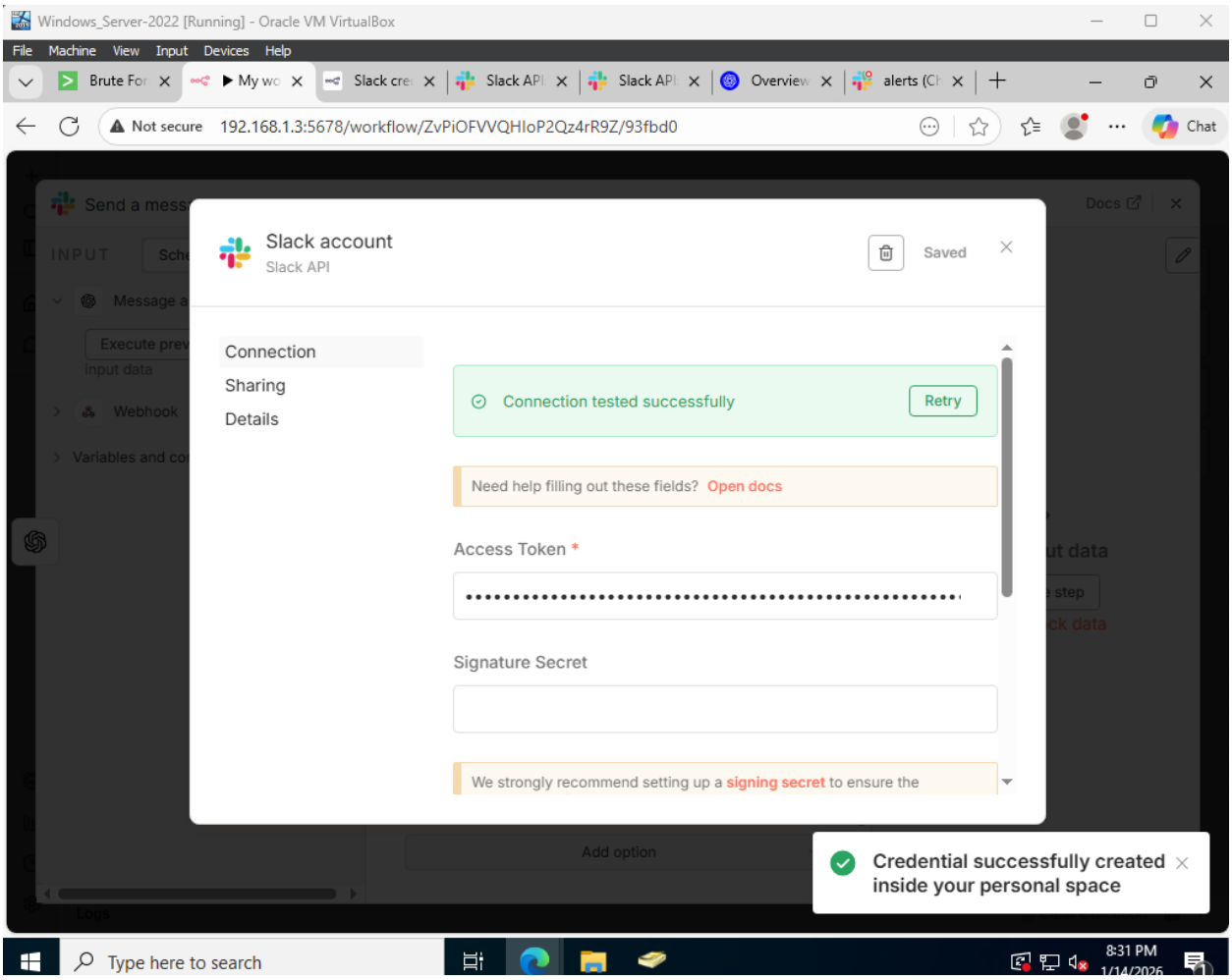

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Brute Force | Splunk 10.0
My workflow - n8n
Overview | OpenAI Platfc
alerts (Channel) - Studen
Not secure 192.168.1.3:5678/workflow/ZvPiOFVVQHIoP2Qz4rR9Z
Chat
Personal / My workflow + Add tag
Publish
Save
Editor
Executions
Evaluations
1 item
POST
Webhook
Execute workflow
Logs
Slack
Search Slack Actions...
Upload a file
MESSAGE ACTIONS
Delete a message
Get a message permalink
Search for messages
Send a message
Send message and wait for response
Update a message
REACTION ACTIONS
Add a reaction
Get a reaction
Remove a reaction
Your device is missing important updates.
Select this icon for more info.
Type here to search
1/14/2026

