Adrian Kurowski

Windows Server Home Lab

Event Log Forwarding

Set up centralized log collection from a domain-joined client to the Domain Controller using Windows Event Collector.

Implementation

- On the Domain Controller, opened Event Viewer > Subscriptions > Created a new subscription for Event ID 4625 (Logon Failures).
- Added the client machine using 'Select Computers' and chose 'Minimize Latency'.
- On the client, opened PowerShell as administrator and ran 'wecutil qc' to configure Windows Event Collector.
- Enabled WinRM service using 'Start-Service WinRM'.

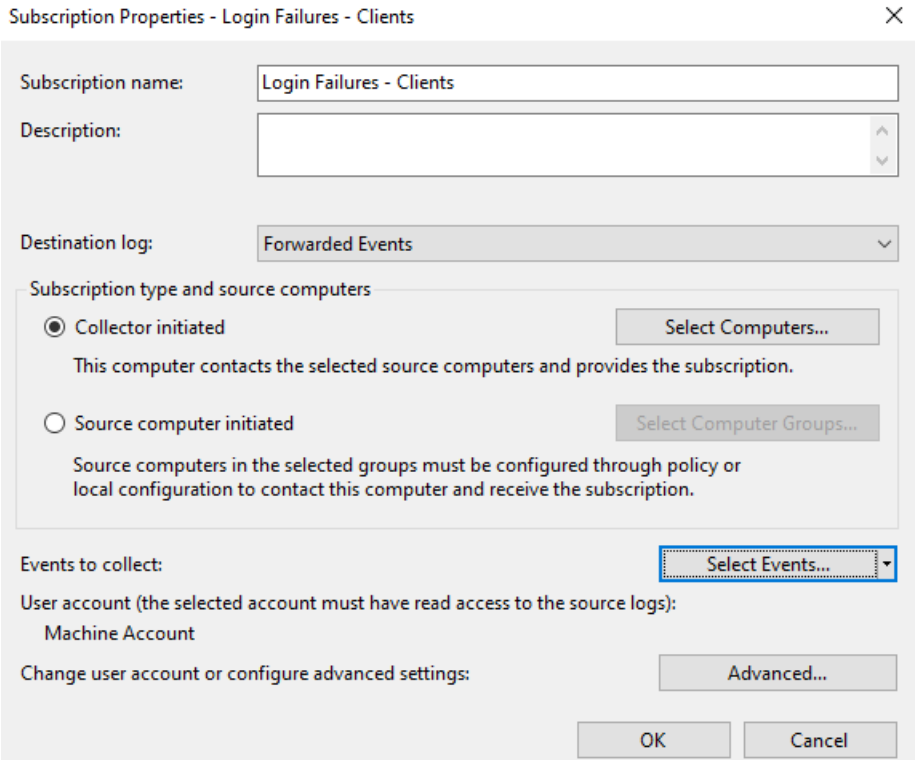
Issue

Subscription status showed 'Access is denied (0x5)'.

Resolution

- Opened 'Active Directory Users and Computers' > Navigated to 'Builtin > Event Log Readers'.
- Added the client computer by typing 'ADVM$', clicking 'Object Types' and selecting 'Computers'.
- Forced Group Policy update with 'gpupdate /force'.
- Restarted EventLog and WinRM services.
- Verified success in Event Viewer > Subscriptions > Runtime Status and saw logs populate

under 'Forwarded Events'.



Backup and Restore Simulation

Simulate system state backup and restore in preparation for domain recovery.

Implementation

- Installed 'Windows Server Backup' via Server Manager > Features.
- Opened 'Windows Server Backup' > Chose 'Backup Once' > Selected 'Custom' > Added 'System State'.
- Saved the backup to a secondary drive.
- Deleted a domain user via 'Active Directory Users and Computers' to simulate accidental removal.

