

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | |
| **FINAL PROJECT DOCUMENTATION**  Team Leader: LAKSHMI M,  Members: POURIA M, MANJINder S, Kien N, SAHar M, ALIREZA O, ALIREZA T, PARSA N, Suteash S, TONY T, TOBY H  Group 3 | MAY 2025, 2024 | | |
|  | |  |

# Table of Contents

[Table of Contents 1](#_Toc158791397)

[Network Topology 2](#_Toc988377888)

[Network Overview 3](#_Toc1119269172)

[Enterprise Network 3](#_Toc1974039212)

[Core Network Devices 3](#_Toc2059438314)

[WAN Technologies: 4](#_Toc1274949759)

[IP Plan for WAN Links: 4](#_Toc191657364)

[Tunnel Configuration – DMVPN 5](#_Toc1695049746)

[LAN Design 6](#_Toc905676589)

[IGP – OSPF Configuration 8](#_Toc162514589)

[EGP – BGP Configuration 8](#_Toc1699962484)

[MPLS Core 9](#_Toc969190895)

[NAT Gateway – R4 9](#_Toc1439471909)

[Access Layer (Switch S3) 9](#_Toc1703904244)

[Conclusion 9](#_Toc283064620)

[Windows 10](#_Toc329596759)

[Active Directory & GPO Configuration 10](#_Toc375132047)

[Burnaby: AD Sites and Services 10](#_Toc1366278099)

[Burnaby: Active Directory Users and Computers – OU Design 10](#_Toc286698004)

[Burnaby: DNS Configuration 11](#_Toc1778072889)

[Burnaby: Cluster Manager – File Server Role 13](#_Toc199155260)

[Burnaby: Network Configuration – IP Address Assignment 13](#_Toc1028262900)

[Burnaby: Server Properties 14](#_Toc1302213597)

[Burnaby: DHCP Scope and Load-Balanced Failover 15](#_Toc2003025850)

[Burnaby: Cluster Storage Validation – iSCSI Devices 17](#_Toc926702756)

[Richmond: DHCP Address Pool and Exclusion Configuration 17](#_Toc993475410)

[Richmond: DHCP Scope Options 17](#_Toc155420415)

[Richmond: Reverse DNS Zone Validation 17](#_Toc988516126)

[Richmond: Defender Real-Time Protection GPO 17](#_Toc790063376)

[Richmond: USB Blocking GPO Enforcement 17](#_Toc716080457)

[Richmond: USB GPO – Vancouver Comparison for Cross-Validation 17](#_Toc1342051346)

[Richmond: Password Policy GPO Settings 17](#_Toc363647233)

[Richmond: Audit Policy Enforcement GPO 17](#_Toc162477861)

[Richmond: AD Organizational Units – GPO Scoping 17](#_Toc639104663)

[Richmond: NTFS Permissions Enforcement via Security Groups 17](#_Toc1356044235)

[Richmond: Departmental File Shares Verification 17](#_Toc2069164890)

[Vancouver: DNS Configuration – DC1 Forward/Reverse Zones 17](#_Toc114876574)

[Vancouver: DC1 IP Configuration Validation 17](#_Toc1435650376)

[Vancouver: DNS Configuration – DC2 Forward/Reverse Zones 17](#_Toc1635489795)

[Vancouver: DC2 IP Configuration Validation 17](#_Toc433046365)

[Vancouver: DHCP Scope Failover Verification 17](#_Toc1345672010)

[Vancouver: PC DHCP Lease Verification 17](#_Toc405537921)

[Vancouver: Server Validation – G3-DC1-Van 17](#_Toc795859997)

[Vancouver: Server Validation – G3-DC2-Van 17](#_Toc1131737632)

[AWS Cloud Infrastructure Deployment 17](#_Toc1725336698)

[Introduction 17](#_Toc87153706)

[Topology 17](#_Toc1955015266)

[VPC and Subnet Design 17](#_Toc355683954)

[Security Groups configuration 17](#_Toc1270537034)

[EC2 Web Server and Autoscaling 17](#_Toc1963509849)

[Application Load Balancing 17](#_Toc354234201)

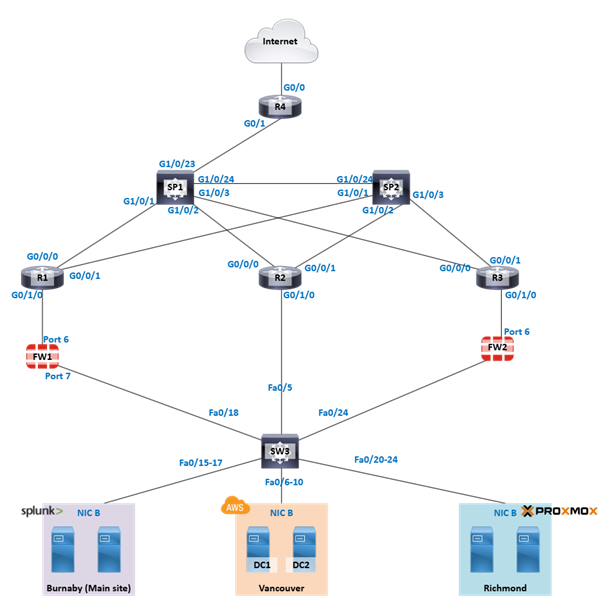
[VPN Configuration (Hybrid Networking) 17](#_Toc831423598)

[Routing and Connectivity 17](#_Toc1640316894)

[Additional Configuration Highlights 17](#_Toc535703581)

[Conclusion 17](#_Toc591307167)

# Network Topology



# Network Overview

We designed and implemented a 3-site enterprise network using a dual WAN topology with IPv4 and IPv6 addressing. The sites include Burnaby, Downtown Vancouver, and Richmond. WAN connectivity is achieved using DMVPN and MPLS Layer 3 VPN. Site-to-site FortiGate VPNs and Splunk-based log forwarding were integrated into the architecture.

This project involved deploying FortiGate firewalls at both the Burnaby and Vancouver sites, where we successfully configured IPsec VPN tunnels for secure site-to-site communication. A Proxmox hypervisor in Richmond allowed us to host critical services, while DC1 and DC2 data centers in Vancouver provided core infrastructure on AWS. The network backbone includes routers (R1, R2, R3), core switches, and dual WAN connectivity through Service Providers (SP1 and SP2) with routes advertised via OSPF and BGP.

The visual network diagram clearly reflects our layered approach: each site connects through its respective FortiGate firewall and router, uplinked to the core switch SW3. From there, end-hosts such as Splunk Forwarders, servers, and VMs are segmented using VLAN interfaces. The Burnaby site houses the Splunk stack, enabling log aggregation from firewalls and the network. Overall, this topology highlights strong segmentation, redundancy, and scalability in design, aligned with real-world enterprise environments.

# Enterprise Network

This report outlines the deployment and configuration of an enterprise WAN infrastructure using Cisco routers and switches. The design integrates Dynamic Multipoint VPN (DMVPN) for scalable VPN communication, OSPF and BGP for routing, MPLS for label-switched forwarding, and IPv6 dual-stack configuration for future-ready connectivity.

### Core Network Devices

**Main Routers:**

* R1 (Hub - Burnaby)
* R2 (Spoke 1 - Vancouver)
* R3 (Spoke 2 - Richmond)

**Service Providers:**

* SP1 (IPv4 core)
* SP2 (IPv6/MPLS core)

**Access Layer:**

* S3 (VLAN assignments to each site)

**NAT Gateway:**

* R4 (NAT between private/public spaces)

### WAN Technologies:

* **Provider A**: DMVPN (uses EIGRP)
* **Provider B**: MPLS L3 VPN (uses OSPF)

Each site connects to SP1 and SP2 using /30 subnets from two major WAN blocks: 152.19.0.0/16 for SP1 and 162.19.0.0/16 for SP2. For example, Burnaby connects to SP1 using 152.19.0.0/30 and to SP2 using 162.19.0.0/30. The interfaces are mapped as follows: SP1 uses interfaces Gig1/0/x and SP2 uses Gig1/0/x, while customer routers (R1-R3) use Gig0/0/0 and Gig0/0/1 for WAN uplinks. This IP schema ensures clear separation and route control for each WAN provider.

The WAN topology includes redundant ISP links per site, with each routed over separate transport technologies. EIGRP was used to manage routing over the DMVPN network due to its support for summarization and scalability, while OSPF was used over the MPLS links to ensure faster convergence and interoperability with other enterprise environments. Routing is managed using OSPF and BGP for dynamic failover and optimized path selection. All routers also support mGRE/IPsec tunnels as part of the DMVPN solution, ensuring secure and scalable inter-site communication.

### IP Plan for WAN Links:

* IPv4 Overlay: 10.3.1.0/24
* IPv6 Overlay: 2001:10:3:1::/64
* NBMA (Underlay): 152.19.0.0/24

### Tunnel Configuration – DMVPN

**Technology:** Multipoint GRE (mGRE) + NHRP  
**Routing Protocols over Tunnel:** OSPFv3 + IPv6  
**Key Parameters:**

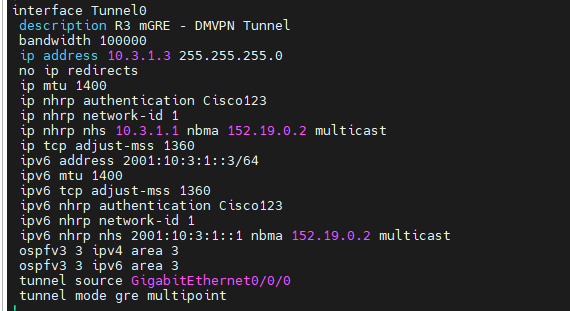
* tunnel mode gre multipoint
* ip nhrp network-id 1
* ip nhrp authentication Cisco123
* ip tcp adjust-mss 1360, mtu 1400 to prevent fragmentation

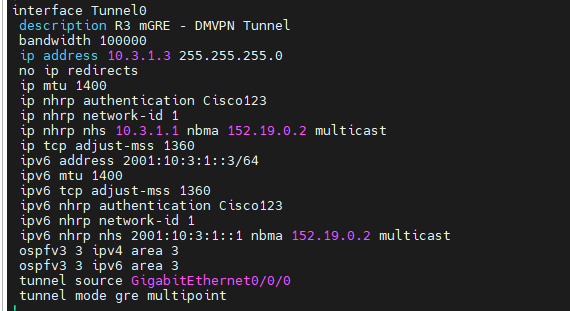
**Tunnel IPs:**

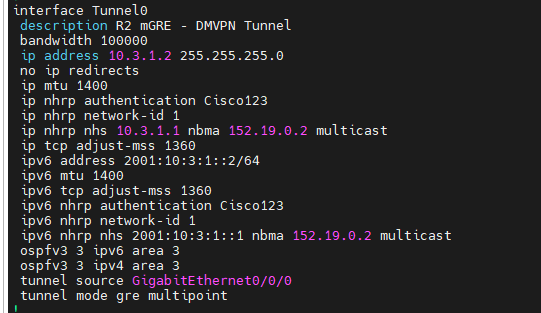
* R1: 10.3.1.1, 2001:10:3:1::1
* R2: 10.3.1.2, 2001:10:3:1::2
* R3: 10.3.1.3, 2001:10:3:1::3

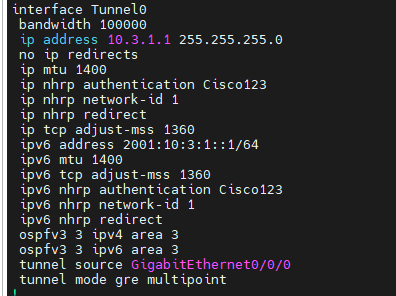
R2 and R3 register with R1 as their NHS (Next Hop Server) using NBMA addresses over public IPs.