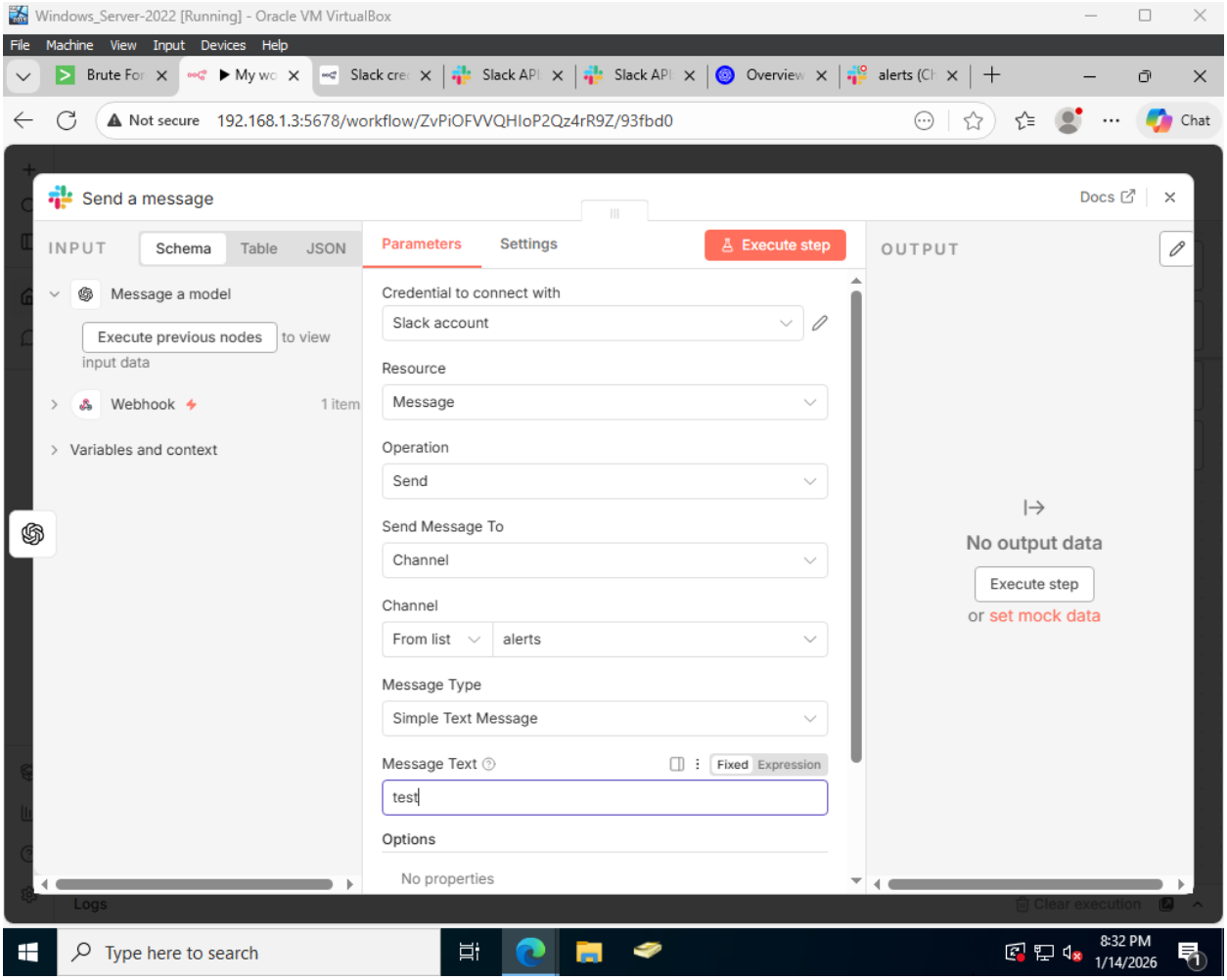

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
https://api.slack.com/apps
slack api
Documentation
Tutorials
Your Apps
Your Apps
Name app & choose workspace
App Name
Alerts
Don't worry - you'll be able to change this later.
Pick a workspace to develop your app 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
Your App Configuratio
Learn about tokens
Generate Token
Don't see an app you're looking for? Sign in to another workspace.
Type here to search
8:23 PM
1/14/2026

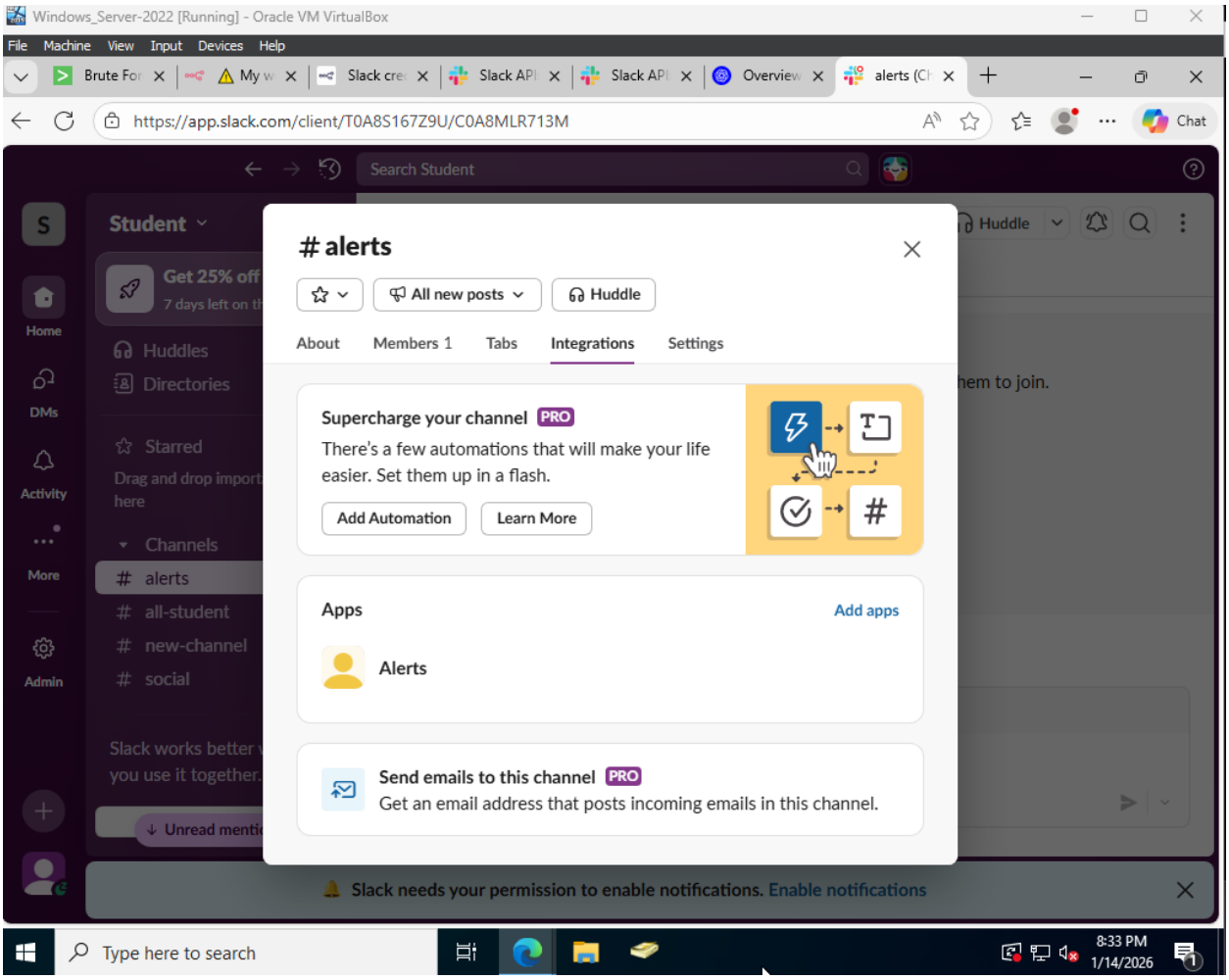

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
https://api.slack.com/apps/A0A8U2L3Z5G?created=1
Chat
Alerts
Basic Information
Settings
Basic Information
Collaborators
Socket Mode
Install App
Manage Distribution
Features
App Home
Agents & AI Apps...
Work Object Previe...
Workflow Steps...
Org Level Apps
Incoming Webhooks
Interactivity & Shor...
Slash Commands
Steps from Apps
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
A0A8U2L3Z5G
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
Discard Changes
Save Changes
Type here to search
8:23 PM
1/14/2026