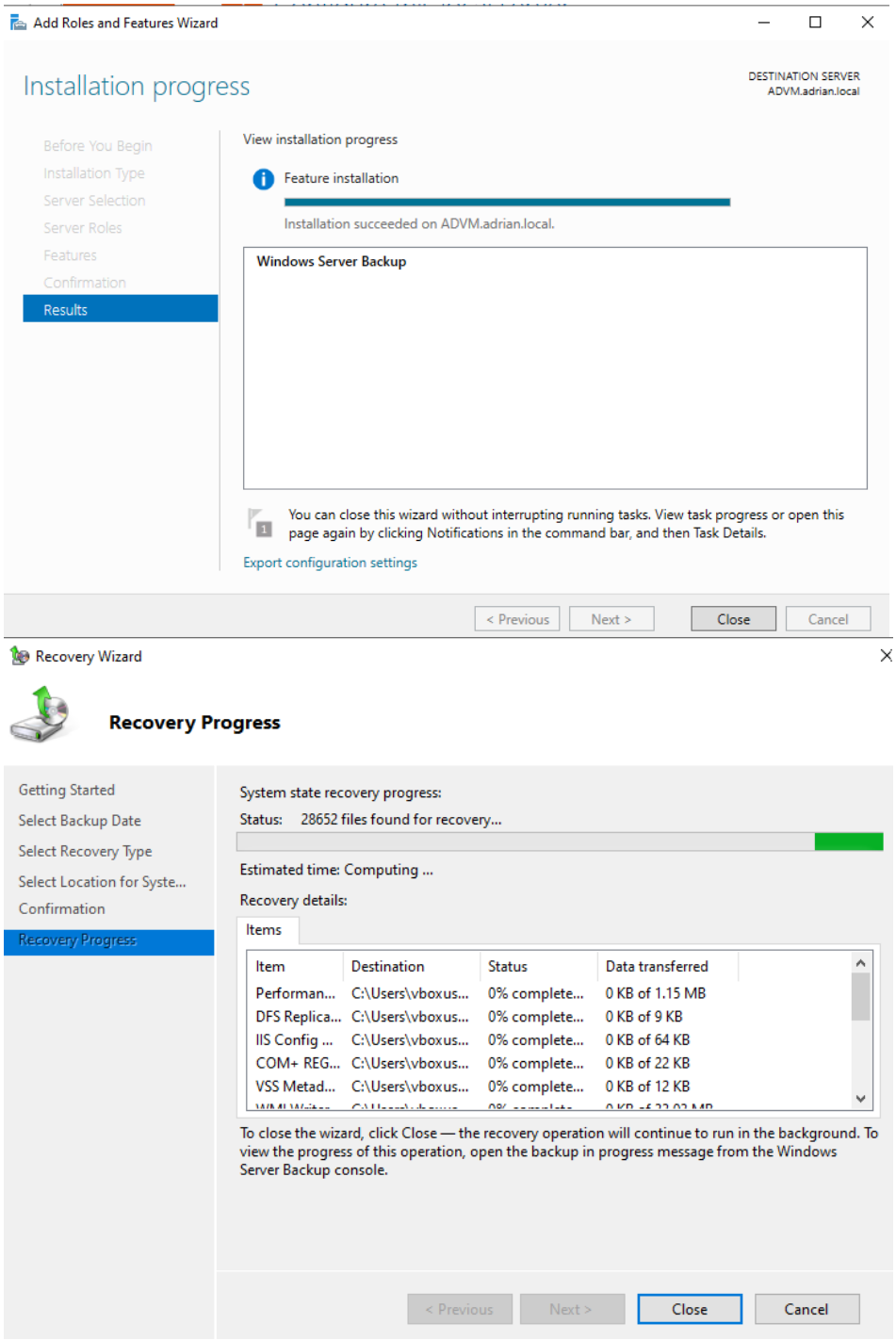
Issue

Full system state restore could not be performed without entering Directory Services Restore Mode (DSRM).

Resolution

- Walked through the 'Recover' wizard up to confirmation to show process.
- Noted that full restoration would require reboot into DSRM and running: 'wbadmin start systemstaterecovery -version:<version>'.

Adrian Kurowski



DHCP + DNS Logging

Track IP lease distribution and DNS queries through built-in logging systems.

<u>Implementation</u>

- Installed DHCP and DNS roles via Server Manager.

Adrian Kurowski

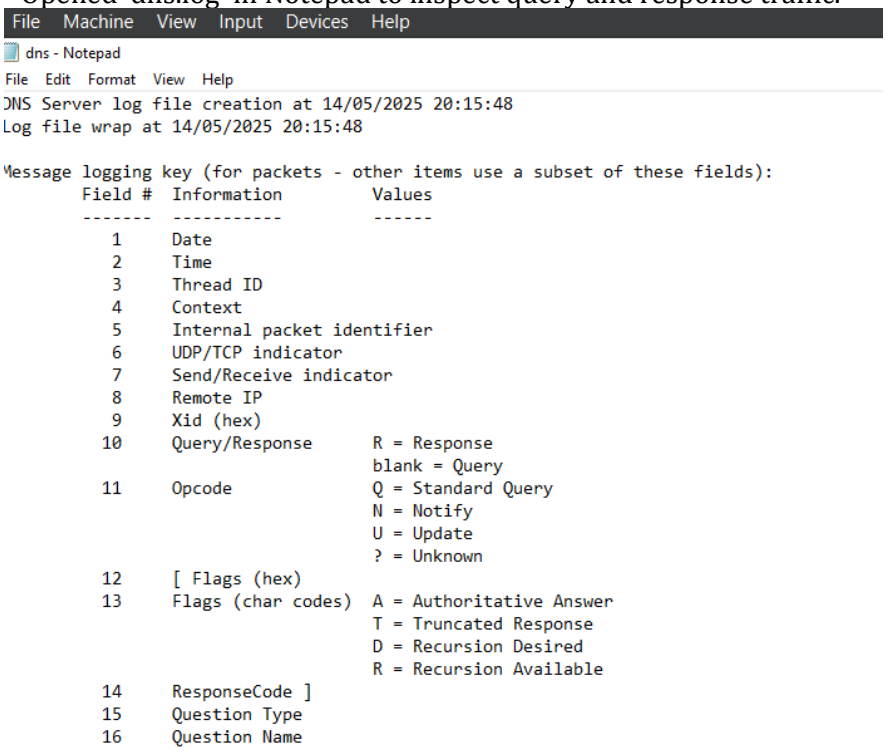
- Configured a DHCP scope: 10.0.2.100–150 with gateway and DNS pointing to the DC.
- Verified lease by renewing client IP using 'ipconfig /release' and 'ipconfig /renew'.
- For DNS, opened DNS Manager > Server Properties > Enabled Debug Logging.