**Tunnel Interfaces**: Each site uses Tunnel0 interfaces with NHRP, IPsec, OSPFv3, and proper MTU settings.









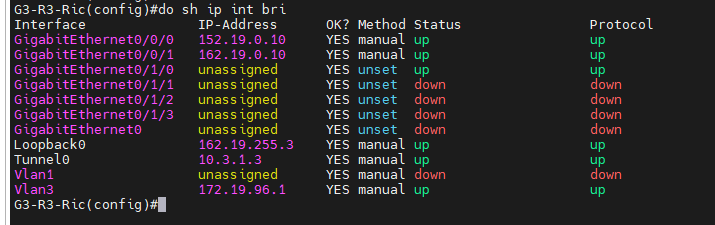
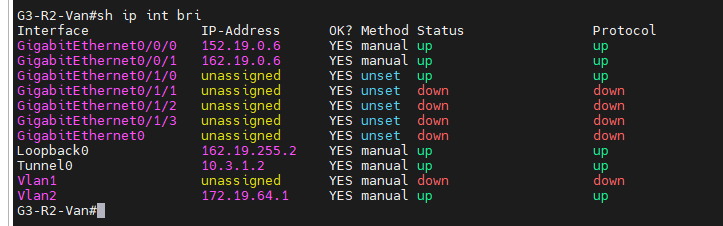
### LAN Design

The LAN architecture is segmented across three main sites. At each location, VLANs are configured for local traffic separation and control. In Burnaby, VLAN 1 (172.19.1.0/24) hosts internal servers and the Splunk stack. The Vancouver site operates on VLAN 2 (172.19.64.0/24), providing data center access to DC1 and DC2 hosted on AWS. Richmond uses VLAN 3 (172.19.96.0/24) and integrates Proxmox for virtualization.

Each VLAN is mapped to corresponding switch interfaces (e.g., Fa0/6-10 for VLAN 2) and routed through its respective gateway on the FortiGate firewall. Interfaces such as Port 7 on each FortiGate provide default gateway functionality for the local LAN. Internal routing is handled via static routes and OSPF where appropriate.

This structure not only segments network traffic but also allows granular firewall policy enforcement and easy scalability. The Layer 2 and Layer 3 segmentation ensures minimal broadcast domains and simplifies troubleshooting while maintaining high network performance.

**Addressing Scheme**:

* IPv4: 172.19.0.0/16
* IPv6: FD00:DB8:19::/48

### **IGP – OSPF Configuration**

All routers use **OSPF Process ID 3** with **Area 3**:

* MPLS LDP is auto-enabled with mpls ldp autoconfig
* Passive interfaces are used on access VLANs for security
* Loopbacks are advertised for BGP peering

### **EGP – BGP Configuration**

All core routers run **iBGP AS 3**:

* Peering is done using **Loopback0 interfaces**
* Peer-group “GRP3” is used for config reuse
* update-source Loopback0 ensures loopback-to-loopback BGP peering
* **Address Families:**
  + ipv4 with redistribute connected
  + vpnv4 with send-community extended for MPLS VPN propagation

### **MPLS Core**

* **SP2** is the MPLS core router with LDP enabled and connected to all core routers
* Advertises a default route into the OSPF domain
* Has BGP peering with core routers to carry VPNv4 routes

### **NAT Gateway – R4**

* NAT overload configuration maps all internal addresses to a public IP on interface Gig0/0 using ACL 1 (permit any)
* Routes configured to reach core and external networks
* Acts as exit point for internet-bound traffic

### **Access Layer (Switch S3)**

**VLANs:**

* VLAN 1 – Core/Admin
* VLAN 2 – Vancouver users
* VLAN 3 – Richmond users

Ports are statically assigned per VLAN and trunks are avoided for simplicity.

### **Conclusion**

This project successfully implemented a **scalable and secure enterprise network** leveraging:

* DMVPN for site-to-site connectivity
* Dual-stack IPv4/IPv6
* OSPF and BGP for dynamic routing
* MPLS for VPN scalability

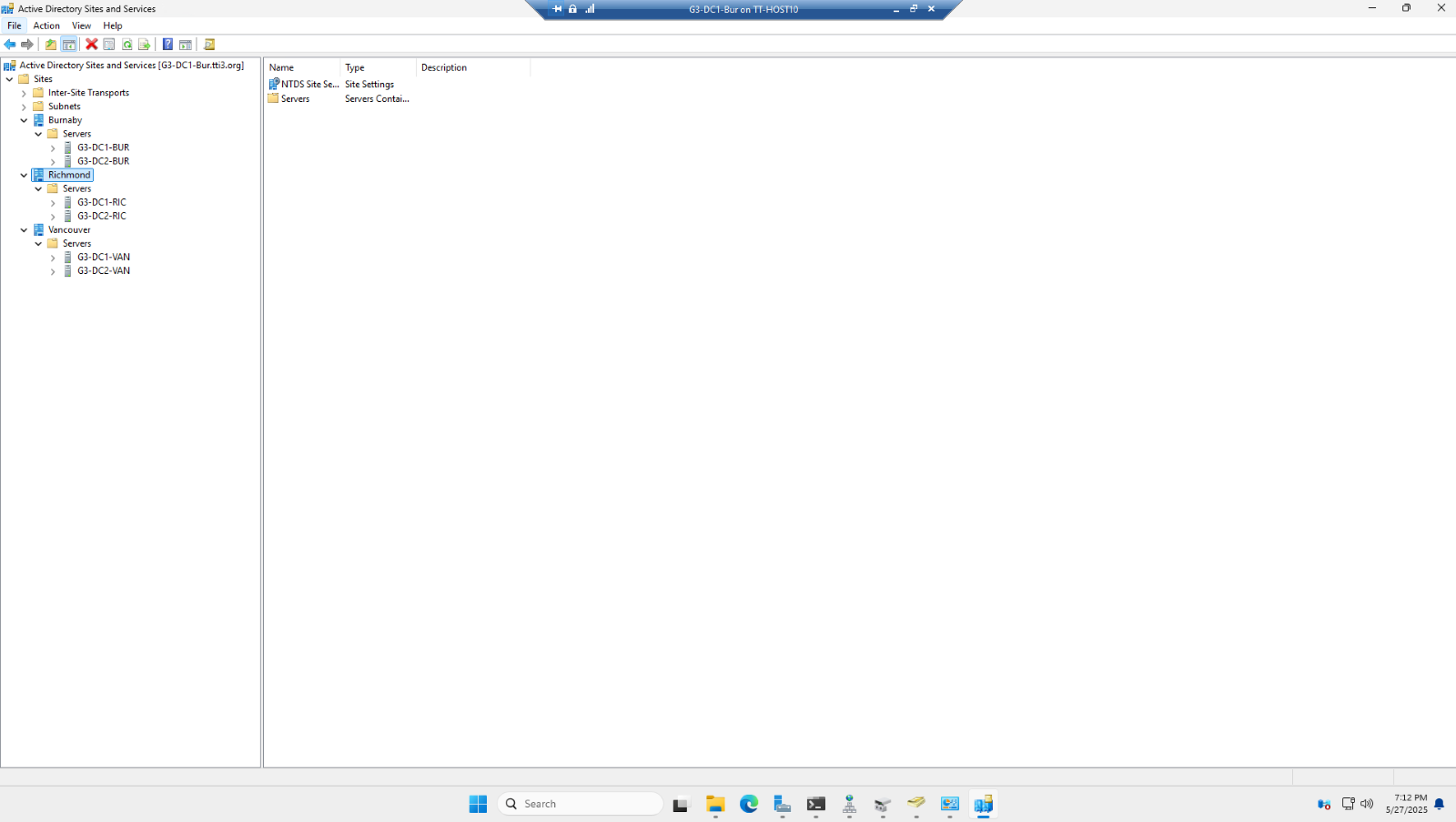
The modular design supports future site additions with minimal reconfiguration effort.