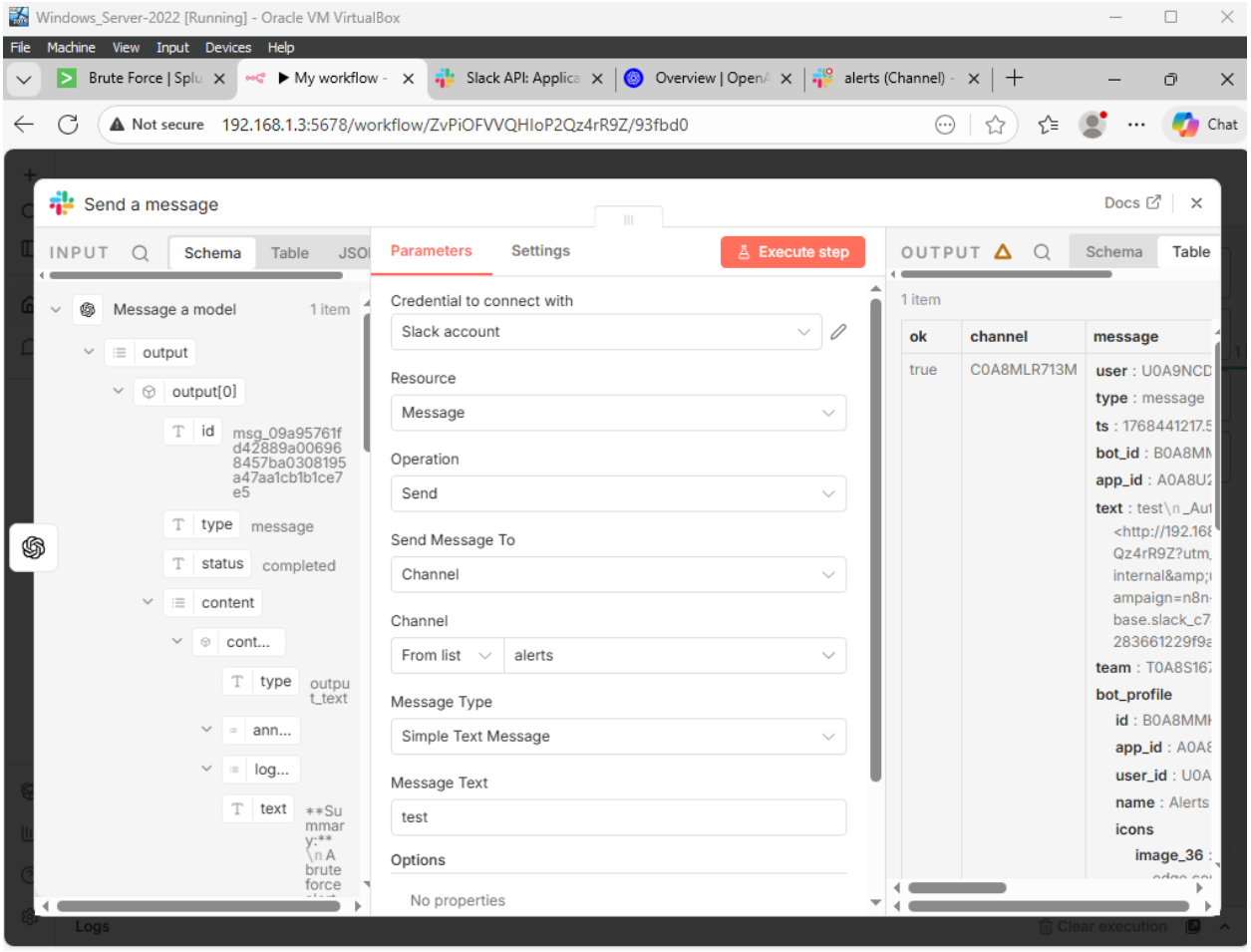

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Brute Force
My workfl
Slack creden
Slack API: Ap
Overview | C
alerts (Chan
https://api.slack.com/apps/A0A8U2L3Z5G/oauth?
Chat
A Slack app's capabilities and permissions are governed by the scopes it requests.
Bot 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
https://api.slack.com/apps/A0A8U2L3Z5G/oauth?success=1
slack api
Documentation
Tutorials
Your Apps
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
OAuth & Permissions
Event Subscriptions
User ID Translation
App Manifest
Beta Features
Submit to Slack Marketplace
automatically expire after they're issued within your app code. View documentation.
Success!
At least one redirect URL needs to be set below before this app can be opted into token rotation
Opt In
OAuth Tokens
These tokens were automatically generated when you installed the app to Student. You can use these to authenticate your app. Learn more.
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

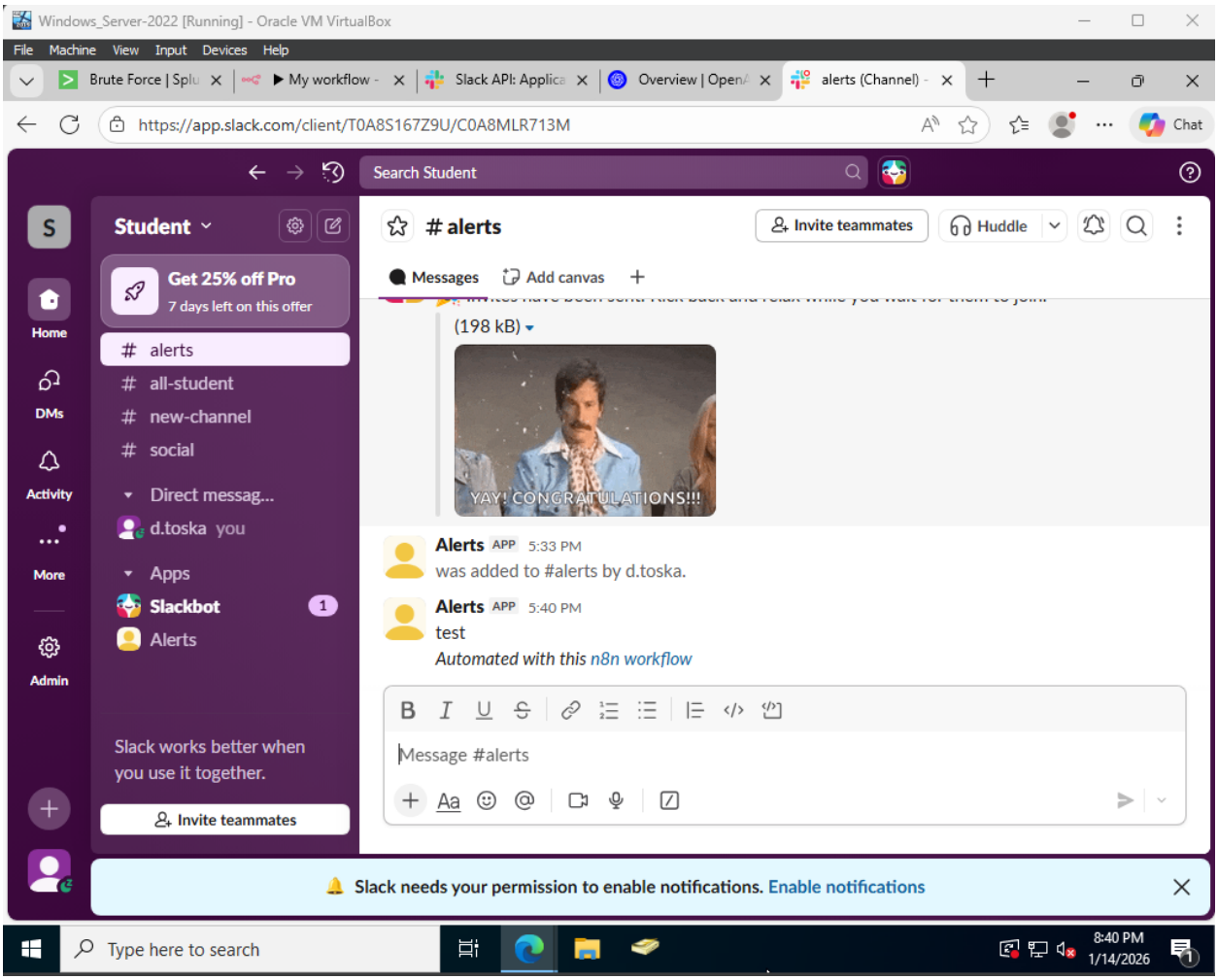

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Not secure 192.168.1.3:5678/workflow/ZvPiOFVVQHIoP2Qz4rR9Z/93fbd0
Chat
Slack account
Slack API
Saved
Connection
Sharing
Details
Connection tested successfully
Retry
Need help filling out these fields? Open docs
Access Token *
Signature Secret
We strongly recommend setting up a signing secret to ensure the
Add option
Credential successfully created inside your personal space
Type here to search
8:31 PM
1/14/2026