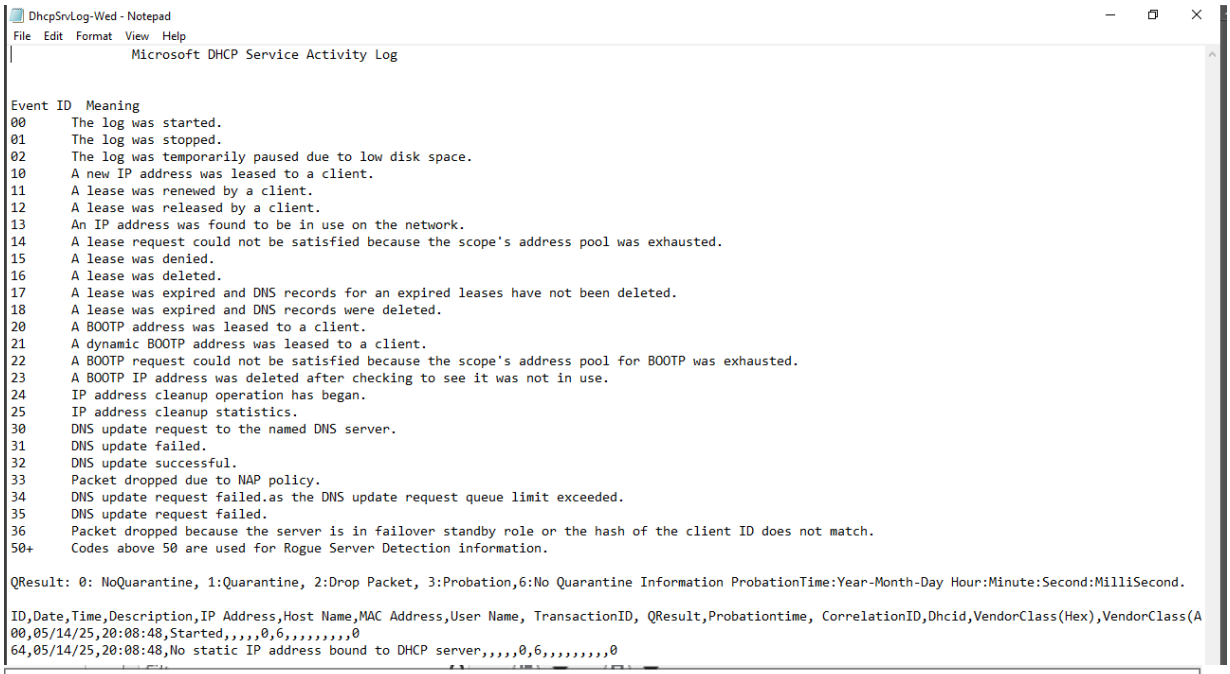
Issue

DHCP logs were empty despite clients online.

Resolution

- Opened Event Viewer > Applications and Services > Microsoft > Windows > DHCP Server > Operational.
- Found logs confirming lease events.
- Verified DHCP log files in 'C:\Windows\System32\dhcp\DhcpSrvLog-*.log'.
- Opened 'dns.log' in Notepad to inspect query and response traffic.

