BlueOak Financial LLC

Create Hybrid Enterprise Network and Cybersecurity Integration

Report Created by Taralkumar Patel

Date: 03-22-2025

Executive Summary

This project established a secure enterprise network infrastructure, integrating on-premises resources with cloud technologies to achieve centralized management and enhanced cybersecurity. Starting with the deployment of a domain controller and automated user management via PowerShell, the network was expanded to include Azure Active Directory for hybrid identity management.

Security policies were enforced through both on-premises and cloud tools, while Microsoft Intune and Defender for Endpoint ensured device compliance and robust threat protection. The project also laid the groundwork for future enhancements, including advanced log analysis, Microsoft Sentinel for proactive threat detection, AI-driven automation, Zero Trust architecture, and SOAR solutions for automated workflows.

This initiative successfully delivered a scalable, hybrid network aligned with modern security and operational needs.

Introduction

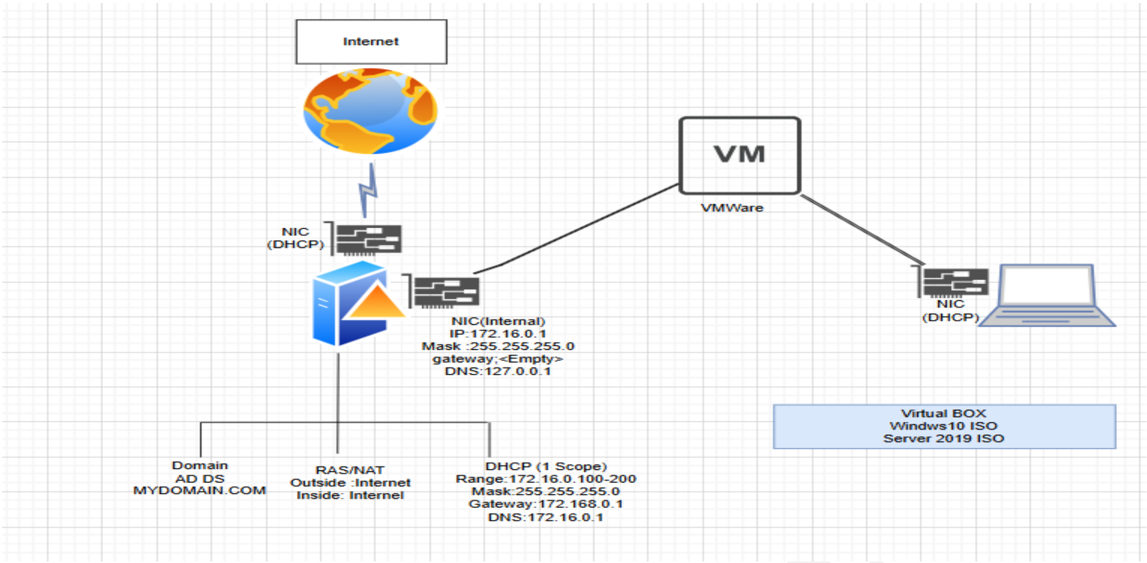
Background: This project was undertaken to address the growing need for a secure, scalable, and centralized network infrastructure to support the organization’s operational goals. With an increasing reliance on cloud technologies and the need for robust cybersecurity, the project aimed to modernize and unify on-premises and cloud environments. while preparing for future innovations like Zero Trust architecture and AI-driven automation. It ensured the infrastructure could meet evolving business and cybersecurity demands.

Objectives:

- Build an enterprise network with a domain controller.
- Automate user management using PowerShell.
- Integrate with Azure AD for centralized management.
- Deploy VMs, VLANs and NSGs on Azure Environment.
- Enforce security policies and onboard devices to Intune and Defender.
- Lay the foundation for advanced cybersecurity solutions like Sentinel and SOAR.

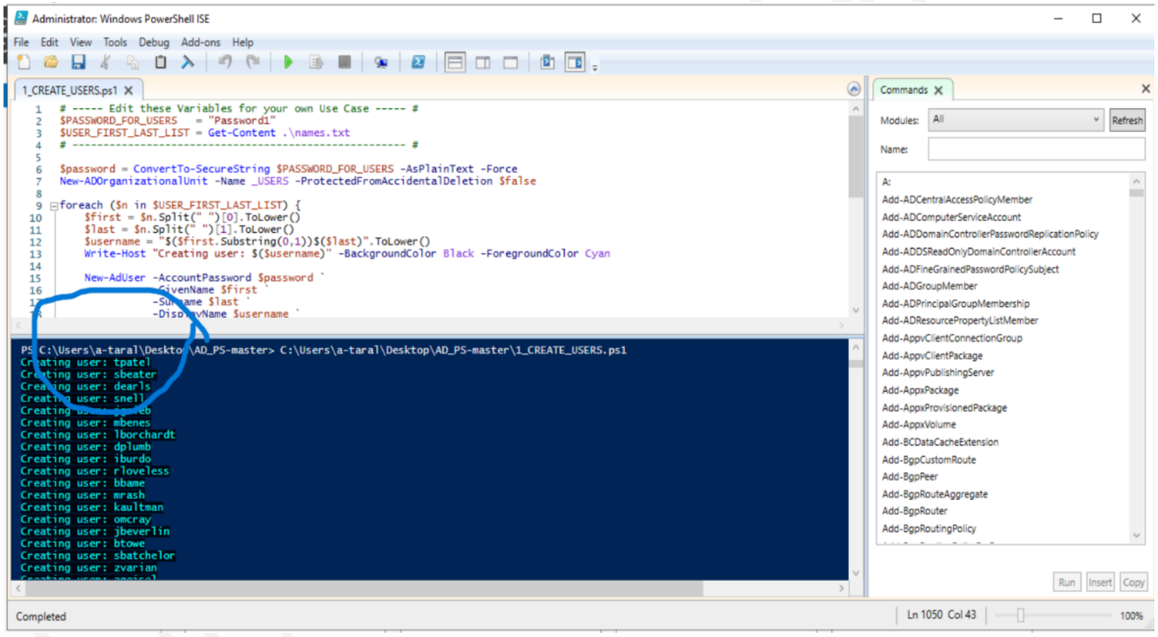
Configuration

- **Domain Controller and windows 10 Setup (On-Premises):**



- Downloaded Oracle Virtual BOX and Windows 10 ISO image and server 2019 ISO image from oracle and Microsoft website.
- Configured Windows Server 2019 and Windows 10 in VirtualBox, ensuring the virtual machine settings were optimized based on Above given diagram, Network adapter, the hardware capabilities of my host PC. This included adjusting the allocated memory, CPU cores, and storage space to balance performance and system stability.
- In Windows server check internet adapter Configured internal adapter.
    - Clicked on change adapter Option in settings > Network & Internet > Ethernet
    - Right Clicked on Internal adapter Properties > TCP/ IPv4 > General > use following Ip address > followed diagram > DNS server address – Loopback address
- Created Domain/ AD DS.
    - Go to server manager > add role and features > Server selection > Server Roles – Active Directory Domain Services > Install
    - Post deployment configuration Clicked yellow flag besides manage > Add Forest > Root domain name >provided optional password > Install - restarted the server.
- Created own dedicated admin account.
    - Start > Active Directory Users and Computers > clicked mydomain.com > New > Organizational Unit > Name OU- clicked on it > created new user with logon name and password – Uncheck password never expires > Finish.
    - Right clicked created User in OU > Member of > add > Enter object name and checked names > apply. Sign out and check if successful. Log in with Dedicated admin account.
- Install RAS/NAT to allow windows 10 client to access internet through Domain controller.
    - Add roles and features > Select server > Server Roles > Remote access > Role services > Routing > Add features > Install > Close

  - Tools > Routing and remote access > click DC (Local) > configure and enable > NAT > Select use public Interface to connect to internet > Finish
- Configure DHCP
  - Add roles and features > Select server > Server Roles > DHCP > Install > Close
  - Tools > DHCP > Click IPv4 > New Scope > Followed diagram to assign IP address Range > Lease duration > Config DHCP Options > Entered DC Ip address for default gateway > Activate Scope > Finish.
  - Right clicked DHCP Server to Authorize > refresh. Check IpV4 and IPv6 turned green. Note: Turned Off IE enhance Security configuration to browse internet from server
- Created 1000+ random users using PowerShell script with Random and my name tpatel.
  - Open PowerShell as administrator > Opened PowerShell script > set -Executionpolicy unrestricted > Run the script with navigating to script directory