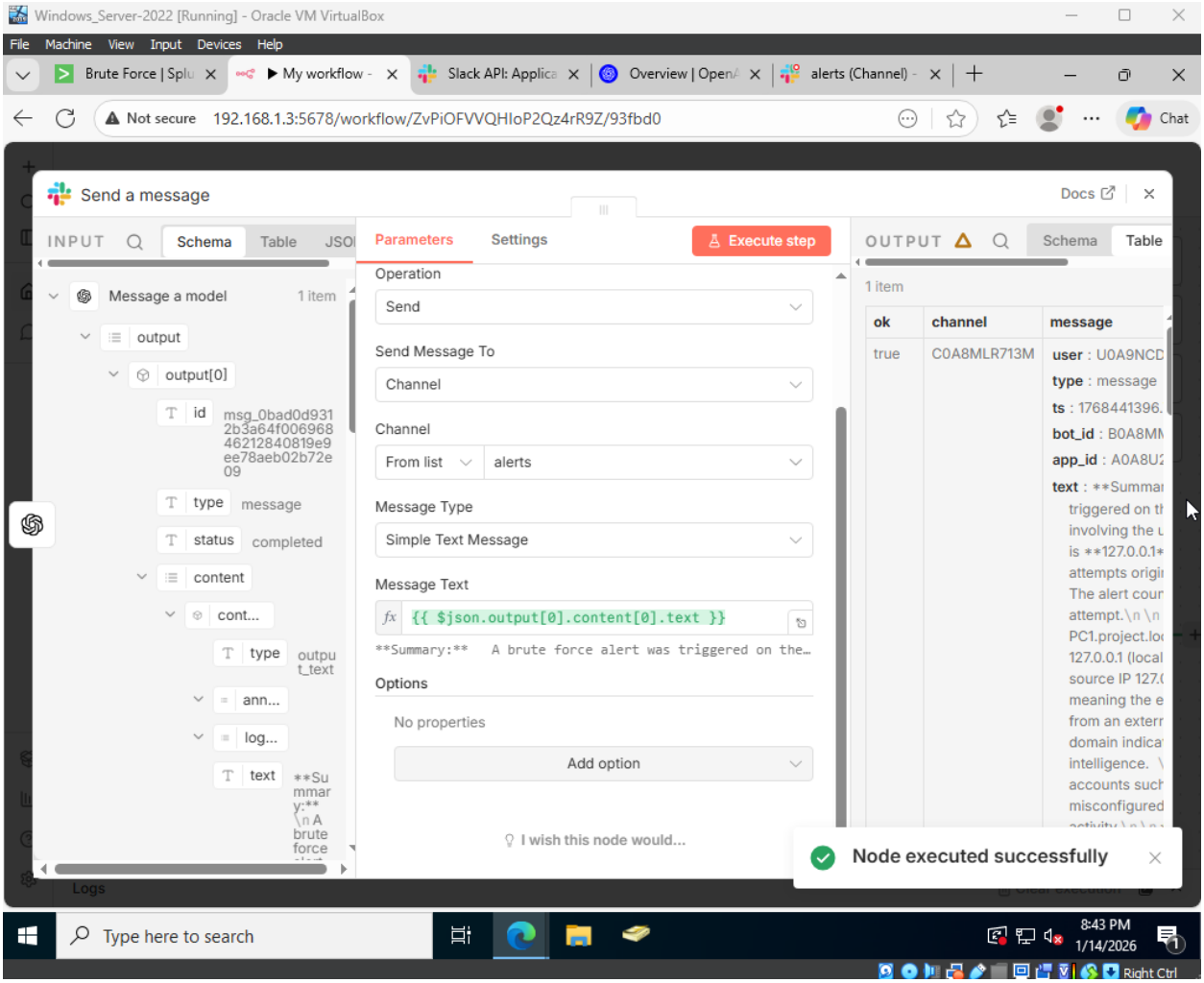

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Not secure 192.168.1.3:5678/workflow/ZvPiOFVVQHIoP2Qz4rR9Z/93fbd0
Chat
Send a message
Docs
INPUT
Schema
Table
JSON
Message a model
Execute previous nodes to view input data
Webhook
1 item
Variables and context
Parameters
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
Fixed
Expression
test
Options
No properties
OUTPUT
No output data
Execute step
or set mock data
Logs
Clear execution
Type here to search
8:32 PM
1/14/2026


Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
https://app.slack.com/client/T0A8S167Z9U/C0A8MLR713M
Search Student
Student
Get 25% off
Huddles
Directories
Starred
Channels
alerts
all-student
new-channel
social
Home
DMs
Activity
More
Admin
alerts
All new posts
Huddle
About
Members 1
Tabs
Integrations
Settings
Supercharge your channel PRO
There's a few automations that will make your life easier. Set them up in a flash.
Add Automation
Learn More
Apps
Add apps
Alerts
Send emails to this channel PRO
Get an email address that posts incoming emails in this channel.
Slack needs your permission to enable notifications. Enable notifications
Type here to search
8:33 PM
1/14/2026