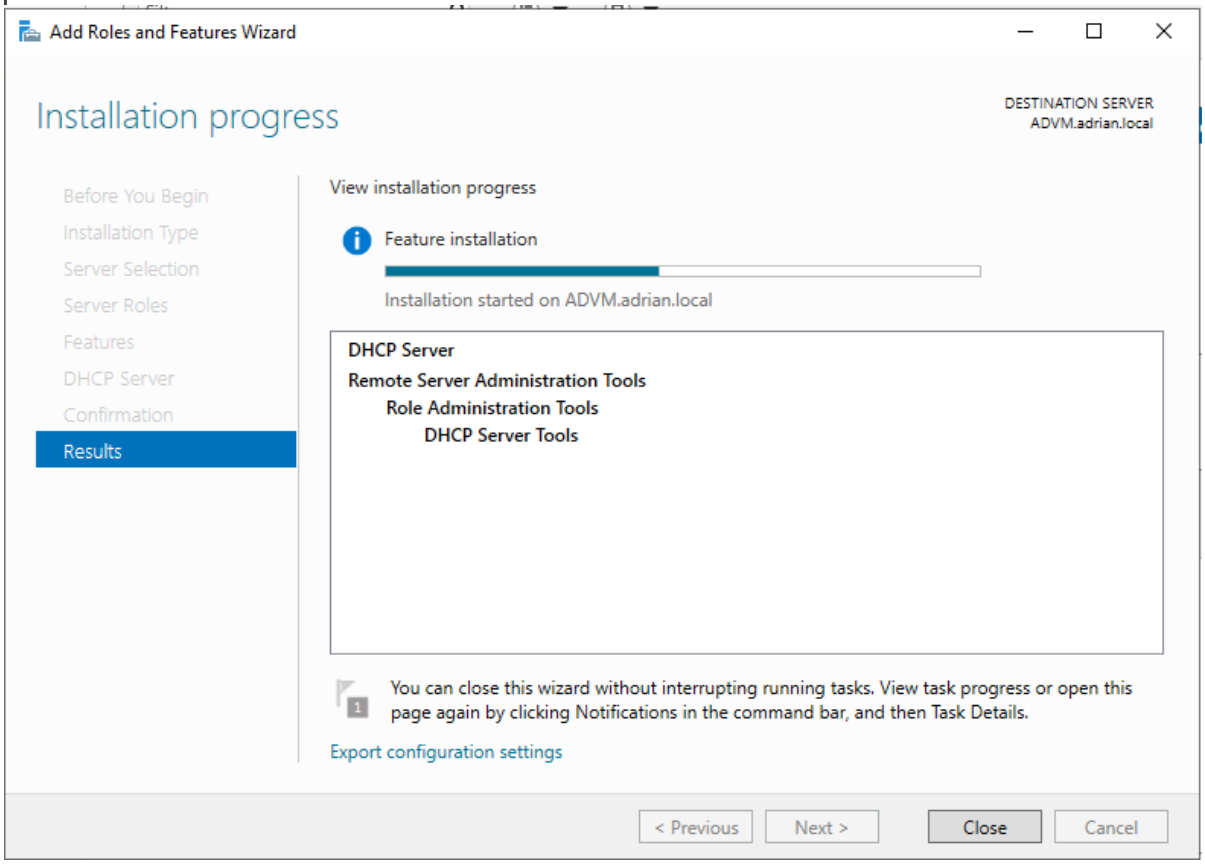




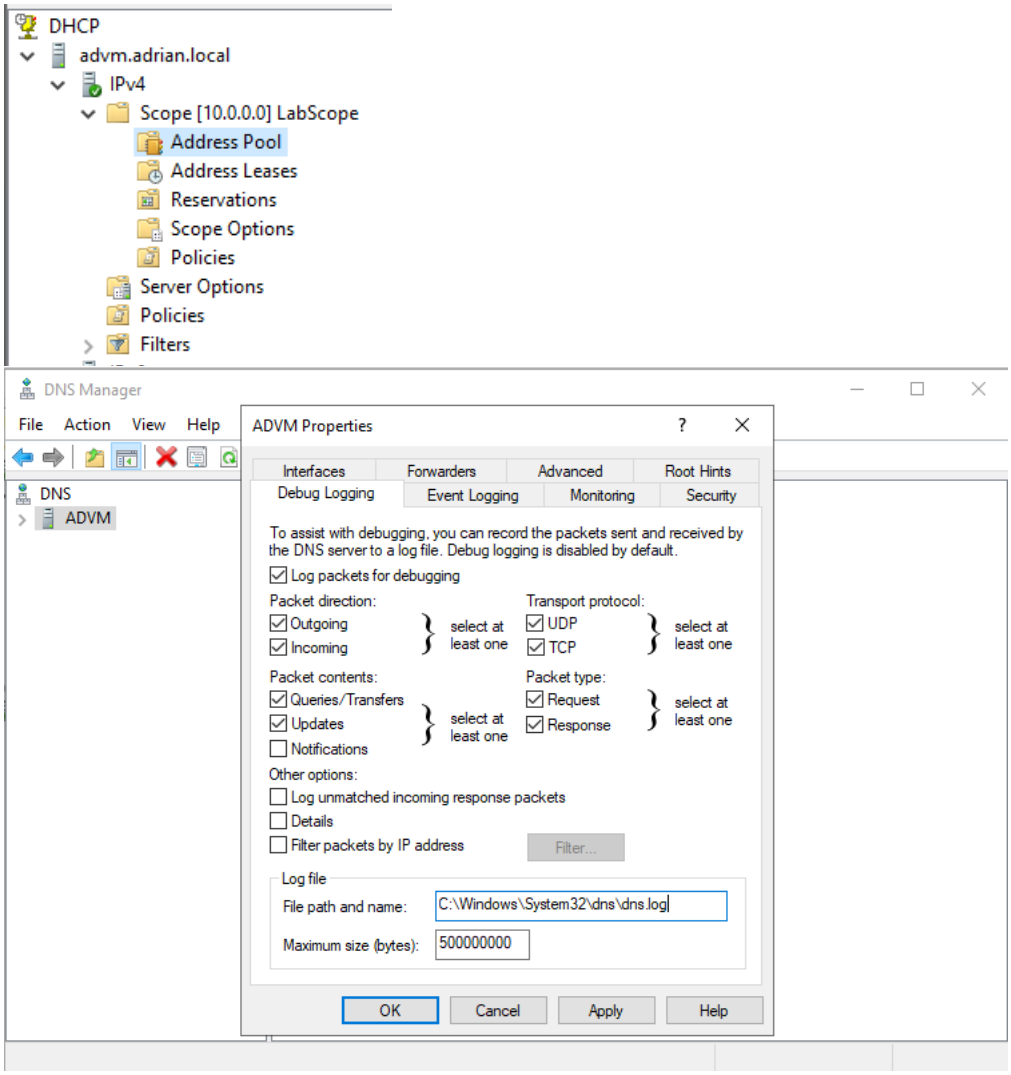
DhcpSrvLog-Wed - Notepad

File Edit Format View Help

```
                Microsoft DHCP Service Activity Log


Event ID  Meaning
00      The log was started.
01      The log was stopped.
02      The log was temporarily paused due to low disk space.
10      A new IP address was leased to a client.
11      A lease was renewed by a client.
12      A lease was released by a client.
13      An IP address was found to be in use on the network.
14      A lease request could not be satisfied because the scope's address pool was exhausted.
15      A lease was denied.
16      A lease was deleted.
17      A lease was expired and DNS records for an expired leases have not been deleted.
18      A lease was expired and DNS records were deleted.
20      A BOOTP address was leased to a client.
21      A dynamic BOOTP address was leased to a client.
22      A BOOTP request could not be satisfied because the scope's address pool for BOOTP was exhausted.
23      A BOOTP IP address was deleted after checking to see it was not in use.
24      IP address cleanup operation has began.
25      IP address cleanup statistics.
30      DNS update request to the named DNS server.
31      DNS update failed.
32      DNS update successful.
