

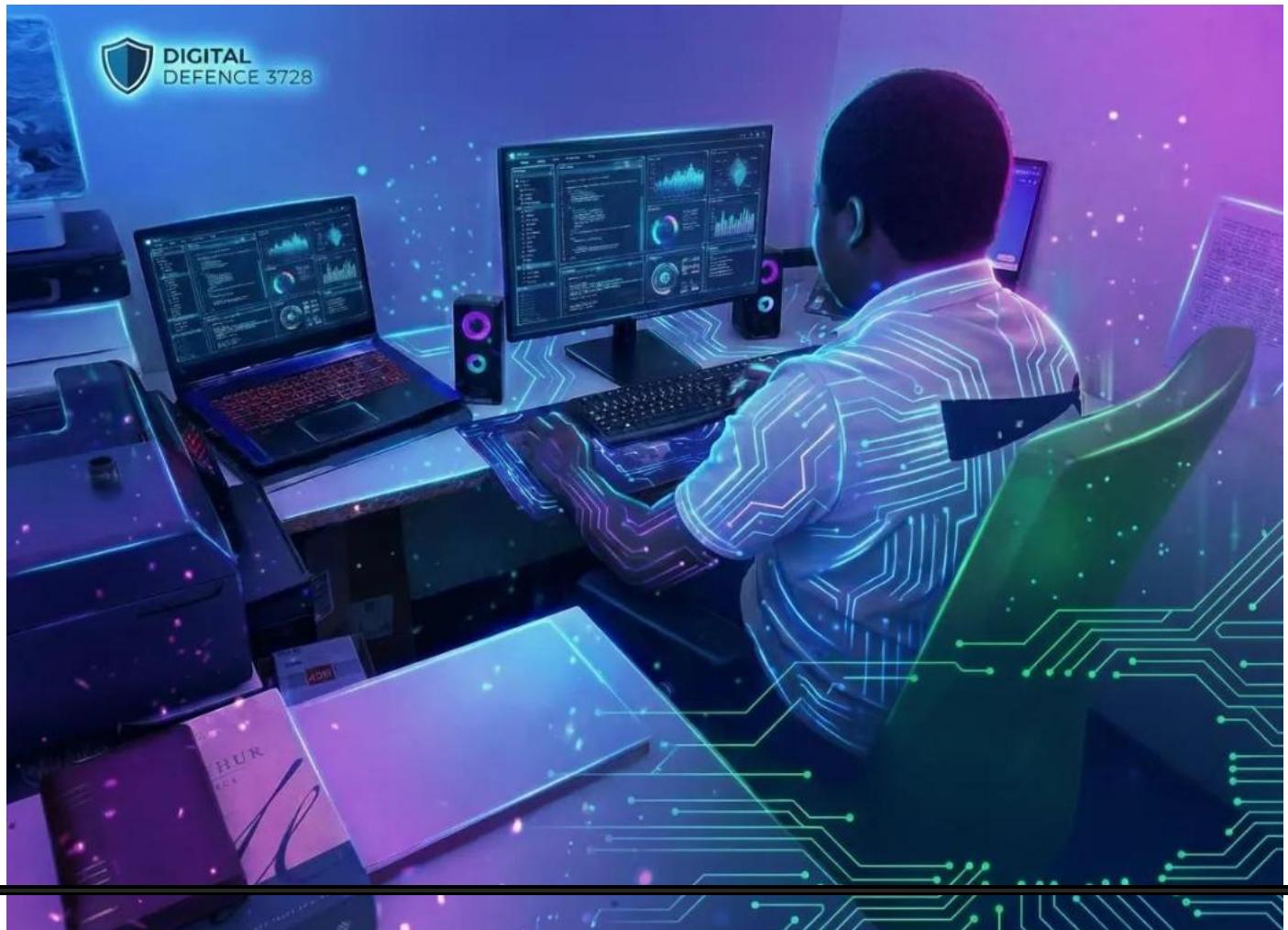
Enterprise Active Directory + SIEM Cybersecurity Home- Lab

Purpose:

Build hands-on SOC analyst skills

Prepared by:

Blessed Muteswa



Digital Defence 3728 — On-Prem SOC Analyst Home Lab

Author: Blessed Muteswa

Introduction

Digital Defence 3728 is an on-premises, virtualized SOC analyst lab designed to demonstrate **Blue-Team** skills: centralized logging. The lab runs on VMware Workstation Pro (host Windows 11) and uses a tightly controlled network with pfSense as gateway and a single AD authoritative DNS server.

Key components

pfSense firewall, Windows Server 2022 (Domain Controller + DNS), Ubuntu Server 24.04 LTS running Splunk Enterprise, a hardened Jumpbox (Windows 11 LTSC), a domain-joined Windows client, and two exercise systems (Kali, Metasploitable2).

All configuration, troubleshooting and verification steps are included, so the lab is fully reproducible and suitable.

Hardware Optimization for my MSI Laptop

- Host System: Windows 11 (Hypervisor Host)
- CPU: Intel i5 6 cores, 12 Logical Processors
- RAM: 40GB Total
- Storage: 1TB SSD + 500GB SSD NVMe
- Storage: 500GB SSD (Primary for VMs),
- 500GB NVMe (Host OS & Applications)

Goal: stable, repeatable SOC work; minimal risk of host lag.

Host reserve: 8 GB RAM; reserve 4 logical processors for host → 32 GB RAM and 8 logical processors available to VMs.

1 — SUMMARY / OUTCOMES	6
2 — ARCHITECTURE & VM SIZING	6
3 — FILES / ISOS (OFFICIAL SOURCES)	8
4 — STEP-BY-STEP BUILD — OVERVIEW	8
5 — PFSENSE INSTALLATION & CONFIGURATION	9
A. VMware network preparation (host)	9
B. Created pfSense VM	10
C. Installed pfSense (console)	11
D. Assigned interfaces (console)	13
E. GUI setup	14
F. DHCP & DNS settings	15
G. Firewall rules	16
H. Remote syslog forwarding to Splunk	17
I. Validation	18
6 — WINDOWS SERVER 2022: INSTALLED, DC PROMOTION & DNS & DC TROUBLESHOOTING REF: 6-(F)	20
A. OS installation & static IP	20
C. Promote to forest root (new domain)	23
D. DNS forwarders	24
E. Netlogon / DNS registration & validation	25
F. DC troubleshooting	27
G. Validation	29
7 — JUMPBOX (WINDOWS 11 LTSC): INSTALL, HARDENING & TOOLS	31

A. Installation:	31
B. Networking	33
i. Hardening baseline	33
C. Tools and rationale	36
D. Quick hardening commands	37
E. Access validation	38
8 — UBUNTU SERVER 24.04 LTS: INSTALLATION, NETWORKING, HARDENING & SPLUNK	39
A. Install Ubuntu Server 24.04	39
B. Static Netplan configuration (authoritative)	43
C. Hardening (baseline)	46
D. Splunk Enterprise installation	56
E. Validation tests	63
9 — WINDOWS CLIENT: DOMAIN JOIN, SPLUNK UF & SYSMON	66
A. Networking & DNS	66
B. Domain join	66
C. Splunk Universal Forwarder install	73
D. Configure UF inputs for Windows Event Logs	74
E. Install Sysmon	76
F. Validate ingestion in Splunk	78
10 — KALI & METASPLOITABLE2: CONTROLLED USAGE	78
Kali static IP (Network Manager):	79
11 — TROUBLESHOOTING LOG (CHRONOLOGICAL ORDER)	79
SRV Lookup / DNS Failure on Domain Controller (DC) Symptom	79
Set-NetConnectionProfile Refusing Domain Authenticated	80
Ubuntu DNS Using 127.0.0.53 and NXDOMAIN/SERVFAIL	80

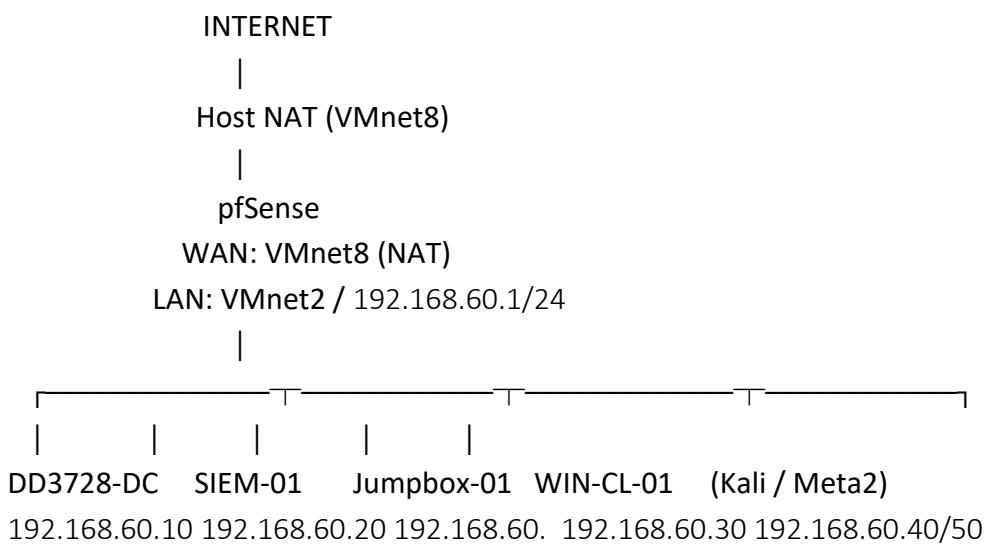
Wrong Subnet Symptom	80
RDP / Firewall / Profile Mismatches	81
12 — VERIFICATION & VALIDATION COMMANDS	81
Windows DC	81
Ubuntu SIEM	81
Splunk searches	81
13 — WHY THE DOMAIN CONTROLLER IS AUTHORITATIVE DNS	82
14 — KALI / METASPLOITABLE: NETWORK SETUP	82

1 — Summary / Outcomes

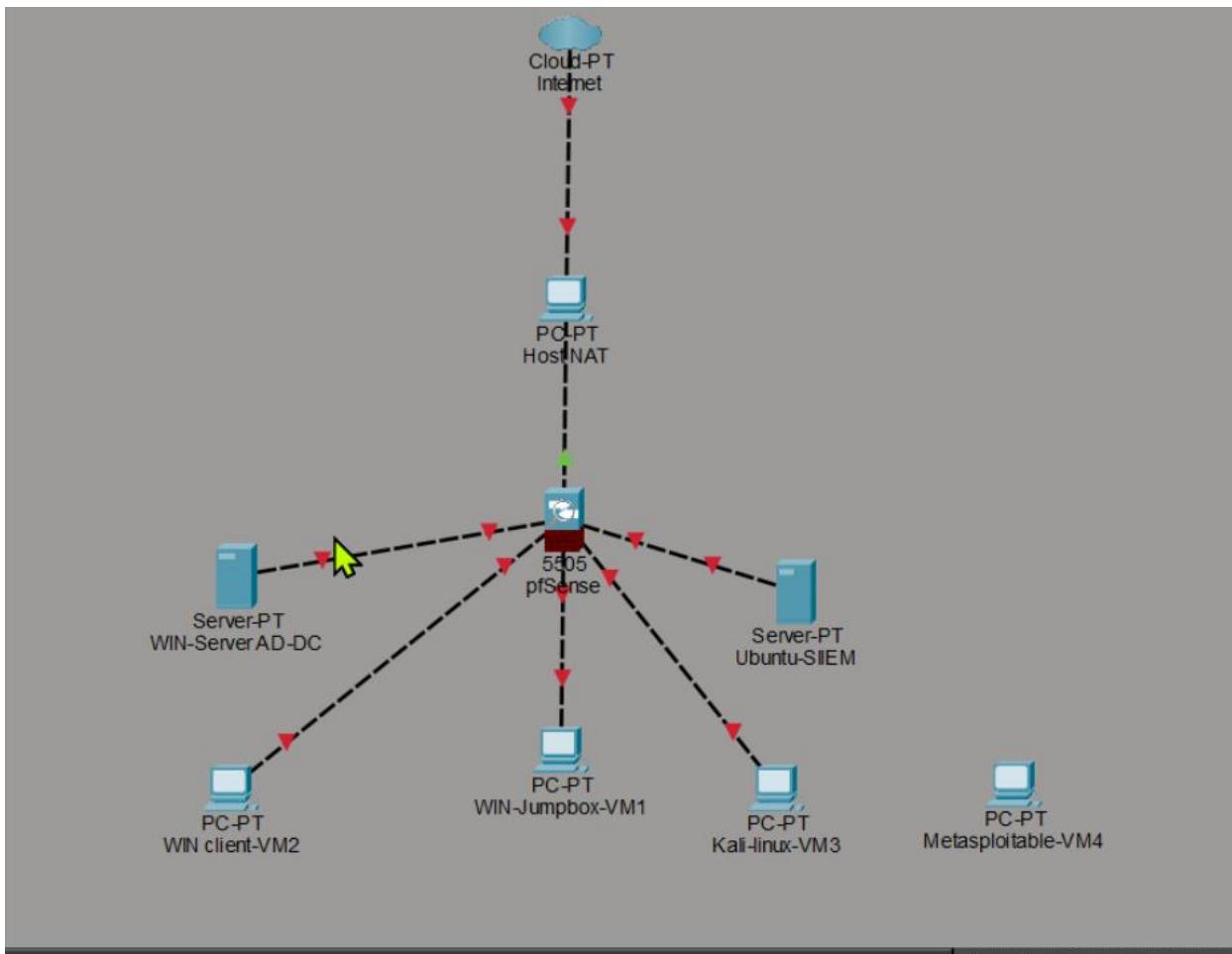
- Built a Blue-Team SOC lab named **Digital Defence 3728**.
- Achieved: AD + DNS health, pfSense gateway + NAT, Splunk Enterprise running and accepting logs, Jumpbox management access (SSH/RDP), Windows UF and Sysmon telemetry ingestion, and controlled attacker/test hosts.
- Captured and resolved real faults: DC rename → stale DNS/glue A record; Ubuntu Netplan/cloud-init override; incorrect subnet assignment; RDP profile & firewall issues; all fixes and verification commands are documented.

2 — Architecture & VM sizing

Network: single isolated lab LAN 192.168.60.0/24, pfSense LAN 192.168.60.1, DC/DNS 192.168.60.10, SIEM 192.168.60.20



[screenshot ]



VM sizing (final):

- pfSense: 1 vCPU / 1 GB RAM / 10 GB disk
- Windows Server 2022 (DC): 2 vCPU / 4 GB RAM / 80 GB disk
- Ubuntu Server (SIEM): 4 vCPU / 12 GB RAM / 200 GB disk
- Jumpbox (analyst): 2 vCPU / 8 GB RAM / 80 GB disk
- Windows Client: 2 vCPU / 4 GB RAM / 80 GB disk
- Kali: 2 vCPU / 2 GB RAM / 40 GB disk
- Metasploitable2: 1 vCPU / 1 GB RAM / 20 GB disk

3 — Files / ISOs (official sources)

Downloaded official images only (evaluation or community builds):

- pfSense: <https://www.pfsense.org/download/>
- Ubuntu Server 24.04 LTS: <https://ubuntu.com/download/server>
- Splunk Enterprise (Linux): https://www.splunk.com/en_us/download.html
- Splunk Universal Forwarder (Windows):
https://www.splunk.com/en_us/download/universal-forwarder.html
- Windows Server Evaluation / Windows 11 Enterprise LTSC: Microsoft Evaluation Center
- Kali Linux: <https://www.kali.org/get-kali/>
- Metasploitable2: Rapid7 / official archived images

4 — Step-by-step build — overview

High-level order of execution:

1. Created VMware networks (VMnet8 NAT, VMnet1 Host-only 192.168.60.0/24), disable host DHCP on the host-only network.
2. Created VMs with sizing above (attach ISOs).
3. Installed pfSense (assigned WAN = VMnet8, LAN = VMnet1), set LAN IP 192.168.60.1, enabled DHCP for lab.
4. Installed Windows Server 2022, configured static IP, installed AD DS & DNS, promoted to domain digitaldefence3728.lab (DC).
5. Installed Ubuntu Server, configured static network to 192.168.60.20, hardened netplan/cloud-init, installed Splunk Enterprise.
6. Configured pfSense syslog to forward to Splunk, set firewall rules.
7. Created Jumpbox VM (Windows 11 LTSC), set DNS to DC, installed tools.
8. Created Windows client, set DNS to DC, joined domain, installed Splunk UF and Sysmon.

9. Added Kali & Metasploitable2, kept powered off when not testing.

10. Validated logs in Splunk and ran sample searches.

Each major section below pairs steps with commands and validation checks.

5 — pfSense installation & configuration

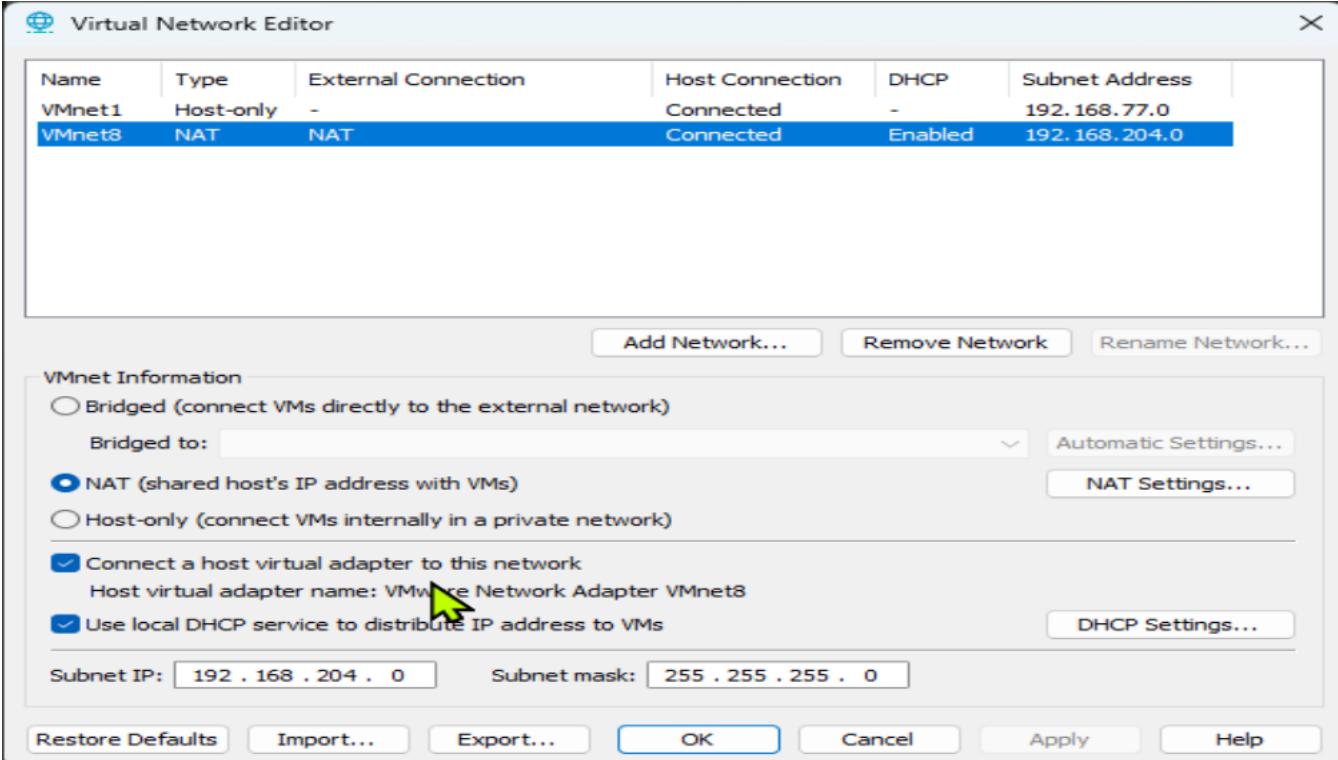
Goal: pfSense provides a safe gateway for internet access and isolates the lab LAN, while forwarding logs to the Splunk SIEM.

A. VMware network preparation (host)

- Opened VMware Workstation → Edit → Virtual Network Editor (Ran as Administrator).
- VMnet8: NAT (defaults) — used for pfSense WAN.
- Added VMnet1: Host-only, Subnet 192.168.60.0, Mask 255.255.255.0 — Disabled VMware DHCP (pfSense will provide DHCP).
- Saved configuration.

[screenshots  ]

VMnet8: NAT | WAN | DHCP Enabled



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	-	192.168.77.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.204.0

VMnet Information

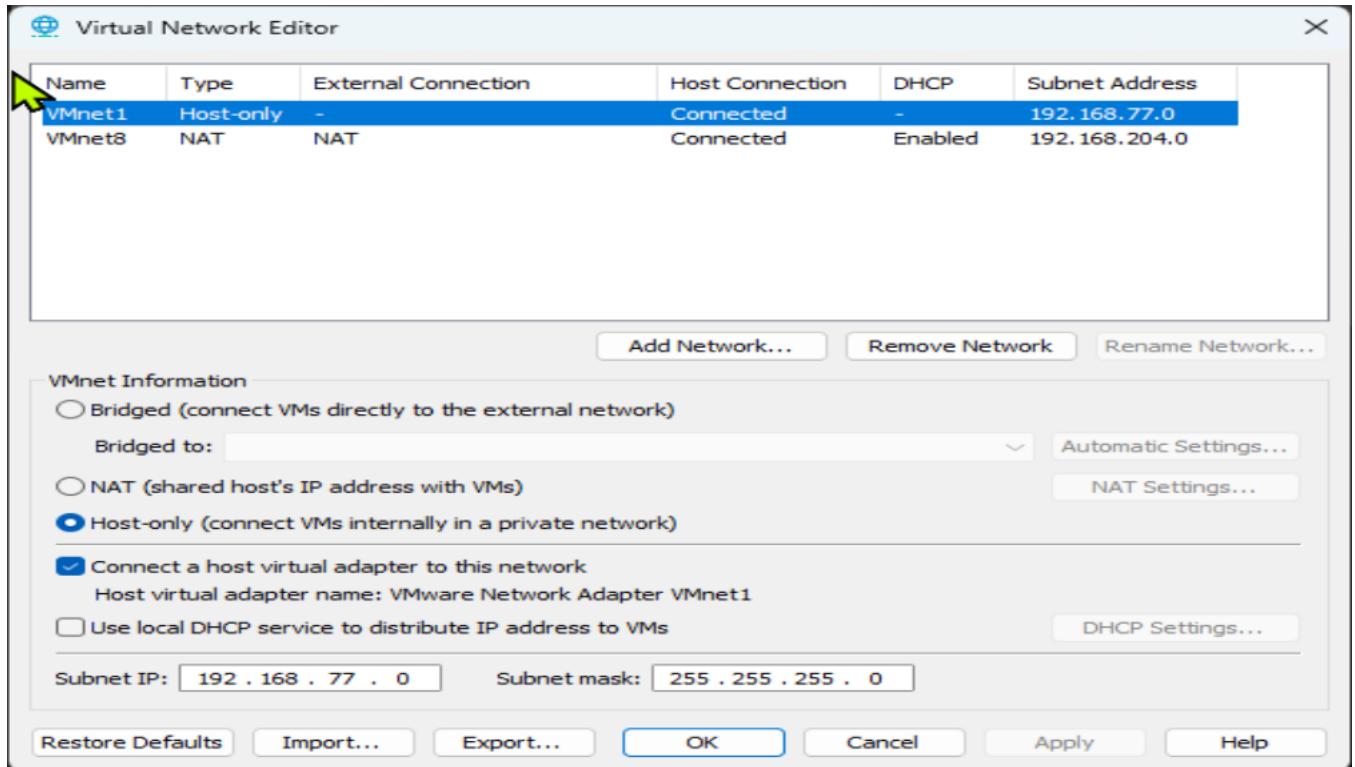
Bridged (connect VMs directly to the external network)
 NAT (shared host's IP address with VMs)
 Host-only (connect VMs internally in a private network)

Connect a host virtual adapter to this network
Host virtual adapter name: **VMware Network Adapter VMnet8**

Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 204 . 0 Subnet mask: 255 . 255 . 255 . 0

Buttons: Add Network... Remove Network Rename Network... Automatic Settings... NAT Settings... DHCP Settings... Restore Defaults Import... Export... OK Cancel Apply Help

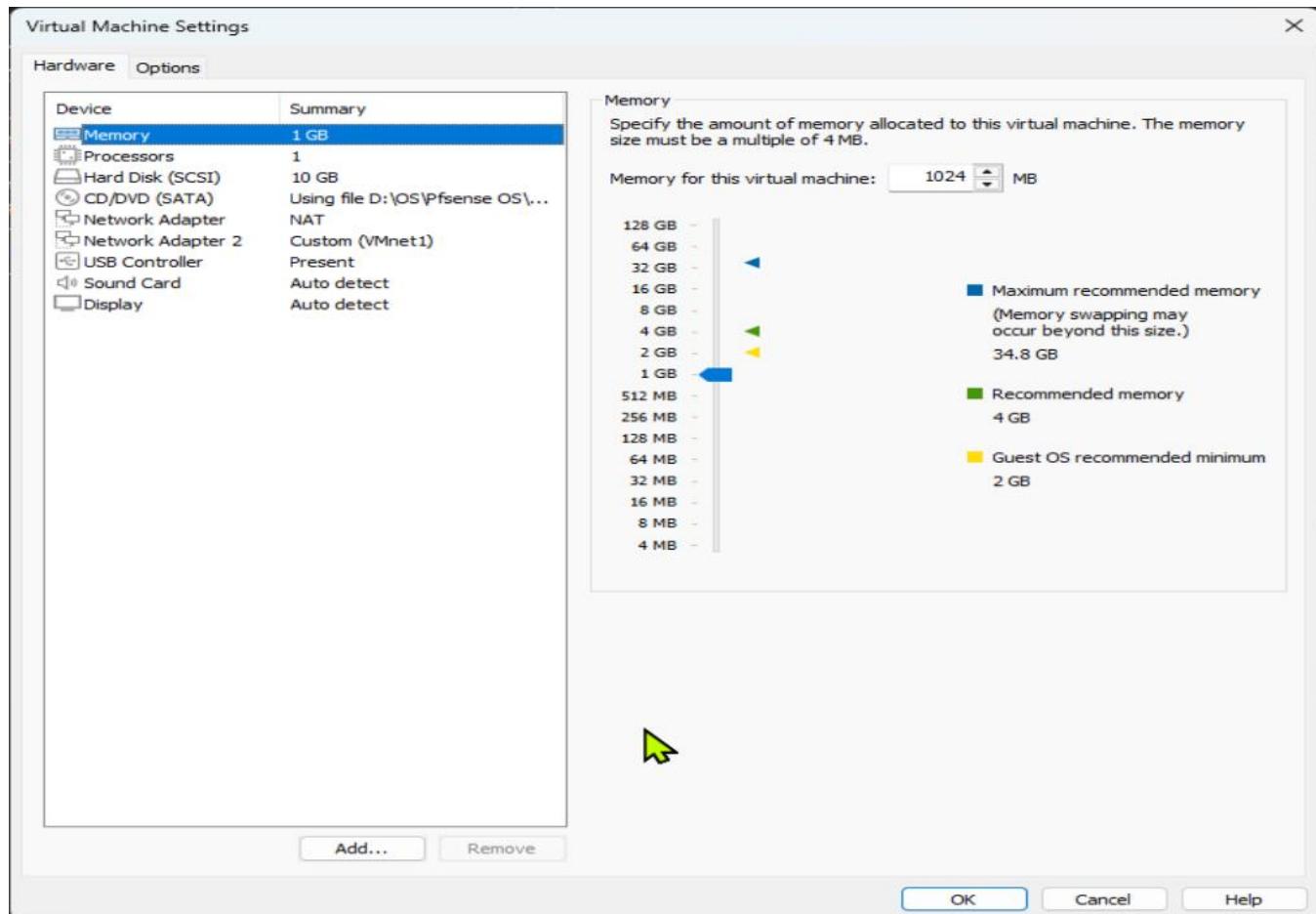


VMnet1: LAN | DHCP Disabled

B. Created pfSense VM

- Guest OS: Netgate-Installer v1.1
- Disk: 10GB, thin provisioned.
- Memory: 1 GB.
- CPU: 1 vCPU.
- Network adapters:
 - Adapter 1 → VMnet8 (WAN).
 - Adapter 2 → VMnet1 (LAN).