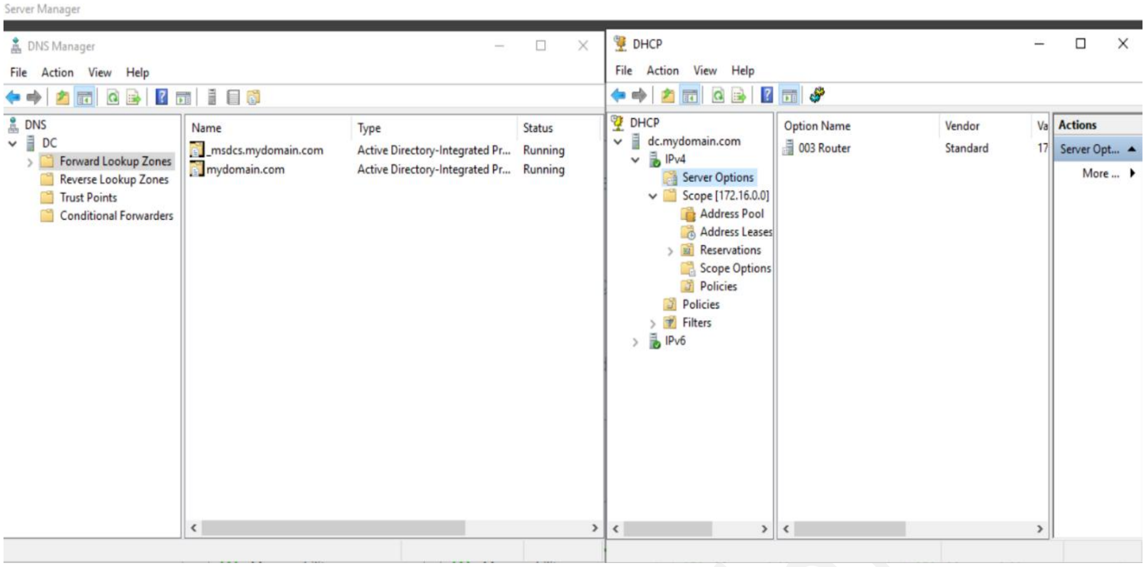

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
1_CREATE_USERS.ps1
Commands
Modules: All
Refresh
Name:
A:
Add-ADCentralAccessPolicyMember
Add-ADComputerServiceAccount
Add-ADDomainControllerPasswordReplicationPolicy
Add-ADDSReadOnlyDomainControllerAccount
Add-ADFineGrainedPasswordPolicySubject
Add-ADGroupMember
Add-ADPrincipalGroupMembership
Add-ADResourcePropertyListMember
Add-AppvClientConnectionGroup
Add-AppvClientPackage
Add-AppvPublishingServer
Add-AppxPackage
Add-AppxProvisionedPackage
Add-AppxVolume
Add-BCDataCacheExtension
Add-BgpCustomRoute
Add-BgpPeer
Add-BgpRouteAggregate
Add-BgpRouter
Add-BgpRoutingPolicy
Run
Insert
Copy
Completed
Ln 1050 Col 43
100%

```
# ----- Edit these Variables for your own Use Case ----- #
$PASSWORD_FOR_USERS   = "Password1"
$USER_FIRST_LAST_LIST = Get-Content .\names.txt
# ------------------------------------------------------ #

$password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false

foreach ($n in $USER_FIRST_LAST_LIST) {
    $first = $n.Split(" ")[0].ToLower()
    $last = $n.Split(" ")[1].ToLower()
    $username = "$($first.Substring(0,1))$($last)".ToLower()
    Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan

    New-AdUser -AccountPassword $password `
               -GivenName $first `
               -Surname $last `
               -DisplayName $username `
```

```
PS C:\Users\a-taral\Desktop\AD_PS-master> C:\Users\a-taral\Desktop\AD_PS-master\1_CREATE_USERS.ps1
Creating user: tpatel
Creating user: sbeater
Creating user: dearls
Creating user: snell
Creating user: [illegible]
Creating user: mbenes
Creating user: lborchardt
Creating user: dplumb
Creating user: iburdo
Creating user: rloveless
Creating user: bbame
Creating user: mrash
Creating user: kaultman
Creating user: omcray
Creating user: jbeverlin
Creating user: btowe
Creating user: sbatchelor
Creating user: zvarian
```

  - Checked the created Users in Active Directory Users and Computers > Users

- Tried to ping windows 10 client from DC and did not see the default gateway – Time to troubleshoot.
  - Logged in to DC – checked the lease, Checked the IPv4 server option which was not configured. Right clicked on IPv4 server Options > Selected 003 Router > Added DC IP address > Apply > Restarted Server options.



Name	Type	Status
_msdcs.mydomain.com	Active Directory-Integrated Pr...	Running
mydomain.com	Active Directory-Integrated Pr...	Running

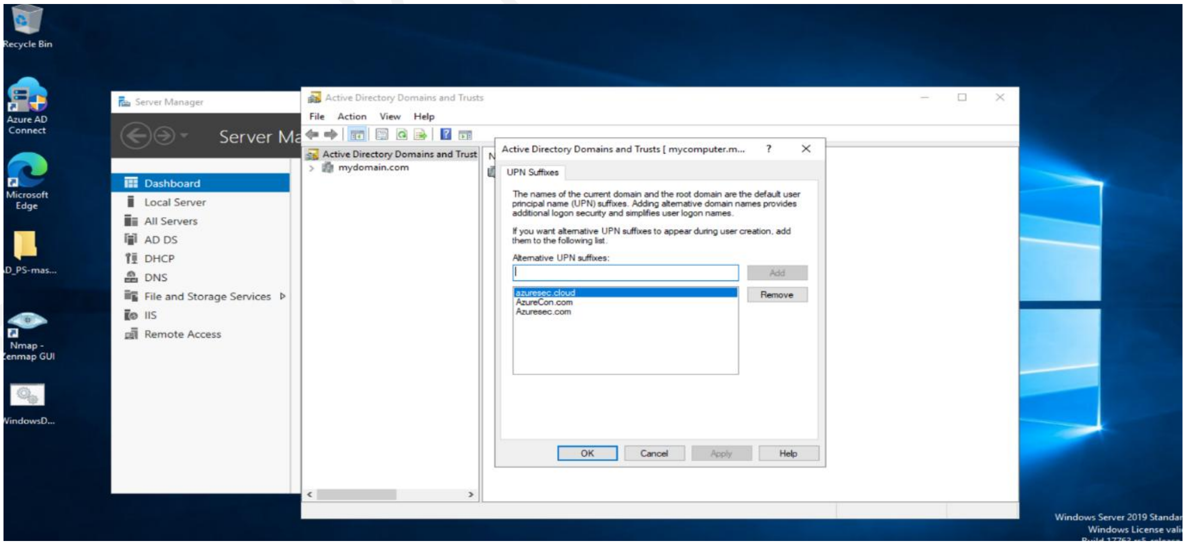
Option Name	Vendor	Va
003 Router	Standard	17

- On windows client Run CMD as Administrator tried the ping to server, Google.com and checked the Connectivity – Result was successful.

- **Azure AD Integration**

  - Setup steps for Azure AD Connect.

    - On DC go to tools > Active directory Domain and trust > DC properties > Add UPN Suffixes (Domian) > Apply > OK.
    - Go to Active directory Users and Computers > User > properties > Account > Change the extension of user logon name > azuresec. cloud > Apply.



The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.