33      Packet dropped due to NAP policy.
34      DNS update request failed.as the DNS update request queue limit exceeded.
35      DNS update request failed.
36      Packet dropped because the server is in failover standby role or the hash of the client ID does not match.
50+     Codes above 50 are used for Rogue Server Detection information.

QResult: 0: NoQuarantine, 1:Quarantine, 2:Drop Packet, 3:Probation,6:No Quarantine Information ProbationTime:Year-Month-Day Hour:Minute:Second:MilliSecond.

ID,Date,Time,Description,IP Address,Host Name,MAC Address,User Name, TransactionID, QResult,Probationtime, CorrelationID,Dhcid,VendorClass(Hex),VendorClass(A
00,05/14/25,20:08:48,Started,,,,,0,6,,,,,,,,,0
64,05/14/25,20:08:48,No static IP address bound to DHCP server,,,,,0,6,,,,,,,,,0
```



Adrian Kurowski



Group Policy and Scheduled Tasks

Apply GPOs to deploy daily scheduled tasks and configure login banner.

Implementation

- Created a GPO linked to 'IT Team' OU.
- Configured: User Configuration > Preferences > Control Panel Settings > Scheduled Tasks.
- Set task to run PowerShell script from C:\Scripts\LogTask.ps1 with elevated privileges.
- Used 'schtasks' to confirm registration.
- Configured login banner using: Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options.