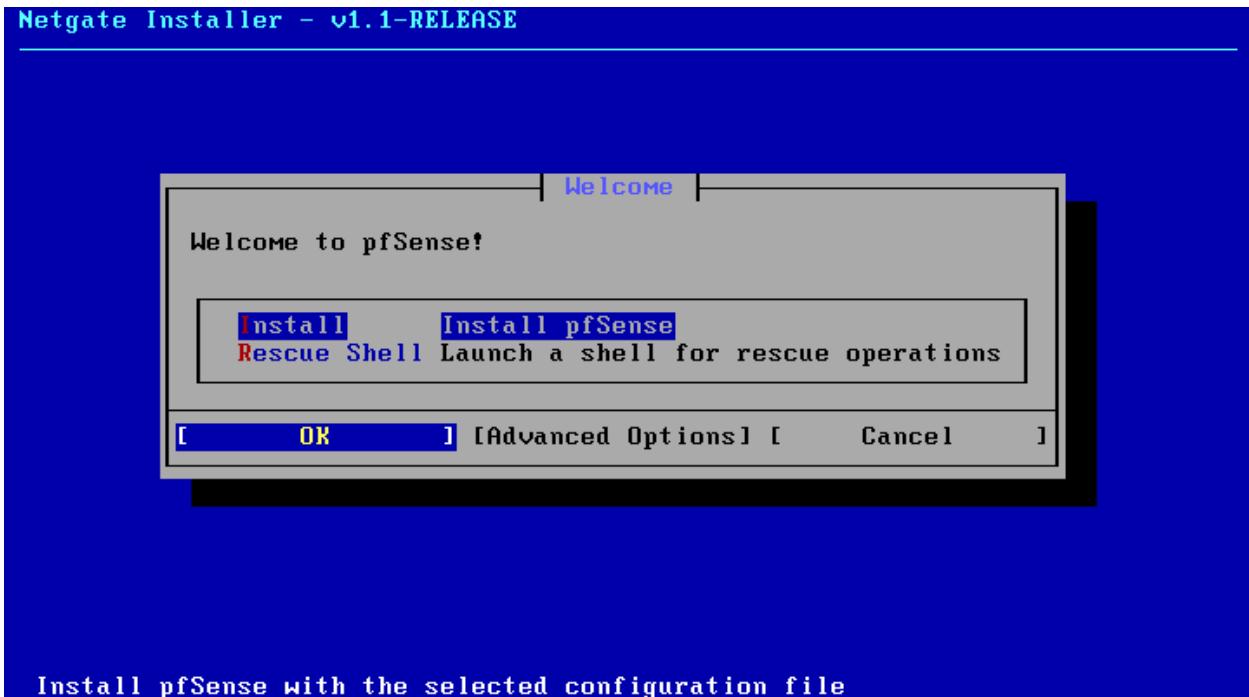
[screenshots]



C. Installed pfSense (console)

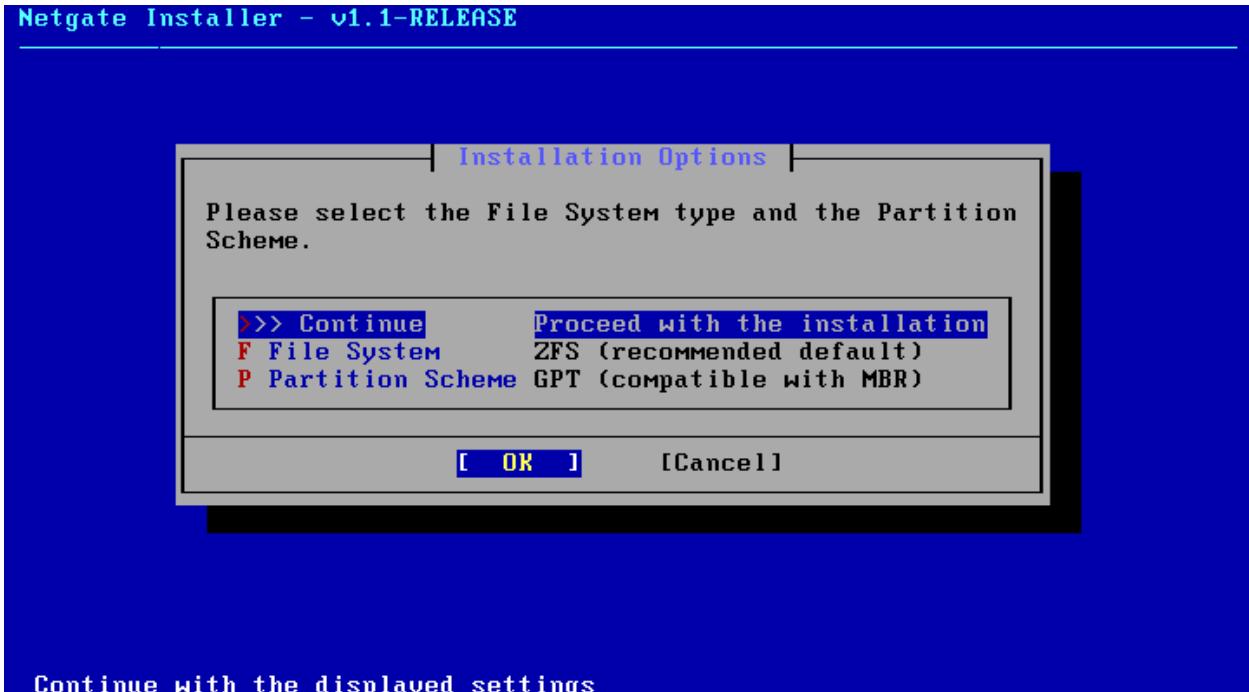
- Booted from pfSense ISO and followed installer defaults.
- Accepted partitioning and standard options; rebooted into installed pfSense.

[screenshots ↗ ↘]



Install pfSense with the selected configuration file

Netgate Installer - v1.1-RELEASE



Continue with the displayed settings

```
----- Installation Details -----  
Installing Current Stable Version (2.8.1)  
Selected configuration file: default (blank) configuration.  
Exporting the network settings to pfSense.  
Selected file system type and partition scheme: ZFS and GPT.  
ZFS Pool Name: pfSense.  
Installing pkg:  
Updating pfSense-core repository catalogue...  
Fetching meta.conf: . done  
Fetching data.pkg: . done  
Processing entries: . done  
pfSense-core repository update completed. 4 packages processed.  
Updating pfSense repository catalogue...  
Fetching meta.conf: . done
```

D. Assigned interfaces (console)

At pfSense console:

- Option 1: Assign interfaces — chose NIC mapped to VMnet8 [em0] as WAN and NIC mapped to VMnet1 [em1] as LAN.
- Option 2: Set LAN IP to 192.168.60.1 with prefix /24. Enabled DHCP.

[screenshot  ]

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.8.1-RELEASE amd64 20251126-2112
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 6a7e325b34b69ded18f2

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 192.168.204.128/24
LAN (lan) -> em1 -> v4: 192.168.60.1/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults       13) Update from console
5) Reboot system                   14) Enable Secure Shell (sshd)
6) Halt system                     15) Restore recent configuration
7) Ping host                       16) Restart PHP-FPM
8) Shell

Enter an option: █
```

E. GUI setup

From Jumpbox on LAN:

- Browsed to <https://192.168.60.1>
- Ran setup wizard:
 - Hostname: dd3728-pfsense.
 - Domain: dd3728.lab.
 - WAN: DHCP (VMnet8).
 - LAN: 192.168.60.1/24.
 - Admin password: *****

[screenshots  ]

The screenshot shows the pfSense Status / Dashboard page. At the top, there's a header with the pfSense logo and navigation links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A "Sign in" button and a "Finish setup" link are also present.

System Information

Name	dd3728-pfSense.dd3728.lab
User	admin@192.168.60.102 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 6a7e325b34b69ded18f2
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Mon Mar 24 2025 Boot Method: BIOS
Version	2.8.1-RELEASE (amd64) built on Wed Nov 26 23:12:00 SAST 2025 FreeBSD 15.0-CURRENT
CPU Type	Intel(R) Core(TM) i5-10500H CPU @ 2.50GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- [Upgrade Your Support](#)
- [Community Support Resources](#)
- [Netgate Global Support FAQ](#)
- [Official pfSense Training by](#)

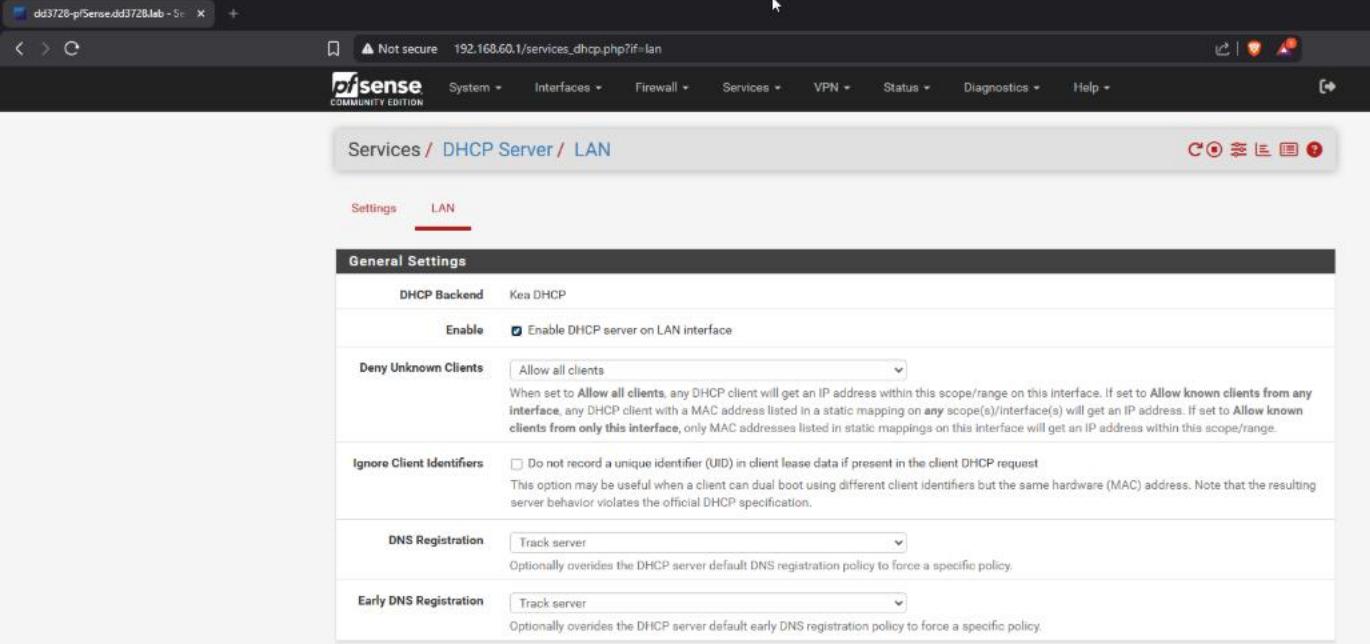
At the bottom, there's a toolbar with icons for File, Search, and various system functions, along with the date and time (12/12/2025, 2:23 AM).

F. DHCP & DNS settings

In pfSense GUI:

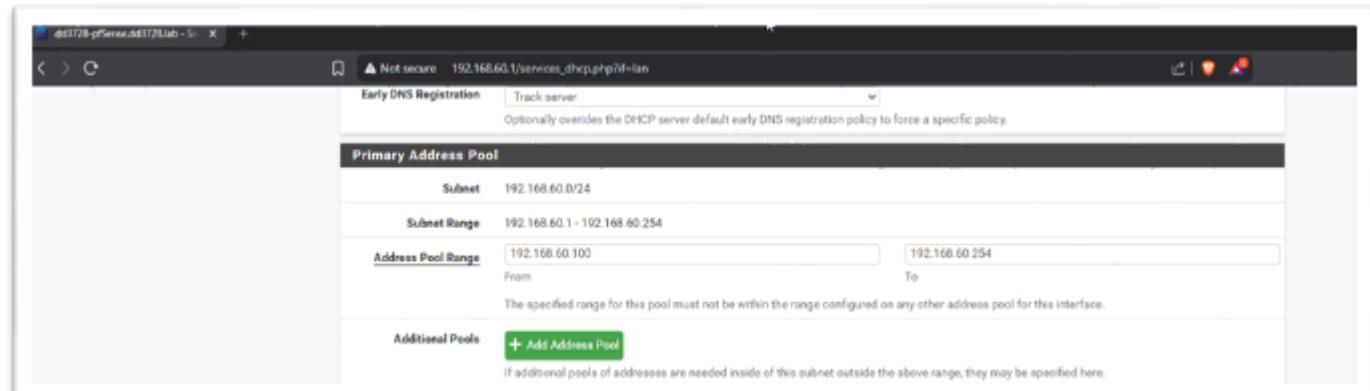
- Navigated to: Services → DHCP Server → LAN.
- Enabled DHCP (optional but convenient).
- Range: 192.168.60.100 → 192.168.60.254.
- **DNS servers:** set 192.168.60.10 (the Domain Controller) as DNS server, so clients use AD DNS for name resolution (instead of pfSense).

[screenshots]



The screenshot shows the pfSense DHCP Server LAN settings page. The 'General Settings' section includes:

- DHCP Backend: Kea DHCP
- Enable: Enable DHCP server on LAN interface
- Deny Unknown Clients: Allow all clients (with a note about scope/range and known clients)
- Ignore Client Identifiers: Do not record a unique identifier (UID) in client lease data if present in the client DHCP request (with a note about dual boot and MAC addresses)
- DNS Registration: Track server (with a note about overriding default policy)
- Early DNS Registration: Track server (with a note about overriding default early DNS registration policy)



The screenshot shows the pfSense DHCP Server LAN settings page, specifically the Primary Address Pool configuration. It includes:

- Subnet: 192.168.60.0/24
- Subnet Range: 192.168.60.1 - 192.168.60.254
- Address Pool Range: From 192.168.60.100 To 192.168.60.254 (with a note about overlapping ranges)
- Additional Pools: + Add Address Pool (button)

G. Firewall rules

- Firewall → Rules → LAN: added baseline “Allow LAN net → any” rule for lab convenience.
- Kept default WAN deny rules.
- Enabled logging on reject/deny rules to feed meaningful traffic into Splunk.

[[screenshots](#)  ]

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/2.84 MB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓ 13/2.13 MB	IPv4	192.168.60.0/24	*	*	*	*	*		Allow SOC outbound traffic	
✗ 0/0 B	IPv4	192.168.60.40	*	192.168.60.0/24	*	*	*		Block direct attack to SOC network	

Actions:

H. Remote syslog forwarding to Splunk

- Status → System Logs → Settings → Remote Logging Options.
- Remote log server: 192.168.60.20 .
- Port: 514 (UDP) .
- Applied and saved.

[screenshots]

Enable Remote Logging Send log messages to remote syslog server

Source Address LAN
This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol IPv4
This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; if an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers 192.168.60.20:514 IP:port IP:port

Remote Syslog Contents

- Everything
- System Events
- Firewall Events
- DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- General Authentication Events
- Captive Portal Events
- VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
- Gateway Monitor Events
- Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
- Network Time Protocol Events (NTP Daemon, NTP Client)
- Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set alogd on the remote server to accept syslog messages from pfSense.

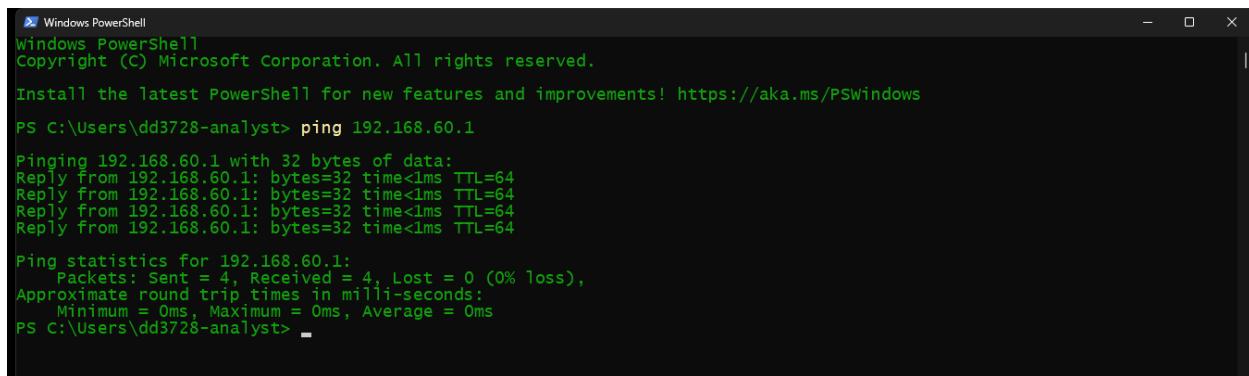
Actions:

I. Validation

From Jumpbox (PowerShell):

```
#powershell
pinged 192.168.60.1
```

[screenshots ↗ ↘]



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

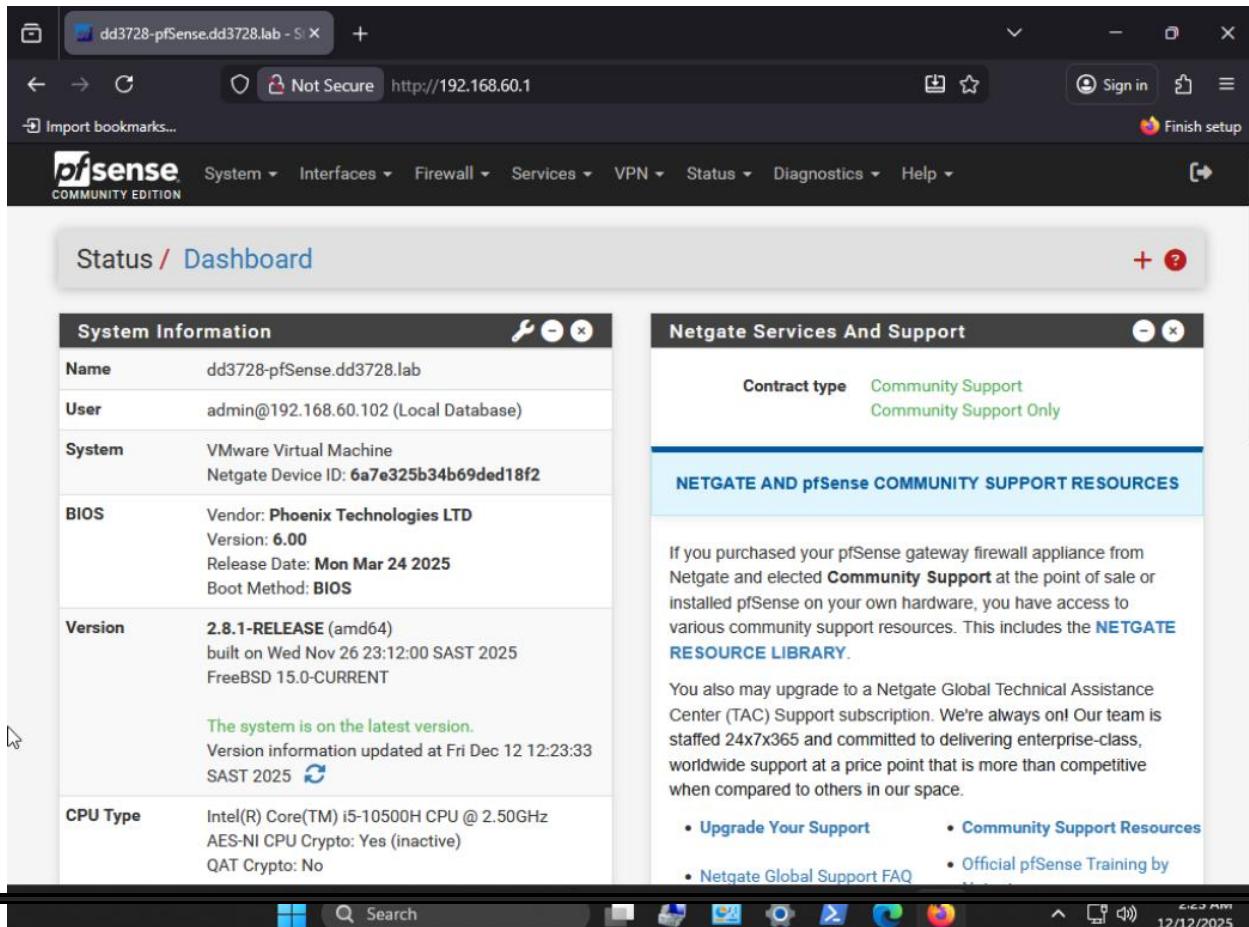
PS C:\Users\dd3728-analyst> ping 192.168.60.1

Pinging 192.168.60.1 with 32 bytes of data:
Reply from 192.168.60.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.60.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\dd3728-analyst> -
```

- Browse to <https://192.168.60.1> and confirmed pfSense GUI loads.

[screenshots ↗ ↘]



System Information	
Name	dd3728-pfSense.dd3728.lab
User	admin@192.168.60.102 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 6a7e325b34b69ded18f2
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Mon Mar 24 2025 Boot Method: BIOS
Version	2.8.1-RELEASE (amd64) built on Wed Nov 26 23:12:00 SAST 2025 FreeBSD 15.0-CURRENT
CPU Type	Intel(R) Core(TM) i5-10500H CPU @ 2.50GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

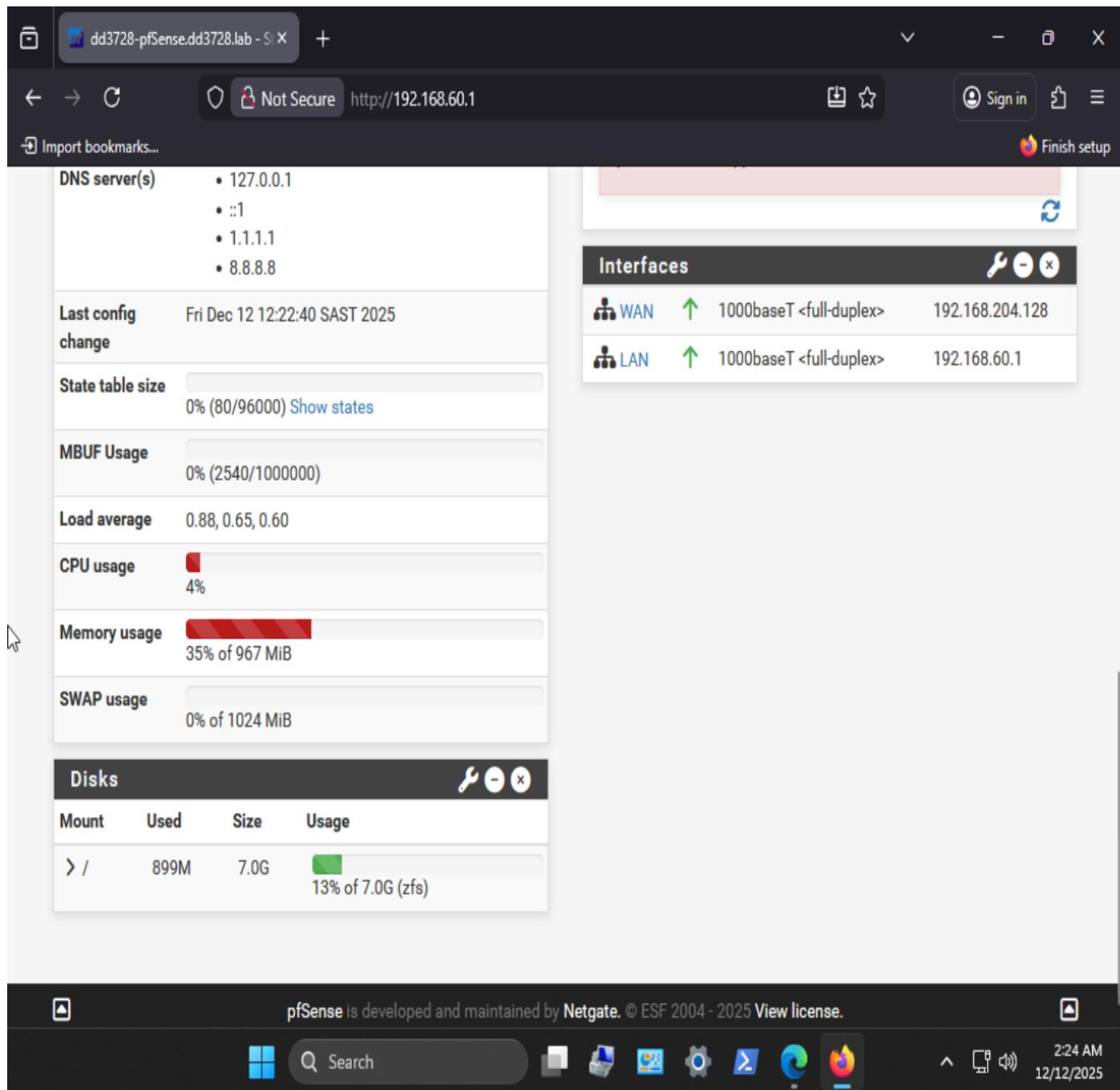
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by

On pfSense GUI: Status → Interfaces:

- Confirmed WAN has an IP from VMnet8 (NAT).
- Confirmed LAN is 192.168.60.1/24.

[screenshots  ]



The screenshot shows the pfSense Status interface. On the left, there's a sidebar with various status metrics:

- DNS server(s)**: 127.0.0.1, ::1, 1.1.1.1, 8.8.8.8
- Last config change**: Fri Dec 12 12:22:40 SAST 2025
- State table size**: 0% (80/96000) [Show states](#)
- MBUF Usage**: 0% (2540/1000000)
- Load average**: 0.88, 0.65, 0.60
- CPU usage**: 4%
- Memory usage**: 35% of 967 MiB
- SWAP usage**: 0% of 1024 MiB

On the right, the **Interfaces** section shows two entries:

 WAN	 1000baseT <full-duplex>	192.168.204.128	 
 LAN	 1000baseT <full-duplex>	192.168.60.1	 

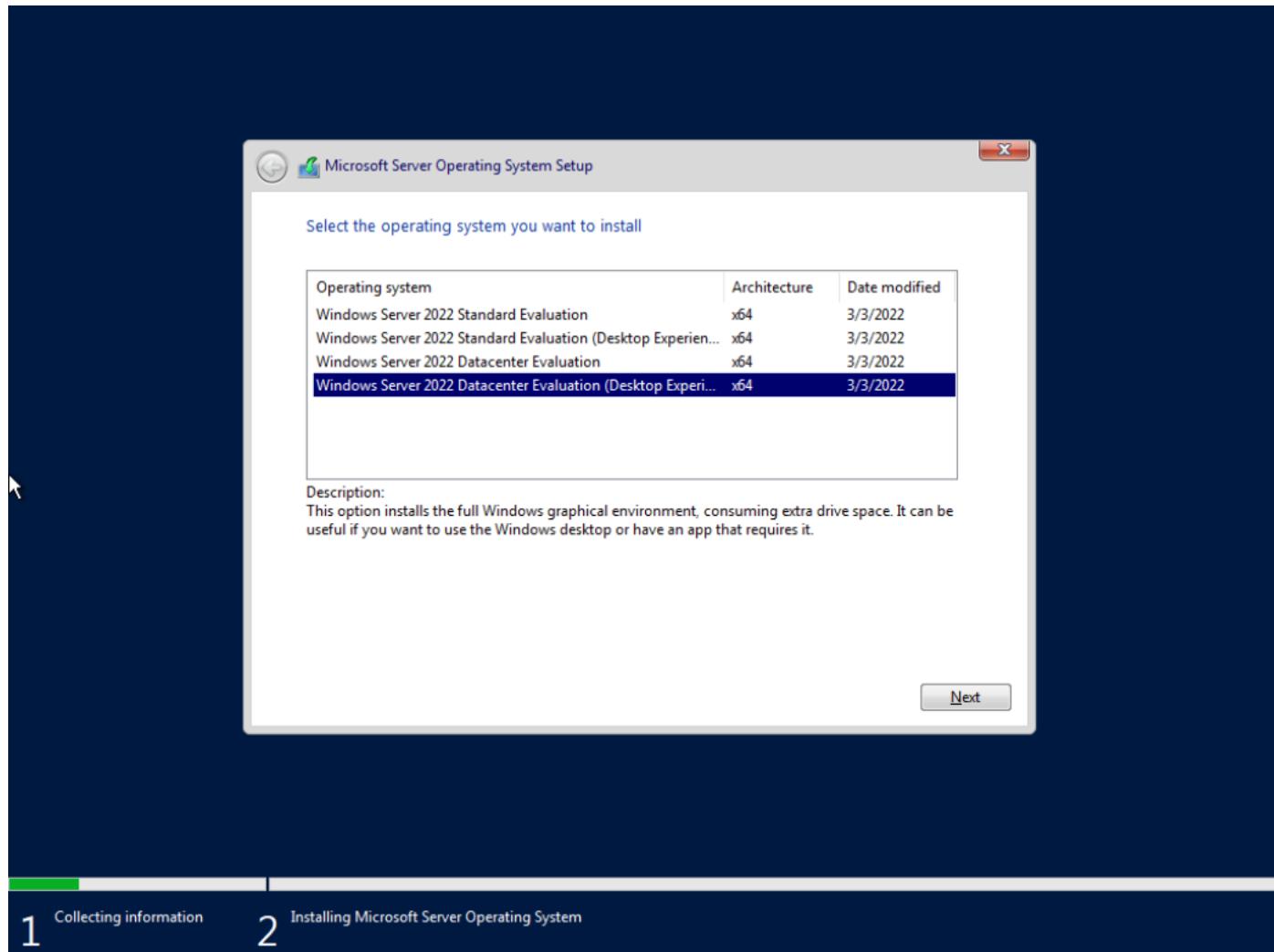
At the bottom, there's a footer with the pfSense logo and copyright information, along with a search bar and various navigation icons.

6 — Windows Server 2022: installed, DC promotion & DNS & DC troubleshooting ref: 6-(F)

Goal: Created digitaldefence3728.lab, made the DC authoritative for AD DNS, and validated Netlogon SRV registrations.