# **Windows**

### Active Directory & GPO Configuration

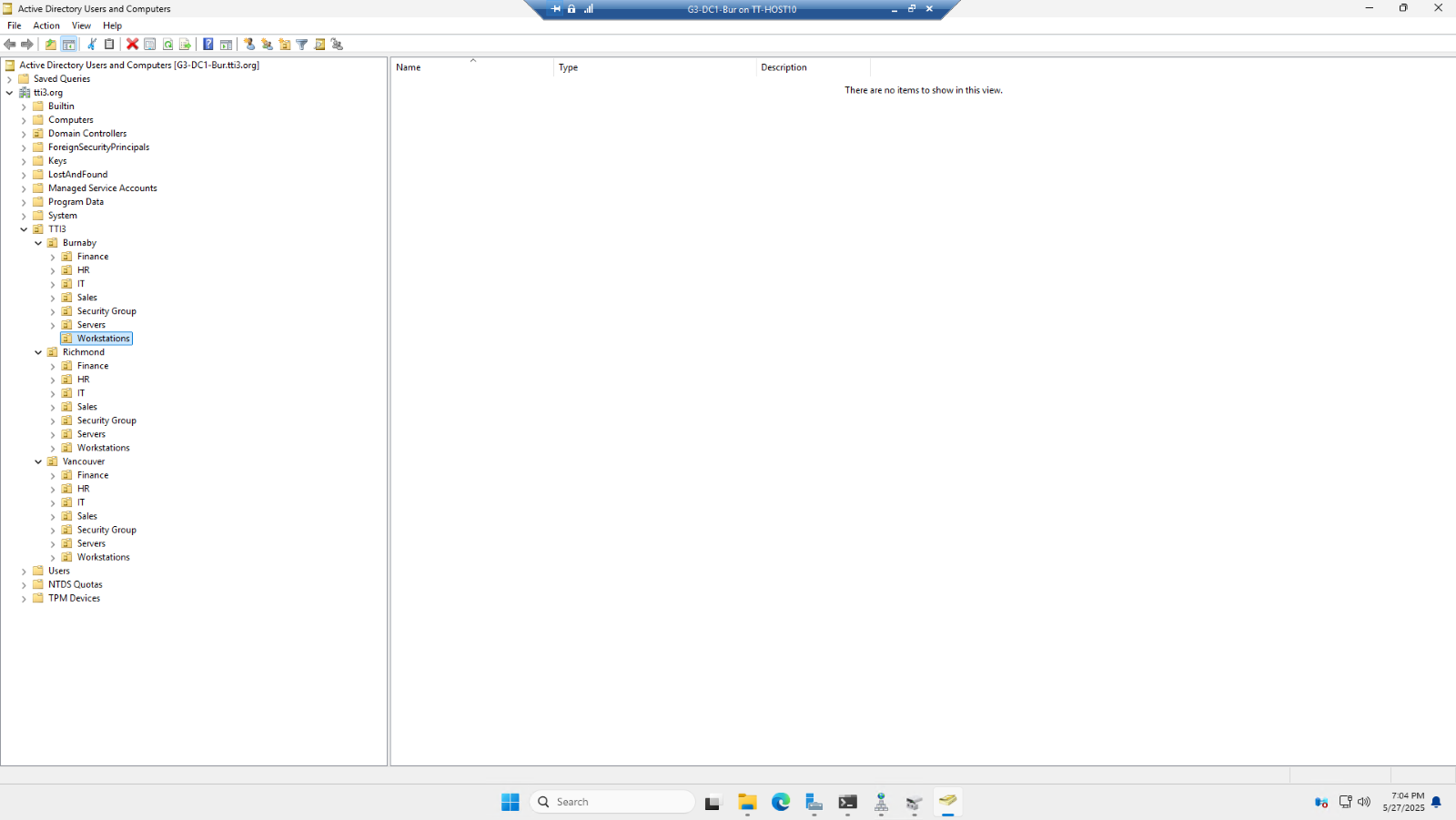
A multiple-site Active Directory (AD) infrastructure was deployed, with domain controllers placed in Burnaby, Richmond, and Vancouver. This design ensures high availability and low latency for authentication and directory services across all campuses. DNS and DHCP roles were assigned to the domain controllers at each site. Organizational Units (OUs) were created for various departments, and Group Policy Objects (GPOs) were applied accordingly to enforce security, drive mappings, and system restrictions.

### Burnaby: AD Sites and Services



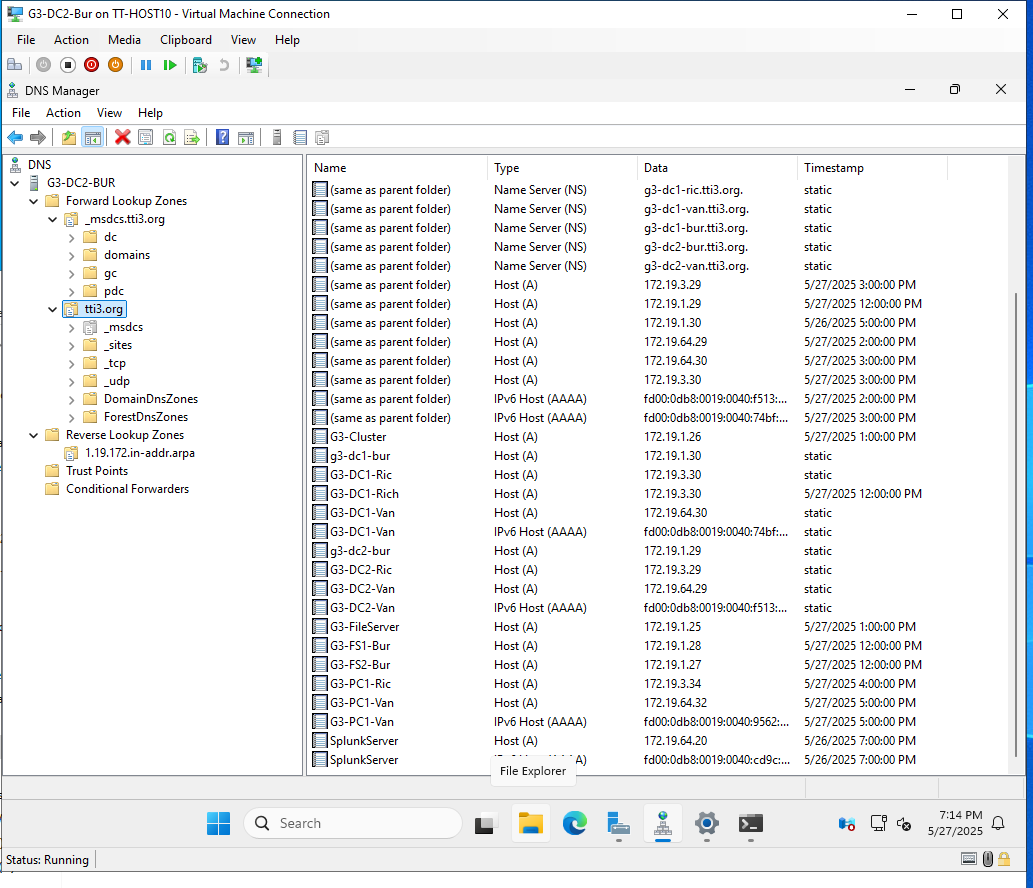
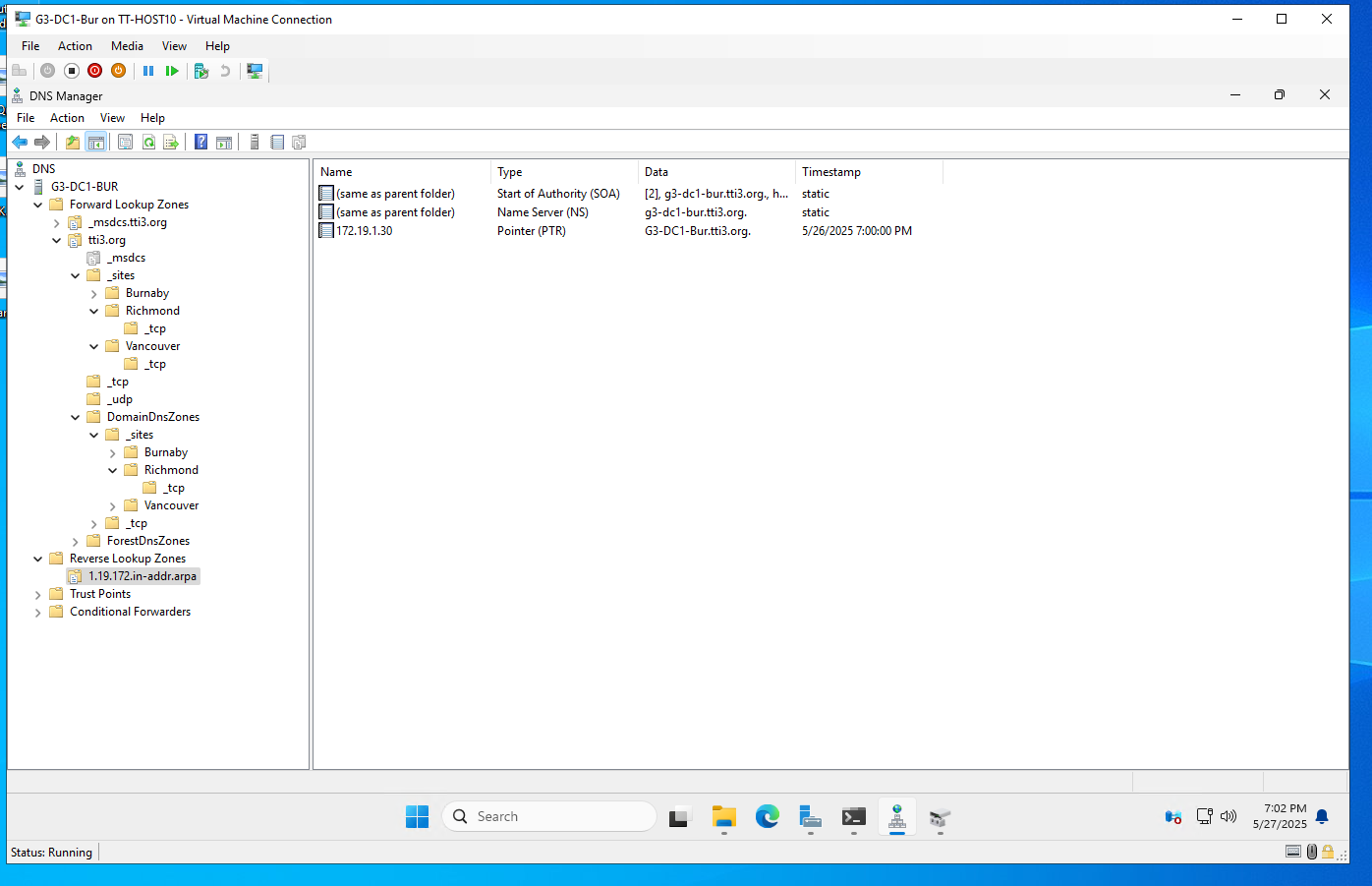
This screenshot demonstrates the successful configuration of Active Directory Sites and Services, showing clearly defined site links between Burnaby, Richmond, and Vancouver. It confirms that inter-site replication is functioning as intended, ensuring both redundancy and efficient replication across campuses.

### Burnaby: Active Directory Users and Computers – OU Design



This highlights the OU (Organizational Unit) hierarchy used to structure accounts and computers by location and department. Each campus (Burnaby, Richmond, Vancouver) has a set of nested OUs including Finance, HR, IT, Sales, Security Groups, Servers, and Workstations. This logical grouping supports delegated administration and targeted GPO application. For example, USB blocking GPOs were applied only to the Workstations OUs, while server maintenance GPOs were restricted to Server OUs. This method follows best practices in enterprise AD design, ensuring scalability, manageability, and security.