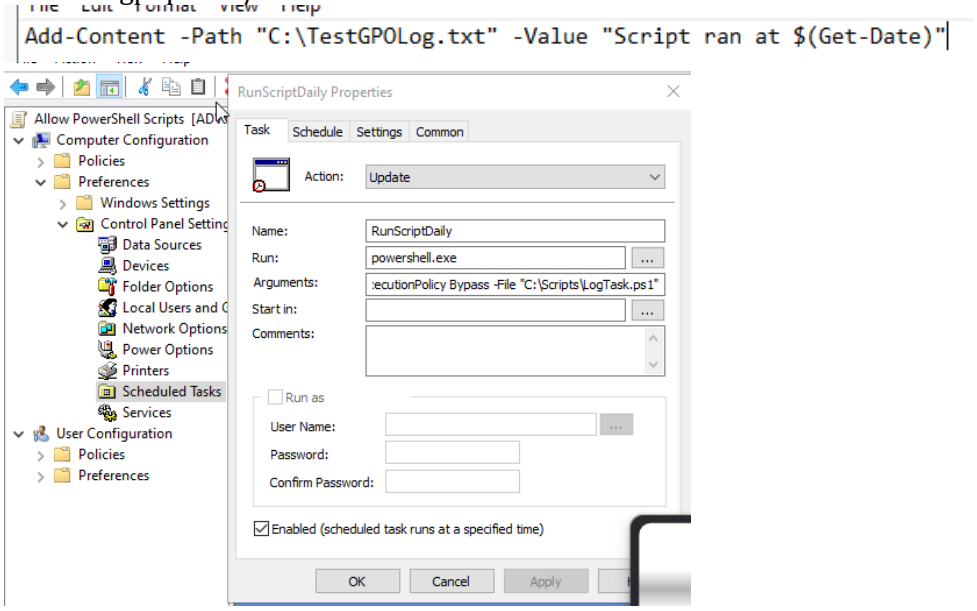
Issue

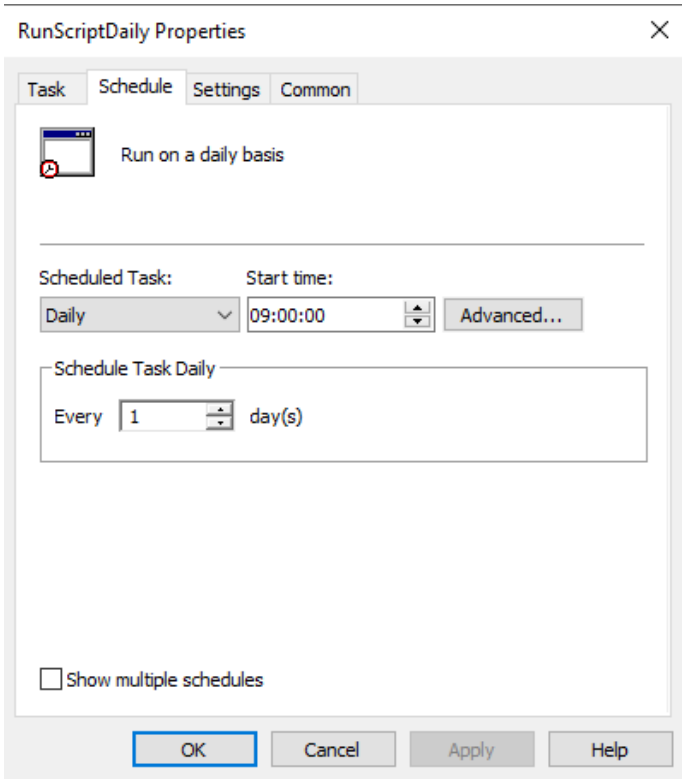
Task failed due to blocked script execution.

Resolution

- Enabled GPO: 'Turn on Script Execution' > Allow all scripts.

- Re-ran 'gpupdate /force' and confirmed success.