A. OS installation & static IP

[screenshots  ]

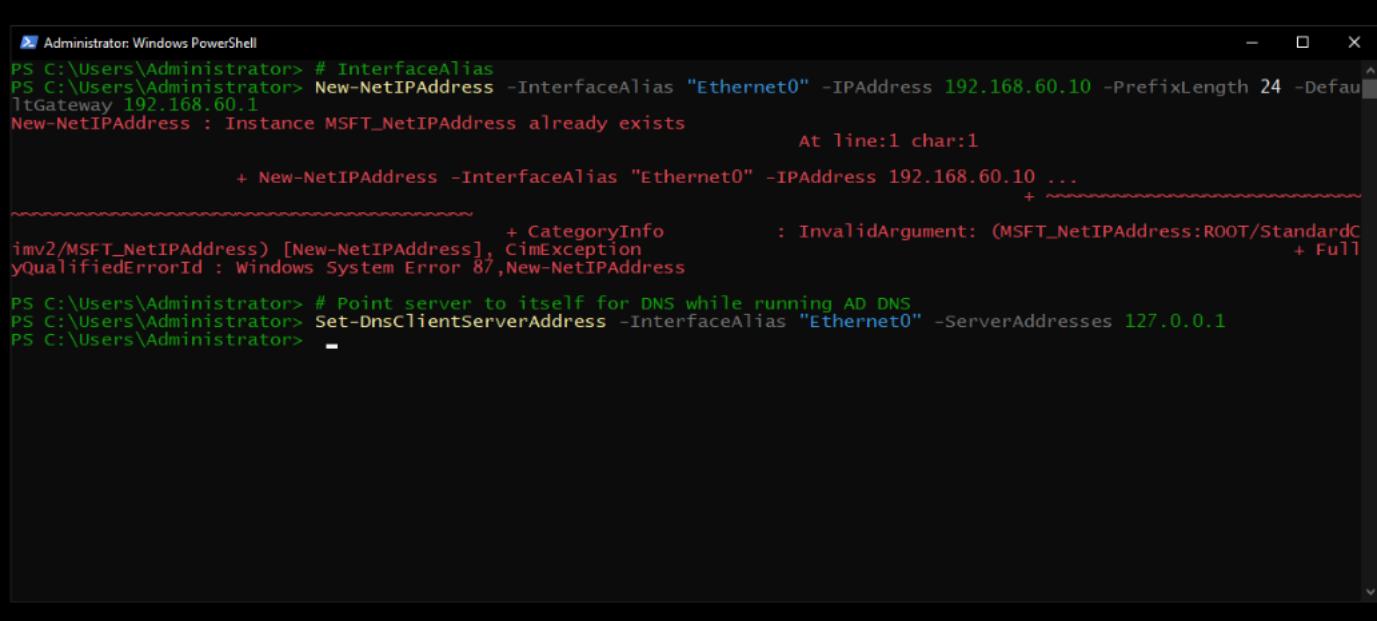


- After Windows Server installation and network driver readiness,
- configured static networking (ran as Administrator):

```
#powershell
```

```
New-NetIPAddress -InterfaceAlias "Ethernet0" -IPAddress  
192.168.60.10 -PrefixLength 24 -DefaultGateway 192.168.60.1  
Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" -  
ServerAddresses 127.0.0.1
```

[screenshots  ]



Verified:

```
#powershell
```

```
ipconfig /all
```

[screenshots  ]

B. Installed AD DS role

#powershell

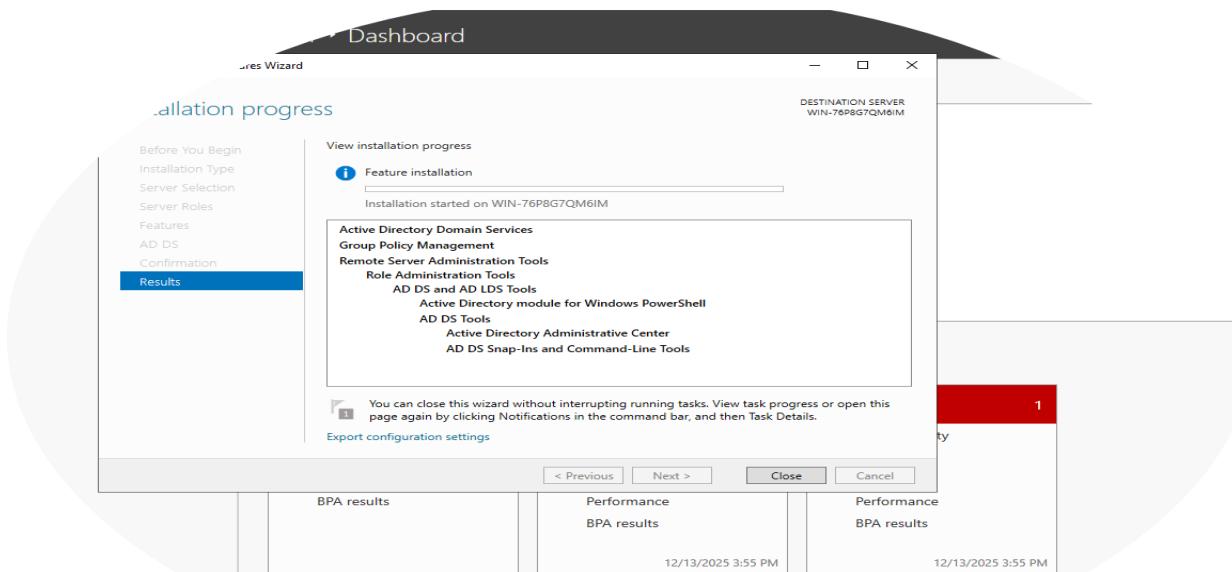
```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

Purpose

“By executing this command, the server will be prepared to function as a domain controller, allowing for centralized management of user and computer accounts in a domain environment.”

Note: AD DS was installed via GUI instead

[screenshots]



C. Promote to forest root (new domain)

```
#powershell
```

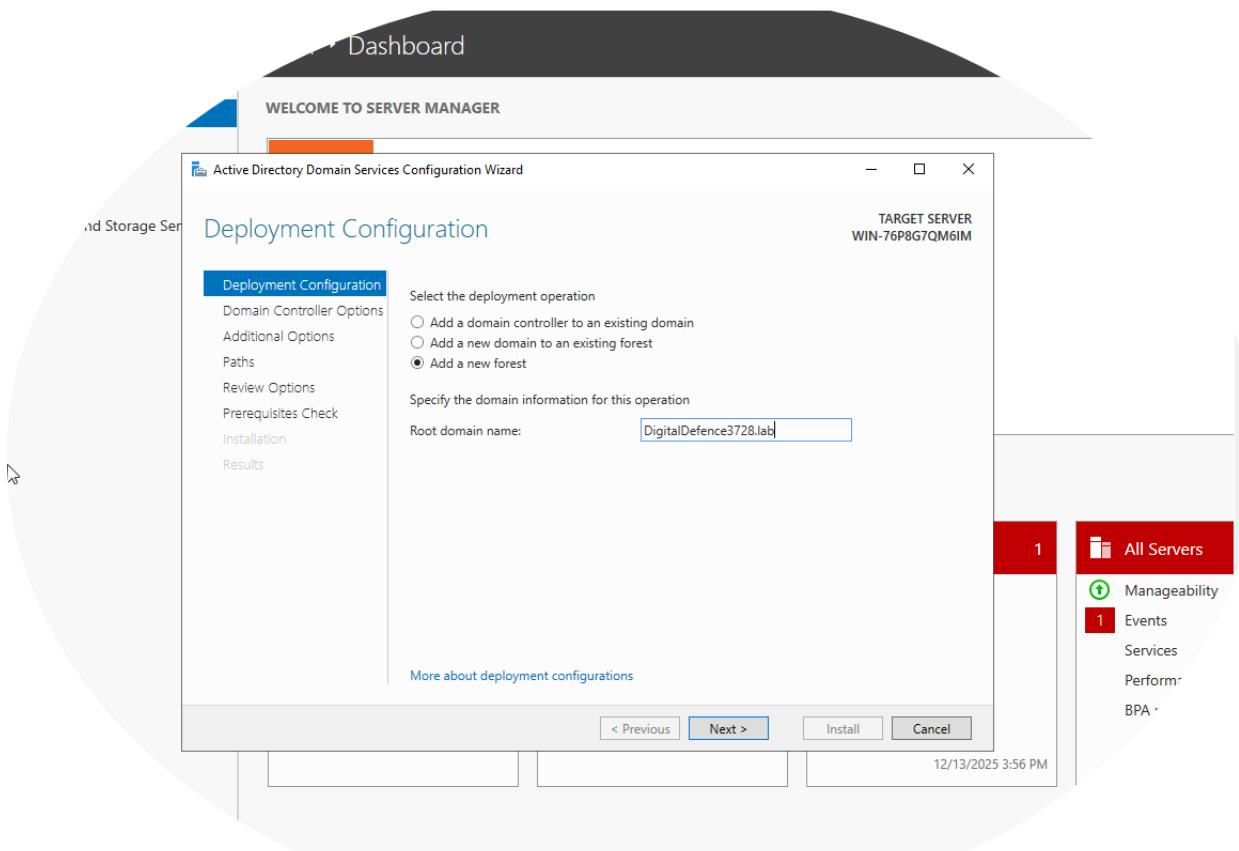
```
Install-ADDSForest -DomainName "digitaldefence3728.lab" -  
DomainNetbiosName "DD3728" -InstallDNS
```

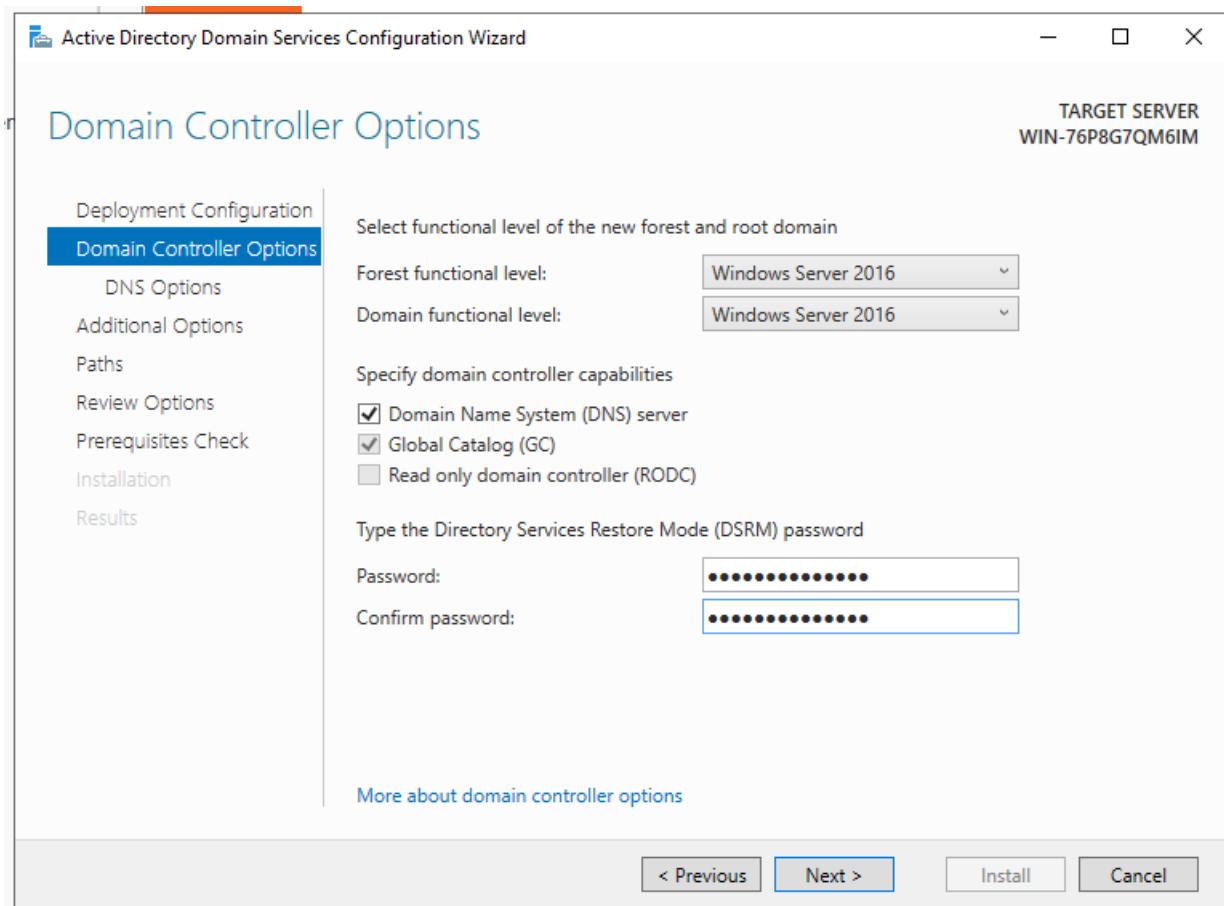
Purpose

"This command effectively sets up a new Active Directory forest named "digitaldefence3728.lab" with the NetBIOS name "DD3728" and installs the necessary DNS services needed for domain functionality. It serves as a foundational step in deploying Active Directory services."

- Set Directory Services Restore Mode (DSRM) password when prompted.
- Rebooted server after promotion.

[screenshots  ]





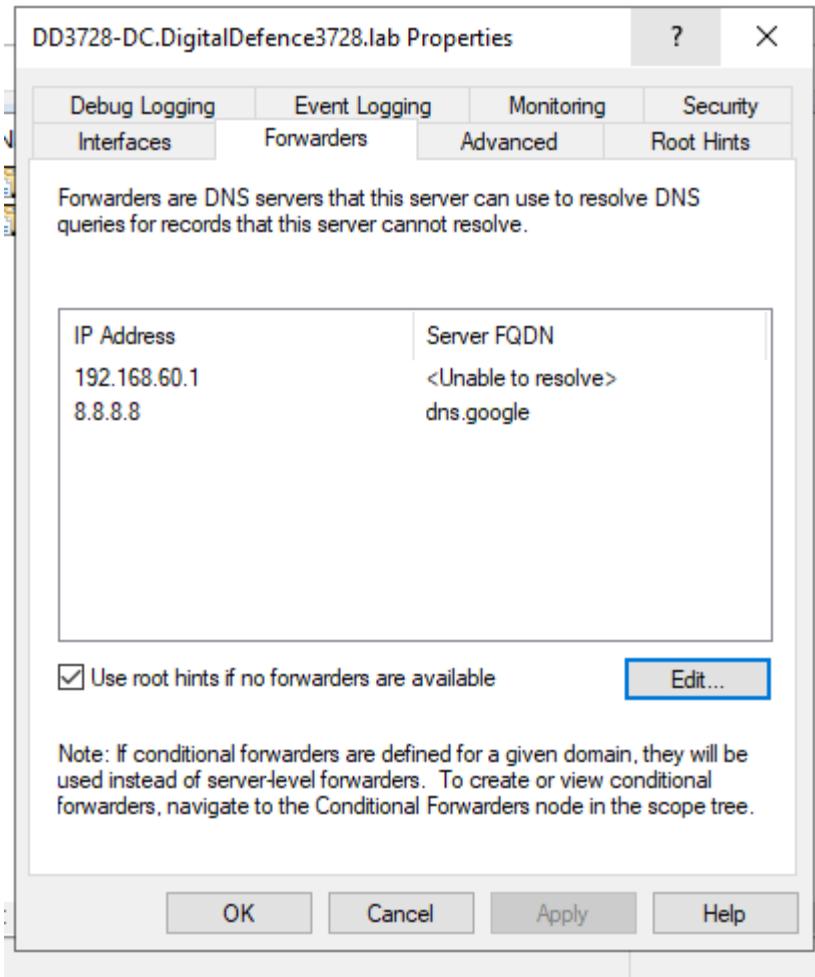
D. DNS forwarders

In DNS Manager → Server → Properties → Forwarders:

- Add pfSense IP 192.168.60.1 and FQDN dns.google → IP 8.8.8.8 a public resolver as a secondary forwarder for resilience.

"The Domain Controller is the authoritative DNS for the AD domain and therefore resolves all internal SRV/A records. For Internet name resolution, the DC forwards unknown queries to our gateway (pfSense) centralized outbound DNS, logging and policy enforcement. pfSense then forwards to public resolvers (e.g., dns.google). This split of responsibilities — DC = internal authority, pfSense = outbound resolver/filter — mirrors enterprise best practice and keeps Active Directory service discovery reliable and auditable."

[screenshots]



Server FQDN: <Unable to resolve> next to 192.168.60.1

"That message simply says the DC cannot reverse-resolve the IP 192.168.60.1 to a hostname. It does not prevent forwarder functionality."

PowerShell equivalent:

```
#powershell
Add-DnsServerForwarder -IPAddress 192.168.60.1
Add-DnsServerForwarder -IPAddress 8.8.8.8
```

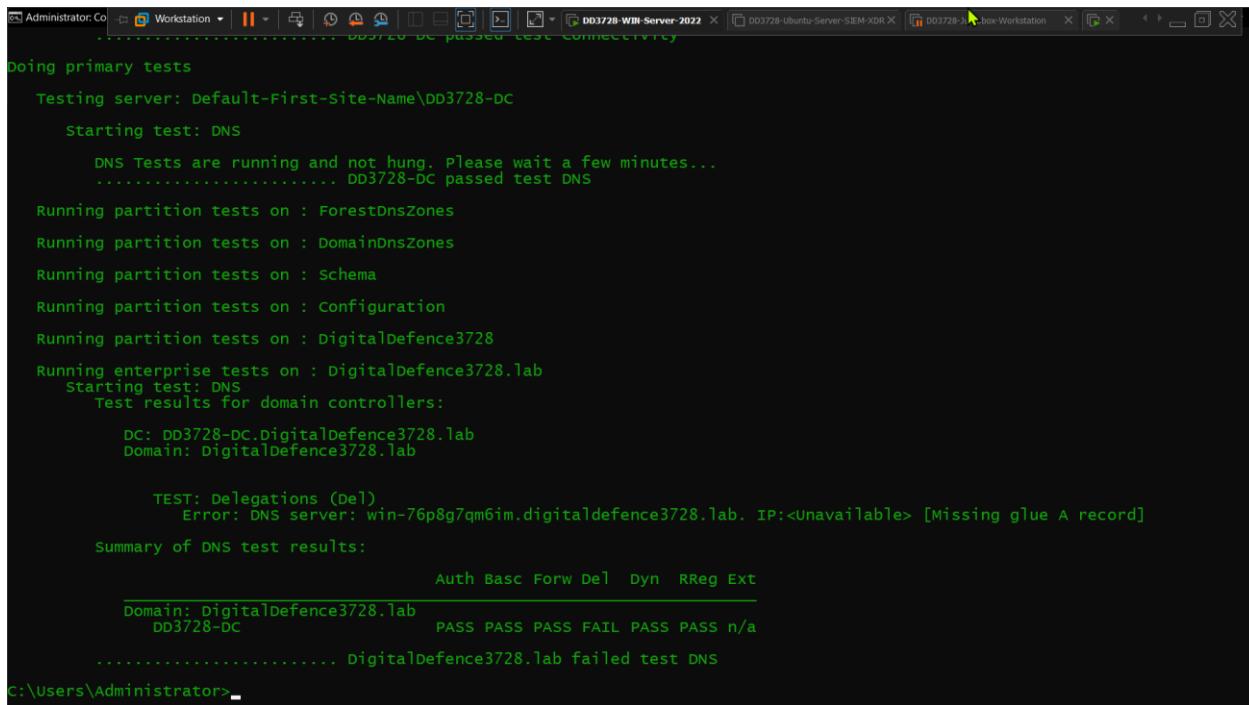
E. Netlogon / DNS registration & validation

```
#powershell [elevated] :
```

```
ipconfig /registerdns
net stop netlogon
net start netlogon
nltest /dsregdns
dcdiag /test:dns
```

Expected: DNS tests pass with proper SRV records and no missing glue A records.

[screenshot   failed ]



```
Administrator: C:\> Doing primary tests
Testing server: Default-First-Site-Name\DD3728-DC
Starting test: DNS
DNS Tests are running and not hung. Please wait a few minutes...
..... DD3728-DC passed test DNS
Running partition tests on : ForestDnsZones
Running partition tests on : DomainDnsZones
Running partition tests on : Schema
Running partition tests on : Configuration
Running partition tests on : DigitalDefence3728
Running enterprise tests on : DigitalDefence3728.lab
Starting test: DNS
Test results for domain controllers:
DC: DD3728-DC.DigitalDefence3728.lab
Domain: DigitalDefence3728.lab

TEST: Delegations (Del)
Error: DNS server: win-76p8g7qm6im.digitaldefence3728.lab, IP:<unavailable> [Missing glue A record]

summary of DNS test results:
Auth Basc Forw Del Dyn RReg Ext
Domain: DigitalDefence3728.lab
DD3728-DC PASS PASS PASS FAIL PASS PASS n/a
..... DigitalDefence3728.lab failed test DNS
C:\users\Administrator>
```

 Reason why DNS test failed = ref: DC troubleshoot = 6_F 

I executed the following command sequence to ensure proper DNS registration and functionality related to the Netlogon service on the domain controller. This is critical for maintaining network authentication and domain operations.

Command Breakdown

ipconfig /registerdns: forces the computer to register its DNS records to the DNS server. Essential for allowing other devices to locate the domain controller.

net stop netlogon: Stops the Netlogon service, which is responsible for facilitating user authentication and accounts in the domain. Stopping it may be necessary to refresh its state.

net start netlogon: Restarts the Netlogon service, re-establishing connections and ensuring it can communicate effectively with the domain controller.

nlttest /dsregdns: This command triggers registration of the domain controller's DNS records. It confirms that the domain controller is properly registered in the domain.

dcdiag /test:dns: This diagnostic tool tests the DNS health of the domain controller, ensuring that DNS queries and configurations are functioning correctly. It helps identify any configuration issues that may affect network operations.

Purpose

"This sequence of commands was executed to validate and refresh the DNS registration of the domain controller, ensuring optimal communication and authentication across the network."

F. DC troubleshooting

DC hostname was changed after promotion:

1. Removed stale A and PTR records in DNS Manager for the old hostname
(WIN-78P8G7QM6IM)
 - ★ Through **DC event view** I managed to trace when the last was I logged off prior to hostname change.

Channel: Security

Computer: **WIN-78P8G7QM6IM _ WIN76P8G7QM6IM.DigitalDefence3728.lab**

12/14/2025 9:54:00 PM

[screenshots  ]

old host name → **WIN76P8G7QM6IM.DigitalDefence3728.lab**

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Windows Logs, Application, Security, System, and Forwarded Events. The Security log is selected. The right pane shows a list of events with the title "Security Number of events: 40,792 (0) New events available". One event is highlighted: "Event 4647, Microsoft Windows security auditing". The details pane shows the event was triggered by "User initiated logoff" and provides a subject summary. The properties pane on the right lists various actions like Open Saved Log..., Create Custom View..., and Help.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	12/14/2025 9:42:01 PM	Microsoft Windows security auditing.	4626	Other Policy Change Events
Audit Success	12/14/2025 9:42:01 PM	Microsoft Windows security auditing.	4696	Process Creation
Audit Success	12/14/2025 9:42:01 PM	Microsoft Windows security auditing.	4688	Process Creation
Audit Success	12/14/2025 9:54:01 PM	Eventlog	1100	Service shutdown
Audit Success	12/14/2025 9:54:01 PM	Microsoft Windows security auditing.	4647	Logoff
Audit Success	12/14/2025 9:55:50 PM	Microsoft Windows security auditing.	4742	Computer Account Management
Audit Success	12/14/2025 9:55:50 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	12/14/2025 9:55:50 PM	Microsoft Windows security auditing.	4742	Computer Account Management

2. Created correct A and PTR records for the new hostname (DD3728-DC → 192.168.60.10).

DD3728-DC → digitaldefence3728.lab

[screenshots ↗ ↘]

XML view

This screenshot shows the same Event Viewer interface but with the "XML View" option selected in the details pane. The XML representation of the event data is displayed, including the event ID, source, date, time, task category, and detailed subject information. The properties pane on the right remains visible.

```

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5470-4994-a5ba-3e3b0328c30d}" />
    <EventID>4647</EventID>
    <Version>0</Version>
    <Level>0</Level>
    <Task>12544</Task>
    <Opcode>0</Opcode>
    <Keywords>0x0020000000000000</Keywords>
    <TimeCreated SystemTime="2025-12-14T19:54:24.7455611Z" />
    <EventRecordID>3054</EventRecordID>
  </System>
  <Correlation />
  <Execution ProcessID="704" ThreadID="852" />
  <Channel>Security</Channel>
  <Computer>DD3728-DC.DigitalDefence3728.lab</Computer>
  <Security />
  <System />
  <EventData>
    <Data Name="SubjectUserSid">S-1-5-18</Data>
    <Data Name="SubjectUserName">DD3728-DC\$</Data>
    <Data Name="SubjectDomainName">DIGITALDEFENCE</Data>
    <Data Name="SubjectLogonId">0007</Data>
    <Data Name="LogonType">0</Data>
    <Data Name="LogonGuid" Value="00000000-0000-0000-0000-000000000000"></Data>
    <Data Name="TargetUserName">UMFD-1</Data>
    <Data Name="TargetDomainName">Font Driver Host</Data>
  </EventData>
</Event>

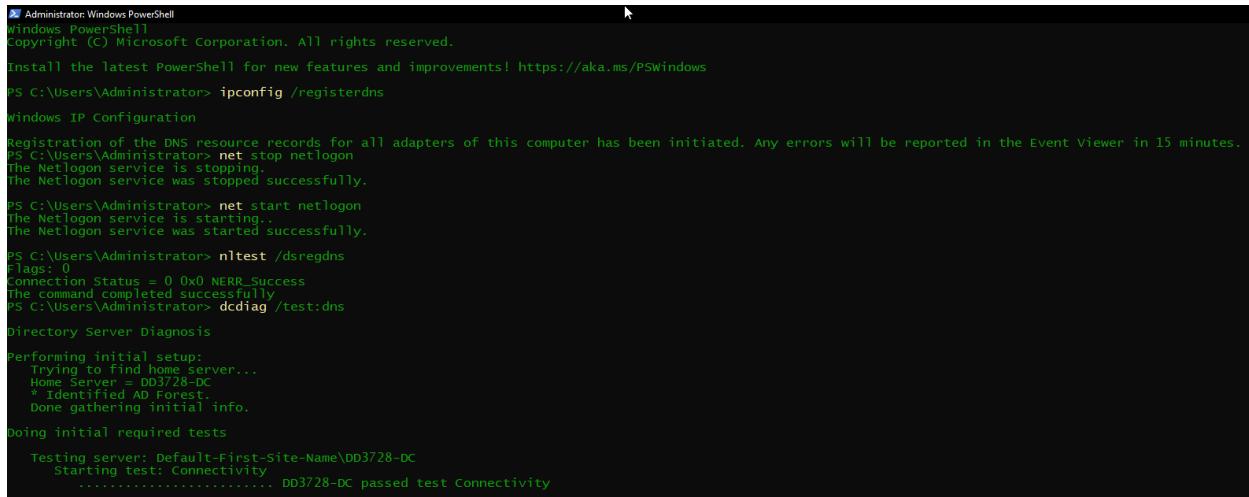
```

3. Re-ran:

```
#powershell
ipconfig /registerdns
net stop netlogon
net start netlogon
```

```
nltest /dsregdns
dcdiag /test:dns
```

[screenshot] DNS tests pass



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.

PS C:\Users\Administrator> net stop netlogon
The Netlogon service is stopping.
The Netlogon service was stopped successfully.

PS C:\Users\Administrator> net start netlogon
The Netlogon service is starting.
The Netlogon service was started successfully.

PS C:\Users\Administrator> nltest /dsregdns
Flags: 0
Connection Status = 0x0 NERR_Success
The command completed successfully.

PS C:\Users\Administrator> dcdiag /test:dns

Directory Server Diagnosis

Performing initial setup:
  Trying to find home server...
  Home Server = DD3728-DC
  * Identified AD Forest.
  Done gathering initial info.

Doing initial required tests

  Testing server: Default-First-Site-Name\DD3728-DC
    Starting test: Connectivity
      ..... DD3728-DC passed test Connectivity
```

Doing primary tests

```
Testing server: Default-First-Site-Name\DD3728-DC

Starting test: DNS

  DNS Tests are running and not hung. Please wait a few minutes...
  ..... DD3728-DC passed test DNS

  Running partition tests on : ForestDnsZones

  Running partition tests on : DomainDnsZones

  Running partition tests on : Schema

  Running partition tests on : Configuration

  Running partition tests on : DigitalDefence3728

  Running enterprise tests on : DigitalDefence3728.lab
    Starting test: DNS
    ..... DigitalDefence3728.lab passed test DNS

PS C:\Users\Administrator>
```

G. Validation

```
#powershell

dcdiag /v
nslookup
set type=SRV
_ldap._tcp.dc._msdcs.digitaldefence3728.lab
```

Command Breakdown

dcdiag /v:

Purpose: This command runs the Domain Controller Diagnostic tool in verbose mode.

Function: It checks the health of the domain controller and provides detailed output about various aspects, such as replication, connectivity, and DNS configurations. This helps identify potential issues affecting Active Directory functionality.

nslookup:

Purpose: This command is a network administration command-line tool used for querying the Domain Name System (DNS).

Function: It allows you to obtain information about domain names and their corresponding IP addresses.

set type=SRV:

Purpose: This command sets the query type to SRV (Service) records.

Function: SRV records are used to locate specific services, including Active Directory services. By setting up the type to SRV, subsequent queries will focus on these service records.

_ldap._tcp.dc._msdcs.digitaldefence3728.lab:

Purpose: This is a specific DNS query for locating the LDAP service associated with domain controllers in the "digitaldefence3728.lab" domain.

Function: It queries the DNS for SRV records that provide information about LDAP servers that can authenticate users or applications for the specified domain.

Purpose [overall]

Together, these commands are executed to diagnose the health of a domain controller and query the DNS for LDAP service records. This is essential for ensuring that Active Directory services are accessible and functioning correctly, which is critical for user authentication and domain-related tasks.