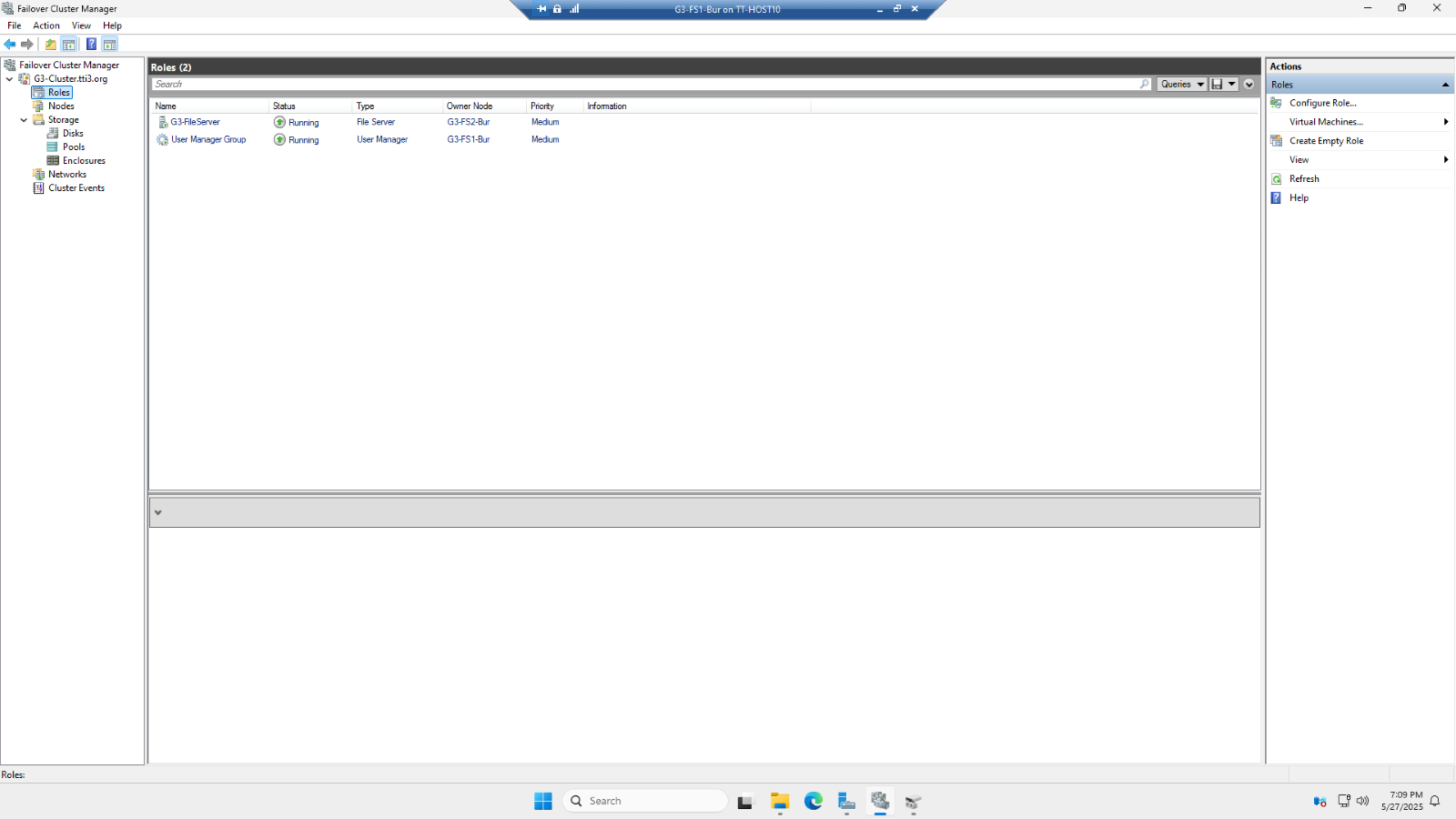
### Burnaby: DNS Configuration



The images above demonstrate the proper setup of forward and reverse lookup zones on multiple domain controllers. Forward zones for tti3.org and site-specific subdomains have been created and populated with accurate Host (A/AAAA) records. The reverse lookup zone 1.19.172.in-addr.arpa has been configured to ensure PTR record resolution. Additionally, the presence of valid Name Server (NS) records across all sites confirms proper DNS delegation and replication.

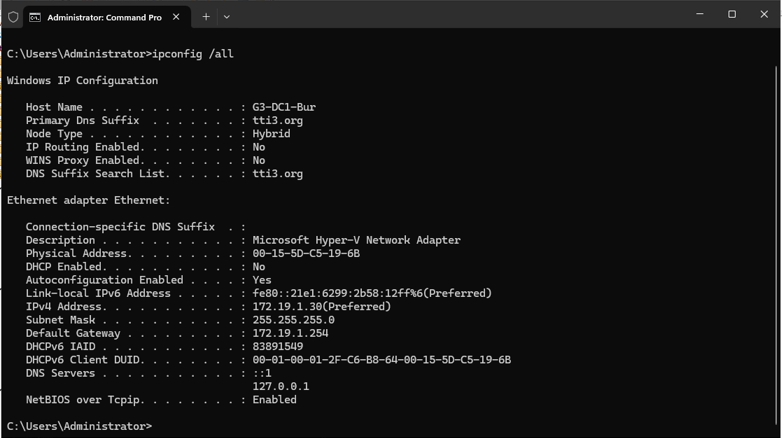
These configurations are essential to ensure reliable name resolution, enable successful domain controller synchronization, and support features such as Group Policy application and secure authentication. Scavenging settings have also been reviewed and configured, helping to automatically clean up stale DNS records and maintain a healthy DNS environment.

### Burnaby: Cluster Manager – File Server Role



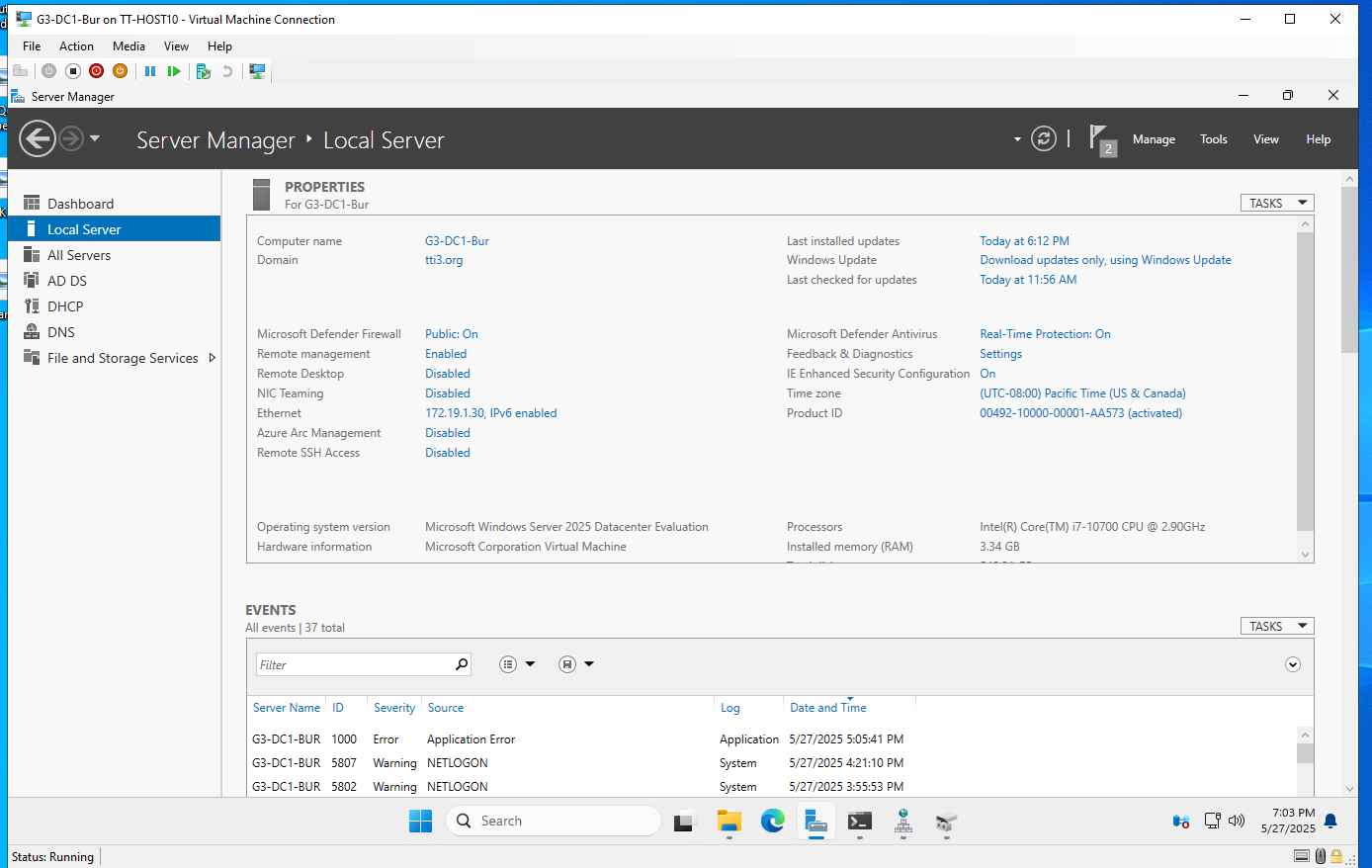
This screenshot verifies the successful deployment of a Windows Server Failover Cluster at the Burnaby datacenter. It shows two active roles — a clustered file server and a user management role — distributed across separate nodes (G3-FS1-Bur and G3-FS2-Bur), confirming high availability. The shared file structure is hosted through the clustered file server, enabling continuous access even during a node failure. This configuration ensures service resilience for critical departmental shares such as HR, Finance, and AllStaff.