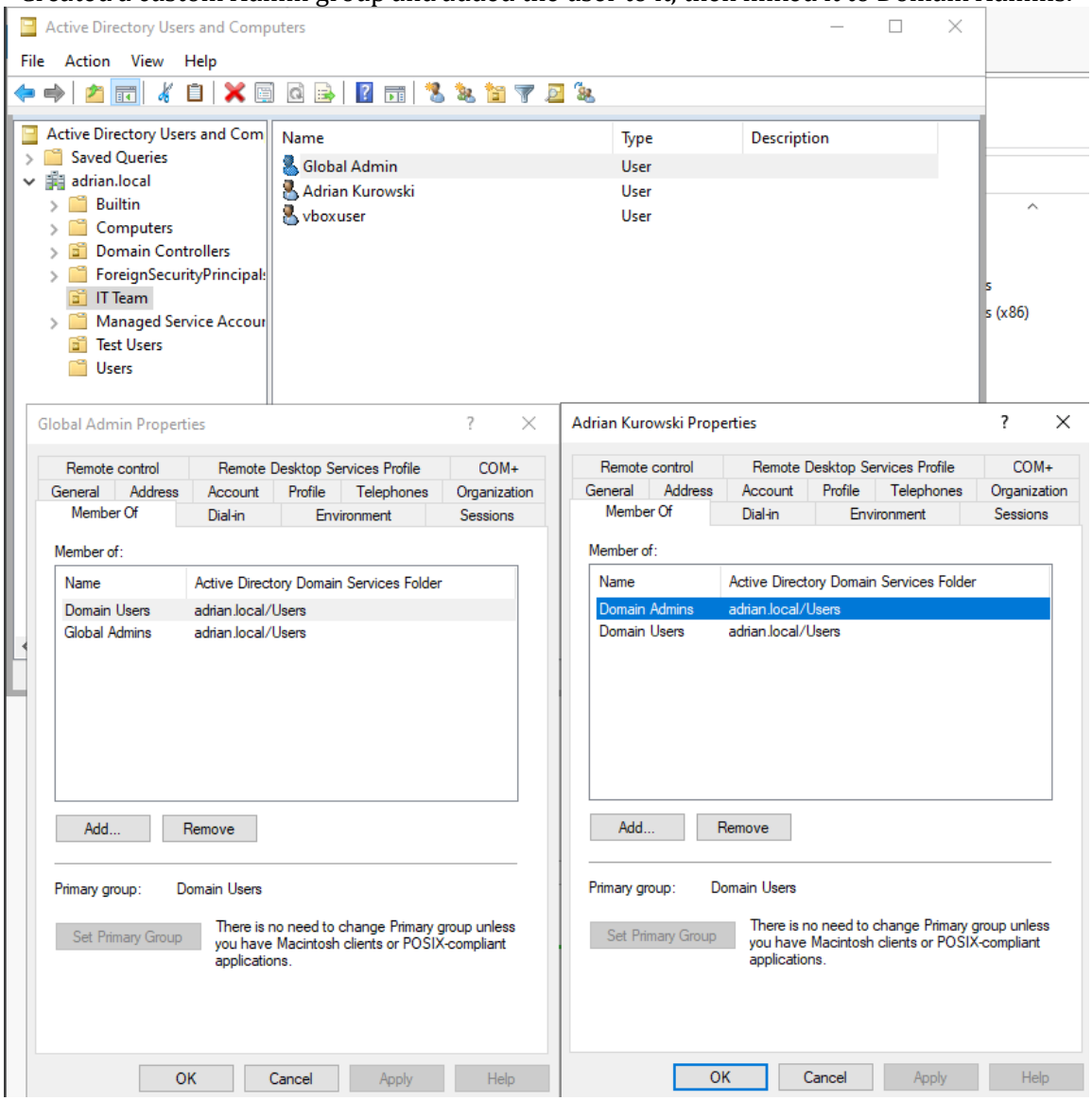




Active Directory Domain Services

- Installed and configured Windows Server 2022 using VirtualBox.
- Promoted the server to a Domain Controller with domain name 'adrian.local'.
- Created Organizational Unit (OU) named 'IT Team'.
-Practiced creating, disabling, and renaming domain user accounts in Active Directory Users and Computers.

- Created a custom Admin group and added the user to it, then linked it to Domain Admins.



Networking and DHCP Configuration

- Configured networking using internal adapter in VirtualBox to allow VM-to-VM communication.
- Set static IP and DNS manually on the client VM for domain join.
- Verified IP address assignment and DNS resolution using ipconfig and Test-NetConnection.
- Enabled DHCP on the server for dynamic IP assignment (testing purposes).

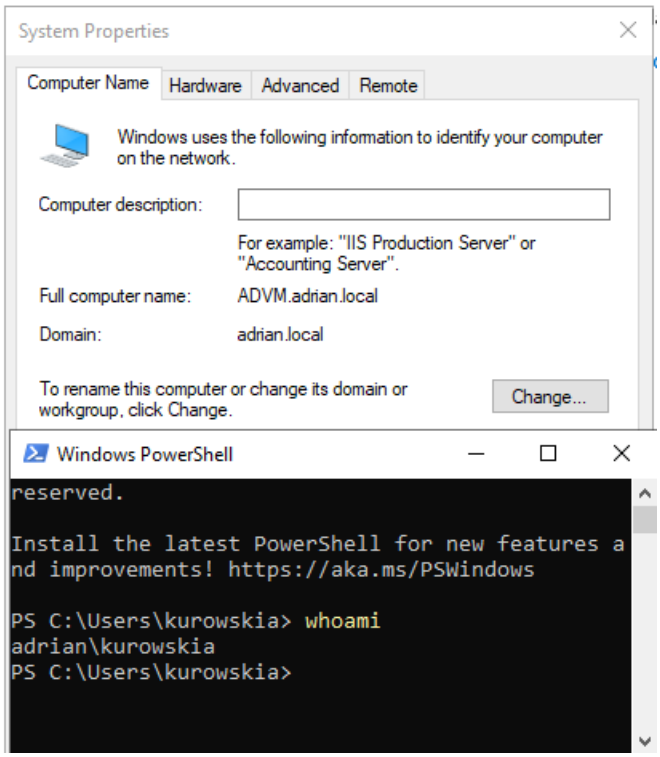
```
PS C:\Users\vboxuser> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : ADVM
   Primary Dns Suffix  . . . . . . . : adrian.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : adrian.local
                                       Home

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : Home
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-0F-CD-38
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fd17:625c:f037:2:4162:dc8d:e376:794(Preferred)
   Link-local IPv6 Address . . . . . : fe80::4162:dc8d:e376:794%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.2.15(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 16 May 2025 13:43:10
   Lease Expires . . . . . . . . . . : 17 May 2025 13:43:10
   Default Gateway . . . . . . . . . : fe80::2%11
                                       10.0.2.2
   DHCP Server . . . . . . . . . . . : 10.0.2.2
   DHCPv6 IAID . . . . . . . . . . . : 101187623
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-AF-1C-87-08-00-27-0F-CD-38
   DNS Servers . . . . . . . . . . . : ::1
                                       10.0.2.3
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS C:\Users\vboxuser>
```

```
PS C:\Windows\system32> Test-NetConnection


ComputerName            : internetbeacon.msedge.net
RemoteAddress           : 13.107.4.52
InterfaceAlias          : Ethernet
SourceAddress           : 10.0.2.15
PingSucceeded           : True
PingReplyDetails (RTT) : 20 ms
```