[screenshot ]

```
Administrator: Windows PowerShell

Running partition tests on : DomainDnsZones
Starting test: CheckSDRefDom
..... DomainDnsZones passed test CheckSDRefDom
Starting test: CrossRefValidation
..... DomainDnsZones passed test CrossRefValidation

Running partition tests on : Schema
Starting test: CheckSDRefDom
..... Schema passed test CheckSDRefDom
Starting test: CrossRefValidation
..... Schema passed test CrossRefValidation

Running partition tests on : Configuration
Starting test: CheckSDRefDom
..... Configuration passed test CheckSDRefDom
Starting test: CrossRefValidation
..... Configuration passed test CrossRefValidation

Running partition tests on : DigitalDefence3728
Starting test: CheckSDRefDom
..... DigitalDefence3728 passed test CheckSDRefDom
Starting test: CrossRefValidation
..... DigitalDefence3728 passed test CrossRefValidation

Running enterprise tests on : DigitalDefence3728.lab
Test omitted by user request: DNS
Test omitted by user request: DNS
Starting test: LocatorCheck
GC Name: \\DD3728-DC.DigitalDefence3728.lab
Locator Flags: 0xe003f3fd
PDC Name: \\DD3728-DC.DigitalDefence3728.lab
Locator Flags: 0xe003f3fd
Time Server Name: \\DD3728-DC.DigitalDefence3728.lab
Locator Flags: 0xe003f3rd
Preferred Time Server Name: \\DD3728-DC.DigitalDefence3728.lab
Locator Flags: 0xe003f3fd
KDC Name: \\DD3728-DC.DigitalDefence3728.lab
Locator Flags: 0xe003f3fd
..... DigitalDefence3728.lab passed test LocatorCheck
Starting test: Intersite
Skipping site Default-First-Site-Name, this site is outside the scope provided by the command line arguments provided.
..... DigitalDefence3728.lab passed test Intersite

PS C:\Users\Administrator> nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server: Unknown
Address: ::1
```

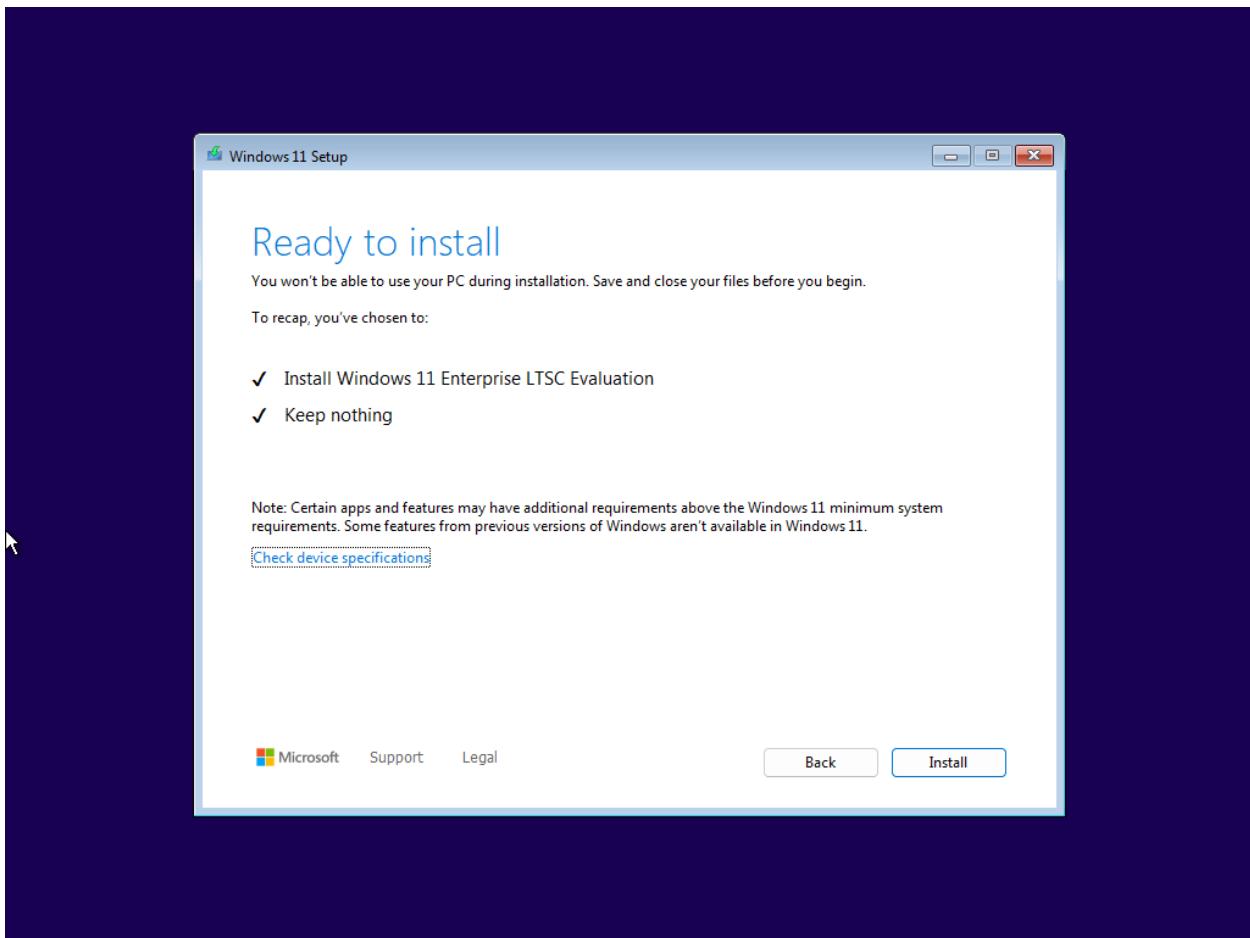
- Expected to see the **DD3728-DC** host in the SRV results.

7 — Jumpbox (Windows 11 LTSC): install, hardening & tools

Goal: Analyst workstation for accessing Splunk (web), SSH to Linux, and RDP to Windows Server, with hardened baseline and investigation tools.

A. Installation:

[screenshots]



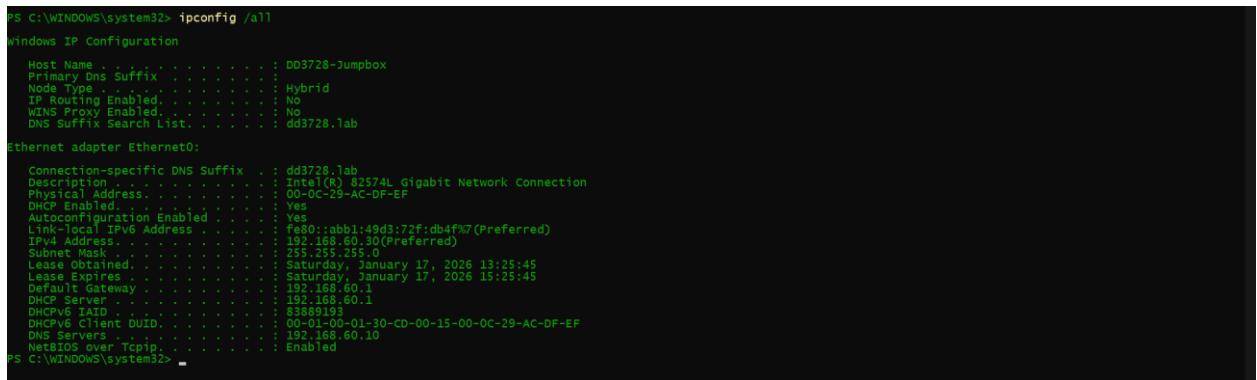
B. Networking

#powershell

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress
192.168.60.30 -PrefixLength 24 -DefaultGateway 192.168.60.1
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -
ServerAddresses 192.168.60.10
```

- Assigned a static IP to the Jumpbox to ensure stable management access and predictable firewall rules.

[screenshots  ]



```
PS C:\WINDOWS\system32> ipconfig /all
Windows IP Configuration

Host Name . . . . . : dd3728-Jumpbox
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List. . . . . : dd3728.lab

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . . . . : dd3728.lab
Description . . . . . : Intel(R) B2574L Gigabit Network Connection
Physical Address . . . . . : 00-0C-29-AC-DF-EF
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::abb1:49d3:72f:db4f%7 (Preferred)
IPv4 Address . . . . . : 192.168.60.30(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : Saturday, January 17, 2026 13:25:45
Lease Expires . . . . . : Saturday, January 17, 2026 15:25:45
Default Gateway . . . . . : 192.168.60.1
DHCP Server . . . . . : 192.168.60.1
DHCPv6 IAID . . . . . : 83889193
DHCPv6 Client DUID . . . . . : 00-01-00-01-30-CD-00-15-00-0C-29-AC-DF-EF
DNS Servers . . . . . : 192.168.60.10
NetBIOS over Tcpip . . . . . : Enabled
PS C:\WINDOWS\system32>
```

i. Hardening baseline

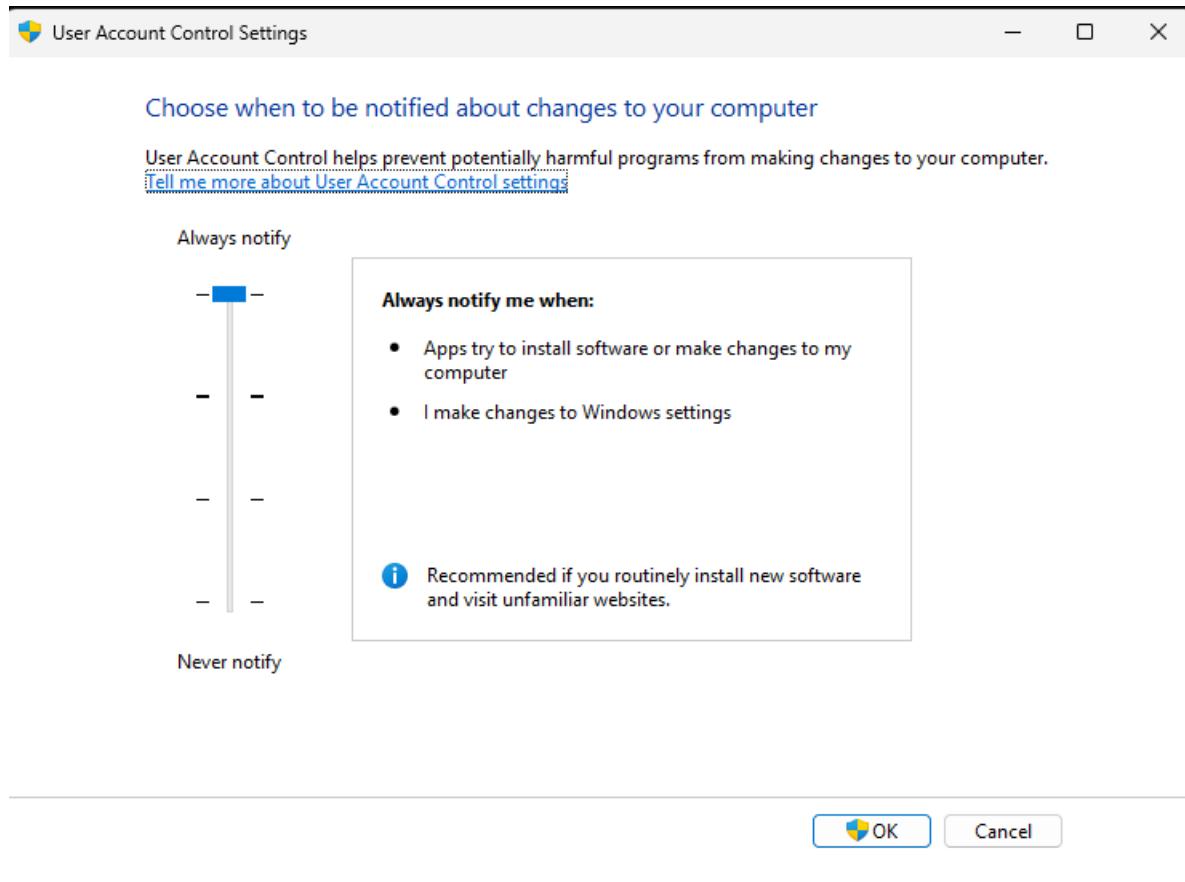
- Enabled Windows Defender and tamper protection.
- Prevents malware and stops local users from disabling security controls.

[screenshots  ]

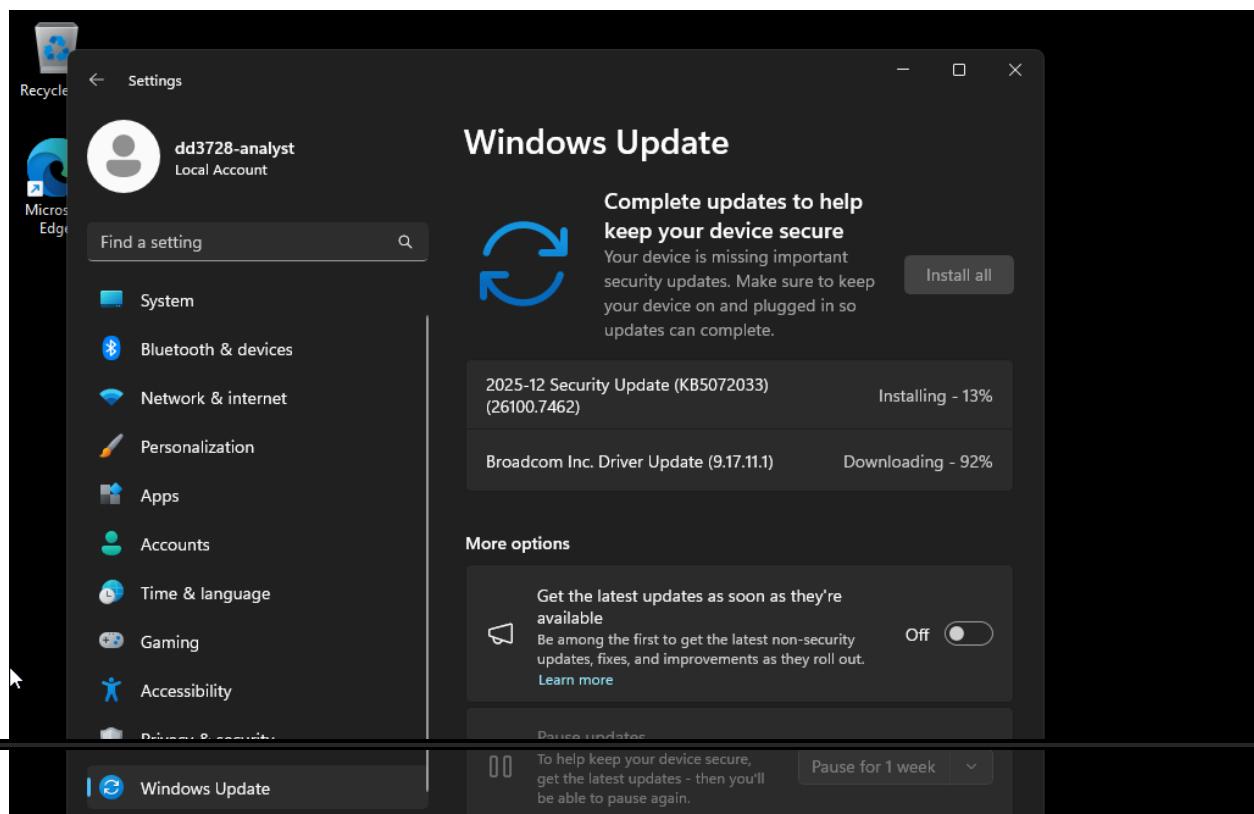


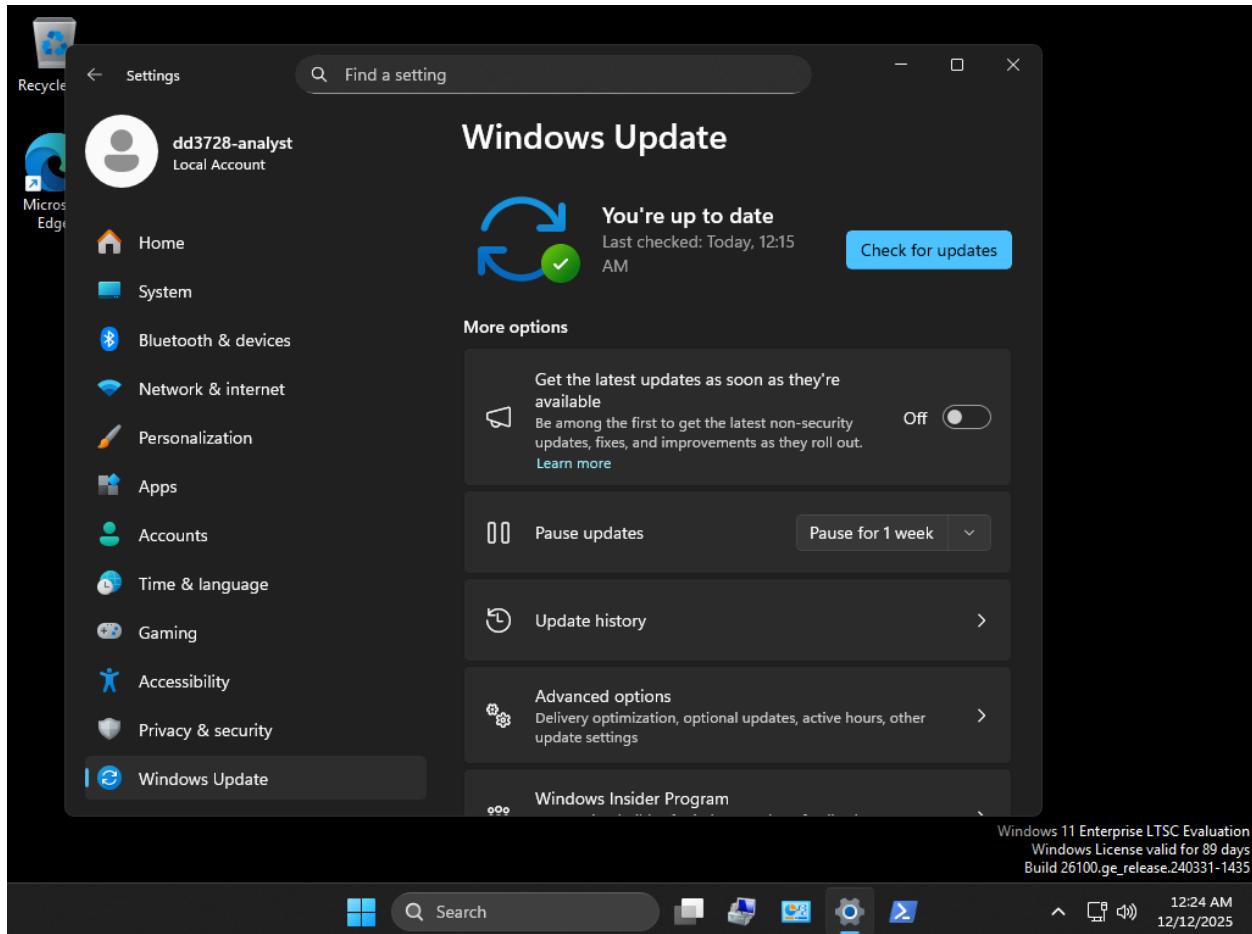
Set UAC to “Always notify”.

- Enforces explicit privilege escalation; reduces silent admin abuse.



- Windows updates





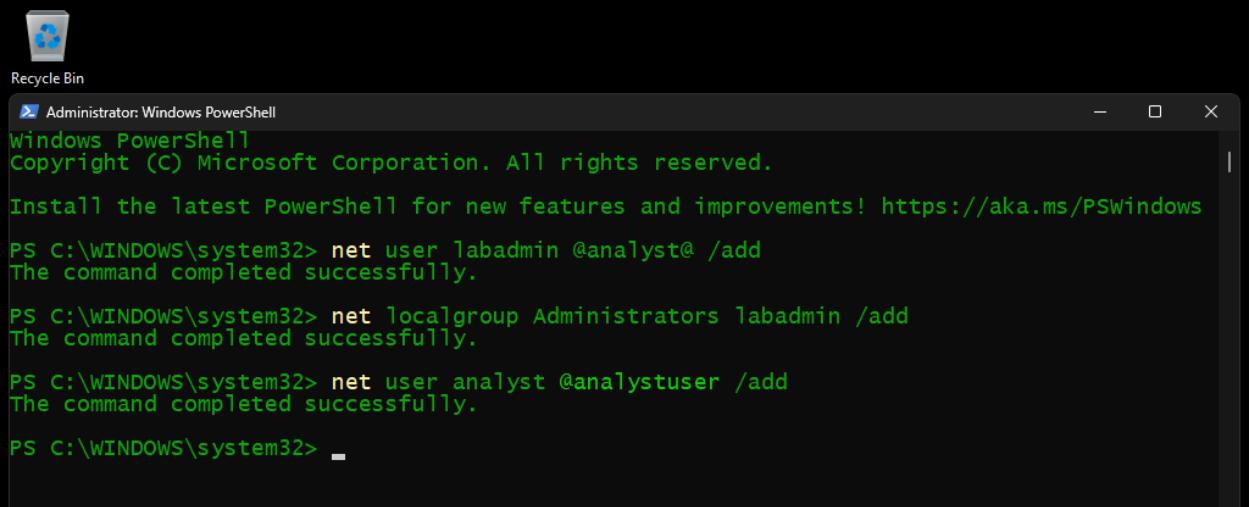
Create separate admin and analyst accounts:

```
#powershell
```

```
net user labadmin ***** /add
net localgroup Administrators labadmin /add
net user analyst ***** /add
```

- Creates a dedicated administrative account to avoid daily-use admin risk.
- Creates a low-privilege analyst account aligned with least-privilege principles.

[screenshots]



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> net user labadmin @analyst@ /add
The command completed successfully.

PS C:\WINDOWS\system32> net localgroup Administrators labadmin /add
The command completed successfully.

PS C:\WINDOWS\system32> net user analyst @analystuser /add
The command completed successfully.

PS C:\WINDOWS\system32>

```

C. Tools and rationale

Installed:

- MobaXterm — SSH/SFTP/X11 client to manage the Linux SIEM and transfer files.
- RDP (built-in) — for GUI admin to the DC and client.
- Browser (Firefox/Brave) — primary Splunk Web client for triage.
- Sysinternals Suite — process and autoruns analysis on Windows endpoints.
- Wireshark — packet capture and network triage.
- PowerShell 7 — modern scripting and remoting.
- KeePass — secure credential vault.
- Visual Studio Code (portable) — scripting and configuration editing.

Chocolatey installed:

```
#powershell

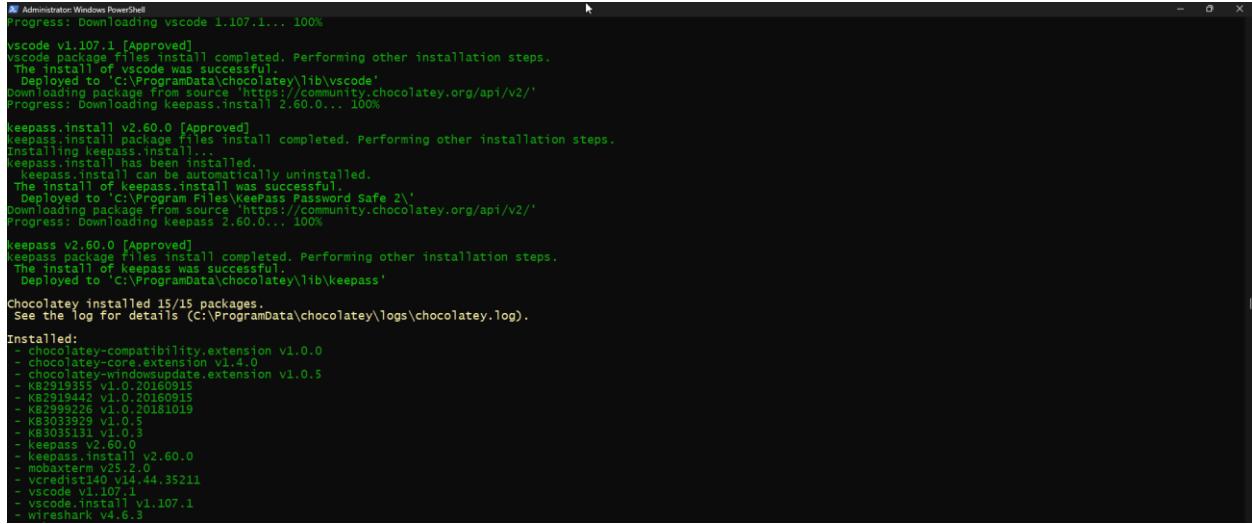
Set-ExecutionPolicy Bypass -Scope Process -Force
iwr https://chocolatey.org/install.ps1 -UseBasicParsing | iex
```

- Temporarily allows script execution for package installation only.
- Installs Chocolatey for repeatable, auditable tool deployment.

```
choco install mobaxterm wireshark vscode keepass -y
```

- Installs core tools quickly and consistently.

[screenshots  ]



```
Administrator: Windows PowerShell
Progress: Downloading vscode 1.107.1... 100%
vscode v1.107.1 [Approved]
vscode package files install completed. Performing other installation steps.
The install of vscode was successful.
  Deployed to 'C:\ProgramData\chocolatey\lib\vscode'
Download package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading keepass.install 2.60.0... 100%
keepass.install v2.60.0 [Approved]
keepass.install package files install completed. Performing other installation steps.
Install of keepass.install has been installed.
  keepass.install can be automatically uninstalled.
  The install of keepass.install was successful.
  Deployed to 'C:\Program Files\KeePass Password Safe 2\' 
Download package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading keepass 2.60.0... 100%
keepass v2.60.0 [Approved]
keepass package files install completed. Performing other installation steps.
The install of keepass was successful.
  Deployed to 'C:\ProgramData\chocolatey\lib\keepass'

Chocolatey installed 15/15 packages.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Installed:
chocolatey-compatibility.extension v1.0.0
chocolatey-core.extension v1.4.0
chocolatey-core.extension v1.0.5
- KB2919355 V1.0.20160915
- KB2919442 V1.0.20160915
- KB299922 V1.0.20181019
- KB3033929 V1.0.5
- KB3055113 V1.0.3
- KeePass v2.60.0
- keepass.install v2.60.0
- mobaxterm v25.2.0
- vcredist140 v14.44.35211
- vscode v1.107.1
- vscode.install v1.107.1
- wireshark v4.6.3
```

D. Quick hardening commands

#powershell

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled
True
```

- Ensures that the Windows Firewall is active across all network profiles.

Firewall rule (ran on DC) to allow RDP only from the Jumpbox:

#powershell

```
New-NetFirewallRule -DisplayName "Allow RDP from DD3738-Jumpbox" -
Direction Inbound -Action Allow -Protocol TCP -LocalPort 3389 -
RemoteAddress 192.168.60.30
```

- Ensures that the Windows Firewall is active across all network profiles.
- Restricts RDP access only to the Jumpbox, reducing lateral-movement risk.

[screenshots  ]

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> New-NetFirewallRule -DisplayName "Allow RDP from DD3728-Jumpbox" -Direction Inbound -Action Allow -Protocol TCP -LocalPort 3389 -Re
moteAddress 192.168.60.30

Name : {5209df4c-ea59-4d6d-a7c0-fb0d85ce3608}
DisplayName : Allow RDP from DD3728-Jumpbox
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform :
Direction : Inbound
Action : Allow
EdgeTraversalPolicy :
LooseSourceMapping :
LocalOnlyMapping :
ProtocolType :
PrimaryStatus : OK
Status : NotApplicable
EnforcementStatus : PersistentStore
PolicyStoresSource : Local
PolicyStoresSourceType :
RemoteDynamicKeywordAddresses :
PolicyAppId :

PS C:\Users\Administrator>

```

Disable SMBv1:

```
#powershell

Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol
```

- Removes SMBv1, eliminating a known legacy attack vector (e.g., EternalBlue).

[screenshots ↗ ↘]

```

Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and i
mprovements! https://aka.ms/PSWindows
PS C:\WINDOWS\system32> #powershell

PS C:\WINDOWS\system32> Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol

Path : 
Online : True
RestartNeeded : False

PS C:\WINDOWS\system32>

```

“These steps show deliberate network design, strict access control, security-first hardening, and disciplined tooling — exactly how a production-grade SOC or SIEM management environment is built.”