### Burnaby: Network Configuration – IP Address Assignment



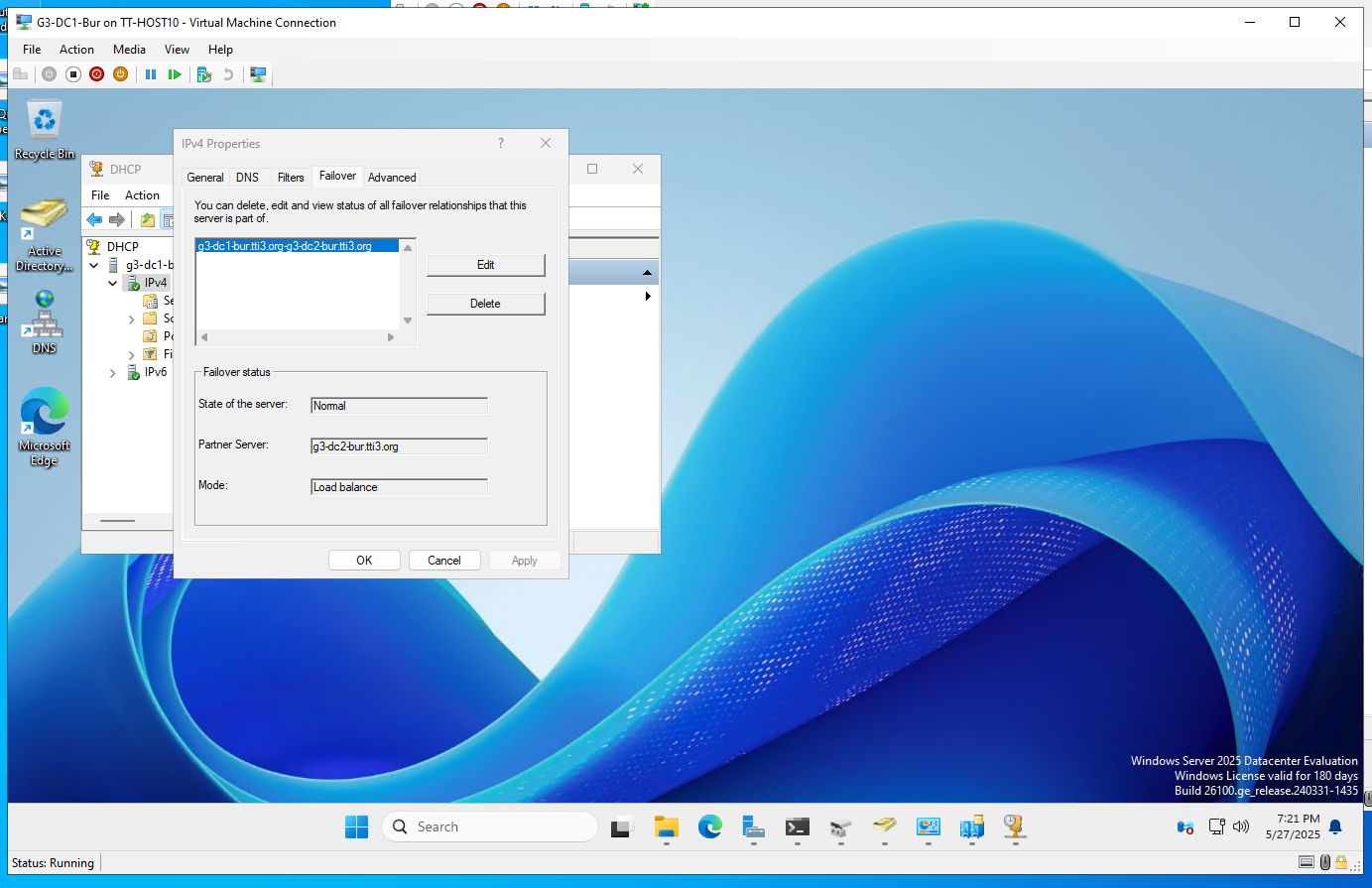
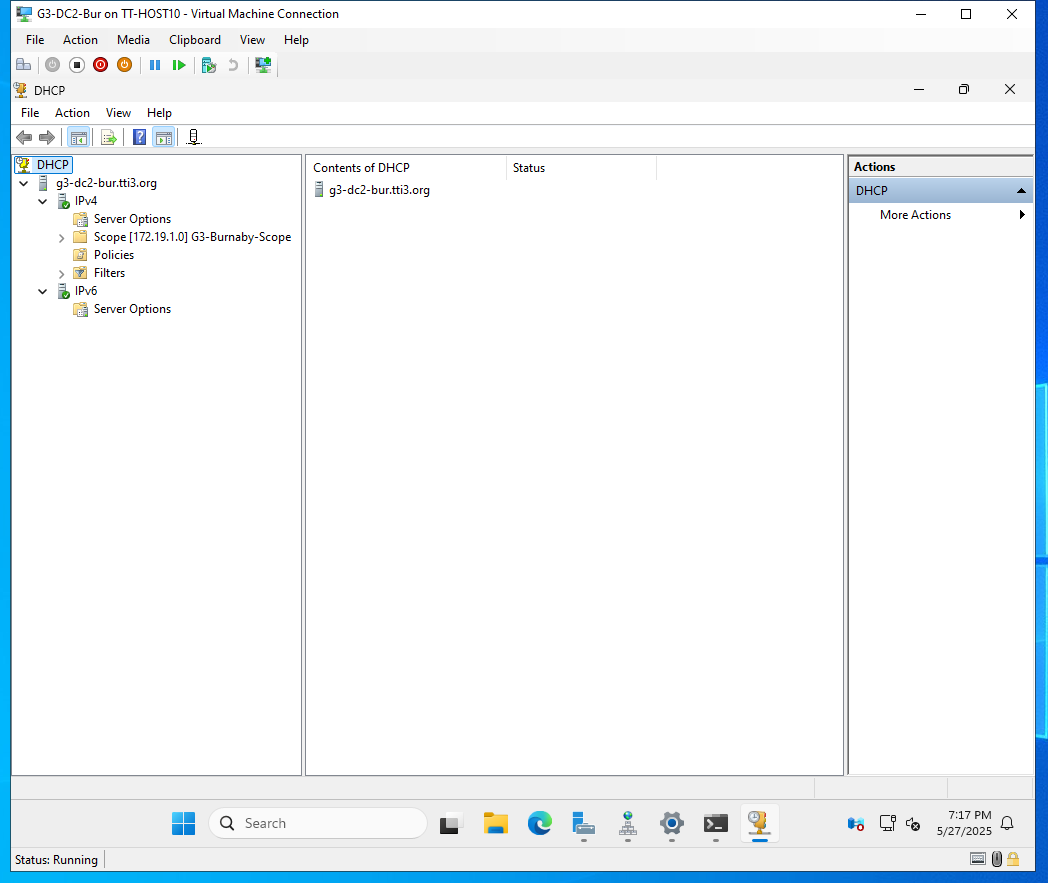
This screenshot shows the result of the ipconfig /all command executed on G3-DC1-Bur. It confirms that the domain controller received its IPv4 address (172.19.1.30) from DHCP, with DNS and gateway information properly assigned. The DNS suffix search list shows integration with the tti3.org domain, and the loopback address is used for internal name resolution. These settings confirm successful network integration and DHCP functionality.

### Burnaby: Server Properties



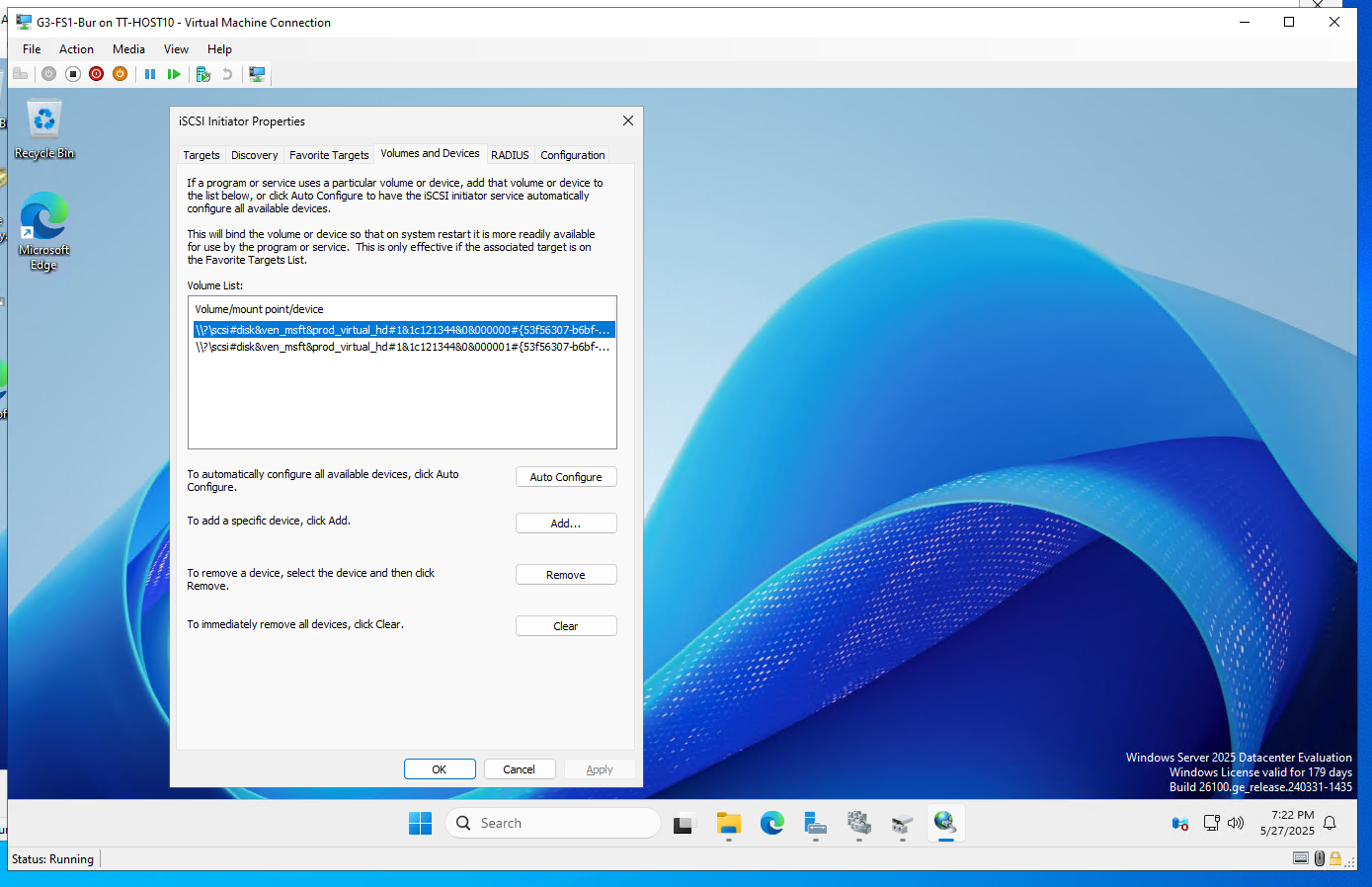
This displays the Server Manager dashboard for G3-DC1-Bur. It verifies that the system is running Windows Server 2025 Datacenter Edition, with domain membership (tti3.org) and real-time protection enabled. Key server roles such as AD DS and DNS are visible, and event logs at the bottom highlight normal system operations, including authentication messages. This overview provides assurance that the server is fully patched, secure, and correctly configured.

### Burnaby: DHCP Scope and Load-Balanced Failover



The first image shows the DHCP configuration on G3-DC2-Bur, which includes the scope 172.19.1.0/24, with options like router and DNS server defined for clients. The second image confirms that DHCP failover is established in load balance mode between G3-DC1-Bur and G3-DC2-Bur. This setup ensures that DHCP leases are available from either server, protecting against single points of failure and supporting uninterrupted connectivity across the Burnaby campus.