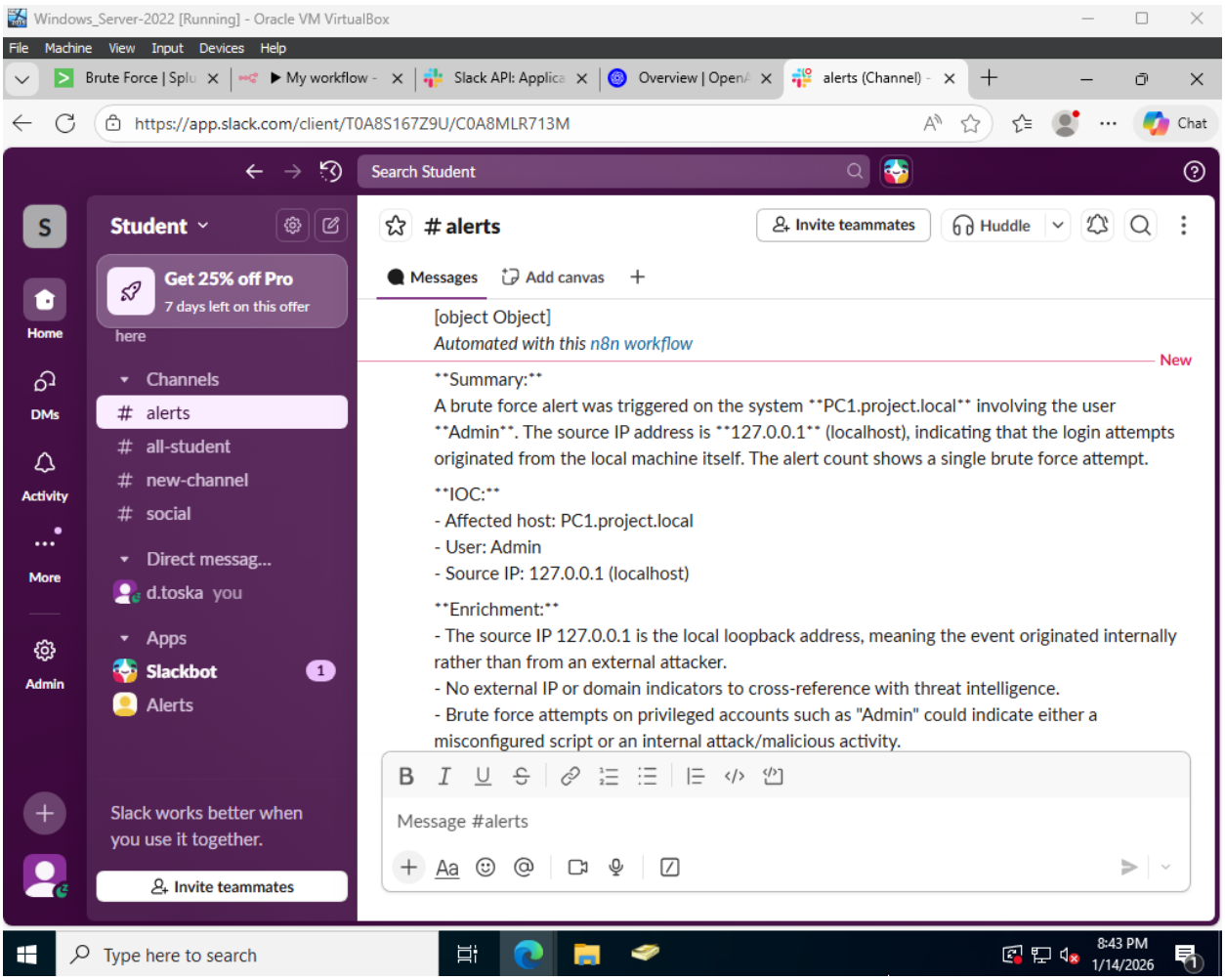


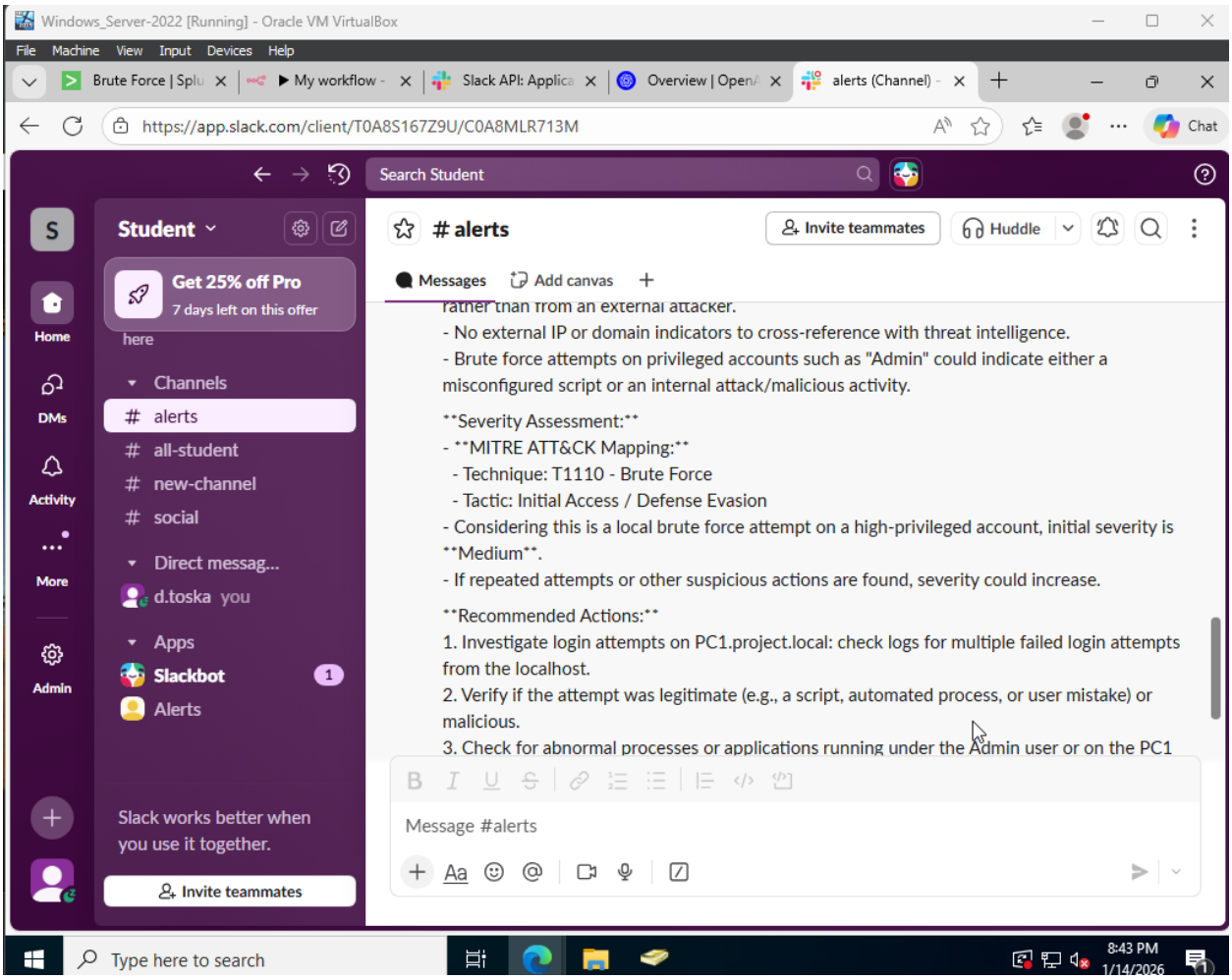
As you can see, the test alert was outputted:

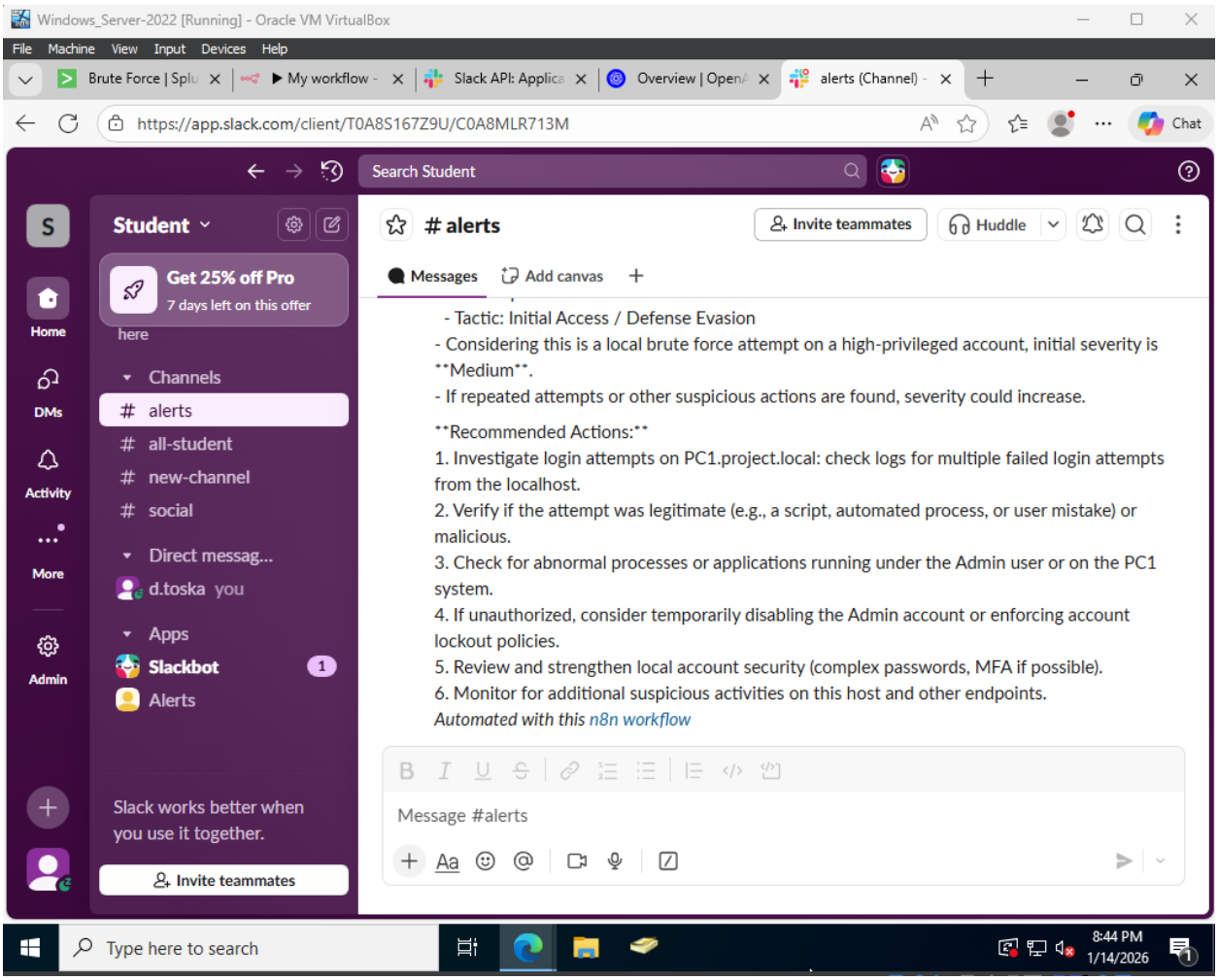

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Brute Force | Splu
My workflow -
Slack API: Applica
Overview | Open
alerts (Channel) -
https://app.slack.com/client/T0A8S167Z9U/C0A8MLR713M
Chat
Search Student
Student
Get 25% off Pro
7 days left on this offer
alerts
Invite teammates
Huddle
Messages
Add canvas
Home
DMs
Activity
More
Admin
alerts
all-student
new-channel
social
Direct messag...
d.toska you
Apps
Slackbot
Alerts
Slack works better when you use it together.
Invite teammates
(198 kB)
YAY! CONGRATULATIONS!!!
Alerts APP 5:33 PM
was added to #alerts by d.toska.
Alerts APP 5:40 PM
test
Automated with this n8n workflow
Message #alerts
Slack needs your permission to enable notifications. Enable notifications
Type here to search
8:40 PM
1/14/2026



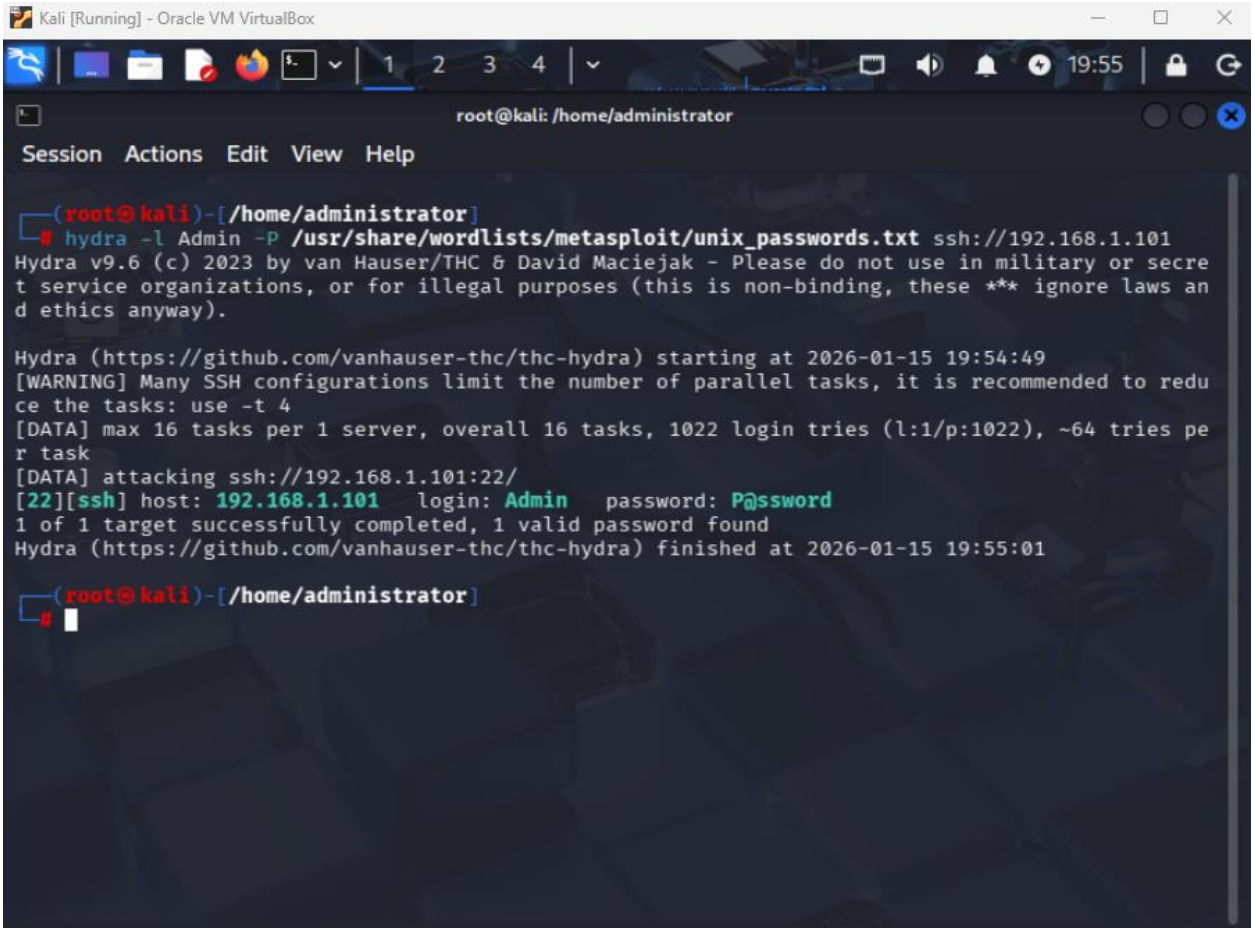
After swapping the test to the AI, it was able to produce the output it made.