E. Access validation

From Jumpbox:

```
#powershell

Test-NetConnection -ComputerName 192.168.60.20 -Port 8000
#Splunk
Test-NetConnection -ComputerName 192.168.60.10 -Port 3389
#DC RDP
ssh dd3728-analyst@192.168.60.20
    • Confirms Splunk Web is reachable from the Jumpbox.
    • Validates controlled RDP access to the Domain Controller.
    • Verifies secure SSH access to the Splunk server.
```

[screenshots  ]

```
PS C:\WINDOWS\system32> Test-NetConnection -ComputerName 192.168.60.20 -Port 8000 # Splunk
ComputerName      : 192.168.60.20
RemoteAddress     : 192.168.60.20
RemotePort        : 8000
InterfaceAlias    : Internet0
SourceAddress     : 192.168.60.30
TcpTestSucceeded  : True

PS C:\WINDOWS\system32> Test-NetConnection -ComputerName 192.168.60.10 -Port 3389 # DC RDP
ComputerName      : 192.168.60.10
RemoteAddress     : 192.168.60.10
RemotePort        : 3389
InterfaceAlias    : Internet0
SourceAddress     : 192.168.60.30
TcpTestSucceeded  : True

dd3728-analyst@dd3728-siem-xdr-server: ~
# via MobaXterm
PS C:\WINDOWS\system32> ssh dd3728-analyst@192.168.60.20
The authenticity of host '192.168.60.20 (192.168.60.20)' can't be established.
ED25519 key fingerprint is SHA256:BzJwFzSmnyM23PglOyZy8Rt1hjR640ZPxk7CLH/628.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added "192.168.60.20" (ED25519) to the list of known hosts.
dd3728-analyst@192.168.60.20: ~
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:      https://ubuntu.com/pro

System information as of Sat Jan 17 06:47:03 PM SAST 2026
System load: 0.05      Processes: 257
Usage of /: 8.3% of 195.80GB  Users logged in: 1
Memory usage: 9%
Swap usage: 0%
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.
https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

35 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

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

Last login: Thu Jan 15 22:00:11 2026 from 192.168.60.30
dd3728-analyst@dd3728-siem-xdr-server: ~
```

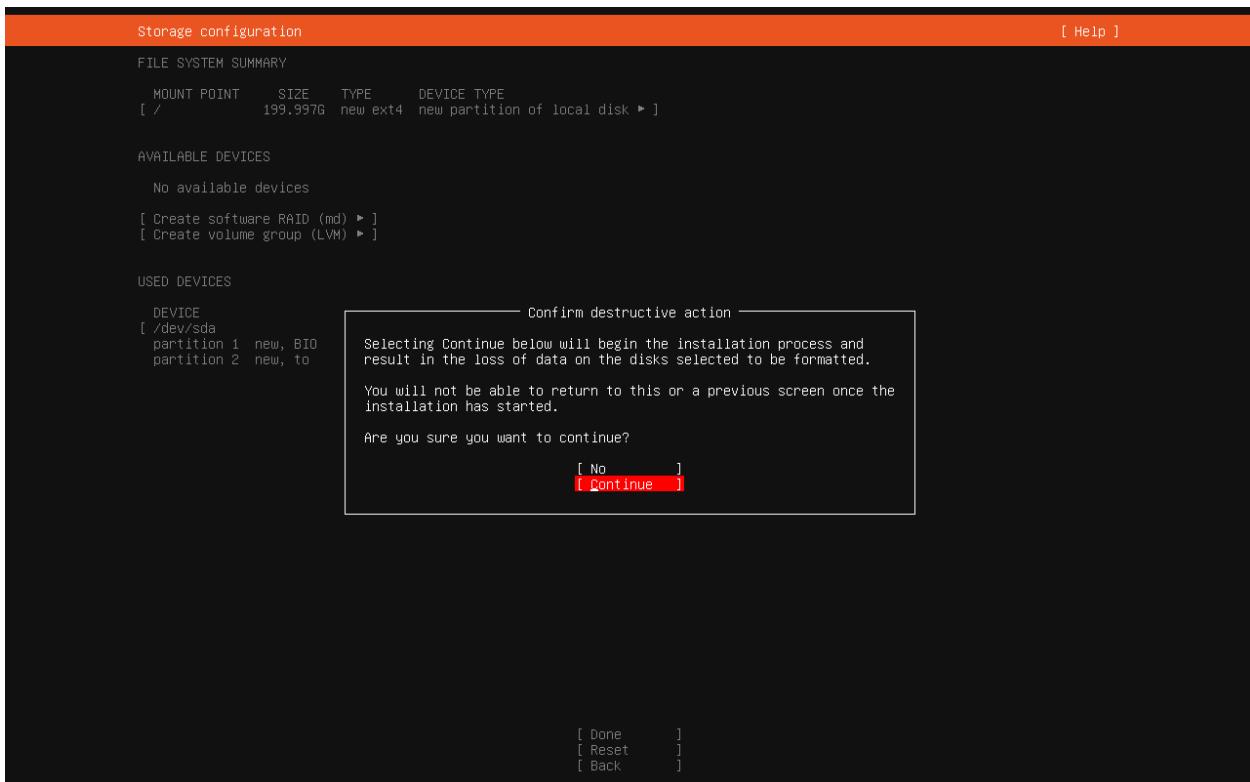
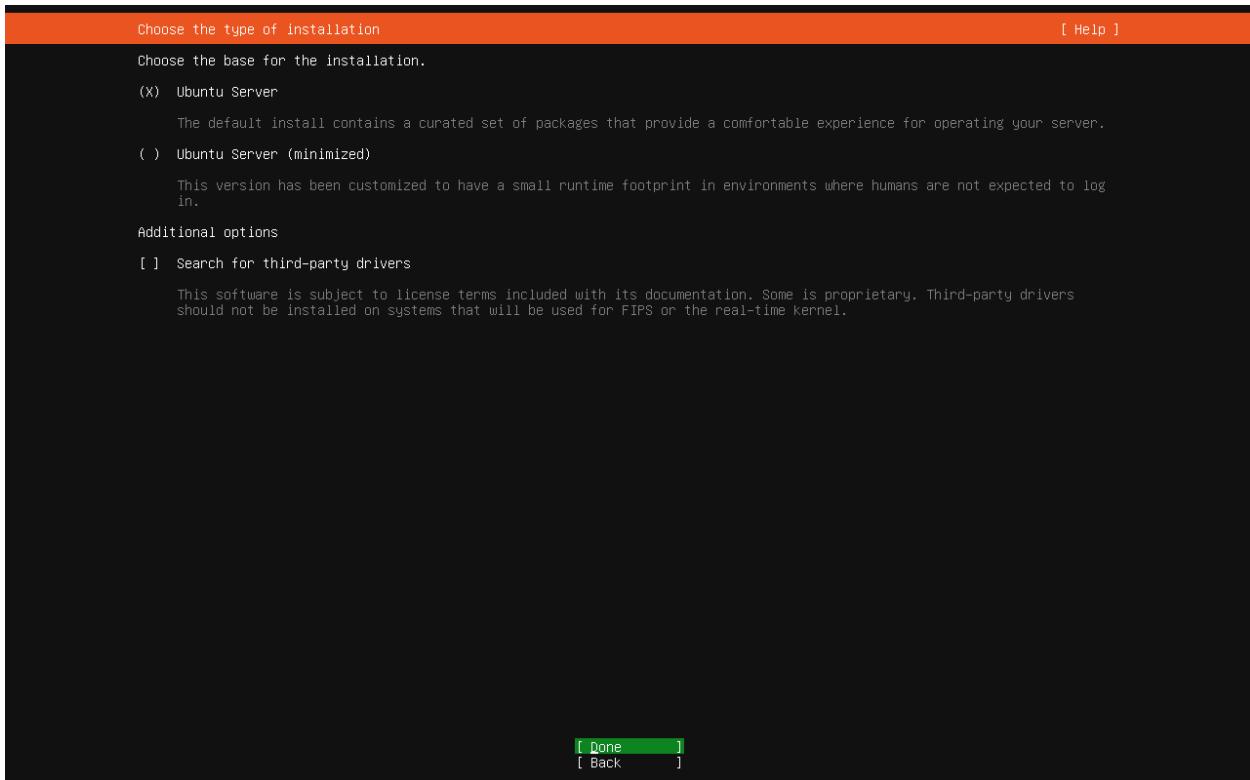
8 — Ubuntu Server 24.04 LTS: installation, networking, hardening & Splunk

Goal: Minimal GUI-less server with static network, hardened baseline, and Splunk Enterprise configured to receive logs.

A. Install Ubuntu Server 24.04

- Used Ubuntu Server ISO

[screenshots  selected 



Installing system [Help]

```

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 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/tmpsskd4ug7/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
setting up swap
apply networking config
writing etc/fstab
configuring multipath
updating packages on target system
configuring pollinate user-agent on target
updating initramfs configuration
configuring target system bootloader
installing grub to target devices
copying metadata from /cdrom
final system configuration
calculating extra packages to install
installing openssh-server
retrieving openssh-server /
curtin command system-install \

```

[View full log]

```

[ 17.798252] cloud-init[1322]: Cloud-init v. 25.1.4-0ubuntu0~24.04.1 finished at Thu, 11 Dec 2025 10:57:54 +0000. Datasource DataSourceNone. Up 17.79 seconds
Ubuntu 24.04.3 LTS dd3728-siem-xdr-server tty1
dd3728-siem-xdr-server login: dd3728-analyst
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Thu Dec 11 10:58:53 AM UTC 2025
System load: 0.05      Processes:          262
Usage of /: 3.4% of 195.80GB  Users logged in:  0
Memory usage: 2%           IPv4 address for ens38: 192.168.60.101
Swap usage:  0%
Expanded Security Maintenance for Applications is not enabled.

41 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/<package>/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

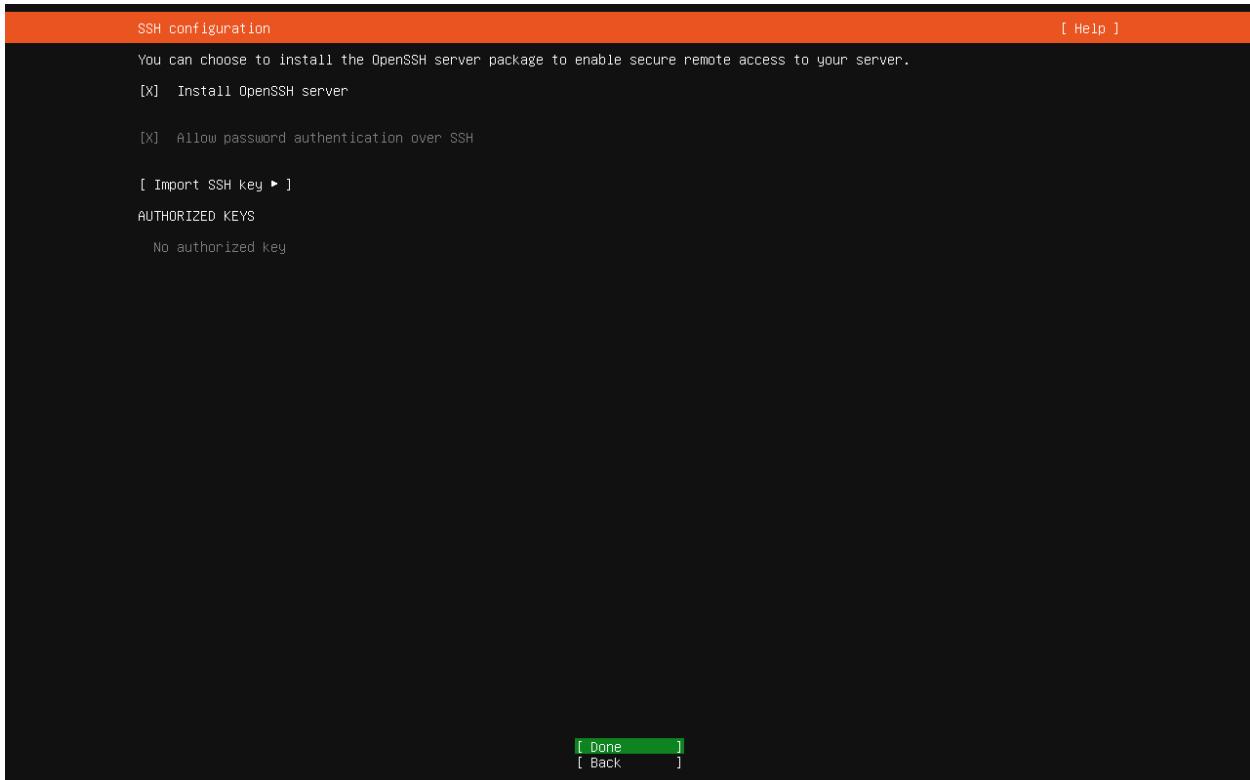
dd3728-analyst@dd3728-siem-xdr-server:~$ 

```

- enabled SSH during installation.
- **Install OpenSSH server:** This option allows you to install the OpenSSH server package, which is essential for remote access to the server via the SSH protocol.

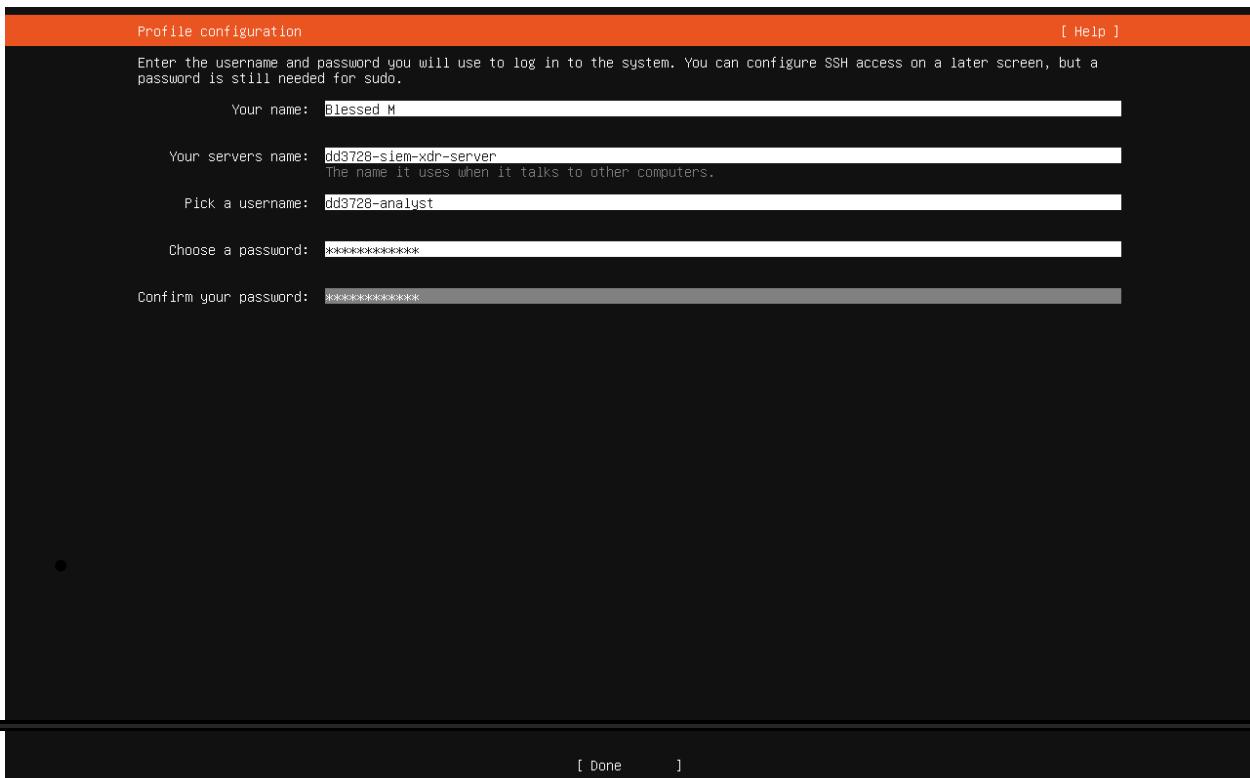
- **Allow password authentication over SSH:** This option permits users to connect to the server using password authentication.

[screenshots  ]



- Created admin user →dd3728-analyst.

[screenshots  ]



B. Static Netplan configuration (authoritative)

- post- [Splunk]install I did manual network configuration/adjust Netplan

Created /etc/netplan/00-installer-config.yaml:

```
#bash
sudo tee /etc/netplan/00-installer-config.yaml <<'EOF'
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: no
      addresses:
        - 192.168.60.20/24
      routes:
        - to: default
          via: 192.168.60.1
      nameservers:
        addresses:
          - 192.168.60.10
EOF
```

- Defines a static IP, gateway, and AD-DNS server, so the SIEM server behaves like a real enterprise server, not a DHCP client.

[screenshots ↗]

```
+ MobaXterm Personal Edition v25.4 +
(SSH client, X server and network tools)

> SSH session to dd3728-analyst@192.168.60.20
  * SSH port: 22
  * SSH compression : ✓
  * SSH-browser : ✓
  * X11-forwarding : ✓ (remote display is forwarded through SSH)
  * For more info, ctrl+click on help or visit our website.

Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Mon Dec 22 09:37:36 PM UTC 2025

System load: 0.1 Processes: 259
Usage of /: 7.4% of 195.80GB Users logged in: 1
Memory usage: 8% IPV4 address for ens33: 192.168.60.20
Swap usage: 0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.
https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.

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

Last login: Sat Dec 20 01:58:00 2025 from 192.168.60.30
dd3728-analyst@dd3728-siem-xdr-server:~$ cd /
dd3728-analyst@dd3728-siem-xdr-server:~$ ls
bin bin usr-is-merged boot cpio dev etc home lib lib64 lib usr-is-merged lost+found media mnt opt proc root run sbin sbin usr-is-merged snap srv swap.img sys lib usr var
dd3728-analyst@dd3728-siem-xdr-server:~$ sudo nano /etc/netplan/00-installer-config.yaml
dd3728-analyst@dd3728-siem-xdr-server:~$ sudo cat /etc/netplan/00-installer-config.yaml
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: no
      addresses:
        - 192.168.60.20/24
      gateway4: 192.168.60.1
      nameservers:
        addresses:
          - 192.168.60.10
dd3728-analyst@dd3728-siem-xdr-server:~$
```

★ Disable cloud-init networking and remove conflicting Netplan file:

```
#bash  
echo 'network: {config: disabled}' | sudo tee  
/etc/cloud/cloud.cfg.d/99-disable-network-config.cfg  
sudo rm -f /etc/netplan/50-cloud-init.yaml
```

- Prevents VMware / cloud-init from overwriting enterprise network settings after rebooting.

[screenshots]

★ Fix permissions and apply:

```
#bash

sudo chown root:root /etc/netplan/00-installer-config.yaml
sudo chmod 600 /etc/netplan/00-installer-config.yaml
sudo netplan generate
sudo netplan apply
sudo systemctl restart systemd-resolved
resolvectl status
```

- The commands demonstrate essential operations for managing network configuration securely on a Linux system. They ensure that the Netplan

configuration file is owned and accessible only by root, apply new network settings, and verify DNS resolution status.

- Activates the static IP, gateway, and DNS and restarts the DNS resolver.

[screenshots]

Validation:

```
#bash  
ip a  
ip route  
nslookup dd3728-dc.digitaldefence3728.lab  
nslookup google.com
```

Confirms:

- Internal AD DNS resolution works
- Internet name resolution works

This verifies correct routing + DNS forwarding.

[screenshots ↗️ ↘️]

```
dd3728-analyst@dd3728-siem-xdr-server:~$ nslookup dd3728-dc.digitaldefence3728.lab
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: dd3728-dc.digitaldefence3728.lab
Address: 192.168.66.10

dd3728-analyst@dd3728-siem-xdr-server:~$ nslookup google.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: google.com
Address: 142.250.31.100
Name: google.com
Address: 142.250.31.102
Name: google.com
Address: 142.250.31.101
Name: google.com
Address: 142.250.31.139
Name: google.com
Address: 142.250.31.138
Name: google.com
Address: 142.250.31.113
Name: google.com
Address: 2607:fbb0:4004:c1d::64
Name: google.com
Address: 2607:fbb0:4004:c1d::6b
Name: google.com
Address: 2607:fbb0:4004:c1d::66
Name: google.com
Address: 2607:fbb0:4004:c1d::71

dd3728-analyst@dd3728-siem-xdr-server:~$ nslookup dd3728-dc.digitaldefence3728.lab
Server: 127.0.0.53
Address: 127.0.0.53#53

dd3728-analyst@dd3728-siem-xdr-server:~$ nslookup google.com
Server: 127.0.0.53
Address: 127.0.0.53#53
```

C. Hardening (baseline)

#Update and basic tools:

#bash

```
sudo apt update && sudo apt upgrade -y
```

Why right after install ↗️ ?

- New servers ship with baseline packages that may have known vulnerabilities; skipping this exposes your system to exploit until manually updated.
- Brings the server to a fully patched, vulnerability-reduced state before production use.

[screenshots ↗️ ↘️]

```
dd3728-analyst@dd3728-siem-xdr-server:~$ whoami
dd3728-analyst
dd3728-analyst@dd3728-siem-xdr-server:~$ ls
dd3728-analyst@dd3728-siem-xdr-server:~$ cd /
dd3728-analyst@dd3728-siem-xdr-server:~$ ls
bin binfmt-support dev etc home lib lib64 lib usr-is-merged lost+found media mnt opt proc root run sbin sbin usr-is-merged snap srv swap.img sys tmp usr var
dd3728-analyst@dd3728-siem-xdr-server:~$ sudo apt update && sudo apt upgrade -y
[sudo] password for dd3728-analyst:
Hit:1 http://za.archive.ubuntu.com/ubuntu InRelease
Hit:2 http://za.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://za.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1,391 kB]
39% [Working]
```

Create Splunk service user:

```
#bash

sudo adduser splunk-dd3728
sudo usermod -aG sudo splunk
```

[screenshots ↗️ ↘️]

```
(SSH client, X server and network tools)
  • SSH session to dd3728-analyst@192.168.60.20
    • Direct SSH : ✓
    • SSH compression : ✓
    • SSH-browswer : ✓
    • X11-forwarding : ✓ (remote display is forwarded through SSH)
  ▶ For more info, ctrl+click on help or visit our website.
```

Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/pro>

System information as of Tue Dec 16 03:20:22 PM UTC 2025

System load:	0.01	Processes:	268
Usage of /:	3.6% of 195.80GB	Users logged in:	0
Memory usage:	8%	IPv4 address for ens33:	192.168.60.20
Swap usage:	0%		

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See <https://ubuntu.com/esm> or run: sudo pro status

Last login: Tue Dec 16 15:13:32 2025 from 192.168.60.30
dd3728-analyst@SIEM-Splunk-ES:~\$ sudo adduser splunk-dd3728
sudo: useradd(1) failed: user 'splunk-dd3728' already exists.
info: Adding user 'splunk-dd3728'.
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'splunk-dd3728' (1001) ...
info: Adding new user 'splunk-dd3728' (1001) with group 'splunk-dd3728 (1001)' ...
info: Creating new directory '/home/splunk-dd3728' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing password for user splunk-dd3728
Enter the new value, or press ENTER for the default
 Full Name []: bless M
 Room Number []: 002
 Work Phone []: 2025
 Home Phone []: 2025
 Other []: 2025
Is the information correct? [y/n] y
info: Adding new user 'splunk-dd3728' to supplemental / extra groups 'users' ...
info: Adding user 'splunk-dd3728' to group 'users' ...
dd3728-analyst@SIEM-Splunk-ES:~\$

What happened ? ↗️

I created:

```
sudo adduser splunk-dd3728
```

- ★ When I should have done created **Splunk service user** like the following bash command ↗️

```
sudo adduser --disabled-password --gecos "" splunk-dd3728
sudo usermod -aG sudo splunk
```

What **--disabled-password --gecos ""** does

Those two flags do **only one thing**:

Flag	Purpose
--disabled-password	Prevents password login for that account

--gecos ""	Skips full-name and metadata prompts
------------	--------------------------------------

★ **That means:**

- A password was set
- The account is interactive
- Someone could SSH or sudo as that account

★ **Why this matters in a SOC environment**

- Splunk service accounts should be:
 - Non-interactive
 - Not usable for login
 - Not usable for SSH

★ **Because:**

- If Splunk is exploited, the attacker should not get a shell.
- According to previous executed bash command, service accounts are slightly weaker than enterprise best practice.

Correct fix [no reinstallation required (Splunk)]

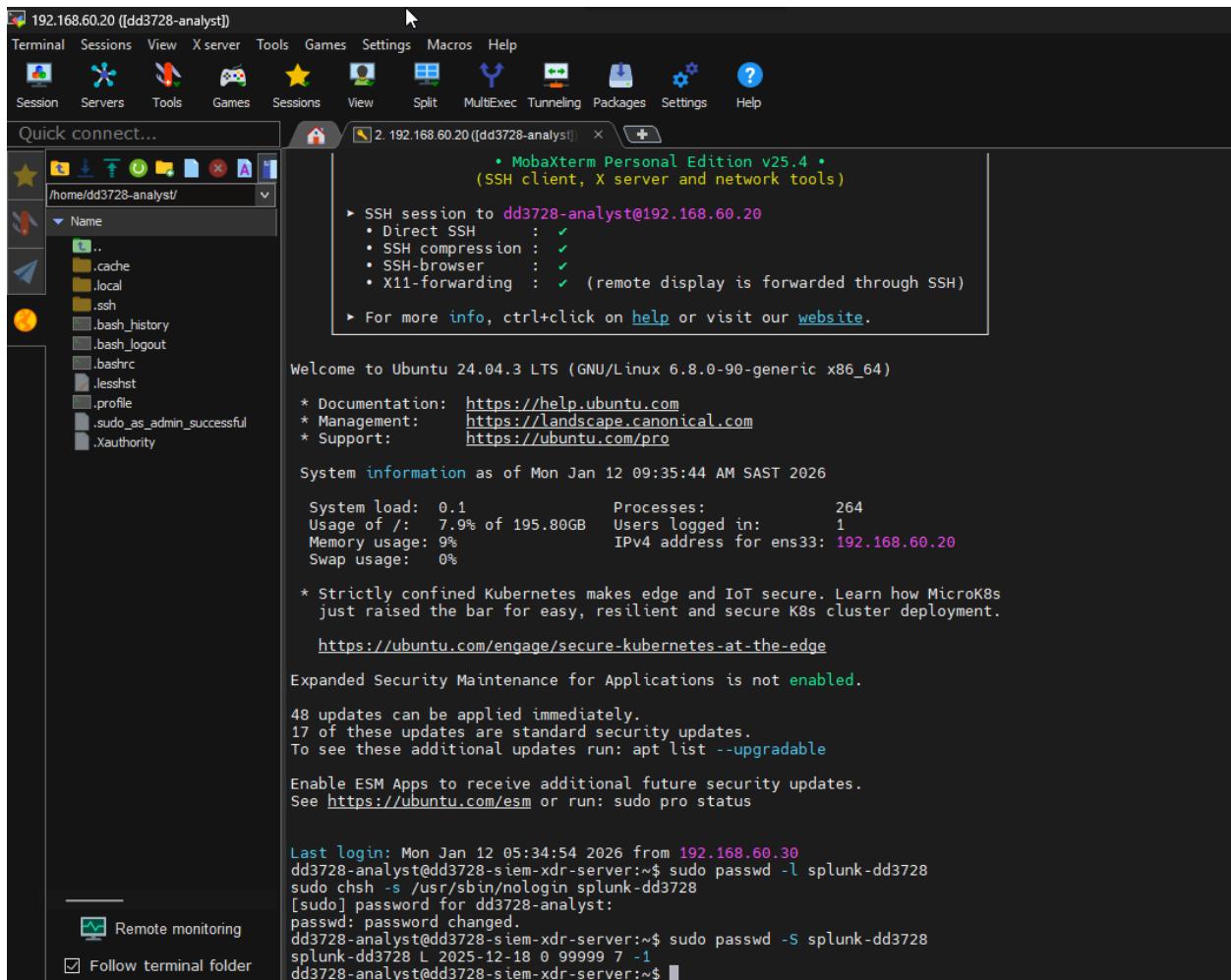
```
#bash

sudo passwd -l splunk-dd3728
sudo chsh -s /usr/sbin/nologin splunk-dd3728
```

This:

- Locks the password
- Prevents shell login
- Converts the account into a true service account

[**screenshots** ↗ ↘]



★ Install auditd:

```
#bash

sudo apt install -y auditd audispd-plugins
```

Enable Linux auditing:

- Provides kernel-level security logging for file access, user activity, and system changes — critical for SOC investigations.

[**screenshots** ↗️ ↻]

★ UFW firewall:

#bash

```
sudo ufw default deny incoming  
sudo ufw default allow outgoing  
sudo ufw allow 22/tcp  
sudo ufw allow 8000/tcp  
sudo ufw allow 9997/tcp  
sudo ufw allow 514/udp  
sudo ufw enable
```

Implements zero-trust host firewalling while allowing only:

- 22 → Admin access (SSH)
 - 8000 → Splunk Web
 - 9997 → Splunk forwarders
 - 514 → pfSense firewall logs

[screenshots]

```

dd3728-analyst@dd3728-siem-xdr-server:~$ sudo nano /etc/ssh/sshd_config
dd3728-analyst@dd3728-siem-xdr-server:~$ sudo systemctl restart ssh
dd3728-analyst@dd3728-siem-xdr-server:~$ sudo ufw default deny incoming
sudo ufw default allow outgoing
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
dd3728-analyst@dd3728-siem-xdr-server:~$ sudo ufw allow 22/tcp      # SSH
sudo ufw allow 8000/tcp    # Splunk Web
sudo ufw allow 9997/tcp   # Splunk Forwarders
sudo ufw allow 514/udp    # Syslog (pfSense)
Rules updated
Rules updated (v6)
dd3728-analyst@dd3728-siem-xdr-server:~$ sudo ufw enable
sudo ufw status
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
Status: active

To          Action    From
--          ----     ---
22/tcp       ALLOW     Anywhere
8000/tcp     ALLOW     Anywhere
9997/tcp     ALLOW     Anywhere
514/udp      ALLOW     Anywhere
22/tcp (v6)  ALLOW     Anywhere (v6)
8000/tcp (v6) ALLOW     Anywhere (v6)
9997/tcp (v6) ALLOW     Anywhere (v6)
514/udp (v6) ALLOW     Anywhere (v6)

```

Time sync:

```
#bash

sudo timedatectl set-timezone Africa/Johannesburg
sudo timedatectl set-ntp true
```

- Ensures accurate timestamps across logs, which is mandatory for threat correlation and investigations.

[screenshot ↗]

```
dd3728-analyst@dd3728-siem-xdr-server:~$ timedatectl set-timezone Africa/Johannesburg
timedatectl set-ntp true
timedatectl status
==== AUTHENTICATING FOR org.freedesktop.timedate1.set-timezone ====
Authentication is required to set the system timezone.
Multiple identities can be used for authentication:
 1. Blessed M (dd3728-analyst)
 2. Blessed M,002,1055560,1055560,1055596 (splunk-dd3728)
Choose identity to authenticate as (1-2): 1-2
Invalid response `1-2'.
==== AUTHENTICATION CANCELED ====
Failed to set time zone: Access denied
==== AUTHENTICATING FOR org.freedesktop.timedate1.set-ntp ====
Authentication is required to control whether network time synchronization shall be enabled.
Multiple identities can be used for authentication:
 1. Blessed M (dd3728-analyst)
 2. Blessed M,002,1055560,1055560,1055596 (splunk-dd3728)
Choose identity to authenticate as (1-2): 2
Password:
==== AUTHENTICATION COMPLETE ====
      Local time: Thu 2025-12-18 04:50:56 UTC
      Universal time: Thu 2025-12-18 04:50:56 UTC
          RTC time: Thu 2025-12-18 04:50:55
        Time zone: Etc/UTC (UTC, +0000)
System clock synchronized: yes
          NTP service: active
    RTC in local TZ: no
dd3728-analyst@dd3728-siem-xdr-server:~$
```

MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Configure resource limits for Splunk:

```
#bash

sudo tee -a /etc/security/limits.conf <<'EOF'
splunk soft nofile 65536
splunk hard nofile 65536
EOF
```

Raise Splunk file limits:

- Prevents Splunk from dropping logs during high-volume ingestion.