Windows Client VM Setup

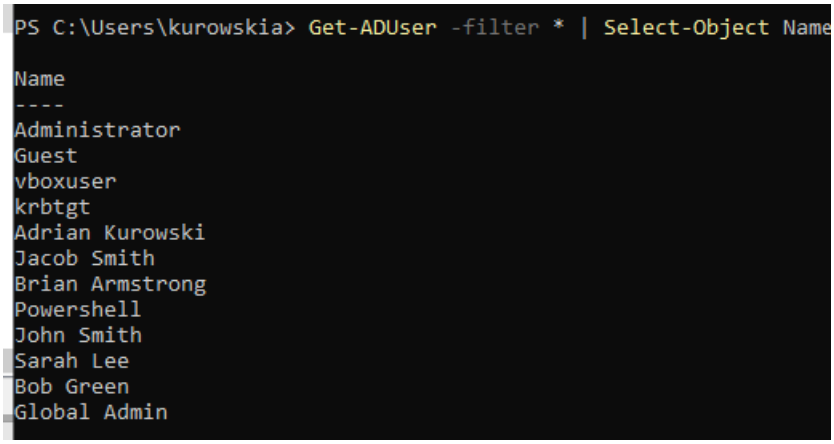
- Created a second VM (Windows 11) and installed the OS using official ISO.
- Configured NIC to be on the same internal network as the Domain Controller.
- Successfully joined the Windows 11 client to the 'adrian.local' domain.
- Tested logging in with domain user accounts.

Adrian Kurowski



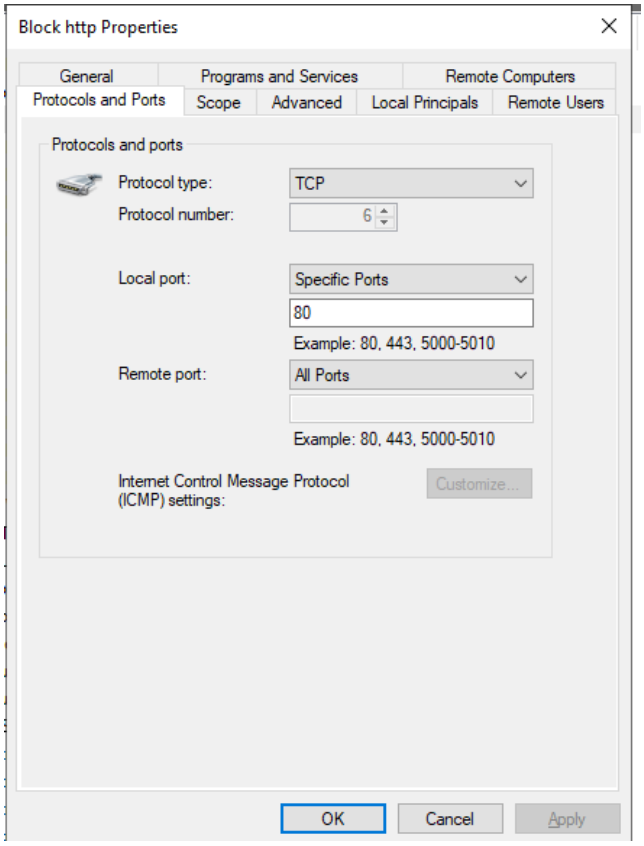
PowerShell Basics

- Practiced using PowerShell for AD user queries and system checks.
- Used commands like Get-ADUser, Export-CSV, Set-DnsClientServerAddress, and Test-NetConnection.



Windows Firewall and Port Testing

- Created inbound rules to block/allow specific ports (e.g., port 80 for HTTP).
- Verified traffic using Test-NetConnection and netstat -ano.
- Installed Telnet client and tested local port connectivity.



Troubleshooting & Lessons Learned

- No network on VM: Resolved by switching VirtualBox adapter to 'Internal Network' and setting static IP.
- Firewall not blocking port 80: Checked rule scope > Confirmed with 'Test-NetConnection' and 'netstat'.
- OU move failed: Removed 'Protect from accidental deletion' via ADUC > Object tab.

Adrian Kurowski

- Telnet failed: Enabled feature via 'Turn Windows Features On or Off'.