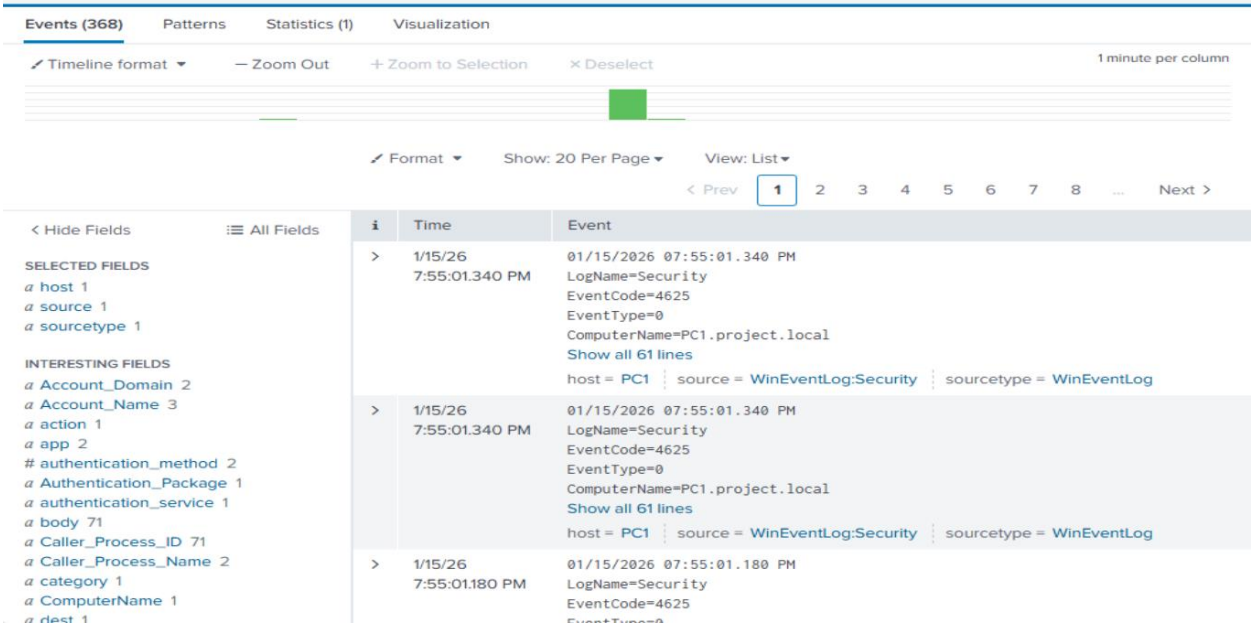

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Brute Force | Splu
My workflow -
Slack API: Applica
Overview | Open
alerts (Channel) -
https://app.slack.com/client/T0A8S167Z9U/C0A8MLR713M
Chat
Search Student
Student
Get 25% off Pro
7 days left on this offer
here
Channels
alerts
all-student
new-channel
social
Direct messag...
d.toska you
Apps
Slackbot
Alerts
Slack works better when you use it together.
Invite teammates
Home
DMs
Activity
More
Admin
alerts
Invite teammates
Huddle
Messages
Add canvas
[object Object]
Automated with this n8n workflow
New
Summary:
A brute force alert was triggered on the system **PC1.project.local** involving the user **Admin**. The source IP address is **127.0.0.1** (localhost), indicating that the login attempts originated from the local machine itself. The alert count shows a single brute force attempt.
IOC:
- Affected host: PC1.project.local
- User: Admin
- Source IP: 127.0.0.1 (localhost)
Enrichment:
- The source IP 127.0.0.1 is the local loopback address, meaning the event originated internally 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.
Message #alerts
Type here to search
8:43 PM
1/14/2026

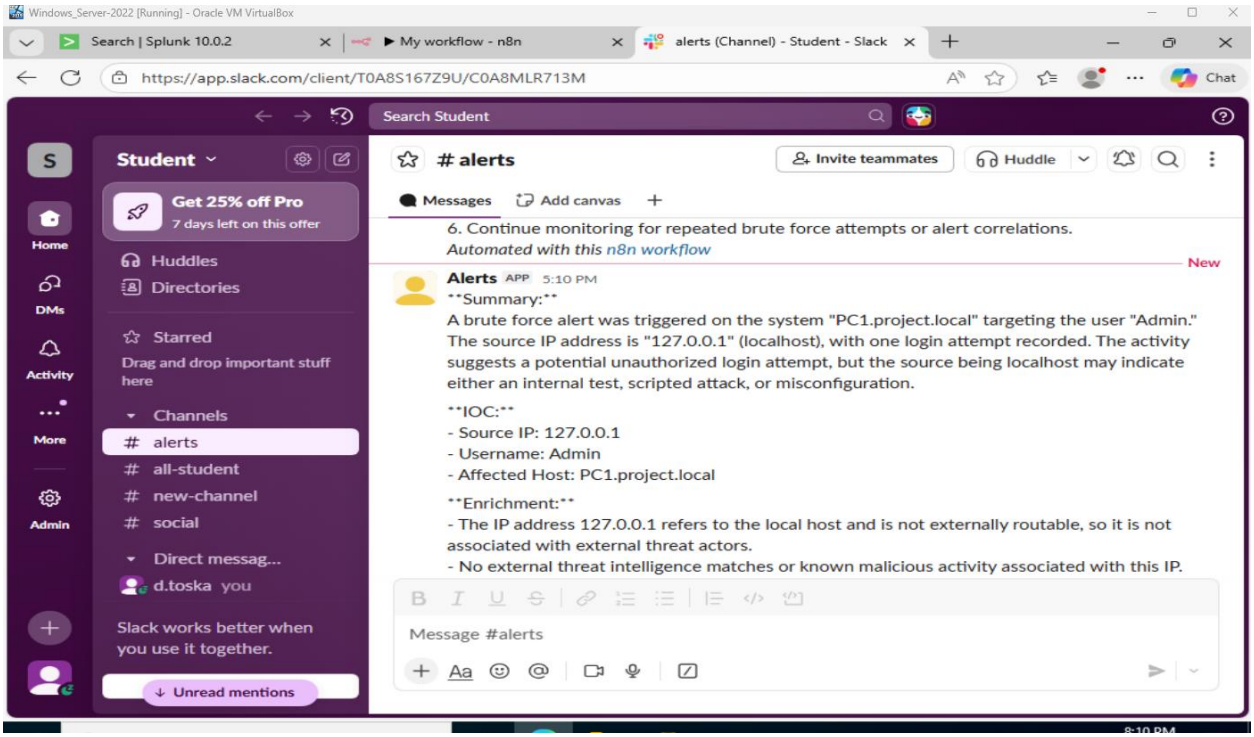

Windows_Server-2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Brute Force | Splu
My workflow -
Slack API: Applica
Overview | OpenA
alerts (Channel) -
https://app.slack.com/client/T0A8S167Z9U/C0A8MLR713M
Chat
Search Student
Student
Get 25% off Pro
7 days left on this offer
here
Home
DMs
Activity
More
Admin
Channels
alerts
all-student
new-channel
social
Direct messag...
d.toska you
Apps
Slackbot
Alerts
Slack works better when you use it together.
Invite teammates
alerts
Invite teammates
Huddle
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
Message #alerts
Type here to search
8:43 PM
1/14/2026