[screenshots ↗️ ↘️]

```
GNU nano 7.2                                     /etc/security/limits.conf *
#<type> can have the two values:
#   - "soft" for enforcing the soft limits
#   - "hard" for enforcing hard limits
#<item> can be one of the following:
#   - cpu - max CPU time (MIN)
#   - cputime - max data size (KB)
#   - fsize - maximum filesize (KB)
#   - memlock - max locked-in-memory address space (KB)
#   - nofile - max number of open file descriptors
#   - rss - max resident set size (KB)
#   - stack - max stack size (KB)
#   - cpu - max CPU time (MIN)
#   - nproc - max number of processes
#   - as - address space limit (KB)
#   - maxlogins - max simultaneous logins for this user
#   - maxsyslogins - max number of logins on the system
#   - priority - the priority to run user process with
#   - locks - max number of file locks the user can hold
#   - suspend - max number of pending signals
#   - msgqueue - max memory used by POSIX message queues (bytes)
#   - nice - max nice value allowed to raise to values: [-20, 19]
#   - rtprio - max realtime priority
#   - chroot - change root to directory (Debian-specific)
#<domain>  <type>  <item>      <value>

##          soft    core      0
#root      hard    core  100000
##          hard    rss     100000
##student   hard    nproc    20
##faculty   soft    nproc    20
##faculty   hard    nproc    50
##ftp       hard    nproc     0
##ftp       -      chroot  /ftp
##student   -      maxlogins  4
# End of file
splunk soft nofile 65536
splunk hard nofile 65536
```

The terminal window includes standard nano key bindings at the bottom: Help, Write Out, Read File, Where Is, Cut, Paste, Execute, Justify, Location, Go To Line, Undo, Set Mark, To Bracket, Copy, Previous, Next, Back, Forward, Prev Word, Next Word.

Why I disabled Transparent Huge Pages (THP)

- Transparent Huge Pages can cause unpredictable latencies, memory fragmentation and pause/stalls in high-throughput, low-latency services (Splunk indexers, etc.). Splunk's own guidance and real-world practice recommend disabling THP to avoid long GC-like pauses and to stabilize indexing/search performance. Disabling THP is a small OS-level change that materially improves reliability for a production SIEM.

```
#!/bin/bash

### BEGIN INIT INFO

# Provides: disable-thp
# Required-Start: $local_fs
# Required-Stop:
# X-Start-Before: couchbase-server
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# Short-Description: Disable THP
# Description: Disables transparent huge pages (THP) on boot, to improve
#               Couchbase performance.

### END INIT INFO

case $1 in
  start)
    if [ -d /sys/kernel/mm/transparent_hugepage ]; then
      thp_path=/sys/kernel/mm/transparent_hugepage
    elif [ -d /sys/kernel/mm/redhat_transparent_hugepage ]; then
      thp_path=/sys/kernel/mm/redhat_transparent_hugepage
    else
      return 0
    fi
```

```

echo 'never' > ${thp_path}/enabled
echo 'never' > ${thp_path}/defrag

re='^0-1]+$'
if [[ $(cat ${thp_path}/khugepaged/defrag) =~ $re ]]
then
    # RHEL 7
    echo 0 > ${thp_path}/khugepaged/defrag
else
    # RHEL 6
    echo 'no' > ${thp_path}/khugepaged/defrag
fi

unset re
unset thp_path
;;
esac

```

What the script does (brief, line-by-line summary)

- The file shown is an init script placed in `/etc/init.d/disable_thp` so it runs at boot.
- It checks for the kernel THP sysfs path (`/sys/kernel/mm/transparent_hugepage`).
- It writes `never` to `${thp_path}/enabled` to turn THP off at runtime.
- It writes `never` or `no` to the `${thp_path}/khugepaged/defrag` file (depending on kernel variants) to stop the khugepaged defragmenter.
- The script contains `### BEGIN INIT INFO` metadata so `init/system` scripts start it in runlevels 2–5 on boot.
- The result: THP and automatic hugepage defragmentation are disabled every boot, ensuring Splunk runs on a predictable memory model.

[screenshot  non-consistent configurations]

```
-rwxr-xr-x 1 root root 2.1K Aug 5 17:14 ufw
-rw-rxr-x 1 root root 1.4K Feb 12 2024 unattended-upgrades
-rw-rxr-x 1 root root 1.3K Aug 5 17:14 uuid
root@dd3728-siem-xdr-server:/etc/init.d# cat /sys/kernel/
cat: /sys/kernel/: Is a directory
root@dd3728-siem-xdr-server:/etc/init.d# cd /sys/kernel/
root@dd3728-siem-xdr-server:/sys/kernel# ls
address_bits cgroup crash_elfcorehdr_size iommu_groups kexec_crash_size mm profiling reboot software_nodes uevent_sequen
boot_params config debug irq kexec_loaded notes rcu_expedited security slab uevent_helper vmemcoreinfo
btif cpu_bytorder fscaps kexec_crash_loaded livepatch oops_count rcu_normal warn_count
root@dd3728-siem-xdr-server:/sys/kernel# cat mm
cat: mm: Is a directory
root@dd3728-siem-xdr-server:/sys/kernel# cd mm
root@dd3728-siem-xdr-server:/sys/kernel/mm# ls
hugepages ksm lru_gen numa_page_idle swap transparent_hugepage
root@dd3728-siem-xdr-server:/sys/kernel/mm# cd transparent_hugepage
root@dd3728-siem-xdr-server:/sys/kernel/mm/transparent_hugepage# ls
defrag hpage_pnd_size hugepages-128kB hugepages-2048kB hugepages-32kB hugepages-64kB shmem_enabled
enabled hugepages-1024kB hugepages-16kB hugepages-256kB hugepages-512kB khugepaged use_zero_page
root@dd3728-siem-xdr-server:/sys/kernel/mm/transparent_hugepage# cat enabled
always [madvise] never
root@dd3728-siem-xdr-server:/sys/kernel/mm/transparent_hugepage# cat defrag
always defer_defer[madvise] never
root@dd3728-siem-xdr-server:/sys/kernel/mm/transparent_hugepage#
root@dd3728-siem-xdr-server:/sys/kernel/mm/transparent_hugepage#
root@dd3728-siem-xdr-server:/sys/kernel/mm/transparent_hugepage#
```

[screenshot consistent configurations]

```

root@dd3728-siem-xdr-server:/sys/kernel/mm/transparent_hugepage# 
root@dd3728-siem-xdr-server:/sys/kernel/mm/transparent_hugepage# cd /etc/init.d
root@dd3728-siem-xdr-server:/etc/init.d# nano disable_thp
apparmor audit cron cryptisks-early disable_thp iscsid kmod open-vm-tools plymouth-log rsync splunk sysstat unattended-upgrades
root@dd3728-siem-xdr-server:/etc/init.d# ls
control-setup.sh cryptisks dbus grub-common keyboard-setup.sh open-tscsi plymouth procps sync screen-cleanups ssh ufw uidd
root@dd3728-siem-xdr-server:/etc/init.d# cat disable_thp
#!/bin/bash

## BEGIN INIT INFO
# Provides:          disable-thp
# Required-Start:    $local_fs
# Required-Stop:
# X-Start-Before:   couchbase-server
# Default-Start:    2 3 4 5
# Default-Stop:     0 6
# Short-Description: Disable THP
# Description:      Disables transparent huge pages (THP) on boot, to improve
#                   Couchbase performance.
## END INIT INFO

case $1 in
start)
    if [ -d /sys/kernel/mm/transparent_hugepage ]; then
        thp_path=/sys/kernel/mm/transparent_hugepage
    elif [ -d /sys/kernel/mm/redhat_transparent_hugepage ]; then
        thp_path=/sys/kernel/mm/redhat_transparent_hugepage
    else
        return 0
    fi

    echo 'never' > ${thp_path}/enabled
    echo 'never' > ${thp_path}/defrag

    re='^([0-1])$'
    if [[ $(< /dev/null cat ${thp_path}/khugepaged/defrag) =~ $re ]]; then
        # RHEL 7
        echo 0 > ${thp_path}/khugepaged/defrag
    else
        # RHEL 6
        echo 'no' > ${thp_path}/khugepaged/defrag
    fi

    unset re
    unset thp_path
    ;;
esac

root@dd3728-siem-xdr-server:/etc/init.d# 

```

```

unset re
unset thp_path
';
esac
root@dd3728-siem-xdr-server:/etc/init.d# ls -lh disable_thp
-rw-r--r-- 1 root root 1015 Dec 18 07:14 disable_thp
root@dd3728-siem-xdr-server:/etc/init.d# chmod 755 disable_thp
root@dd3728-siem-xdr-server:/etc/init.d# ls lh
ls: cannot access 'lh': No such file or directory
root@dd3728-siem-xdr-server:/etc/init.d# ls
apparmor auditd cron cryptisks dbus grub-common keyboard-setup.sh kmod open-vm-tools plymouth-log rsync splunk sysstat unattended-upgrades
apparmor-setup.sh cryptisks dbus grub-common keyboard-setup.sh open-iscsi plymouth procps screen-cleanup ssh utw uuid
root@dd3728-siem-xdr-server:/etc/init.d# ls -lh
total 1089
-rwxr-xr-x 1 root root 3.7K Jul 14 2024 apparmor
-rwxr-xr-x 1 root root 2.3K Jul 8 14:58 aptopt
-rwxr-xr-x 1 root root 3.6K Jan 24 2024 auditd
-rwxr-xr-x 1 root root 1.3K Feb 26 2024 console-setup.sh
-rwxr-xr-x 1 root root 3.1K Aug 5 17:14 cron
-rwxr-xr-x 1 root root 937 Jun 5 2024 cryptisks
-rwxr-xr-x 1 root root 89K Dec 5 2023 cryptisks-early
-rwxr-xr-x 1 root root 3.0K Dec 5 2023 disable_thp
-rwxr-xr-x 1 root root 1015 Dec 18 07:14 disable_thp
-rwxr-xr-x 1 root root 985 Mar 17 2025 grub-common
-rwxr-xr-x 1 root root 1.5K Feb 11 2025 iscsid
-rwxr-xr-x 1 root root 1.5K Feb 26 2024 keyboard-setup.sh
-rwxr-xr-x 1 root root 2.0K Apr 18 2024 kmod
-rwxr-xr-x 1 root root 2.5K Feb 11 2025 open-iscsi
-rwxr-xr-x 1 root root 1.9K Aug 5 17:14 open-vm-tools
-rwxr-xr-x 1 root root 1.4K Mar 21 2024 plymouth
-rwxr-xr-x 1 root root 760 Mar 21 2024 plymouth-log
-rwxr-xr-x 1 root root 950 Mar 24 2024 rsync
-rwxr-xr-x 1 root root 4.1K Aug 5 17:14 rsync
-rwxr-xr-x 1 root root 1.2K Aug 5 17:14 screen-cleanup
-rwx----- 1 root root 980 Dec 18 06:00 splunk
-rwxr-xr-x 1 root root 4.0K Jul 21 15:58 ssh
-rwxr-xr-x 1 root root 1.6K Aug 5 17:14 sysstat
-rwxr-xr-x 1 root root 2.1K Aug 5 17:14 utw
-rwxr-xr-x 1 root root 1.4K Feb 12 2024 unattended-upgrades
-rwxr-xr-x 1 root root 1.3K Aug 5 17:14 uuid
root@dd3728-siem-xdr-server:/etc/init.d#

```

★ Enable unattended security updates:

#bash

```

sudo apt install -y unattended-upgrades
sudo dpkg-reconfigure --priority=low unattended-upgrades

```

Enable automatic security patching

- Keeps the SIEM continuously protected without manual intervention.

What I implemented :

- OS patching
- Least-privilege service accounts
- Host-based firewalling
- Kernel auditing
- Time integrity
- SIEM performance tuning
- Disabled Transparent Huge Pages (THP)
- Automated security maintenance

D. Splunk Enterprise installation

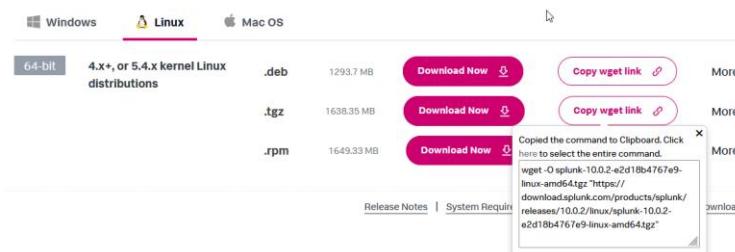
Copy and Paste Splunk https://www.splunk.com/en_us/download.html to /opt
(via MobiXterm SSH from Jumpbox - browser), then:

[screenshots  ]

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



Download:

```
dd3728-analyst@dd3728-siem-xdr-server:/$ cd opt
dd3728-analyst@dd3728-siem-xdr-server:/opt$ sudo wget -O splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz "https://download.splunk.com/products/splunk/releases/10.0.2/linux/splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz"
--2025-12-18 04:56:51-- https://download.splunk.com/products/splunk/releases/10.0.2/linux/splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz
Resolving download.splunk.com (download.splunk.com)... 3.161.94.87, 3.161.94.112, 3.161.94.116, ...
Connecting to download.splunk.com (download.splunk.com)|3.161.94.87|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1717935022 (1.6G) [binary/octet-stream]
Saving to: 'splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz'

splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz      1%[=====] 24.74M 4.46MB/s eta 6m 53s
```

Verify Hash SHA512:

```
dd3728-analyst@dd3728-siem-xdr-server:/$ cd opt
dd3728-analyst@dd3728-siem-xdr-server:/opt$ sudo wget -O splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz "https://download.splunk.com/products/splunk/releases/10.0.2/linux/splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz"
--2025-12-18 04:56:51-- https://download.splunk.com/products/splunk/releases/10.0.2/linux/splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz
Resolving download.splunk.com (download.splunk.com)... 3.161.94.87, 3.161.94.112, 3.161.94.116, ...
Connecting to download.splunk.com (download.splunk.com)|3.161.94.87|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1717935022 (1.6G) [binary/octet-stream]
Saving to: 'splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz'

splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz      100%[=====] 1.60G 3.87MB/s in 9m 10s
2025-12-18 05:06:02 (2.98 MB/s) - 'splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz' saved [1717935022|1717935022]

dd3728-analyst@dd3728-siem-xdr-server:/opt$ ls
splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz
dd3728-analyst@dd3728-siem-xdr-server:/opt$ sha1sum splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz
f3fbe33848ccb120e0624ffbe6050bf093b3a5b8aa3f22605daae4ce2f748cf63ffc2e3552c30684dbf763650b8e28c3e3328c6f201753fccac691e4ec1e  splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz
dd3728-analyst@dd3728-siem-xdr-server:/opt$
```

```
#bash

cd /opt
sudo tar -xvzf splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz-
linux.tgz
sudo chown -R splunk-dd3728:splunk-dd3728 /opt/splunk
```

- Prevents Splunk from running as root — standard SOC security practice.

[**screenshots** ↗️ ↘️]

```
Last login: Thu Dec 18 04:44:04 2025 from 192.168.60.30
dd3728@dd3728-siem-xdr-server:~$ su splunk-dd3728
Password:
splunk-dd3728@dd3728-siem-xdr-server:/home/dd3728-analyst$ cd /
splunk-dd3728@dd3728-siem-xdr-server:$ cd opt
splunk-dd3728@dd3728-siem-xdr-server:/opt$ ls
splunk  splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz
splunk-dd3728@dd3728-siem-xdr-server:/opt$ ll
total 1677688
drwxr-xr-x 3 root root 4096 Dec 18 05:10 .
drwxr-xr-x 23 root root 4096 Dec 11 10:52 ..
drwxr-xr-x 11 10777 10777 4096 Oct 30 00:16 splunk/
-rw-r--r-- 1 root root 1717935022 Nov 14 03:39 splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz
splunk-dd3728@dd3728-siem-xdr-server:/opt$ sudo chown -R splunk-dd3728:splunk /opt/splunk
[sudo] password for splunk-dd3728:
splunk-dd3728@dd3728-siem-xdr-server:/opt$ ll
total 1677688
drwxr-xr-x 3 root root 4096 Dec 18 05:10 .
drwxr-xr-x 23 root root 4096 Dec 11 10:52 ..
drwxr-xr-x 11 splunk-dd3728 splunk-dd3728 4096 Oct 30 00:16 splunk/
-rw-r--r-- 1 root root 1717935022 Nov 14 03:39 splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz
splunk-dd3728@dd3728-siem-xdr-server:/opt$ 
splunk-dd3728@dd3728-siem-xdr-server:/opt$ 
splunk-dd3728@dd3728-siem-xdr-server:/opt$ 
splunk-dd3728@dd3728-siem-xdr-server:/opt$
```

Start Splunk as **splunk-dd3728** user and enable boot-start:

```
#bash
```

```
sudo -u splunk /opt/splunk/bin/splunk start --accept-license
```

- Launches Splunk as a dedicated service account.

```
sudo /opt/splunk/bin/splunk enable boot-start -user splunk
```

- Ensures the SIEM survives reboots like a real SOC server.

[**screenshots** ↗️ ↘️]

```
splunk-dd3728@dd3728-siem-xdr-server:/opt$ 
splunk-dd3728@dd3728-siem-xdr-server:/opt$ 
splunk-dd3728@dd3728-siem-xdr-server:/opt$ 
splunk-dd3728@dd3728-siem-xdr-server:/opt$ sudo -u splunk-dd3728 /opt/splunk/bin/splunk start --accept-license
This appears to be your first time running this version of Splunk.
Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.
```

```
splunk-dd3728@dd3728-siem-xdr-server:/opt$ sudo /opt/splunk/bin/splunk enable boot-start -user splunk-dd3728
[sudo] password for splunk-dd3728:
Sorry, try again.
[sudo] password for splunk-dd3728:
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
splunk-dd3728@dd3728-siem-xdr-server:/opt$ 
splunk-dd3728@dd3728-siem-xdr-server:/opt$ 
splunk-dd3728@dd3728-siem-xdr-server:/opt$ 
splunk-dd3728@dd3728-siem-xdr-server:/opt$
```

Configure receiving:

- Splunk Web: <http://192.168.60.20:8000>
 - Settings → Forwarding and receiving → Add TCP input port 9997.

[screenshots]

Not Secure http://192.168.60.20:8000/en-US/manager/launcher/data/inputs/tcp/cooked?msgid=8639090.1327929524641764&rs=launcher&redirecting=true

Import bookmarks... Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

New Receiving Port

Receive data

Forwarding and receiving > Receive data

Successfully saved "9997".

Showing 1-1 of 1 items

filter

25 per page ▾

Listen on this port	Status	Actions
9997	Enabled Disable	Delete

★ Created index named: network.

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
_audit	Edit Delete Disable	Events	system	5 MB	488.28 GB	46.9K	a month ago	a few seconds ago	\$SPLUNK_DB/_audit/db	-	✓ Active
_configtracker	Edit Delete Disable	Events	system	3 MB	488.28 GB	1.39K	a month ago	an hour ago	\$SPLUNK_DB/_configtracker/db	-	✓ Active
_disapprevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0	-	-	\$SPLUNK_DB/_disapprevent/db	-	✓ Active
_dsclient	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0	-	-	\$SPLUNK_DB/_dsclient/db	-	✓ Active
_diphonenum	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0	-	-	\$SPLUNK_DB/_diphonenum/db	-	✓ Active
_internal	Edit Delete Disable	Events	system	114 MB	488.28 GB	1.1M	a month ago	a few seconds ago	\$SPLUNK_DB/_internal/db	-	✓ Active
_introspection	Edit Delete Disable	Events	system	326 MB	488.28 GB	284K	10 days ago	a few seconds ago	\$SPLUNK_DB/_introspection/db	-	✓ Active
_metrics	Edit Delete Disable	Metrics	system	63 MB	488.28 GB	619K	10 days ago	a few seconds ago	\$SPLUNK_DB/_metrics/db	-	✓ Active
_metrics_rollup	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0	-	-	\$SPLUNK_DB/_metrics_rollup/db	-	✓ Active
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	122	a month ago	6 minutes ago	\$SPLUNK_DB/_telemetry/db	-	✓ Active
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0	-	-	\$SPLUNK_DB/_thefishbucket/db	-	✓ Active
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0	-	-	\$SPLUNK_DB/historydb/db	-	✓ Active
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0	-	-	\$SPLUNK_DB/defaultdb/db	-	✓ Active
network	Edit Delete Disable	Events	search	1 MB	500 GB	126	an hour ago	a few seconds ago	\$SPLUNK_DB/network/db	-	✓ Active
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0	-	-	\$SPLUNK_DB/splunklogger/db	-	✗ Inactive
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0	-	-	\$SPLUNK_DB/summarydb/db	-	✓ Active

What you configured (quick list)

- Splunk to listen for pfSense syslog at UDP 514 (privileged port).
- Changed Splunk input to UDP 1514 (non-privileged).
- Restarted Splunk.
- Opened the host firewall for UDP 1514.
- Verified Splunk is listening on 1514.

"I initially configured Splunk to listen on UDP 514 (standard syslog), but Splunk runs as a non-root service and cannot bind privileged ports. After observing zero tcpdump packets and bind errors in splunkd.log, I moved the input to UDP 1514, opened the firewall, and validated ingestion — maintaining least-privilege and enterprise security best practice."

- ❖ Why each command / config was used

Configured UDP 514 input for pfSense:

```
#bash

sudo tee /opt/splunk/etc/system/local/inputs.conf <<'EOF'
[udp://514]
index = network
sourcetype = pfsense
EOF
```

What it does: Tells Splunk to create a UDP input on port 514 and write events to index=network with sourcetype=pfsense.

Why used: pfSense sends syslog to UDP/514 by default; configuring Splunk for 514 is the natural first step.

[screenshots]

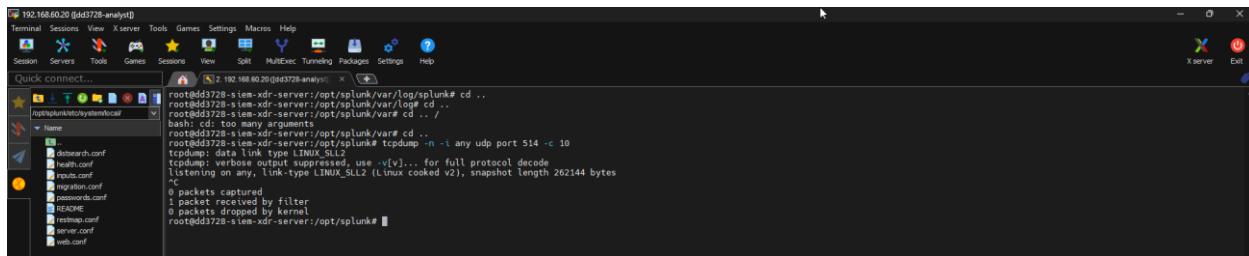
tcpdump captured 0 packets on UDP 514 (diagnostic reasoning)

```
#bash  
sudo tcpdump -n -i any udp port 514 -c 5
```

and saw 0 captured. Possible, immediate causes:

- Splunk never binds UDP 514 (most likely) — Splunk (non-root) cannot bind privileged ports → no process listening ⇒ kernel drops packets or they never targeted this host.
 - Evidence to check: `ss -ulnp | grep 514` (empty → Splunk not listening).
 - Check `splunkd.log` for bind errors.

[screenshots]



Why 1514 is the right decision

“Ports <1024 require root; running Splunk as root is unacceptable for security. Using 1514 keeps Splunk non-privileged and secure while allowing firewall/proxy rules to route or redirect standard syslog traffic as needed.”

1) changed to 1514 ↴ (inputs.conf)

```
sudo tee /opt/splunk/etc/system/local/inputs.conf <<'EOF'
[udp://1514] index = network sourcetype = pfsense EOF
```

What it does: Reconfigures Splunk to listen on UDP 1514 instead of 514.

Why used: Ports below 1024 are privileged — only root can bind them. Splunk runs as a non-root service user (**splunk-dd3728**) for security, so it cannot bind to UDP 514. Using 1514 (>1024) avoids granting Splunk elevated privileges and follows least-privilege practice.

2) restart Splunk ↵(apply changes)

```
sudo -u splunk /opt/splunk/bin/splunk restart
```

What it does: Restarts Splunk as the splunk service user so it reads the new inputs.conf.

Why used: Changes to inputs only take effect after Splunk restarts.

3) allow UDP 1514 through host firewall

```
sudo ufw allow 1514/udp
```

What it does: Opens port 1514/UDP on the Ubuntu host so incoming syslog packets are not blocked.

Why used: Even if Splunk listens, the OS firewall can still drop packets.

4) verify listener

```
sudo ss -ulnp | grep 1514
```

What it does: Shows UDP sockets and the processes listening on them.

Why used: Confirms Splunk is actually bound to 1514 and ready to receive.

```
sudo -u splunk /opt/splunk/bin/splunk restart
```

[**screenshots ↗ ↘**]

```

192.168.60.20 [dd3728-analy] Terminal Sessions View Xserver Tools Games Settings Macros Help Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help Quick connect... [2] 92.168.60.20 [dd3728-analy] * /root@dd3728-siem-xdr-server:/# 1) update inputs.conf to 1514
tee /opt/splunk/etc/system/local/inputs.conf << EOF
index = network
sourceType = pfSense
EOF
# 2) restart splunk
-u splunk /opt/splunk/bin/splunk restart
# 3) allow port in firewall
ufw allow 1514/udp
# 4) verify listeners
ss -ulnp | grep 1514
[udo://1514]
index = network
sourceType = pfSense
-u: command not found
Rule added
Rule added
Rule added (v6)
root@dd3728-siem-xdr-server:/# tee /opt/splunk/etc/system/local/inputs.conf << EOF
[udo://1514]
index = network
sourceType = pfSense
EOF
[udo://1514]
Index = network
sourceType = pfSense
root@dd3728-siem-xdr-server:/# cat /opt/splunk/etc/system/local/inputs.conf
[udo://1514]
index = network
sourceType = pfSense
root@dd3728-siem-xdr-server:/# /opt/splunk/bin/splunk restart
-u splunk: command not found
root@dd3728-siem-xdr-server:/# /opt/splunk/bin/splunk restart
# 3) allow port in Firewall
ufw allow 1514/udp
# 4) verify listener
ss -ulnp | grep 1514
-u: command not found
stopping and deleting rule
skipping adding existing rule (v6)
root@dd3728-siem-xdr-server:/# /opt/splunk/bin/splunk restart
root@dd3728-siem-xdr-server:/#

```



```

192.168.60.20 [dd3728-analy] Terminal Sessions View Xserver Tools Games Settings Macros Help Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help Quick connect... [2] 92.168.60.20 [dd3728-analy] * root@dd3728-siem-xdr-server:/# ss -ulnp | grep 1514
UNCONN 0 0 0.0.0.0:1514 0.0.0.0:* users:(("splunkd",pid=18684,fd=71))
root@dd3728-siem-xdr-server:/# root@dd3728-siem-xdr-server:/# root@dd3728-siem-xdr-server:/# root@dd3728-siem-xdr-server:/# root@dd3728-siem-xdr-server:/# root@dd3728-siem-xdr-server:/# tcpreplay -n 1 -i any udp port 1514 -c 5
tcpreplay: verbose output suppressed, use -vv... for full protocol decode
listening on any, link-type LINUX_SLL2
00:06:09.355672 ens3 In IP 192.168.60.1.514 > 192.168.60.20.1514: SYSLOG syslog.error, length: 105
00:06:09.355693 ens3 In IP 192.168.60.1.514 > 192.168.60.20.1514: SYSLOG daemon.info, length: 97
00:08:19.260200 ens3 In IP 192.168.60.1.514 > 192.168.60.20.1514: SYSLOG daemon.info, length: 97
00:08:19.260200 ens3 In IP 192.168.60.1.514 > 192.168.60.20.1514: SYSLOG daemon.info, length: 97
5 packets captured
7 packets dropped by filter
0 packets dropped by kernel
root@dd3728-siem-xdr-server:/# root@dd3728-siem-xdr-server:/# root@dd3728-siem-xdr-server:/#

```



```

192.168.60.20 [dd3728-analy] Terminal Sessions View Xserver Tools Games Settings Macros Help Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help Quick connect... [2] 92.168.60.20 [dd3728-analy] * root@dd3728-siem-xdr-server:/# /opt/splunk/bin/splunk restart
stopping splunk...
Shutting down... Please wait, as this may take a few minutes.
...
Stopping splunk helpers...
Done.
Splunk> Map. Reduce. Recycle.
Checking prerequisites
  Checking http port [8000]: open
  Checking agent port [8089]: open
  Checking appserver port [127.0.0.1:8085]: open
  Checking kvstore port [8100]: open
  Checking config port [8086]: open
  Checking default config. Done
New certs have been generated in '/opt/splunk/etc/auth'.
  Checking critical directories...
  Checking ...
    Validated: _audit _configtracker _dsappagent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main network summary
  Done
  Checking filesystem compatibility... Done
  Checking conf files for problems...
  Done
  Checking ...
    Validating installed files against hashes from '/opt/splunk/splunk-10.0.2-e2d1b4767e9-linux-amd64-manifest'.
      All installed files intact.
    Done
  All preliminary checks passed.
Starting splunk server daemon (splunkd)...
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://dd3728-siem-xdr-server:8000
root@dd3728-siem-xdr-server:/# ss -ulnp | grep 1514
UNCONN 0 0 0.0.0.0:1514 0.0.0.0:* users:(("splunkd",pid=18684,fd=71))
root@dd3728-siem-xdr-server:/#

```

E. Validation tests

Jumpbox – Splunk Web connectivity test :

#bash

```
curl -I http://192.168.60.20:8000
```

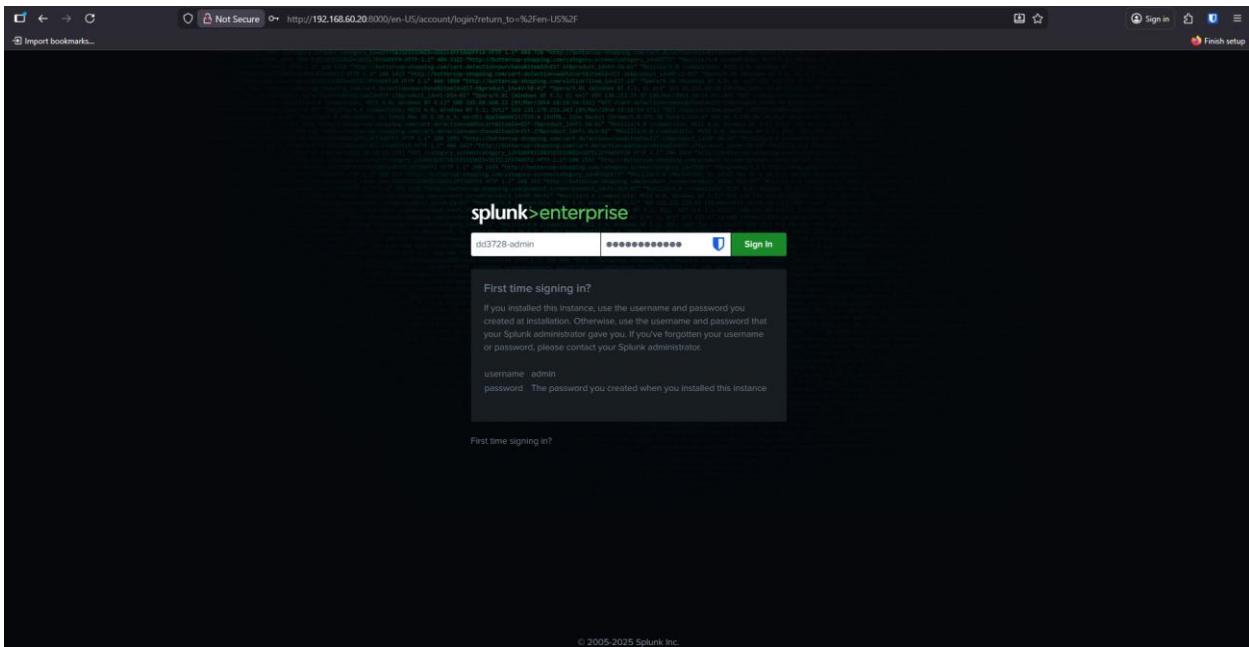
Purpose:

- Verifies that Splunk Web is reachable over the network, and that TCP/8000 is open.