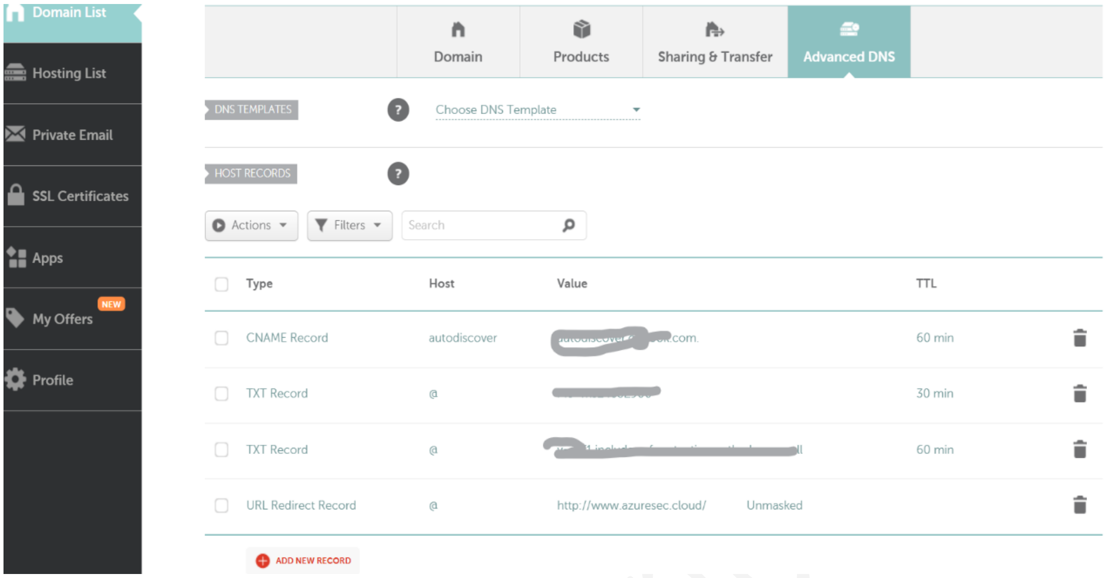
If you want alternative UPN suffixes to appear during user creation, add them to the following list.

Alternative UPN suffixes:

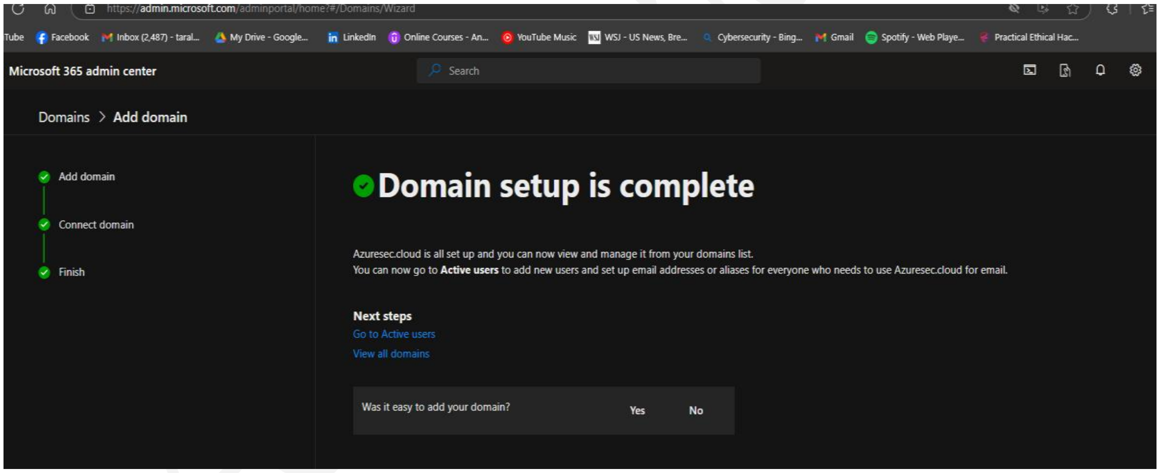
azuresec.cloud
AzureCon.com
Azuresec.com

  - Synchronizing on-premises resources with Azure AD Connect.

    - In Microsoft 365 admin centre go to settings > Domain > Add Domain > Entered UPN Domain from server (Note: Owned the domain from any sites like Namecheap, go daddy etc.) > Verified My own domain by adding some DNS records > Continue.



Type	Host	Value		TTL
CNAME Record	autodiscover	[redacted].com.		60 min
TXT Record	@	[redacted]		30 min
TXT Record	@	[redacted]		60 min
URL Redirect Record	@	http://www.azuresec.cloud/	Unmasked	



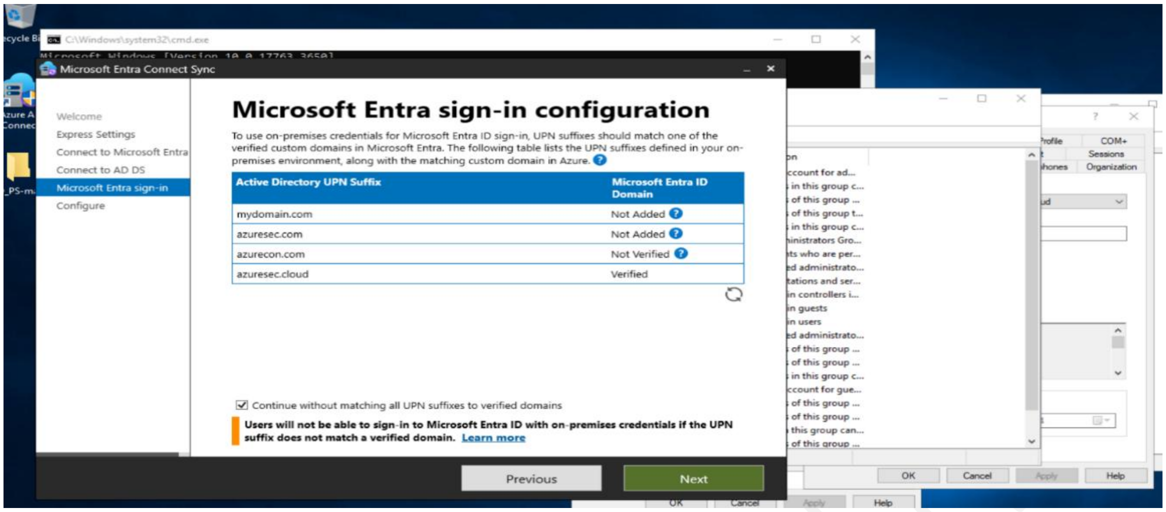
Domain setup is complete

Azuresec.cloud is all set up and you can now view and manage it from your domains list.
You can now go to **Active users** to add new users and set up email addresses or aliases for everyone who needs to use Azuresec.cloud for email.

Next steps
Go to Active users
View all domains

Was it easy to add your domain? Yes No

- Downloaded Azure AD connect on DC > Open it > Use Express settings > Enter Administrator credentials > Verify added domains > Next > install. (Note: System will create a default Azure AD connect service account)



Microsoft Entra sign-in configuration

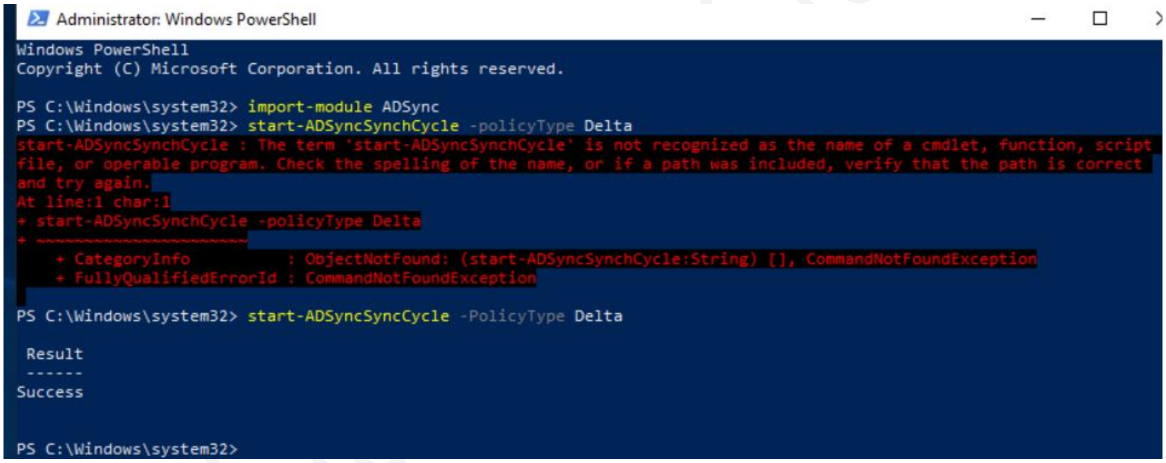
To use on-premises credentials for Microsoft Entra ID sign-in, UPN suffixes should match one of the verified custom domains in Microsoft Entra. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure.