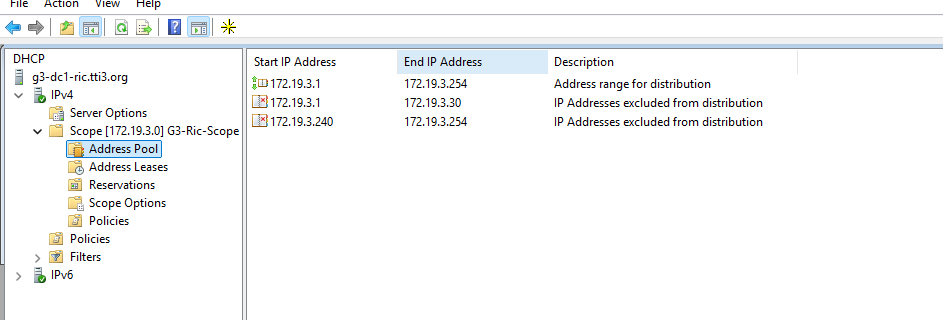
### Burnaby: Cluster Storage Validation – iSCSI Devices



This screenshot shows the iSCSI Initiator configuration on one of the file server nodes. Two virtual hard disks are mounted from a shared SAN over iSCSI, which are then used by the Windows Failover Cluster as shared volumes. This shared storage is a prerequisite for clustered file services and allows data to remain accessible even during node failover. The successful connection to iSCSI targets confirms that the cluster is properly set up to support enterprise file shares.

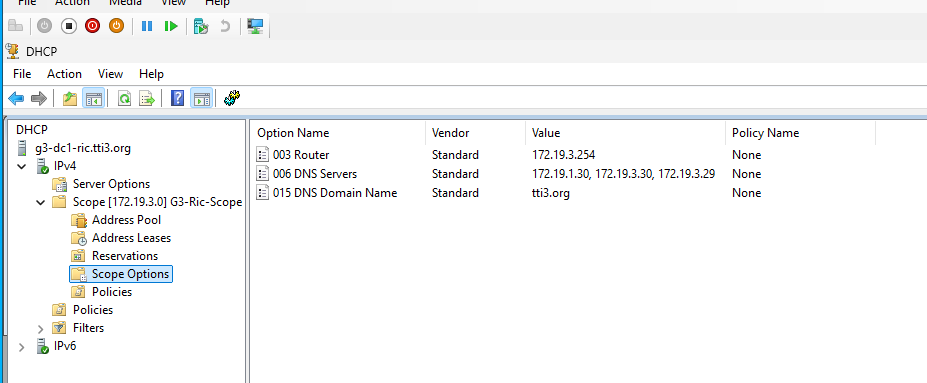
Below is a detailed breakdown of the services validated and implemented in the Richmond site. The configurations mirror Burnaby’s enterprise-grade standards, with emphasis on DHCP scoping, DNS name resolution, GPO enforcement, AD security group structure, and NTFS-based file sharing controls.

### Richmond: DHCP Address Pool and Exclusion Configuration



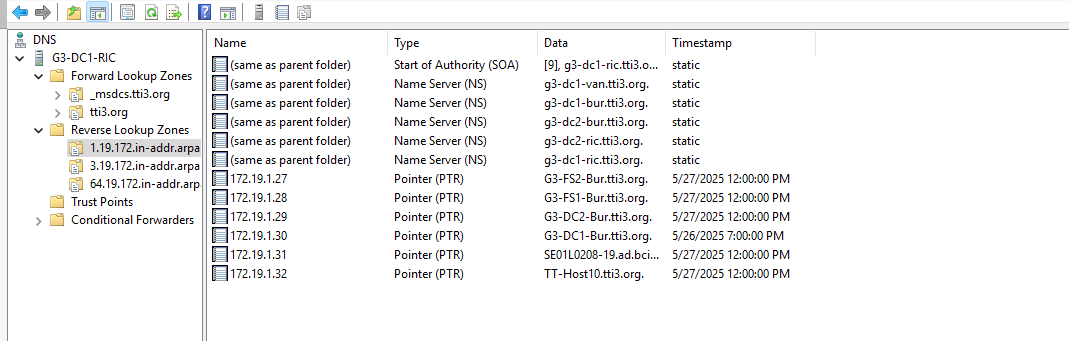
This screenshot shows the DHCP address pool defined on G3-DC1-RIC, which covers the range 172.19.3.1 to 172.19.3.254. Specific exclusions, such as .1 to .30 and .240 to .254, are set aside to reserve addresses for infrastructure devices like servers, routers, and printers. This practice avoids IP conflicts and supports predictable static assignments.

### Richmond: DHCP Scope Options

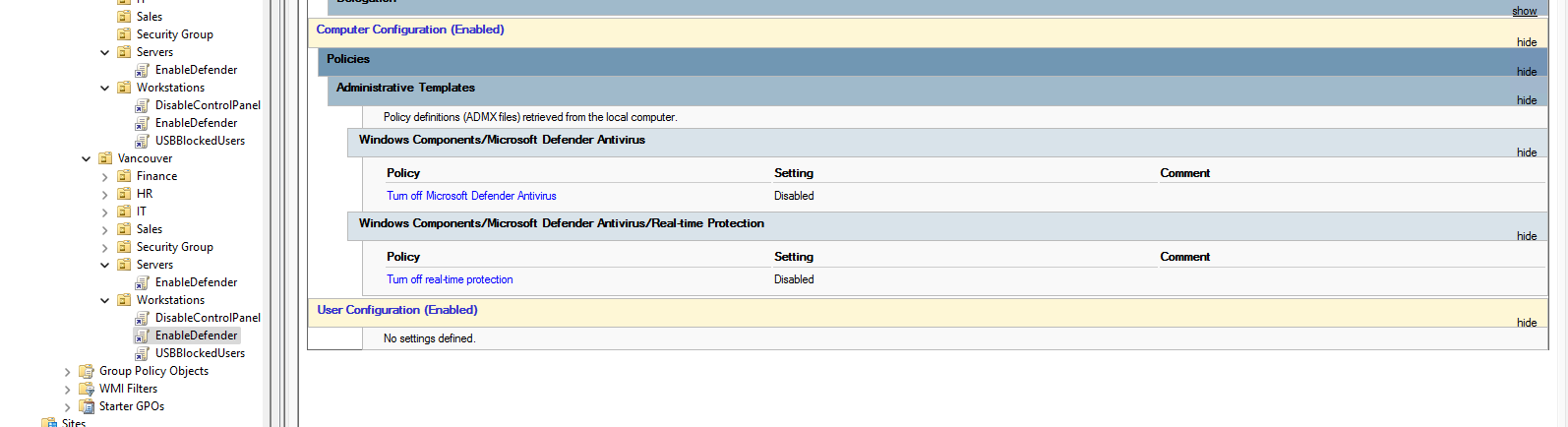


This view from the DHCP console confirms the definition of essential DHCP scope options: the default gateway (router) at 172.19.3.254, DNS servers across sites (172.19.1.30, .29, .30), and the domain name (tti3.org). These options ensure that clients automatically receive network configurations aligned with TTI’s domain infrastructure.

### Richmond: Reverse DNS Zone Validation

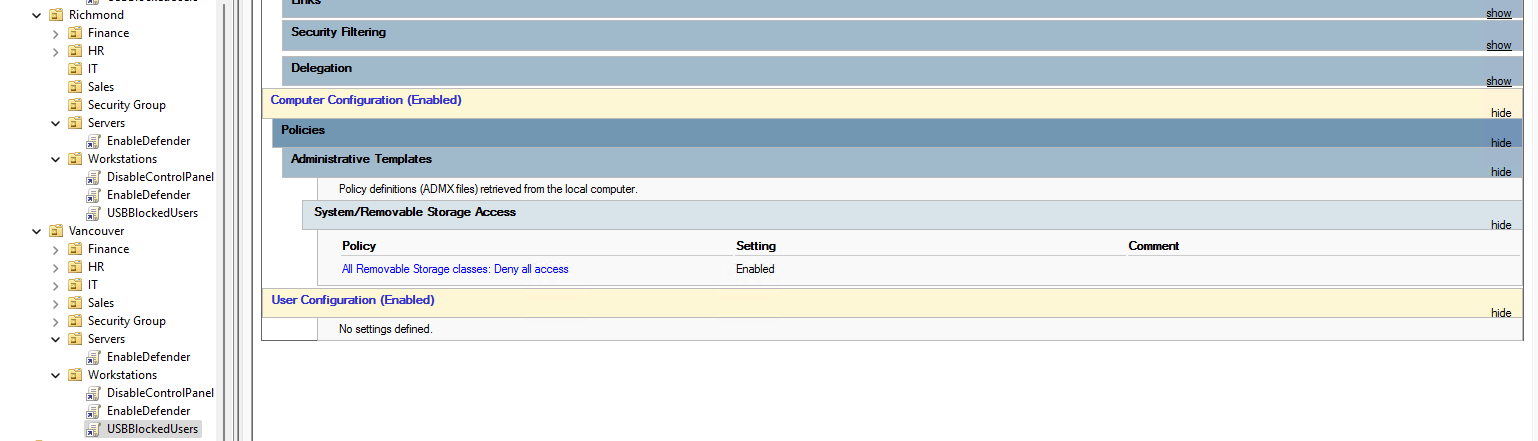
This screenshot from the DNS Manager shows reverse lookup zones configured for Richmond and the broader enterprise. The PTR records confirm that major devices — such as domain controllers and file servers — are resolvable via their IP addresses. This bi-directional resolution supports log auditing, secure access policies, and replication monitoring.

### Richmond: Defender Real-Time Protection GPO



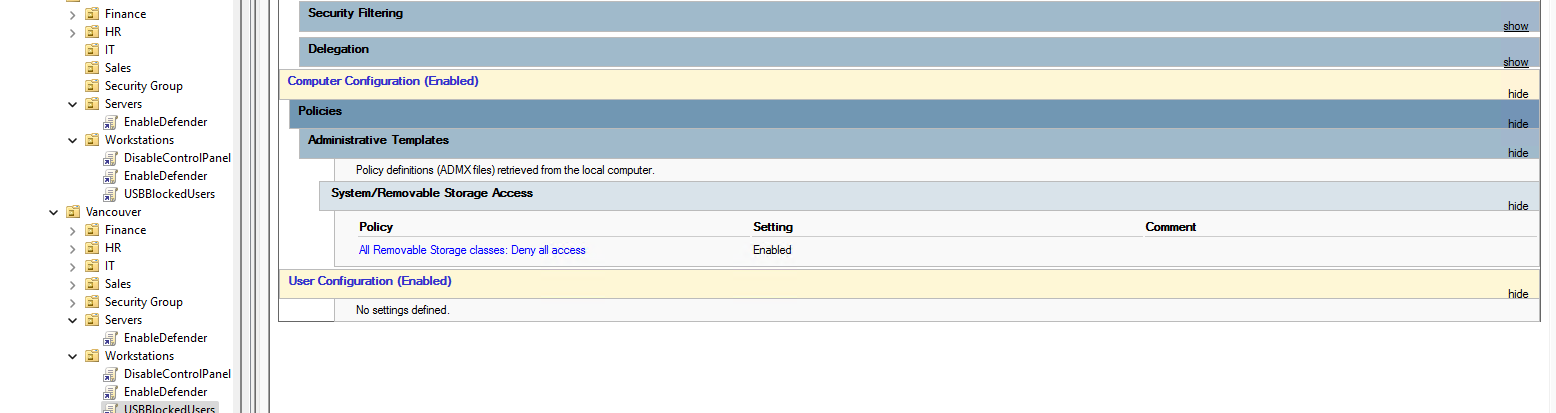
The image shows a GPO applied to Richmond servers that ensures Windows Defender Antivirus, and its real-time protection is enabled. The policies override user settings and prevent tampering, aligning with institutional standards for endpoint protection.