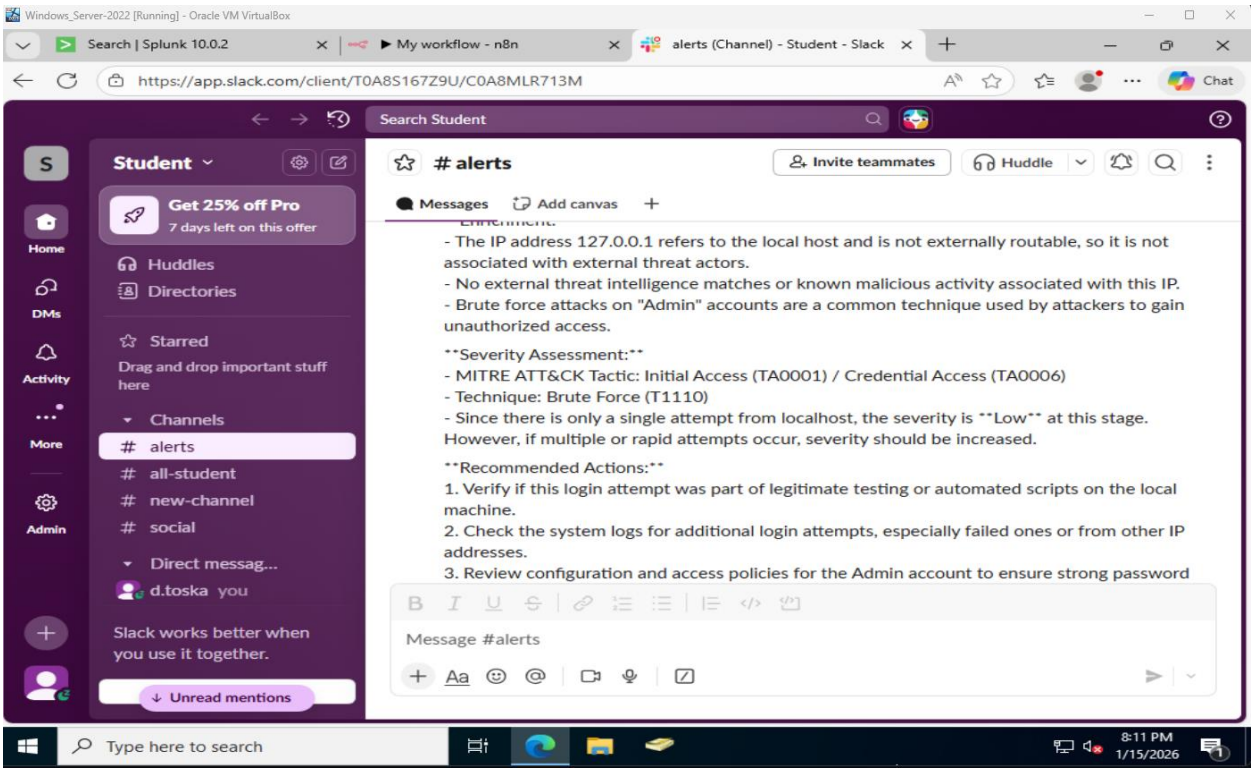


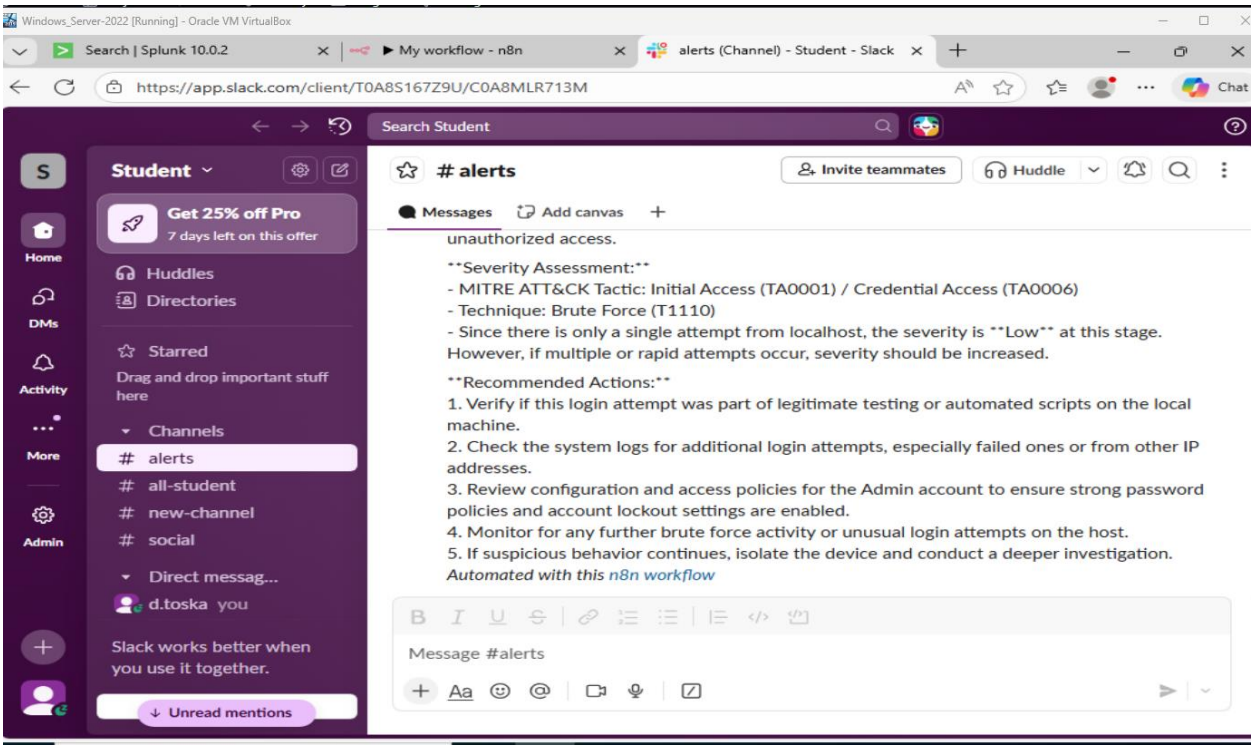
I will now use Hydra to create logs for the alert to trigger and send to n8n:


Kali [Running] - Oracle VM VirtualBox
1 2 3 4
19:55
root@kali: /home/administrator
Session Actions Edit View Help
(root㉿kali)-[/home/administrator]
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 2026-01-15 19:54:49
[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 2026-01-15 19:55:01
(root㉿kali)-[/home/administrator]
#


Events (368)
Patterns
Statistics (1)
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 minute per column
Format
Show: 20 Per Page
View: List
< Prev 1 2 3 4 5 6 7 8 ... Next >
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Account_Domain 2
a Account_Name 3
a action 1
a app 2
authentication_method 2
a Authentication_Package 1
a authentication_service 1
a body 71
a Caller_Process_ID 71
a Caller_Process_Name 2
a category 1
a ComputerName 1
a dest 1
i Time Event
> 1/15/26 7:55:01.340 PM
01/15/2026 07:55:01.340 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=PC1.project.local
Show all 61 lines
host = PC1 source = WinEventLog:Security sourcetype = WinEventLog
> 1/15/26 7:55:01.340 PM
01/15/2026 07:55:01.340 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=PC1.project.local
Show all 61 lines
host = PC1 source = WinEventLog:Security sourcetype = WinEventLog
> 1/15/26 7:55:01.180 PM
01/15/2026 07:55:01.180 PM
LogName=Security
EventCode=4625


Windows_Server-2022 [Running] - Oracle VM VirtualBox
Search | Splunk 10.0.2
My workflow - n8n
alerts (Channel) - Student - Slack
https://app.slack.com/client/T0A8S167Z9U/C0A8MLR713M
Chat
Search Student
Student
Get 25% off Pro
7 days left on this offer
Huddles
Directories
Starred
Drag and drop important stuff here
Channels
alerts
all-student
new-channel
social
Direct messag...
d.toska you
Slack works better when you use it together.
Unread mentions
Home
DMs
Activity
More
Admin
alerts
Invite teammates
Huddle
Messages
Add canvas
6. Continue monitoring for repeated brute force attempts or alert correlations.
Automated with this n8n workflow
New
Alerts APP 5:10 PM
Summary:
A brute force alert was triggered on the system "PC1.project.local" targeting the user "Admin." The source IP address is "127.0.0.1" (localhost), with one login attempt recorded. The activity suggests a potential unauthorized login attempt, but the source being localhost may indicate either an internal test, scripted attack, or misconfiguration.
IOC:
- Source IP: 127.0.0.1
- Username: Admin
- Affected Host: PC1.project.local
Enrichment:
- The IP address 127.0.0.1 refers to the local host and is not externally routable, so it is not associated with external threat actors.
- No external threat intelligence matches or known malicious activity associated with this IP.
Message #alerts


Windows_Server-2022 [Running] - Oracle VM VirtualBox
Search | Splunk 10.0.2
My workflow - n8n
alerts (Channel) - Student - Slack
https://app.slack.com/client/T0A8S167Z9U/C0A8MLR713M
Chat
Search Student
Student
Get 25% off Pro
7 days left on this offer
Huddles
Directories
Starred
Drag and drop important stuff here
Channels
alerts
all-student
new-channel
social
Direct messag...
d.toska you
Slack works better when you use it together.
Unread mentions
alerts
Invite teammates
Huddle
Messages
Add canvas
- The IP address 127.0.0.1 refers to the local host and is not externally routable, so it is not associated with external threat actors.
- No external threat intelligence matches or known malicious activity associated with this IP.
- Brute force attacks on "Admin" accounts are a common technique used by attackers to gain unauthorized access.
Severity Assessment:
- MITRE ATT&CK Tactic: Initial Access (TA0001) / Credential Access (TA0006)
- Technique: Brute Force (T1110)
- Since there is only a single attempt from localhost, the severity is **Low** at this stage. However, if multiple or rapid attempts occur, severity should be increased.
Recommended Actions:
1. Verify if this login attempt was part of legitimate testing or automated scripts on the local machine.
2. Check the system logs for additional login attempts, especially failed ones or from other IP addresses.
3. Review configuration and access policies for the Admin account to ensure strong password
Message #alerts
Type here to search
8:11 PM
1/15/2026



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