Active Directory UPN Suffix	Microsoft Entra ID Domain
mydomain.com	Not Added
azuresec.com	Not Added
azurecon.com	Not Verified
azuresec.cloud	Verified

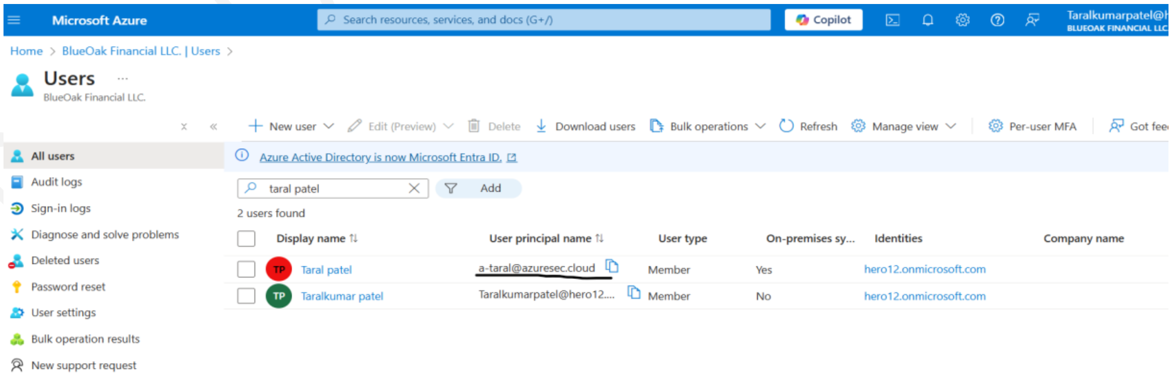
☑ Continue without matching all UPN suffixes to verified domains

Users will not be able to sign-in to Microsoft Entra ID with on-premises credentials if the UPN suffix does not match a verified domain. Learn more

- Open PowerShell administrator > Import -Module Ad Sync > Start -ADSyncSyncCycle -policyType Delta > verified all users Sync from DC to Azure Entra ID.



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

PS C:\Windows\system32> import-module ADSync
PS C:\Windows\system32> start-ADSyncSynchCycle -policyType Delta
start-ADSyncSynchCycle : The term 'start-ADSyncSynchCycle' is not recognized as the name of a cmdlet, function, script
file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct
and try again.
At line:1 char:1
+ start-ADSyncSynchCycle -policyType Delta
+ ~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (start-ADSyncSynchCycle:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Windows\system32> start-ADSyncSyncCycle -PolicyType Delta