### Richmond: USB Blocking GPO Enforcement



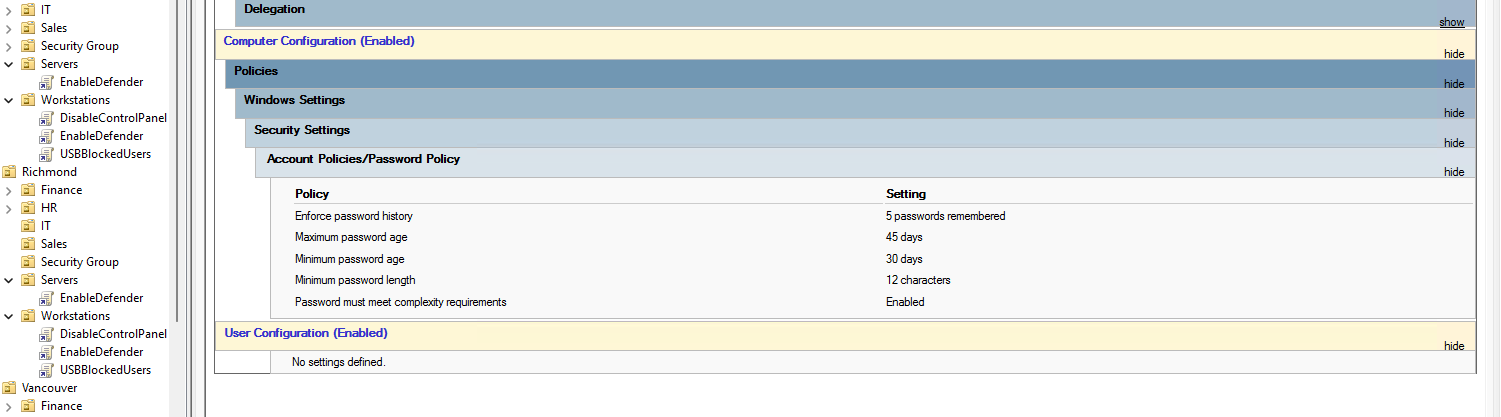
This policy blocks access to all removable storage systems. Applied to the Richmond Workstations OU, it ensures that unauthorized USB devices are not recognized, reducing risk of data leaks or malware infections.

### Richmond: USB GPO – Vancouver Comparison for Cross-Validation



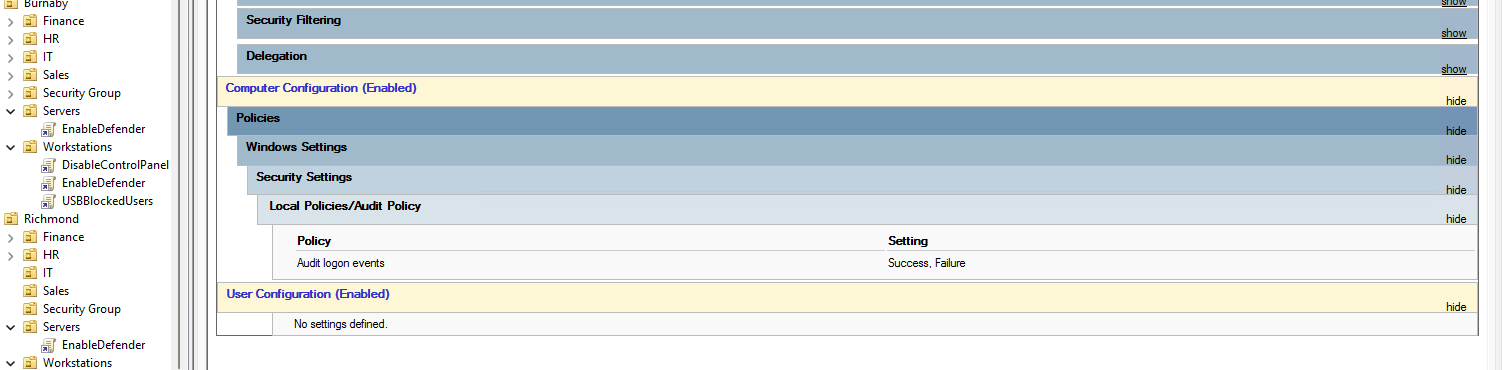
This Vancouver-side is used to compare enforcement across sites. It validates that identical USB blocking policies are consistently deployed to Workstations OUs across all campuses, reinforcing policy uniformity and centralized control.

### Richmond: Password Policy GPO Settings



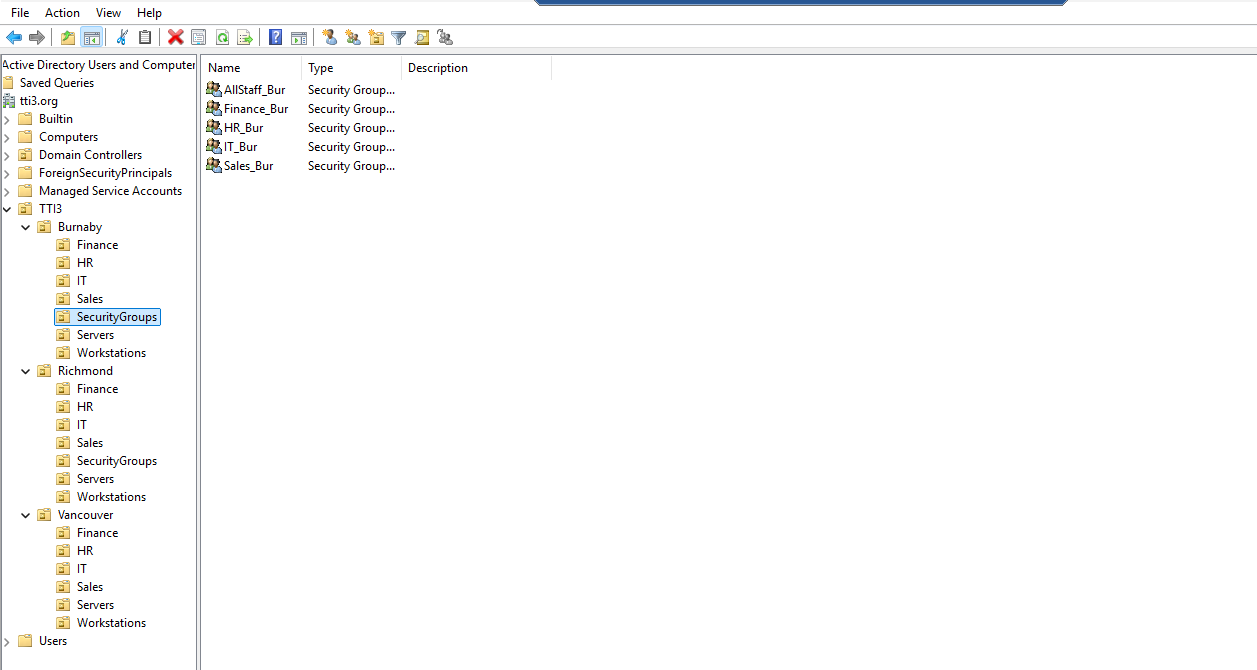
This image shows the Password Policy settings applied to all Richmond users. The GPO enforces password history (5 remembered), maximum/minimum age, complexity requirements, and minimum length. These controls are essential for domain security and compliance.

### Richmond: Audit Policy Enforcement GPO



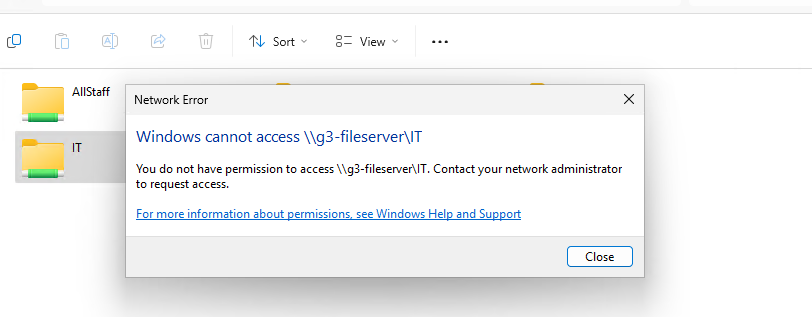
This confirms that a GPO is in place to log both successful and failed logon attempts. This level of auditing is critical for accountability, forensic analysis, and threat detection.

### Richmond: AD Organizational Units – GPO Scoping



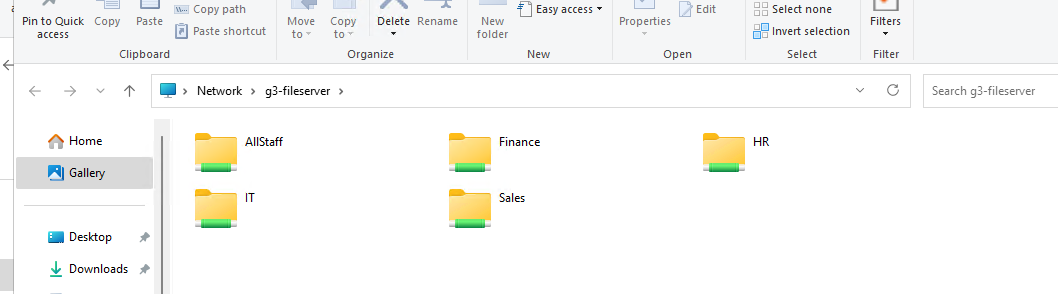
The OU structure is shown again here from the Richmond perspective. It demonstrates how servers, workstations, and departments are logically grouped, enabling site-specific GPO targeting. OUs like USBBlockedUsers or EnableDefender illustrate role-based access control and policy delegation.