What it proves:

- Network routing is correct
- Firewall allows access
- Splunk Web service is listening

[screenshots  ]



Splunk Server – Process validation ✅ :

```
#bash
ps aux | grep splunk
```

Purpose:

- Confirms that Splunk services are running on the server.

What it proves:

- Splunkd is active
 - No startup or service failure
 - Splunk is capable of receiving and indexing data

[screenshots]

Splunk Web – Data ingestion validation :

- Search:

#spl

```
index=network sourcetype=pfsense | head 20
```

Purpose:

- Checks whether pfSense logs are being successfully indexed.

What it proves:

- UDP input is working
 - Correct index assignment
 - Logs are searchable in Splunk

[screenshots]

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query `index=network sourcetype=pfSense | head 20`. The results pane displays 7 events from Jan 15, 2026, at 12:06:09 AM. All events are from host `192.168.60.001` on port `554` (source type `pfSense`). The events include a `DHCP` solicit and a `syslogd` connection refused message.

Time	Event
Jan 15 00:06:09 192.168.60.1	1 2026-01-15T00:06:09.680738+02:00 dd3728-pfSense.dd3728.lab dhcp6c 42213 -- Sending Solicit
Jan 15 00:06:09 192.168.60.1	host = 192.168.60.001 source = udp:554 sourcetype = pfSense
Jan 15 00:06:09 192.168.60.1	1 2026-01-15T00:06:09.680738+02:00 dd3728-pfSense.dd3728.lab dhcp6c 42213 -- Sending Solicit
Jan 15 00:06:09 192.168.60.1	host = 192.168.60.001 source = udp:554 sourcetype = pfSense
Jan 15 00:06:09 192.168.60.1	1 2026-01-15T00:06:09.681108+02:00 dd3728-pfSense.dd3728.lab syslogd -- -- sendto: connection refused
Jan 15 00:06:09 192.168.60.1	host = 192.168.60.001 source = udp:554 sourcetype = pfSense
Jan 15 00:06:09 192.168.60.1	1 2026-01-15T00:06:09.681108+02:00 dd3728-pfSense.dd3728.lab nginx -- -- 2026/01/15 00:04:41 [error] 95654#100258: send() failed (54: Connection reset by peer) while logging t
Jan 15 00:06:09 192.168.60.1	o syslog, server: unix:/var/run/log
Jan 15 00:06:09 192.168.60.1	host = 192.168.60.001 source = udp:554 sourcetype = pfSense
Jan 15 00:06:09 192.168.60.1	1 2026-01-15T00:06:09.681108+02:00 dd3728-pfSense.dd3728.lab sshguard 7329 -- Now monitoring attacks.
Jan 15 00:06:09 192.168.60.1	host = 192.168.60.001 source = udp:554 sourcetype = pfSense

9—Windows Client: domain join, Splunk UF & Sysmon

Goal: Generate realistic endpoint telemetry for Splunk.

A. Networking & DNS

#powershell

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" -  
ServerAddresses 192.168.60.10  
New-NetIPAddress -InterfaceAlias "Ethernet0" -IPAddress  
192.168.60.100 -PrefixLength 24 -DefaultGateway 192.168.60.1
```

[screenshots ↗️ ↘️]

```
Administrator: Windows PowerShell  
PS C:\WINDOWS\system32> New-NetIPAddress -InterfaceAlias "Ethernet0" -IPAddress 192.168.60.100 -PrefixLength 24 -DefaultGateway 192.168.60.1  
PS C:\WINDOWS\system32> #powershell  
PS C:\WINDOWS\system32> PS C:\WINDOWS\system32> Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" -ServerAddresses 192.168.60.10  
PS C:\WINDOWS\system32> ipconfig /all  
Windows IP Configuration  
Host Name . . . . . : 003728-WIN-Client  
Primary Dns Suffix . . . . . :  
Node Suffix . . . . . : Hybrid  
DnD Routing Enabled . . . . . : No  
WINS Proxy Enabled . . . . . : No  
Ethernet adapter Ethernet0:  
Connection-specific DNS Suffix . :  
Description . . . . . : Intel(R) Dual Band Wireless-AC 7265  
Physical Address . . . . . : 80-0C-29-F3-75-52  
DHCP Enabled . . . . . : No  
Autocounting Enabled . . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::6600:1c0ff:fe10:75c2%20(PREFERRED)  
IPv4 Address . . . . . : 192.168.60.100  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.60.1  
DHCPv6 IAID . . . . . : 335047433  
DHCPv6 Client DUID . . . . . : 00-01-00-08-01-31-00-5C-60-00-0C-29-F3-75-52  
DNS Servers . . . . . : 192.168.60.10  
NetBIOS over Tcpip . . . . . : Enabled  
PS C:\WINDOWS\system32>
```

B. Domain join

#powershell

```
Add-Computer -DomainName digitaldefence3728.lab -Credential
digitaldefence\administrator -Restart
```

Domain successfully joined ✓

[screenshots ↗️ ↘️]

Administrator: Windows PowerShell

```
Windows IP Configuration

Host Name . . . . . : DD3728-CLIENT
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : dd3728.lab

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . . . . :
Description . . . . . :
Physical Address. . . . . :
DHCP Enabled. . . . . :
Autoconfiguration Enabled . . . . . :
Link-local IPv6 Address . . . . . :
IPv4 Address. . . . . :
Subnet Mask . . . . . :
Lease Obtained. . . . . :
Lease Expires . . . . . :
Default Gateway . . . . . :
DHCP Server . . . . . :
DHCPv6 IAID . . . . . :
DHCPv6 Client DUID. . . . . :
DNS Servers . . . . . : 192.168.60.10
NetBIOS over Tcpip. . . . . : Enabled

PS C:\WINDOWS\system32> Add-Computer -DomainName digitaldefence3728.lab -Credential digitaldefence\ben -Restart
```

Windows PowerShell credential request

User name: digitaldefence\ben

Enter your credentials.

OK Cancel

Windows PowerShell

```
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> ipconfig /all

Windows IP Configuration

Host Name . . . . . : DD3728-CLIENT
Primary Dns Suffix . . . . . : DigitalDefence3728.lab
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : DigitalDefence3728.lab
dd3728.lab

Ethernet adapter Ethernet0:

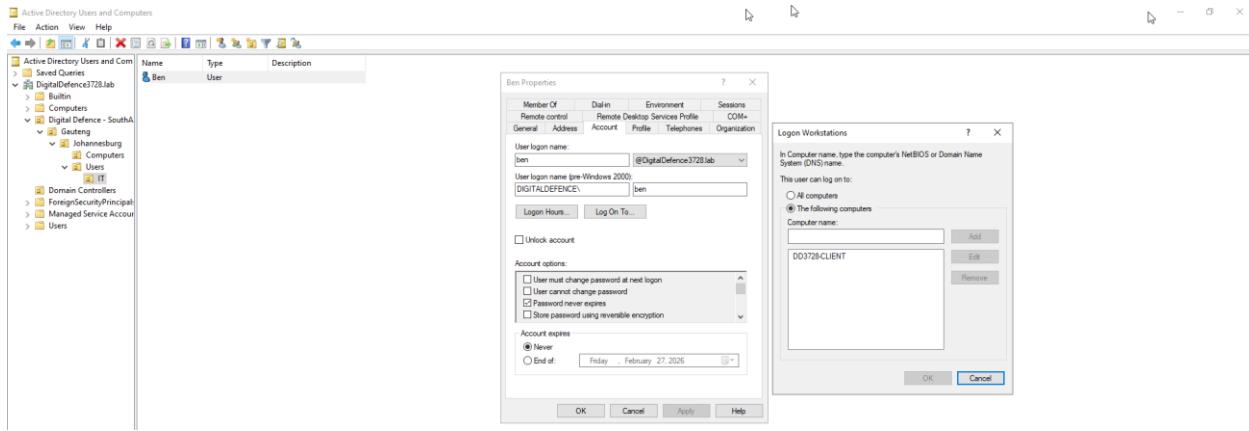
Connection-specific DNS Suffix . . . . . : dd3728.lab
Description . . . . . : Intel(R) 8257UL Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-8A-7A-E8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . :
fe80::727b:216b:820:7c58%13(PREFERRED)
IPv4 Address . . . . . : 192.168.60.100(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, January 28, 2026 6:47:34 AM
Lease Expires . . . . . : Wednesday, January 28, 2026 8:47:34 AM
Default Gateway . . . . . : 192.168.60.1
DHCP Server . . . . . : 192.168.60.1
DHCPv6 IAID . . . . . : 83801191
DHCPv6 Client DUID. . . . . : 00-0C-29-81-31-00-73-61-00-0C-29-8A-7A-E8
DNS Servers . . . . . : 192.168.60.10
NetBIOS over Tcpip. . . . . : Enabled

PS C:\WINDOWS\system32>
```

Other user

i Prior win-client DC join, I had already set up a client user named Ben and added DD3728-CLIENT VM machine under user Ben to Log-on using that machine.

[screenshot  



★ Below is a brief, precise, explanation of what I configured and why.
Before Windows UF installation.

```
/opt/splunk/etc/apps/admin-demo/local/indexes.conf
```

[network]

- homePath = \$SPLUNK_DB/network/db
- coldPath = \$SPLUNK_DB/network/colddb
- thawedPath = \$SPLUNK_DB/network/thaweddb

- #sizing & lifecycle
- maxTotalDataSizeMB = 512000
- homePath.maxDataSizeMB = 300000
- maxDataSize = 20
- maxHotBuckets = 5
- frozenTimePeriodInSecs = 100697600

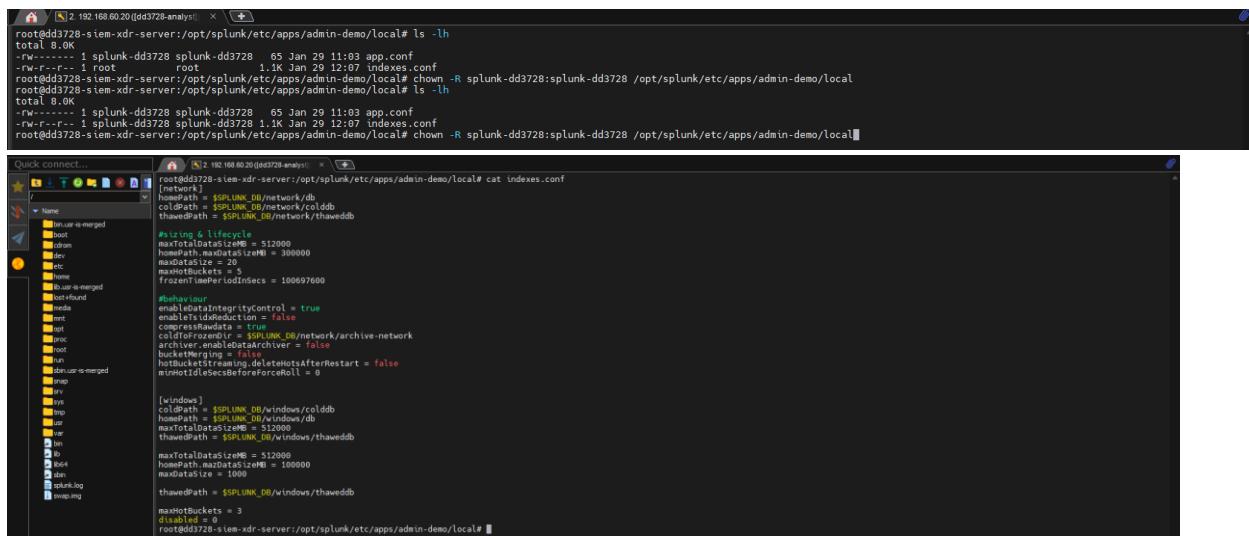
- #behaviour
- enableDataIntegrityControl = true
- enableTsidxReduction = false
- compressRawdata = true
- coldToFrozenDir = \$SPLUNK_DB/network/archive-network
- archiver.enableDataArchiver = false
- bucketMerging = false
- hotBucketStreaming.deleteHotsAfterRestart = false
- minHotIdleSecsBeforeForceRoll = 0

[windows]

- coldPath = \$SPLUNK_DB/windows/colddb
- homePath = \$SPLUNK_DB/windows/db
- maxTotalDataSizeMB = 512000
- thawedPath = \$SPLUNK_DB/windows/thaweddb
- maxTotalDataSizeMB = 512000
- homePath.mazDataSizeMB = 100000
- maxDataSize = 1000

- thawedPath = \$SPLUNK_DB/windows/thaweddb
- maxHotBuckets = 3
- frozenTimePeriodInSecs = 100697600
- archiver.enableDataArchiver = 0
- bucketMerging = 0

[screenshots 🔍 ↻]



```

root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/admin-demo/local# ls -lh
total 8.0K
-rw-r--r-- 1 splunk-dd3728 splunk-dd3728 65 Jan 29 11:03 app.conf
-rw-r--r-- 1 root          root          1.1K Jan 29 12:07 indexes.conf
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/admin-demo/local# chown -R splunk-dd3728:splunk-dd3728 /opt/splunk/etc/apps/admin-demo/local
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/admin-demo/local# ls -lh
total 8.0K
-rw-r--r-- 1 splunk-dd3728 splunk-dd3728 65 Jan 29 11:03 app.conf
-rw-r--r-- 1 root          root          1.1K Jan 29 12:07 indexes.conf
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/admin-demo/local# chown -R splunk-dd3728:splunk-dd3728 /opt/splunk/etc/apps/admin-demo/local

```

Quick connect... [root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/admin-demo/local] cat indexes.conf

```

[windows]
homePath = $SPLUNK_DB/windows/db
coldPath = $SPLUNK_DB/windows/colddb
thawedPath = $SPLUNK_DB/windows/thaweddb

#sizing & lifecycle
maxTotalDataSizeMB = 512000
homePath.mazDataSizeMB = 300000
maxDataSize = 20
maxHotBuckets = 5
frozenTimePeriodInSecs = 100697600

#sharable
enableSharedIntegrityControl = true
enableSharedDeduction = false
compressRawData = true
collectRawData = true
$SPLUNK_DB/network/archive-network
archiver.enableDataArchiver = false
bucketMerging = false
highWaterMarkDeleteJobsAfterRestart = false
minHoldTimeSecsBeforeForceRoll = 0

[windows]
coldPath = $SPLUNK_DB/windows/colddb
homePath = $SPLUNK_DB/windows/db
maxTotalDataSizeMB = 512000
thawedPath = $SPLUNK_DB/windows/thaweddb

maxTotalDataSizeMB = 512000
homePath.mazDataSizeMB = 100000
maxDataSize = 20
maxHotBuckets = 3
disabled = true

```

Why I created a dedicated admin app (admin-demo)

- I removed custom index definitions from the Search app and moved them into a separate admin-level app.
- This follows Splunk enterprise best practice
- Prevents upgrades from overwriting configs
- Separates platform administration from user/search content

[screenshot 🔍 ↻]

The screenshot shows the Splunk Enterprise App Listing interface. A modal window titled 'Create App' is open, prompting for app details. The 'Name' field contains 'admin-demo'. The 'Folder name' field also contains 'admin-demo'. The 'Version' field is set to '1.0.0'. Under 'Visible', the 'Yes' radio button is selected. The 'Author' field is filled with 'digitaldefence3728'. The 'Description' field contains the placeholder 'keep all config in a separate app level'. The 'Template' dropdown is set to 'barebones'. An 'Upload asset' field is present with a placeholder 'Drop your file here or browse...'. At the bottom right of the modal are 'Cancel' and 'Save' buttons, with 'Save' being highlighted.

The screenshot shows the Splunk Enterprise App Listing interface after the app has been created. The 'admin-demo' app is now listed in the main table of available apps. It has a blue selection box around its row. The table includes columns for Name, Actions, Folder Name, Version, Check for Updates, Visibility, Sharing, Status, and App Origin. The 'admin-demo' app is listed under 'Actions' as 'Edit properties' and 'Folder Name' as 'admin-demo'. Its status is 'Enabled | Disable' and 'Status' is 'Splunk'.

The screenshot shows a terminal session on a root shell of a Splunk server. The command 'ls' is run in the '/opt/splunk/etc/apps' directory. The output lists various Splunk apps and their versions. The 'admin-demo' directory is highlighted with a red arrow and a blue selection box. Other visible files include 'introspection_generator_addon', 'python_upgrade_readiness_app', 'splunk_dashboard_studio', 'splunk_httpinput', 'splunk_metrics_workspace', 'splunk_secure_gateway', 'splunk_webhook', 'sample_app', 'splunk_data-management', 'splunk_ingest_actions', 'splunk_monitoring_console', 'splunk_pipeline_builders', 'splunk_deploymentServerConfig', 'splunk_lightForwarder', 'splunk_gdt', 'splunk_forwarder', 'splunk_oily_cloud', 'splunk_internal_metrics', 'splunk_rapid_dsl', 'splunk_visual_exporter', and 'splunk_rolling_upgrade'.

```

root@dd3728-siem-xdr-server:/opt/splunk/etc/apps# ls
admin-demo introspection_generator_addon python_upgrade_readiness_app splunk_dashboard_studio splunk_httpinput splunk_metrics_workspace splunk_secure_gateway
alert_logevent journald_input sample_app splunk_data-management splunk_ingest_actions splunk_monitoring_console splunk_visual_exporter
alert_webhook sample_app splunk_deploymentServerConfig splunk_lightForwarder splunk_pipeline_builders user-prefs
appsbrowser learned splunk_app_for_splunk_oily_cloud SplunkForwarder
audit_trail legacy splunk_archiver splunk_gdt
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps# ls -l
total 13K
drwxr-xr-x 6 splunk-dd3728 splunk-dd3728 4.0K Jan 29 09:04 admin-demo
drwxr-xr-x 7 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 alert_logevent
drwxr-xr-x 7 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 alert_webhook
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 appsbrowser
drwxr-xr-x 7 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 audit_trail
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 introspection_generator_addon
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 journald_input
drwxr-xr-x 8 splunk-dd3728 splunk-dd3728 4.0K Jan 14 23:08 launcher
drwxr-xr-x 5 splunk-dd3728 splunk-dd3728 4.0K Dec 18 07:18 learned
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 legacy
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 python_upgrade_readiness_app
drwxr-xr-x 6 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 sample_app
drwxr-xr-x 9 splunk-dd3728 splunk-dd3728 4.0K Jan 14 23:13 search*
drwxr-xr-x 9 splunk-dd3728 splunk-dd3728 4.0K Mar 27 2023 splunk_app_for_splunk_oily_cloud
drwxr-xr-x 6 splunk-dd3728 splunk-dd3728 4.0K Dec 09:18 splunk_archiver
drwxr-xr-x 6 splunk-dd3728 splunk-dd3728 4.0K Oct 18 07:18 splunk_dashboard_studio
drwxr-xr-x 6 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:14 splunk_data-management
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 SplunkDeploymentServerConfig
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 SplunkForwarder
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 splunk_gdt
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 splunk_httpinput
drwxr-xr-x 3 splunk-dd3728 splunk-dd3728 4.0K Dec 19 06:06 splunk_ingest_actions
drwxr-xr-x 9 splunk-dd3728 splunk-dd3728 4.0K Dec 18 07:19 splunk_instrumentation
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 splunk_internal_metrics
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 splunk_lightForwarder
drwxr-xr-x 8 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:14 splunk_metrics_workspace
drwxr-xr-x 11 splunk-dd3728 splunk-dd3728 4.0K Dec 19 04:36 splunk_monitoring_console
drwxr-xr-x 9 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:14 splunk_pipeline_builders
drwxr-xr-x 9 splunk-dd3728 splunk-dd3728 4.0K Jan 14 23:13 splunk_rapid_dsl
drwxr-xr-x 9 splunk-dd3728 splunk-dd3728 4.0K Dec 18 07:18 splunk_visual_exporter
drwxr-xr-x 11 splunk-dd3728 splunk-dd3728 4.0K Dec 19 06:06 splunk_rolling_upgrade
drwxr-xr-x 5 splunk-dd3728 splunk-dd3728 4.0K Oct 17 01:20 splunk_visual_exporter
drwxr-xr-x 4 splunk-dd3728 splunk-dd3728 4.0K Oct 30 02:12 user-prefs
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps# cd admin-demo
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/admin-demo# ls
bin default local metadata

```

★ Improves maintainability, auditing, and portability

Indexes are now managed at:

```
/opt/splunk/etc/apps/admin-demo/local/indexes.conf
```

[screenshot

```
dd3728-analyst@dd3728-siem-xdr-server:~$ sudo su
[sudo] password for dd3728-analyst:
root@dd3728-siem-xdr-server:~# cd /
root@dd3728-siem-xdr-server:~# cd opt
root@dd3728-siem-xdr-server:/opt/splunk
root@dd3728-siem-xdr-server:/opt/splunk# ls
bin  copyright.txt  etc  include  lib  license-eula.txt  LICENSE.txt  openssl  opt  quarantined_files  README-splunk.txt  share  splunk-10.0.2-e2d18b4767e9-linux-amd64-manifest  swidtag  var
splunkd  test
root@dd3728-siem-xdr-server:/opt/splunk/etc# ls
anonymizer  datetime.xml  instance.cfg  log.cfg  login-info.cfg  manager-apps  openldap  shcluster  splunk.version
apps        deployment-apps  licenses  log-cmdline.cfg  log-searchprocess.cfg  master-apps  packages  splunk-enterprise.lic  system
auth       disabled-apps  log-btool.cfg  log-cmdline-debug.cfg  log-tlsproxy.cfg  modules  passwd  splunk-launch.conf  users
copyright.txt  log_d  log_debug.cfg  log-debug.cfg  log-utility.cfg  myUninstall  prettyprint.xsl  splunk-launch.conf.default
audit      legacy  log_d-debug.cfg  log_debug.cfg  log-utility.cfg
root@dd3728-siem-xdr-server:/opt/splunk/etc# cd apps
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps# ls
admin_demo  introspection_generatorAddon  python_upgrade_readiness_app  splunk-dashboard-studio  splunk_httpinput  splunk_metrics_workspace  splunk_secure_gateway
alert_logevent  journald_input  sample_app  splunk_data-management  splunk_ingest_actions  splunk_monitoringconsole  splunk-visual-exporter
app        logstash  search  splunkforwarderServerConfig  splunk_realm-automation  splunk_realm-builders  user-prefs
appsBrowser  learned  splunk_app_for_splunk_oily_cloud  SplunkForwarder  splunk_internal_metrics  splunk_rapid_diag
audit_trail  legacy  splunk_archiver  splunk_gdi  SplunkLightForwarder  splunk_rolling-upgrade
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps# cd search
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/search# ls
local
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/search# cd local
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/search/local# ls
indexes.conf
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/search/local# vi indexes.conf
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/search/local# vi indexes.conf
root@dd3728-siem-xdr-server:/opt/splunk/etc/apps/search/local#
```

Index design intent

- network index → pfSense firewall and network telemetry
- windows index → Windows logs forwarded by the Universal Forwarder
- This separation supports:
 - Clear data ownership
 - Targeted retention and sizing
 - Faster troubleshooting and searches

Network index – pfSense data

- Storage paths
- homePath → Hot/Warm buckets for active firewall logs
- coldPath → Aged network data
- thawedPath → Restored data for investigations

Paths for Data Storage

- homePath = \$SPLUNK_DB/network/db: This defines the primary storage location for the indexer's hot data (the most current data).
- coldPath = \$SPLUNK_DB/network/colddb: This is where older hot data is moved when it's no longer actively being written to but still needs to be stored.
- thawedPath = \$SPLUNK_DB/network/thaweddb: This path stores data that has been archived and is ready for retrieval.

Sizing & Data Lifecycle Management

- maxTotalDataSizeMB = 512000: The maximum limit for total data storage across all indexed data.
- homePath.maxDataSizeMB = 300000: Specific limit for the hot data path.
- maxDataSize = 20: This may refer to the maximum size of individual data buckets.
- maxHotBuckets = 5: Maximum number of active hot data buckets.
- frozenTimePeriodInSecs = 100697600: Duration (in seconds) after which data will be moved to a frozen state (not usable for queries).

Data Handling Behavior

- enableDataIntegrityControl = true: Ensures that data integrity checks are performed, preventing data corruption.
- enableTsidxReduction = false: Disables the reduction of the index size for time series data.
- compressRawdata = true: Enables compression for raw data to save space.
- codToFrozenDir = \$SPLUNK_DB/network/archive-network: Specifies the directory for archiving frozen data.
- archiver.enableDataArchiver = false: The data archiving feature is turned off.
- bucketMerging = false: Disables the merging of smaller data buckets into larger ones to enhance performance.
- hotBucketStreaming.deleteHotsAfterRestart = false: Retains hot buckets even after a system restart.
- minHotIdleSecsBeforeForceRoll = 0: Indicates that there's no minimum idle time before rolling the hot buckets into cold storage.

This index is optimized for:

- Event logs
- Sysmon telemetry
- Endpoint investigations

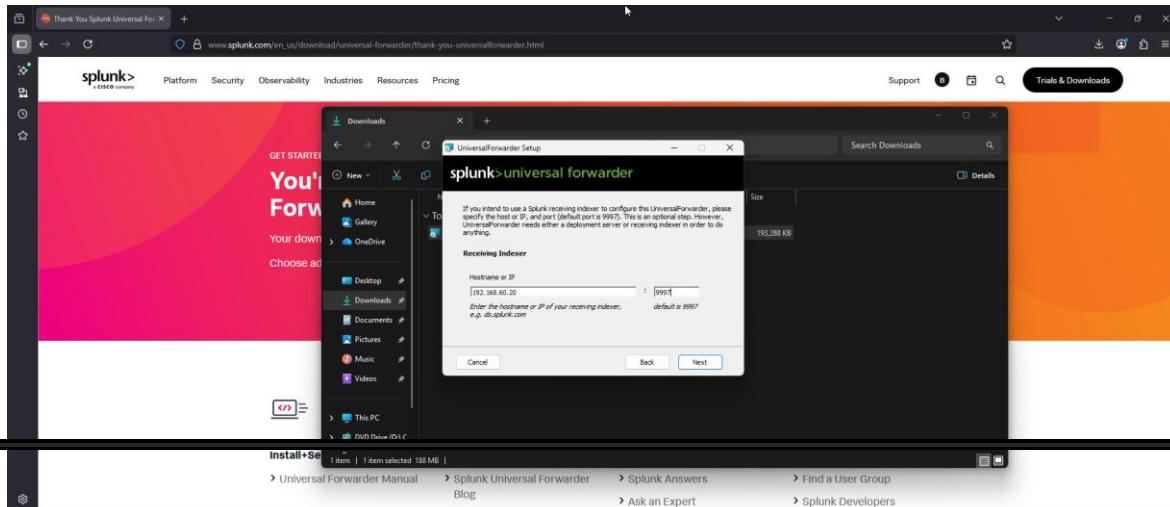
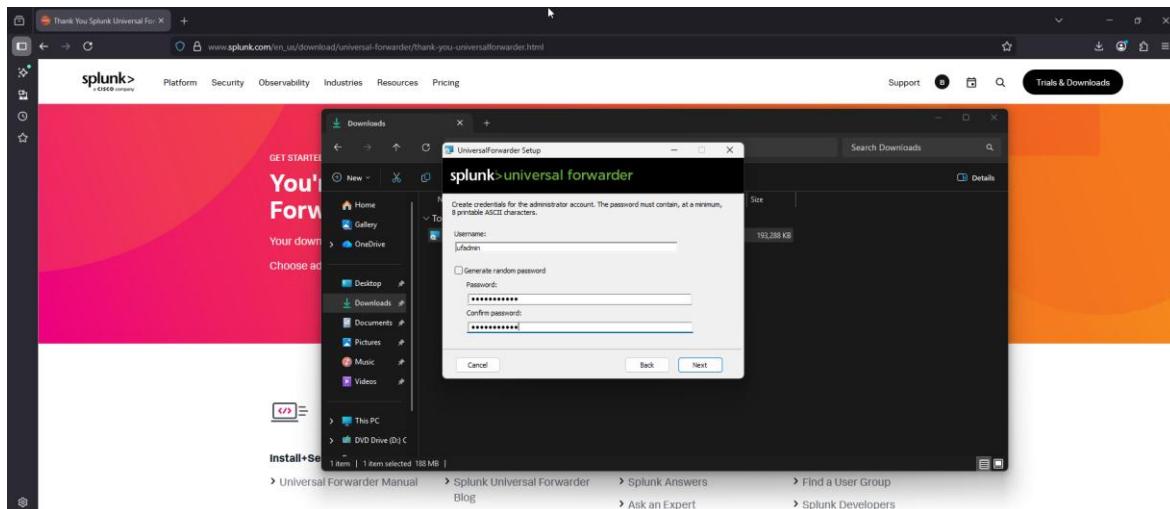
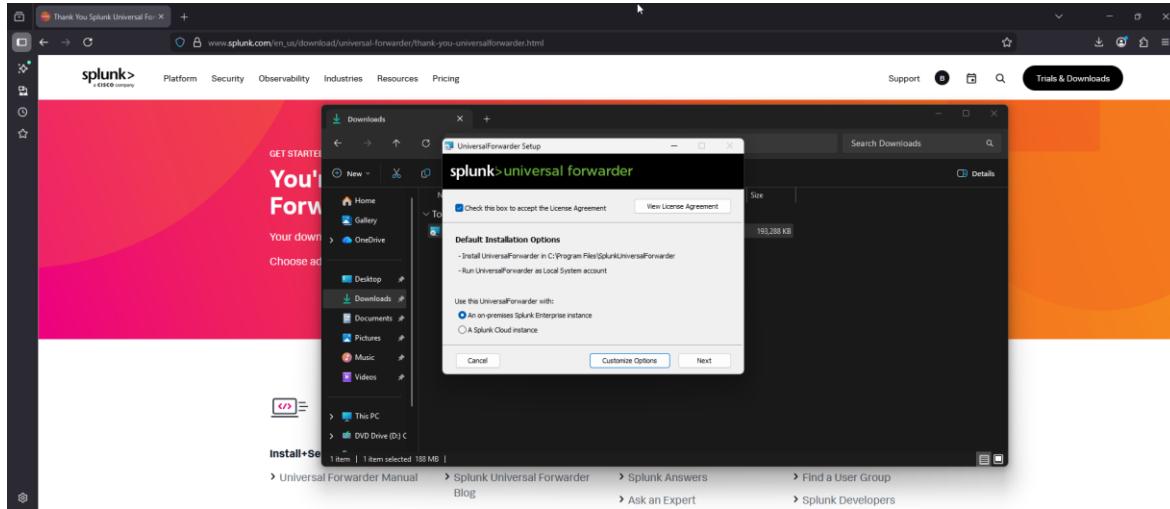
Why this matter?

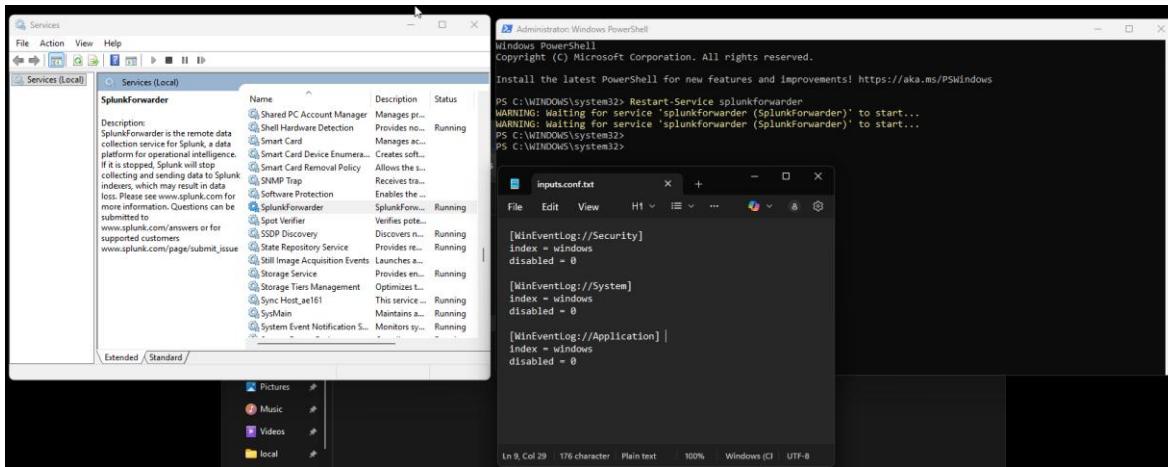
- Demonstrates real-world Splunk administration, not lab shortcuts
- Shows understanding of index lifecycle, performance, and governance
- Aligns with SOC-grade operational standards
- This is how Splunk is structured in production security environments, not demos.

C. Splunk Universal Forwarder install

Gui installation:

[screenshot  ]





D. Configure UF inputs for Windows Event Logs

Create/edit

C:\ProgramFiles\SplunkUniversalForwarder\etc\system\local\inputs.conf:

```
[WinEventLog://Security]
index = windows
disabled = 0
```

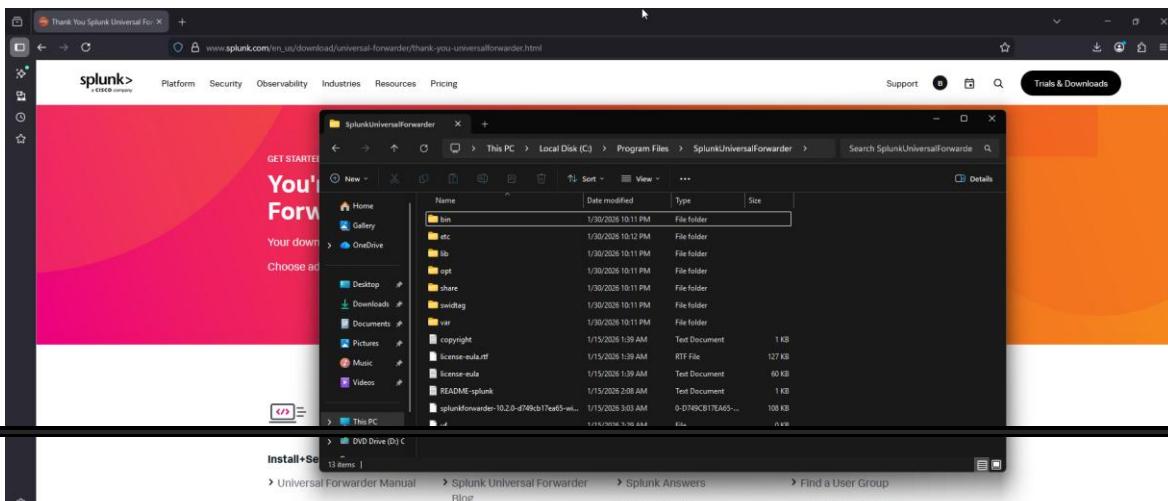
```
[WinEventLog://System]
index = windows
disabled = 0
```

```
[WinEventLog://Application]
index = windows
disabled = 0
```

Restart UF:

powershell

Restart-Service splunkforwarder



Time	Event
2/3/26 9:45:32.472 AM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Security-SPP" Guid="{E23B100-C8C9-472C-A5F9-F2BDFEAP156}" EventSourceName="Software Protection Platform Service"/><EventID Qualifiers="16384">16384</EventID><Version>0</Version><Level>4</Level><Task></Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2023-02-03T07:45:32.472042Z" /><EventRecordID>1879</EventRecordID><CorrelationID></CorrelationID><Execution ProcessID="6688" ThreadID="0" /><Channel>Application</Channel><Computer>003728-CLIENT.DigitalDefence3728.lab</Computer><Security/><System><EventData><Data>2026-03-20T13:28:12Z</Data><Data>RuleEngine</Data><Data>EventData</Data></EventData></System><Event>
2/3/26 9:45:02.550 AM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Security-SPP" Guid="{E23B100-C8C9-472C-A5F9-F2BDFEAP156}" EventSourceName="Software Protection Platform Service"/><EventID Qualifiers="16384">16384</EventID><Version>0</Version><Level>4</Level><Task></Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2023-02-03T07:45:02.550037Z" /><EventRecordID>1874</EventRecordID><CorrelationID></CorrelationID><Execution ProcessID="6688" ThreadID="0" /><Channel>Application</Channel><Computer>003728-CLIENT.DigitalDefence3728.lab</Computer><Security/><System><EventData><Event>
2/3/26 9:41:43.002 AM	TypeService Name="CloudBackupRestoreSvc_d795f" DisplayName="Cloud Backup and Restore Service_d795f" Description="Monitors the system for changes in application and setting states and performs cloud backup and restore operations when required." Path="C:\Windows\system32\svchost.exe -k UnistackSvcGroup" Show all 11 lines

"For the Windows client, I configured Splunk Universal Forwarder telemetry using the production-grade Splunk_TA_windows add-on from Splunkbase."

Quick breakdown

- Started with basic Event Log collection (Security, System, Application) → index=windows
- Upgraded to Splunk_TA_windows add-on - copied to C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\

Outcome

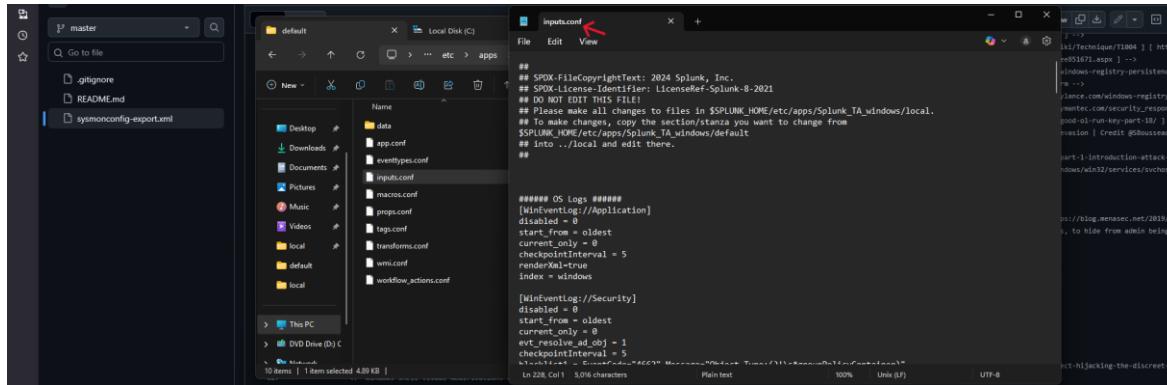
- Core logs: Security, System, Application, Defender AV, ForwardedEvents
- Performance monitoring: WMI every 10min - CPU, Memory, Disk, Services, Processes, Network
- Security telemetry: Registry Run key monitoring, listening ports hourly, installed apps daily
- Infrastructure: DHCP logs, Windows Firewall logs, Windows Update status, AD replication, BIOS data
- Network: Inbound/outbound connection tracking via WinNetMon

Single restart → Restart-Service splunkforwarder → enterprise-grade endpoint telemetry flowing to Splunk.

This shows:

- UF deployment + add-on management
- Enterprise telemetry collection (not just basic logs)
- Production configs
- Security-relevant sources (Defender, Run keys, listening ports)

[screenshot  ]



This screenshot shows the Splunk search interface with the following details:

- Search Bar:** Search Splunk 10.2.0, 192.168.60.20:8000/en-US/app/search/search?earliest=r@latest-r@q=search%20index%3Dwindows%20services&sid=1770105319...
- Panel Headers:** Splunk-enterprise, Apps, Search, Analytics, Datasets, Reports, Alerts, Dashboards.
- Search Results:** New Search, index="windows" services, 6 of 6 events matched, No Event Sampling.
- Event List:** Shows two events from 2/3/26 at 9:55:30 AM. Both events are from host '003728-CLIENT' and source 'WinRegistry' with sourcetype 'WinRegistry'. The first event has a key path of 'HKLM\SYSTEM\ControlSet001\services\w32time\securetime\limits\runtime\securetimeconfidence' and a value name 'data_type="REG_DWORD"'. The second event has a key path of 'HKLM\SYSTEM\ControlSet001\services\w32time\securetime\limits\runtime\securetimelockcount' and a value name 'data_type="REG_DWORD"'. Both events show a value of '1'.

E. Install Sysmon

Downloaded Sysmon [Sysmon v15.15](#) and a vetted configuration SwiftOnSecurity's [sysmonconfig-export.xml](#)

Extracted Sysmon zip file and created Tools folder under C:\ path then Placed in C:\Tools\Sysmon:

[screenshot  ]

```

<!-- RuleGroup -->
<!-- RuleGroup ID 3 : NETWORK CONNECTION INITIATED [NetworkInterface] -->
<!-- COMMENT: By default this configuration takes a very conserva- -->
<!-- tive approach | https://attack.mitre.org/wiki/Command_and_Control -->
<!-- TECHNICAL: For the DestinationPortName, Sysmon uses the GetThrea- -->
<!-- dNetworkPortName function. These are do not initiate their connections, and the -->
<!-- DATA: srcfile, processid, processlist, Image, User, Protocol, -->
<!-- Group name="groupRelation" or>
<!-- GroupCondition match="Include" -->
<!-- Condition: connecting binaries -->
<!-- Image name="Usermode" condition="begin with <c>C:\Users</c>/Image> -->
<!-- Image name="Caution" condition="begin with <c>C:\Windows\Temp</c>/Image> -->
<!-- Image condition="begin with <c>C:\ProgramData</c>/Image> -->
<!-- Normally, network communication should be sourced from IP -->
<!-- Image condition="begin with <c>C:\Windows\Temp</c>/Image> -->
<!-- Image condition="begin with <c>C:\Windows\System</c>/Image> -->
<!-- Image name="Caution" condition="begin with <c>C:\Windows\System</c>/Image> -->
<!-- Image name="Caution" condition="begin with <c>C:\Windows\System32</c>/Image> -->
<!-- Credit: https://www.bl4ck-f4ce.com/2019/07/04/ -->
<!-- Image condition="begin with <c>C:\Windows\Fonts</c>/Image> -->
<!-- Image name="Caution" condition="begin with <c>C:\Windows\Fonts</c>/Image> -->
<!-- Image condition="image">at.exe</Image>

```

```

Administrator Windows PowerShell
PS C:\> cd tools
PS C:\tools> ls
Directory: C:\tools
Mode LastWriteTime Length Name
---- -- - - - -
d----- 2/3/2026 10:04 AM ----- Sysmon

```

Ran:

```
#powershell
```

```
C:\Tools\Sysmon\Sysmon64.exe -accepteula -i
```

```
C:\Tools\Sysmon\sysmonconfig-export.xml
```

[screenshot

Administrator Windows PowerShell

```

PS C:\tools\sysmon> ls
Directory: C:\tools\sysmon
Mode LastWriteTime Length Name
---- -- - - - -
d----- 2/3/2026 9:57 AM ----- Sysmon
-a---- 2/3/2026 9:57 AM 7409 eula.txt
-a---- 2/3/2026 9:57 AM 8480568 Sysmon.exe
-r----- 2/3/2026 9:57 AM 4583248 Sysmon64.exe
-a---- 2/3/2026 9:57 AM 4993448 Sysmon64.exe
-a---- 2/3/2026 9:57 AM 123257 sysmonconfig-export.xml

```

```

PS C:\tools\sysmon> .\sysmon64.exe accepteula -i sysmonconfig-export.xml
System Monitor v5.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.98
Config file validation completed.
Sysmon64 installed.
Starting Sysmon...
Sysmon64 started.
Starting Sysmon64...
Sysmon64 started.
PS C:\tools\sysmon> .\sysmon64.exe status

```

System Monitor v5.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Usage:
Install: Sysmon64.exe -i [<configfile>]
Update configuration: Sysmon64.exe -c [<configfile>]
Install manifest: Sysmon64.exe -m [<manifestfile>]
Print schema: Sysmon64.exe -s
Uninstall: Sysmon64.exe -u [force]
--> Update configuration or an installed Sysmon driver or dump the current configuration if no other argument is provided. Optionally

Microsoft Sysmon Logging - Dev

Services

Name	Description	Status	Startup Type	Log On As
SysMain	System Monitor service	Running	Automatic	Local System
Sysmon64	System Event Notification Service	Running	Automatic	Local System
System Events Broker		Running	Automatic (Delayed Start)	Local System
Task Scheduler		Running	Automatic	Local System
TCP/IP NetBIOS Helper		Running	Automatic (Delayed Start)	Local Service
Telnetd		Disabled	Manual (Delayed Start)	Network

Event Viewer

Operational

Level	Data and Time	Source	Event ID	Task Category
Information	2/3/2026 10:19:32 AM	Sysmon	1	Process Create (rule ProcessCreate)
Information	2/3/2026 10:19:32 AM	Sysmon	1	Process Create (rule ProcessCreate)
Information	2/3/2026 10:19:32 AM	Sysmon	5	Process terminated (rule ProcessTerminate)
Information	2/3/2026 10:19:32 AM	Sysmon	5	Process terminated (rule ProcessTerminate)
Information	2/3/2026 10:19:32 AM	Sysmon	1	Process Create (rule ProcessCreate)
Information	2/3/2026 10:19:32 AM	Sysmon	1	Process Create (rule ProcessCreate)
Information	2/3/2026 10:19:32 AM	Sysmon	5	Process terminated (rule ProcessTerminate)
Information	2/3/2026 10:19:32 AM	Sysmon	5	Process terminated (rule ProcessTerminate)
Information	2/3/2026 10:19:32 AM	Sysmon	1	Process Create (rule ProcessCreate)
Information	2/3/2026 10:19:32 AM	Sysmon	1	Process Create (rule ProcessCreate)
Information	2/3/2026 10:19:32 AM	Sysmon	5	Process terminated (rule ProcessTerminate)
Information	2/3/2026 10:19:32 AM	Sysmon	5	Process terminated (rule ProcessTerminate)

Check event log:

```
#powershell
```

```
Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational -MaxEvents 40
```

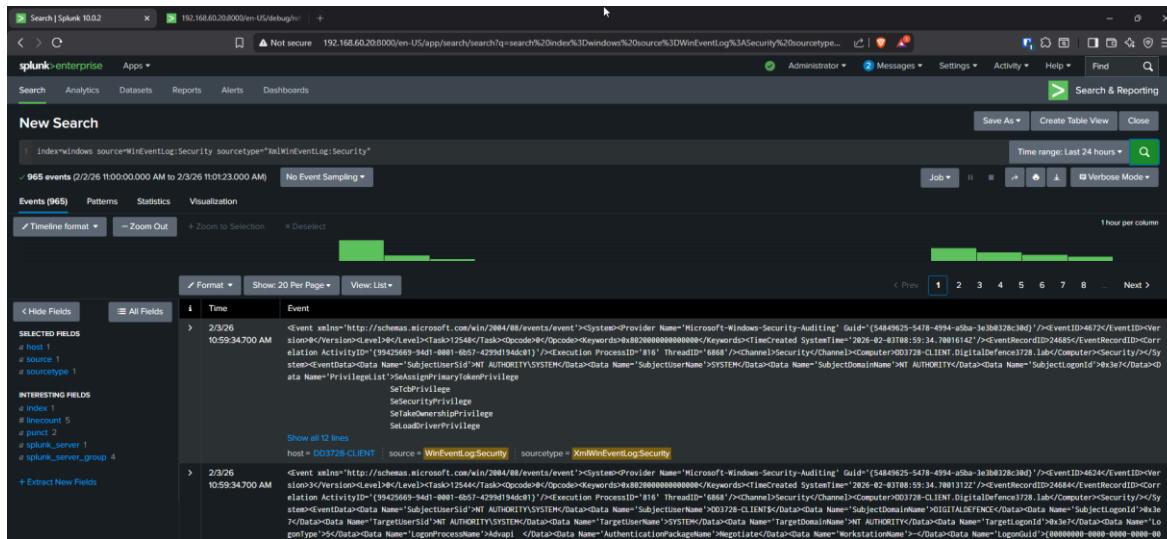
[screenshot]

F. Validate ingestion in Splunk

In Splunk Web:

index=windows sourcetype=WinEventLog:Security

[screenshot]



10 — Kali & Metasploitable2: controlled usage

- Kept Kali and Metasploitable2 on the 192.168.60.0/24 LAN and powered off when not testing.
 - Use Kali for port scanning (nmap), web testing, and limited Metasploit modules to validate detections.

- Metasploitable2 is the intentionally vulnerable Linux target for safe exploitation exercises.

Kali static IP (Network Manager):

```
#bash
```

```
nmcli con mod "Wired connection 1" ipv4.addresses 192.168.60.40/24
ipv4.gateway 192.168.60.1 ipv4.dns 192.168.60.10 ipv4.method
manual
nmcli con up "Wired connection 1"
```

[screenshot  ]



```
(kali㉿kali)-[~/Desktop]
└─# bash
nmcli con mod "Wired connection 1" ipv4.addresses 192.168.60.40/24
ipv4.gateway 192.168.60.1 ipv4.dns 192.168.60.10 ipv4.method
manual
nmcli con up "Wired connection 1"

(kali㉿kali)-[~/Desktop]
└─# ip addr
1: lo <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.255.255.255 scope host loopback
            valid_lft forever preferred_lft forever
            inet 169.254.1.1/16 brd 169.254.255.255 scope global noprefixroute eth0
                link/ether 00:0c:29:b9:05:c1 brd ff:ff:ff:ff:ff:ff
                inet 192.168.60.40/24 brd 192.168.60.255 scope global noprefixroute eth0
                    valid_lft forever preferred_lft forever
                    inet 192.168.60.40/24 brd 192.168.60.255 scope link noprefixroute
                        valid_lft forever preferred_lft forever
(kali㉿kali)-[~/Desktop]
```

Metasploitable2 typically uses DHCP; ensured it gets a 192.168.60.x address from pfSense.

11 — Troubleshooting Log (Chronological Order)

SRV Lookup / DNS Failure on Domain Controller (DC) Symptom

- nslookup _ldap._tcp.dc._msdcs.digitaldefence3728.lab (a command to query DNS for server records) returned "Server Unknown; Address: 127.0.0.1" with no response.

Root Cause:

- The Domain Controller (DC—a server managing Active Directory logins and authentication) was renamed after setup, leaving outdated records for the old hostname in DNS (Domain Name System—the internet's phonebook for translating names to IP addresses).

Fix:

- Old A (hostname-to-IP) and PTR (IP-to-hostname) records were deleted; correct A record for "dd3728-dc" was created; ipconfig /registerdns was run to refresh; Netlogon service was restarted; nltest /dsregdns and dcdiag /test:dns (Domain Controller diagnostic tool) were run until all passed.

Set-NetConnectionProfile Refusing Domain Authenticated

Symptom:

- Windows refused to set the network profile to DomainAuthenticated (a secure Windows network type for domain-joined machines).

Explanation:

- Windows only switched to DomainAuthenticated after DNS and Kerberos (a secure authentication protocol) worked properly; Private profile was used as a temporary fix while Active Directory (AD—a Microsoft directory service for user/device management) DNS issues were resolved.

Ubuntu DNS Using 127.0.0.53 and NXDOMAIN/SERVFAIL

Symptom:

- nslookup showed 127.0.0.53 (Ubuntu's local stub resolver—a lightweight DNS forwarder) as the resolver; internal domain names failed with NXDOMAIN (domain does not exist) or SERVFAIL (server failure) errors.

Root Causes:

- Conflicting Netplan files (Ubuntu's network config tool)—like 50-cloud-init.yaml overriding 00-installer-config.yaml; wrong file permissions; or incorrect subnet (IP network range).

Fix:

- Cloud-init networking was disabled; 50-cloud-init.yaml was deleted; correct IP 192.168.60.20/24 (subnet mask for network range) and nameserver 192.168.60.10 were set in Netplan; secure permissions were applied; netplan generate and netplan apply were run; systemd-resolved (Ubuntu's DNS resolver service) was restarted; validation was done with resolvectl and nslookup.

Wrong Subnet Symptom:

Symptom:

- Security Information and Event Management (SIEM—a tool for monitoring security alerts) was wrongly placed in 192.168.60.0/24 or previously set to 192.168.37.0/24, blocking reach to the DC.

Fix:

- Netplan was updated to 192.168.60.0/24 subnet and re-applied to restore network connectivity.

RDP / Firewall / Profile Mismatches

Symptom:

- Remote Desktop Protocol (RDP—a remote access tool) connection failed until firewall rules and network profiles were fixed.

Fix:

- Remote Desktop firewall group was enabled; network profile was temporarily set to Private; AD DNS health was confirmed, so it switched to DomainAuthenticated.

12 — Verification & validation commands

Windows DC:

```
#powershell
dcdiag /v
nltest /dsregdns
ipconfig /registerdns
ipconfig /all
nslookup dd3728-dc.digitaldefence3728.lab
```

Ubuntu SIEM:

```
#bash
ip a
ip route
resolvectl status
nslookup dd3728-dc.digitaldefence3728.lab
sudo systemctl status splunk
tail -f /opt/splunk/var/log/splunk/splunkd.log
```

Splunk searches:

```
index=endpoint EventCode=1 | sort - _time | head 50
index=network sourcetype=pfsense | head 50
index=windows EventCode=4625 | stats count by Account_Name,
```

```
ComputerName | where count > 3
```

13 — Why the Domain Controller is Authoritative DNS

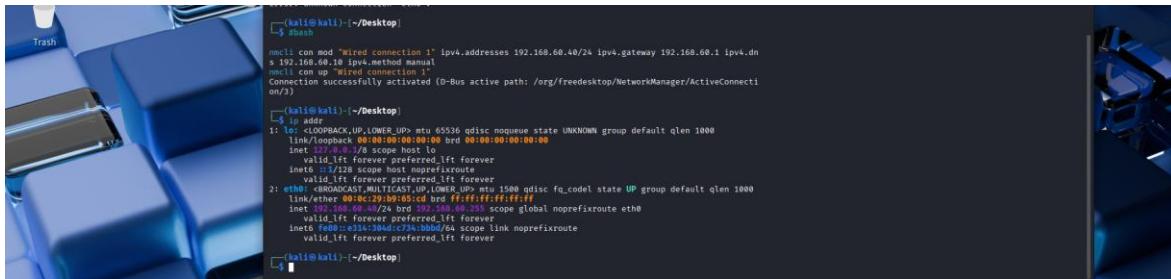
- In Active Directory (AD) environments, Domain Name System (DNS) is the main way clients discover services. Service (SRV) records, Address (A) records, and Pointer (PTR) records help clients locate Lightweight Directory Access Protocol (LDAP), Kerberos authentication, and Global Catalog services.
- These records must live in an AD-integrated DNS zone on Domain Controllers (DCs) to enable secure dynamic updates and proper Group Policy Object (GPO) behavior.
- The Domain Controller at 192.168.60.10 runs DNS and is authoritative for digitaldefence3728.lab.
- PfSense acts as the gateway, Network Address Translation (NAT) device, and optional Dynamic Host Configuration Protocol (DHCP) server—but it does not replace AD DNS.

14 — Kali / Metasploitable: Network Setup

```
#bash
```

```
# Kali static via NetworkManager
nmcli con mod "Wired connection 1" ipv4.addresses 192.168.60.40/24
ipv4.gateway 192.168.60.1 ipv4.dns 192.168.60.10 ipv4.method
manual
nmcli con up "Wired connection 1"
```

[screenshot  ]



```
# Metasploitable set DNS
sudo sh -c 'echo "nameserver 192.168.60.10" > /etc/resolv.conf'
```

[Screenshot  ]

```
default via 192.168.60.1 dev eth0 metric 100
msfadmin@metasploitable:/etc$ sudo sh -c 'echo "nameserver 192.168.60.10" > /etc/resolv.conf'
msfadmin@metasploitable:/etc$ ip route
192.168.60.0/24 dev eth0 proto kernel scope link src 192.168.60.100
default via 192.168.60.1 dev eth0 metric 100
msfadmin@metasploitable:/etc$ cat resolv.conf'
> cat resolv.conf
>
msfadmin@metasploitable:/etc$ cat resolv.conf
nameserver 192.168.60.10
msfadmin@metasploitable:/etc$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:15:27:11 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.100/24 brd 192.168.60.255 scope global eth0
        inet6 fe80::20c:29ff:fe15:2711/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:15:27:1b brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:/etc$
```