 Result
 ------
Success


PS C:\Windows\system32>
```

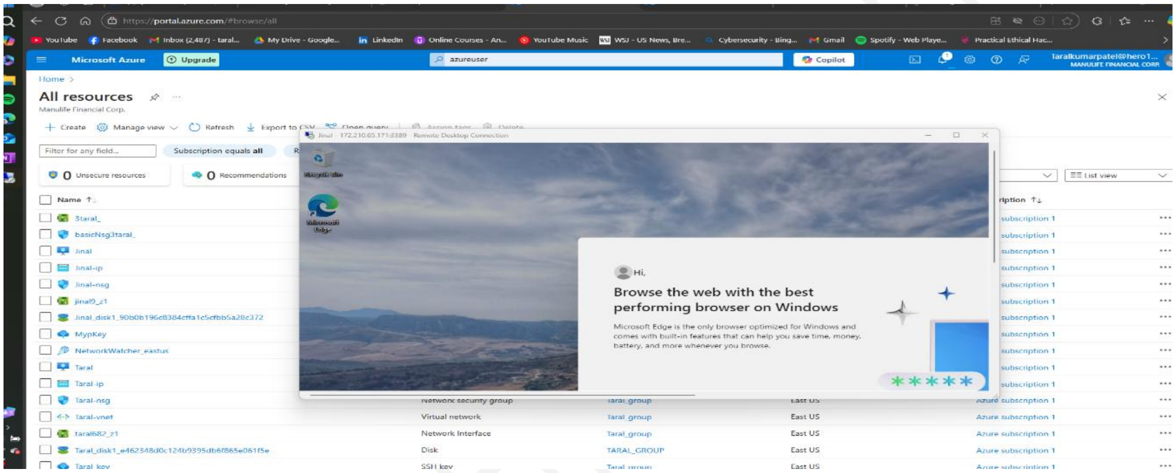


taral patel

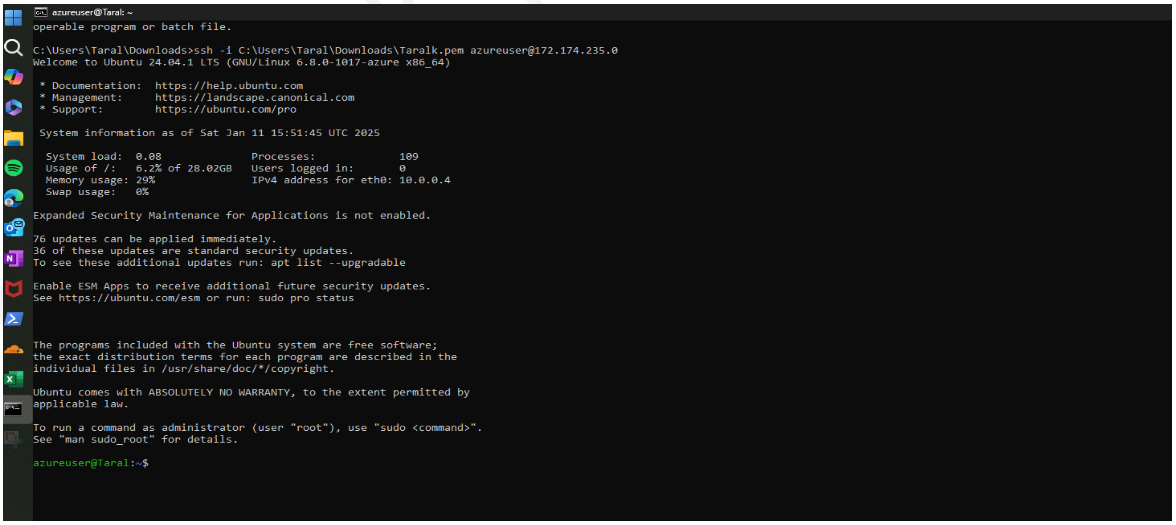
2 users found

Display name	User principal name	User type	On-premises sy...	Identities	Company name
TP Taral patel	a-taral@azuresec.cloud	Member	Yes	hero12.onmicrosoft.com	
TP Taralkumar patel	Taralkumarpatel@hero12....	Member	No	hero12.onmicrosoft.com	

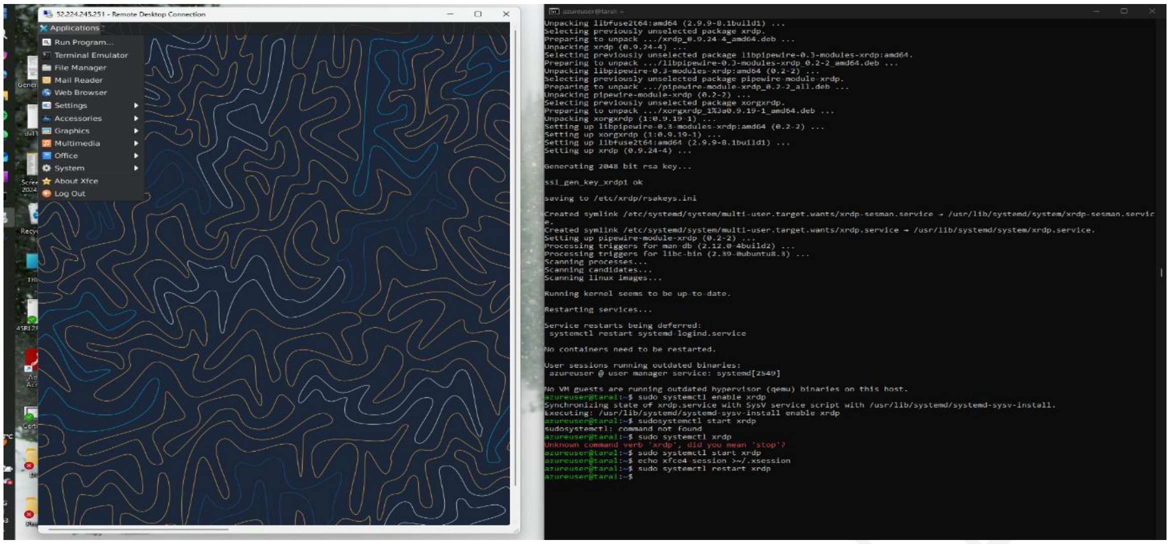
- **Utilizing Azure to Create Resources and Onboard devices:**
    - Deployed VM, V- nets and Network security groups. Deploying windows VMs and Linux VMs are different using connector.
    - Azure portal > Create Resource Group and subscription
    - Go to Virtual Machines > Create > Subscription > Resource group > VM name > Region > Choose Image > Size > Authentication type > Inbound Port rules (For RDP and SSH).
    - Configure Disk > Set up networking – monitoring. Can access the VM.
    - I have created Windows 10, Linux (Ubuntu based)



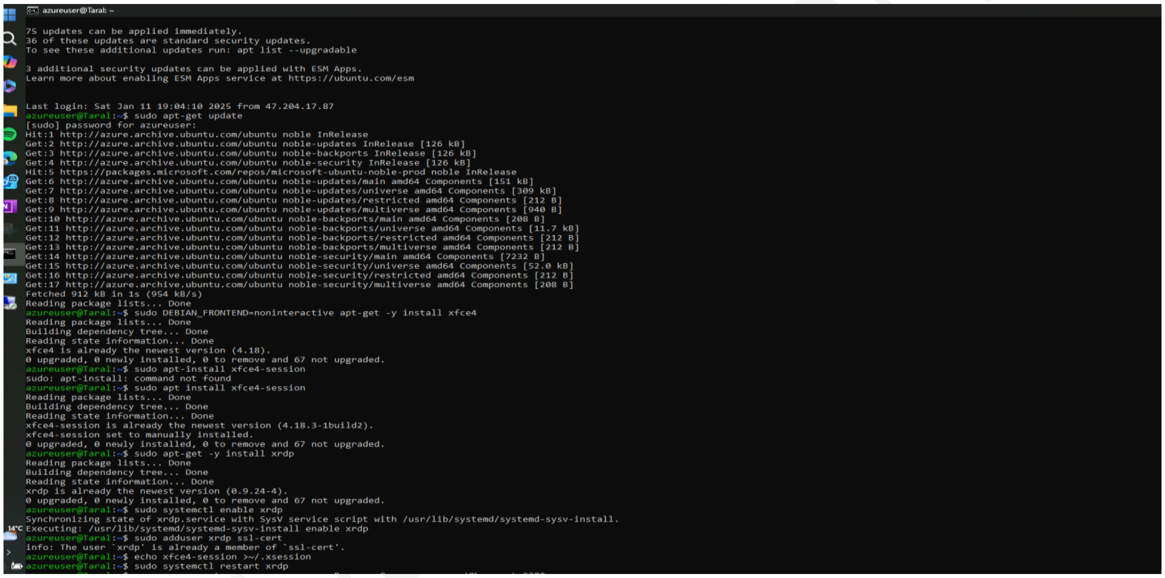
Name ↑↓				ription ↑↓
3taral_				subscription 1
basicNsg3taral_				subscription 1
Jinal				subscription 1
Jinal-ip				subscription 1
Jinal-nsg				subscription 1
jinal9_z1				subscription 1
Jinal_disk1_90b0b196c8384cffa1c5cfbb5a28c372				subscription 1
MypKey				subscription 1
NetworkWatcher_eastus				subscription 1
Taral				subscription 1
Taral-ip				subscription 1
Taral-nsg	Network security group	Taral_group	East US	Azure subscription 1
Taral-vnet	Virtual network	Taral_group	East US	Azure subscription 1
taral682_z1	Network Interface	Taral_group	East US	Azure subscription 1
Taral_disk1_e462348d0c124b9395db6f865e061f5e	Disk	TARAL_GROUP	East US	Azure subscription 1
Taral_key	SSH key	Taral_group	East US	Azure subscription 1



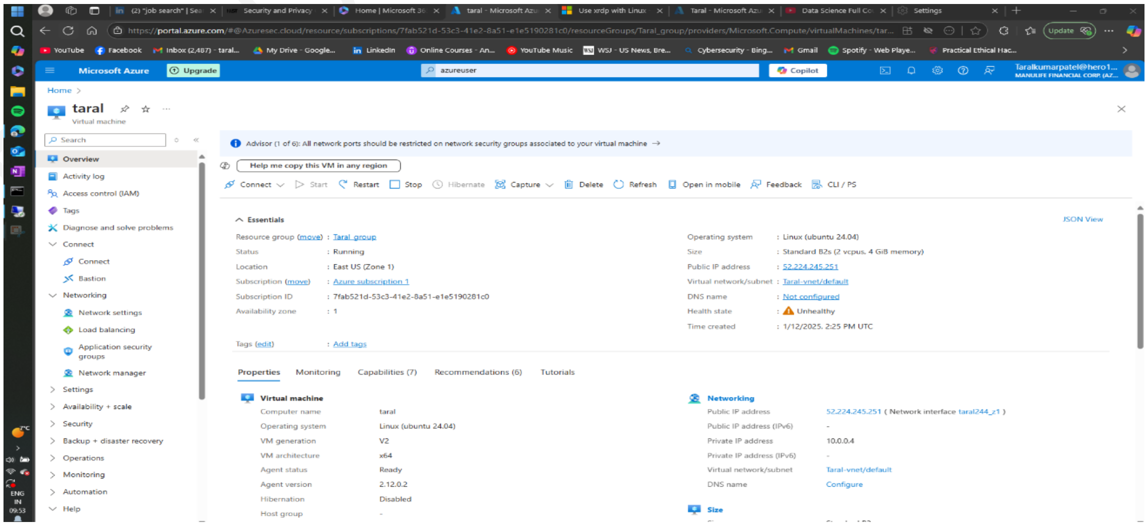
```
operable program or batch file.

C:\Users\Taral\Downloads>ssh -i C:\Users\Taral\Downloads\Taralk.pem azureuser@172.174.235.0
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1017-azure x86_64)

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

 System information as of Sat Jan 11 15:51:45 UTC 2025

  System load:  0.08              Processes:             109
  Usage of /:   6.2% of 28.02GB   Users logged in:       0
  Memory usage: 29%               IPv4 address for eth0: 10.0.0.4
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

76 updates can be applied immediately.
36 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


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/*/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.

azureuser@Taral:~$
```



```
Unpacking libfuse2t64:amd64 (2.9.9-8.1build1) ...
Selecting previously unselected package xrdp.
Preparing to unpack .../xrdp_0.9.24-4_amd64.deb ...
Unpacking xrdp (0.9.24-4) ...
Selecting previously unselected package libpipewire-0.3-modules-xrdp:amd64.
Preparing to unpack .../libpipewire-0.3-modules-xrdp_0.2-2_amd64.deb ...
Unpacking libpipewire-0.3-modules-xrdp:amd64 (0.2-2) ...
Selecting previously unselected package pipewire-module-xrdp.
Preparing to unpack .../pipewire-module-xrdp_0.2-2_all.deb ...
Unpacking pipewire-module-xrdp (0.2-2) ...
Selecting previously unselected package xorgxrdp.
Preparing to unpack .../xorgxrdp_1%3a0.9.19-1_amd64.deb ...
Unpacking xorgxrdp (1:0.9.19-1) ...
Setting up libpipewire-0.3-modules-xrdp:amd64 (0.2-2) ...
Setting up xorgxrdp (1:0.9.19-1) ...
Setting up libfuse2t64:amd64 (2.9.9-8.1build1) ...
Setting up xrdp (0.9.24-4) ...

Generating 2048 bit rsa key...

ssl_gen_key_xrdp1 ok

saving to /etc/xrdp/rsakeys.ini

Created symlink /etc/systemd/system/multi-user.target.wants/xrdp-sesman.service → /usr/lib/systemd/system/xrdp-sesman.servic
e.
Created symlink /etc/systemd/system/multi-user.target.wants/xrdp.service → /usr/lib/systemd/system/xrdp.service.
Setting up pipewire-module-xrdp (0.2-2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...

Service restarts being deferred:
 systemctl restart systemd-logind.service

No containers need to be restarted.

User sessions running outdated binaries:
 azureuser @ user manager service: systemd[2549]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
azureuser@taral:~$ sudo systemctl enable xrdp
Synchronizing state of xrdp.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable xrdp
azureuser@taral:~$ sudosystemctl start xrdp
sudosystemctl: command not found
azureuser@taral:~$ sudo systemctl xrdp
Unknown command verb 'xrdp', did you mean 'stop'?
azureuser@taral:~$ sudo systemctl start xrdp
azureuser@taral:~$ echo xfce4-session >~/.xsession
azureuser@taral:~$ sudo systemctl restart xrdp
azureuser@taral:~$
```



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

3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


Last login: Sat Jan 11 19:04:10 2025 from 47.204.17.87
azureuser@Taral:~$ sudo apt-get update
[sudo] password for azureuser:
Hit:1 http://azure.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:5 https://packages.microsoft.com/repos/microsoft-ubuntu-noble-prod noble InRelease
Get:6 http://azure.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [309 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:9 http://azure.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:10 http://azure.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:11 http://azure.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [11.7 kB]
Get:12 http://azure.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [212 B]
Get:13 http://azure.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:14 http://azure.archive.ubuntu.com/ubuntu noble-security/main amd64 Components [7232 B]
Get:15 http://azure.archive.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.0 kB]
Get:16 http://azure.archive.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:17 http://azure.archive.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Fetched 912 kB in 1s (954 kB/s)
Reading package lists... Done
azureuser@Taral:~$ sudo DEBIAN_FRONTEND=noninteractive apt-get -y install xfce4
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
xfce4 is already the newest version (4.18).
0 upgraded, 0 newly installed, 0 to remove and 67 not upgraded.
azureuser@Taral:~$ sudo apt-install xfce4-session
sudo: apt-install: command not found
azureuser@Taral:~$ sudo apt install xfce4-session
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
xfce4-session is already the newest version (4.18.3-1build2).
xfce4-session set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 67 not upgraded.
azureuser@Taral:~$ sudo apt-get -y install xrdp
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
xrdp is already the newest version (0.9.24-4).
0 upgraded, 0 newly installed, 0 to remove and 67 not upgraded.
azureuser@Taral:~$ sudo systemctl enable xrdp
Synchronizing state of xrdp.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable xrdp
azureuser@Taral:~$ sudo adduser xrdp ssl-cert
info: The user `xrdp' is already a member of `ssl-cert'.
azureuser@Taral:~$ echo xfce4-session >~/.xsession
azureuser@Taral:~$ sudo systemctl restart xrdp
```



taral

Virtual machine

Advisor (1 of 6): All network ports should be restricted on network security groups associated to your virtual machine →

Essentials

Resource group (move) : Taral_group
Status : Running
Location : East US (Zone 1)
Subscription (move) : Azure subscription 1
Subscription ID : 7fab521d-53c3-41e2-8a51-e1e5190281c0
Availability zone : 1

Tags (edit) : Add tags

Operating system : Linux (ubuntu 24.04)
Size : Standard B2s (2 vcpus, 4 GiB memory)
Public IP address : 52.224.245.251
Virtual network/subnet : Taral-vnet/default
DNS name : Not configured
Health state : ⚠ Unhealthy
Time created : 1/12/2025, 2:25 PM UTC

Virtual machine

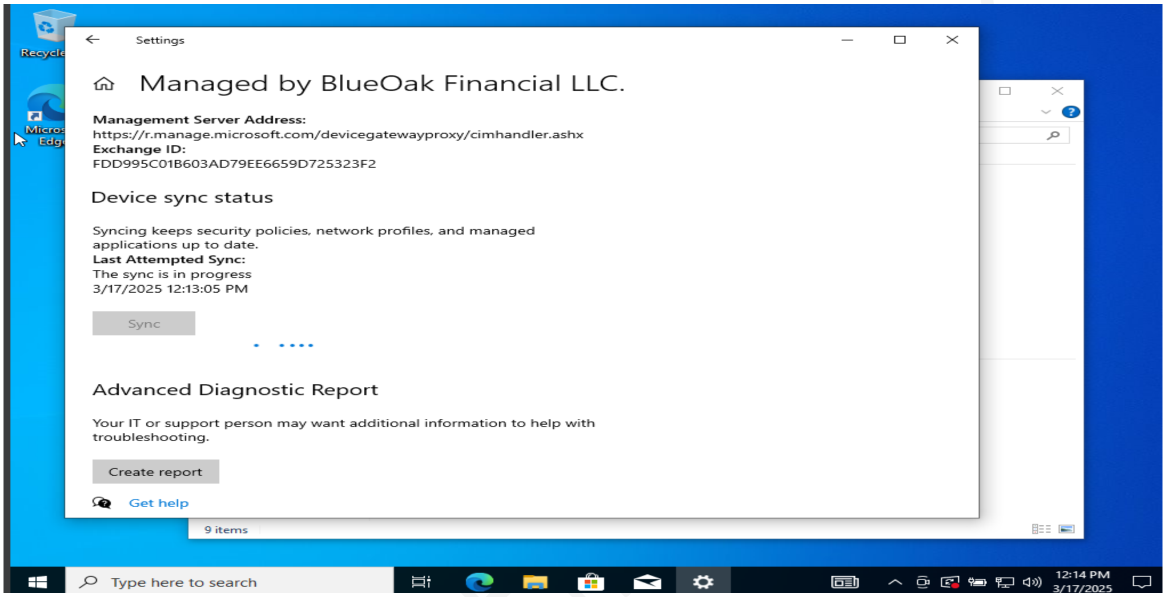
Computer name	taral
Operating system	Linux (ubuntu 24.04)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.12.0.2
Hibernation	Disabled
Host group	-

Networking

Public IP address	52.224.245.251 (Network interface taral244_z1)
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	Taral-vnet/default
DNS name	Configure

Size

- **Intune and defender:**
    - Before Onboarding check that device can be onboarded on Intune or Defender. Deploying this first time Anyone can have different learning experience.
    - Windows 10 or 11 devices can be onboarded on Intune by setting on School or organization email in settings and sync them and with compliance policy.



Managed by BlueOak Financial LLC.

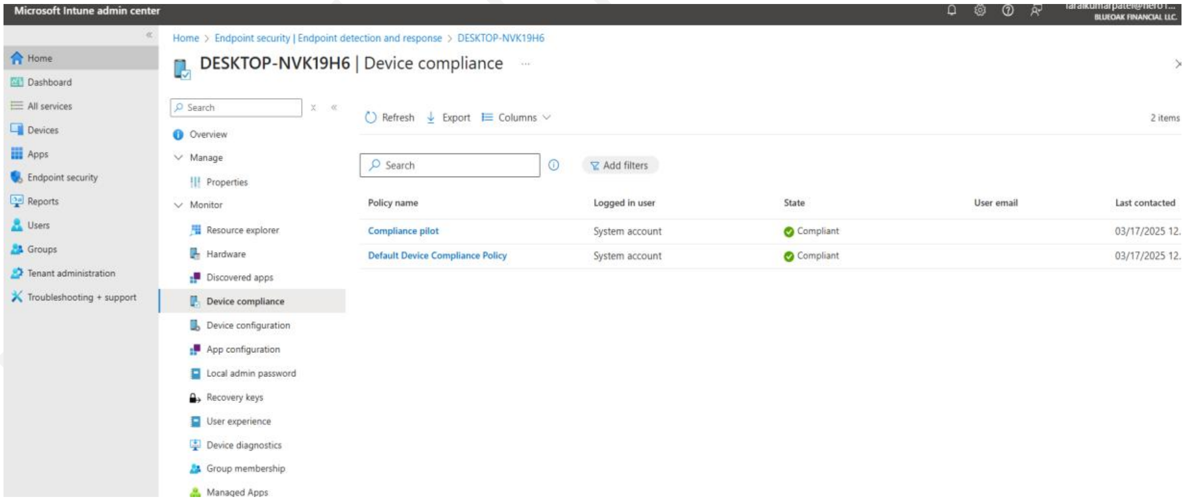
Management Server Address:
https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx
Exchange ID:
FDD995C01B603AD79EE6659D725323F2

Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.
Last Attempted Sync:
The sync is in progress
3/17/2025 12:13:05 PM

Advanced Diagnostic Report

Your IT or support person may want additional information to help with troubleshooting.

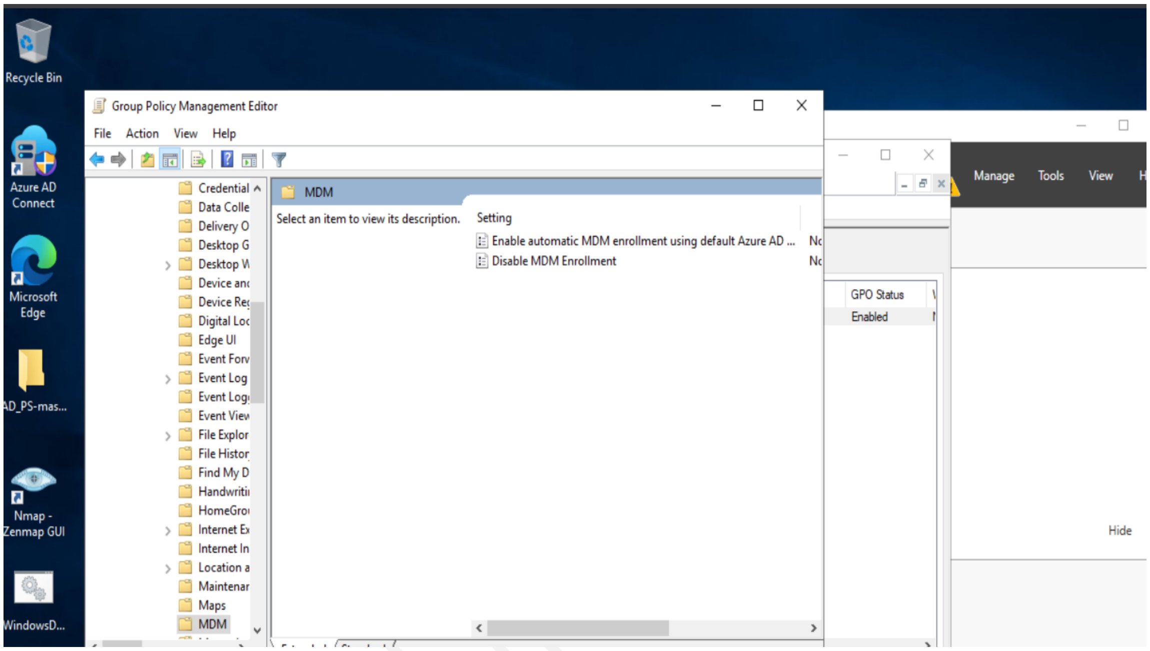


DESKTOP-NVK19H6 | Device compliance

Policy name	Logged in user	State	User email	Last contacted
Compliance pilot	System account	✓ Compliant		03/17/2025 12.
Default Device Compliance Policy	System account	✓ Compliant		03/17/2025 12.

- Onboarded to Device to Microsoft Defender for Endpoint using Deploying preconfigured policy
- However, onboarding server was crone job and completely different approach. Troubleshooted driver dependencies, Corrupted VM issue. (Thanks to Backups and failover plans – **Always Remember.**

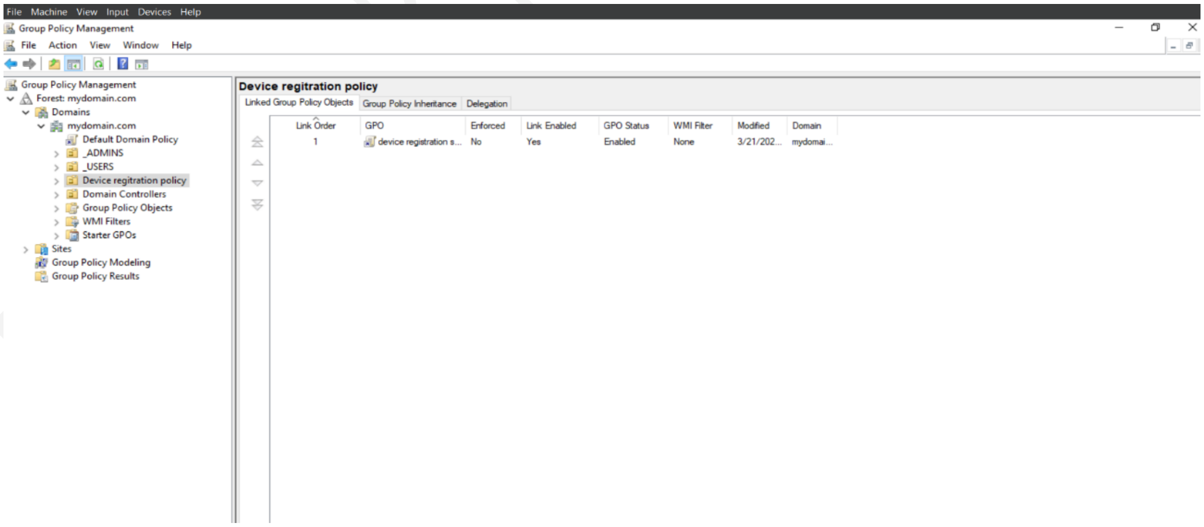
- Go to Server (DC) – Go to Active directory users and Computers> OU > Create New OU > Move server Object in new created OU
- Open Group Policy object > Create a GPO in this Domain and link it here > Name GPO > OK.
- Edit GPO by enabling the by enabling administrative templates for



MDM

Select an item to view its description.

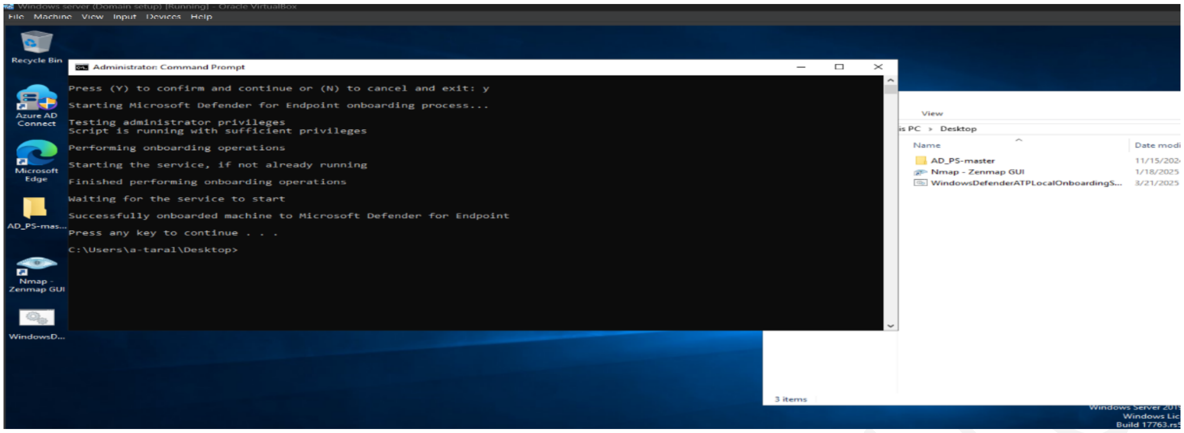
Setting	
Enable automatic MDM enrollment using default Azure AD ...	Nc
Disable MDM Enrollment	Nc



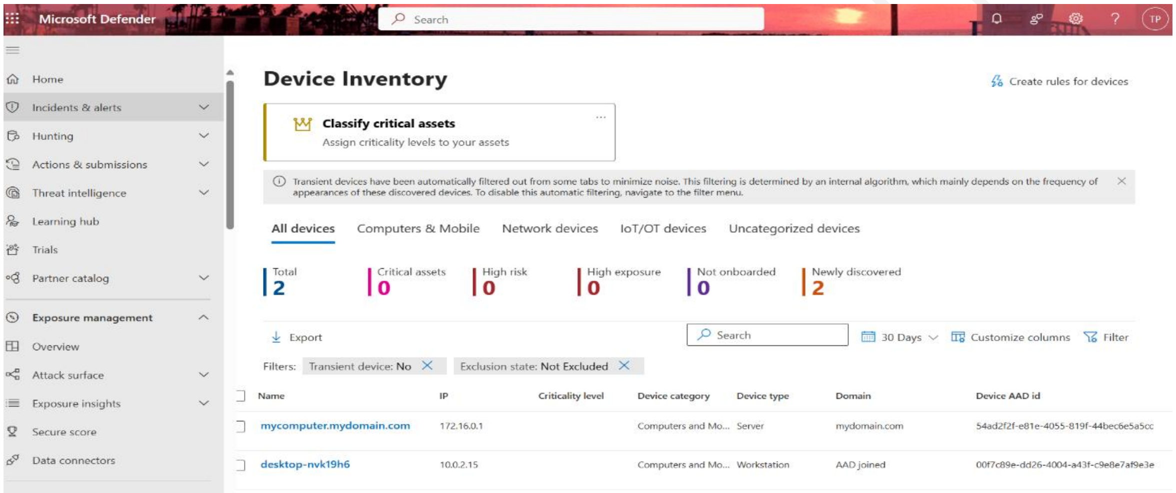
Device regitration policy

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	device registration s...	No	Yes	Enabled	None	3/21/202...	mydomai...

- Now Run the Onboarded package in DC CMD to Onboard device on defender – Successful.


Windows server (Domain setup) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Azure AD Connect
Microsoft Edge
AD_PS-mas...
Nmap - Zenmap GUI
WindowsD...
Administrator: Command Prompt
View
is PC > Desktop
Name
Date modi
AD_PS-master 11/15/202
Nmap - Zenmap GUI 1/18/2025
WindowsDefenderATPLocalOnboardingS... 3/21/2025
3 items
Windows Server 201
Windows Lic
Build 17763.rs

```
Press (Y) to confirm and continue or (N) to cancel and exit: y
Starting Microsoft Defender for Endpoint onboarding process...
Testing administrator privileges
Script is running with sufficient privileges
Performing onboarding operations
Starting the service, if not already running
Finished performing onboarding operations
Waiting for the service to start
Successfully onboarded machine to Microsoft Defender for Endpoint
Press any key to continue . . .
C:\Users\a-taral\Desktop>
```



Device Inventory

Classify critical assets
Assign criticality levels to your assets

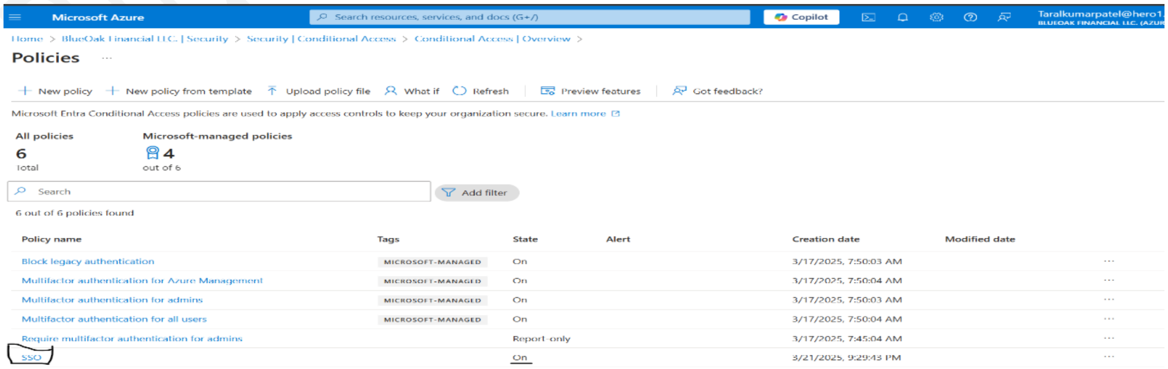
Transient devices have been automatically filtered out from some tabs to minimize noise. This filtering is determined by an internal algorithm, which mainly depends on the frequency of appearances of these discovered devices. To disable this automatic filtering, navigate to the filter menu.

Total	Critical assets	High risk	High exposure	Not onboarded	Newly discovered
2	0	0	0	0	2

Filters: Transient device: No | Exclusion state: Not Excluded

Name	IP	Criticality level	Device category	Device type	Domain	Device AAD id
mycomputer.mydomain.com	172.16.0.1		Computers and Mo...	Server	mydomain.com	54ad2f2f-e81e-4055-819f-44bec6e5a5cc
desktop-nvk19h6	10.0.2.15		Computers and Mo...	Workstation	AAD joined	00f7c89e-dd26-4004-a43f-c9e8e7af9e3e

- **SSO policy:**
  - Assigning this policy supposed to be first step, Not in my case. I have to done multiple authentication every time across servces while completing this project, erious hurdle.
  - For SSO I have created Conditional access policy in azure for seamless access between all my services Microsoft 365 Admin centre, Azure Portal, Intune and microsoft Defender.



Home > BlueOak Financial LLC. | Security > Security | Conditional Access > Conditional Access | Overview >

Policies

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

All policies: 6 Total

Microsoft-managed policies: 4 out of 6

6 out of 6 policies found

Policy name	Tags	State	Alert	Creation date	Modified date
Block legacy authentication	MICROSOFT-MANAGED	On		3/17/2025, 7:50:03 AM	
Multifactor authentication for Azure Management	MICROSOFT-MANAGED	On		3/17/2025, 7:50:04 AM	
Multifactor authentication for admins	MICROSOFT-MANAGED	On		3/17/2025, 7:50:03 AM	
Multifactor authentication for all users	MICROSOFT-MANAGED	On		3/17/2025, 7:50:04 AM	
Require multifactor authentication for admins		Report-only		3/17/2025, 7:45:04 AM	
SSO		On		3/21/2025, 9:29:43 PM	

Solutions Used

- Oracle VM
- Windows Server and AD environment
- Virtualization
- Azure Active Directory (Azure AD)
- Azure AD Connect
- Microsoft Intune
- Microsoft Defender for Endpoint
- (Future plans: Microsoft Sentinel, Defender for Cloud, SOAR solutions)

Lessons Learned

It's important to emphasize the need for thoroughly assessing system integration requirements and leveraging a variety of online resources to address challenges effectively. Troubleshooting connection and Onboarding issues often involves carefully examining system dependencies and their configurations to ensure seamless interoperability and functionality. Always Back Up and Tests your VMs for disaster recovery. Stay organized and never forget to enable SSO For azure Services. Keep in mind the azure naming convention or their services. Navigating azure according to online resource was hurdle as Microsoft always update services name and portals are based on assigned permission. Never forget to apply any theoretical knowledge gained from certificates in Cybersecurity.

Future Recommendations

I aim to design and implement a fully operational enterprise network infrastructure, integrating advanced cybersecurity solutions to enhance security and efficiency. Key initiatives include leveraging advanced log analysis, Microsoft Sentinel for threat detection and response, AI-driven automation for streamlined operations, and Zero Trust architecture to fortify access management. Additionally, I plan to integrate Defender for Cloud for comprehensive cloud protection and deploy a SOAR (Security Orchestration, Automation, and Response) solution to automate workflows and improve incident response capabilities

References

JnHs, *Azure documentation*, *Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/azure/?product=popular (Accessed: 25 March 2025).

Josh Madakor Cyber course - the best hands-on cybersecurity course on the internet! (2025) *LogN Pacific - Helping You Break into IT and Cybersecurity*. Available at: https://joshmadakor.tech/cyber/ (Accessed: 25 March 2025).

Jaeb, J. (2023) *YouTube*. Available at: https://www.youtube.com/watch?v=LR8009GgGAQ (Accessed: 25 March 2025).

Gibson, D. and Shelley, J. (2023) *CompTIA security+: Get certified get ahead: SY0-701 study guide*. United States: Certification Experts, LLC.

Iainfoulds (no date) *Active directory domain services overview*, *Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (Accessed: 10 March 2025).