### Richmond: NTFS Permissions Enforcement via Security Groups



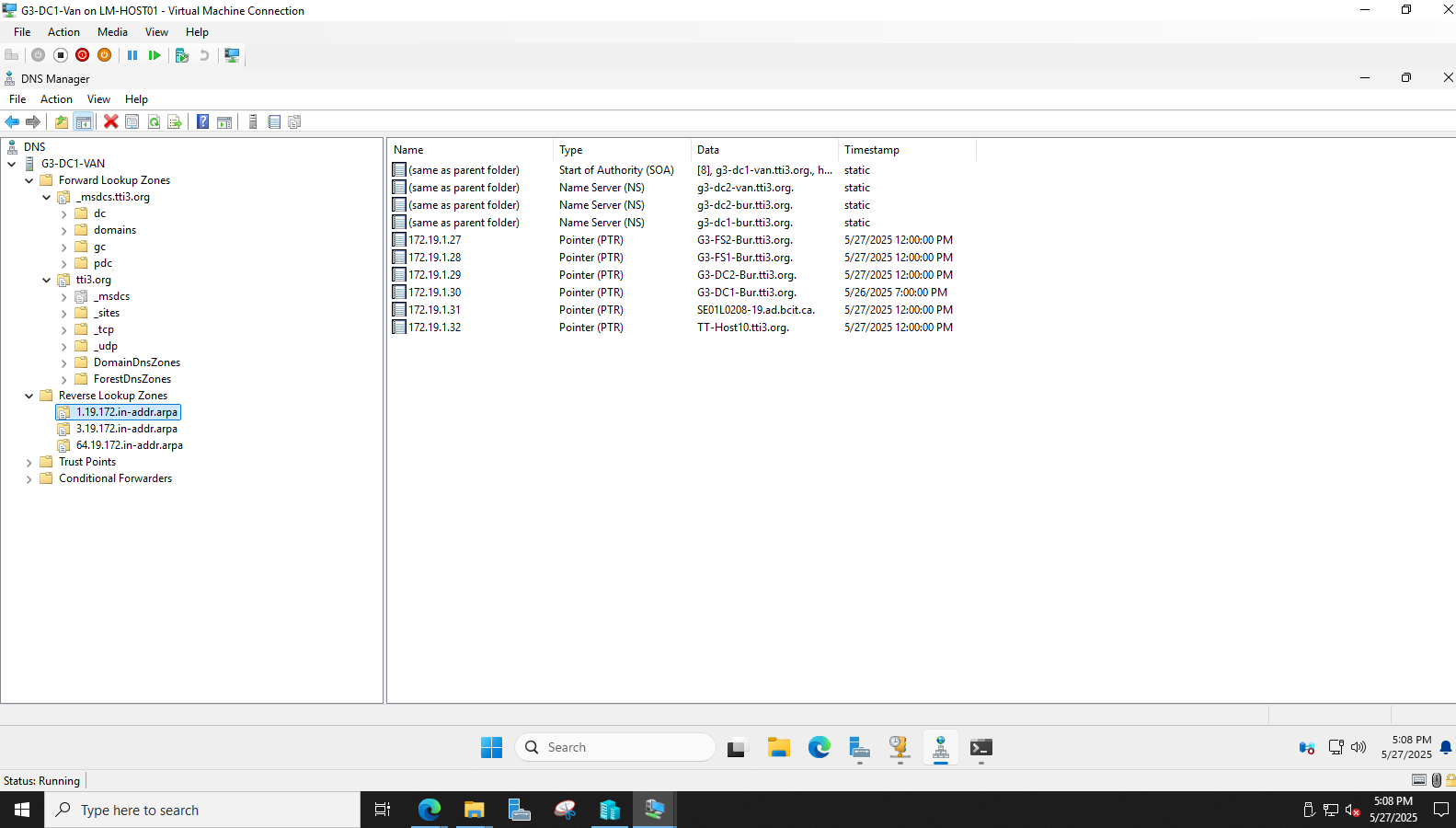
This screenshot validates NTFS file permission enforcement. The user receives a denial message when attempting to access the IT share ([\\g3-fileserver\IT](file:///\\g3-fileserver\IT)) without proper group membership. Access is controlled via AD security groups mapped to departmental shares, ensuring that only authorized users can view or modify sensitive resources.

### Richmond: Departmental File Shares Verification



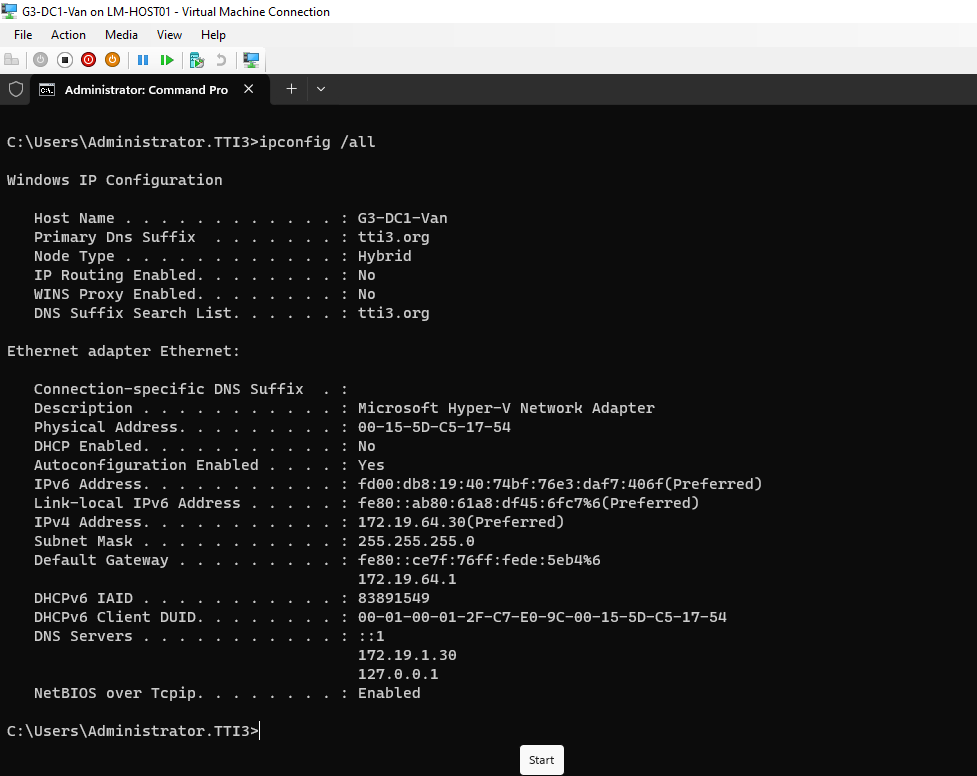
This screenshot shows the shared folders hosted on the clustered file server g3-fileserver. The shared directories — AllStaff, Finance, HR, IT, and Sales — represent mapped network drives accessible by staff based on their group memberships in Active Directory. Each share is assigned NTFS permissions according to role-based access control policies, ensuring that only users in the corresponding security groups can access their departmental resources. This design isolates data between departments, enhances security, and simplifies resource management.

### Vancouver: DNS Configuration – DC1 Forward/Reverse Zones



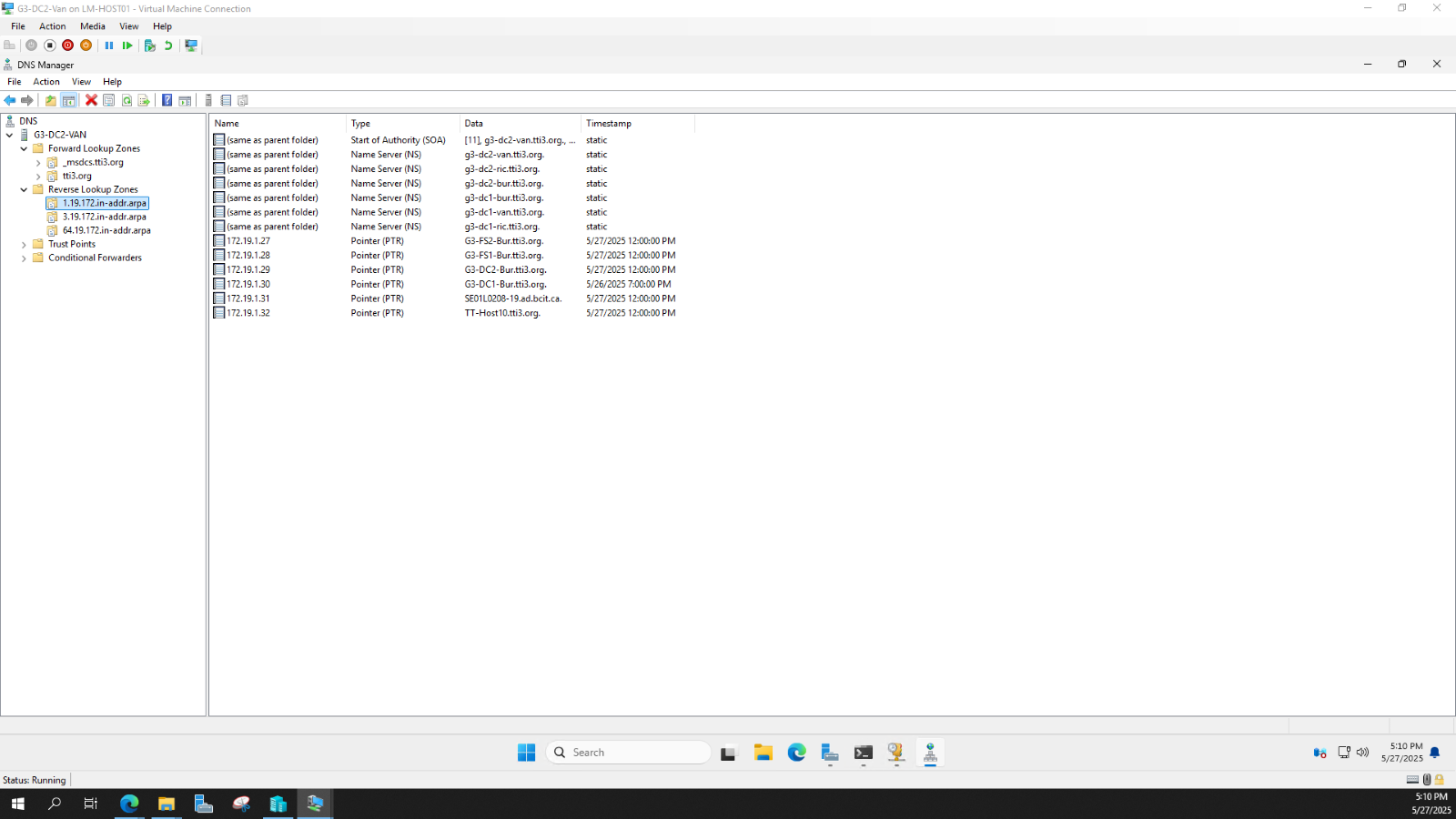
This shows the successful configuration of forward and reverse lookup zones. The presence of authoritative SOA and NS records confirms integration with the domain (tti3.org). PTR records also demonstrate proper reverse resolution for IPs assigned to local resources, supporting troubleshooting, and name resolution.

### Vancouver: DC1 IP Configuration Validation



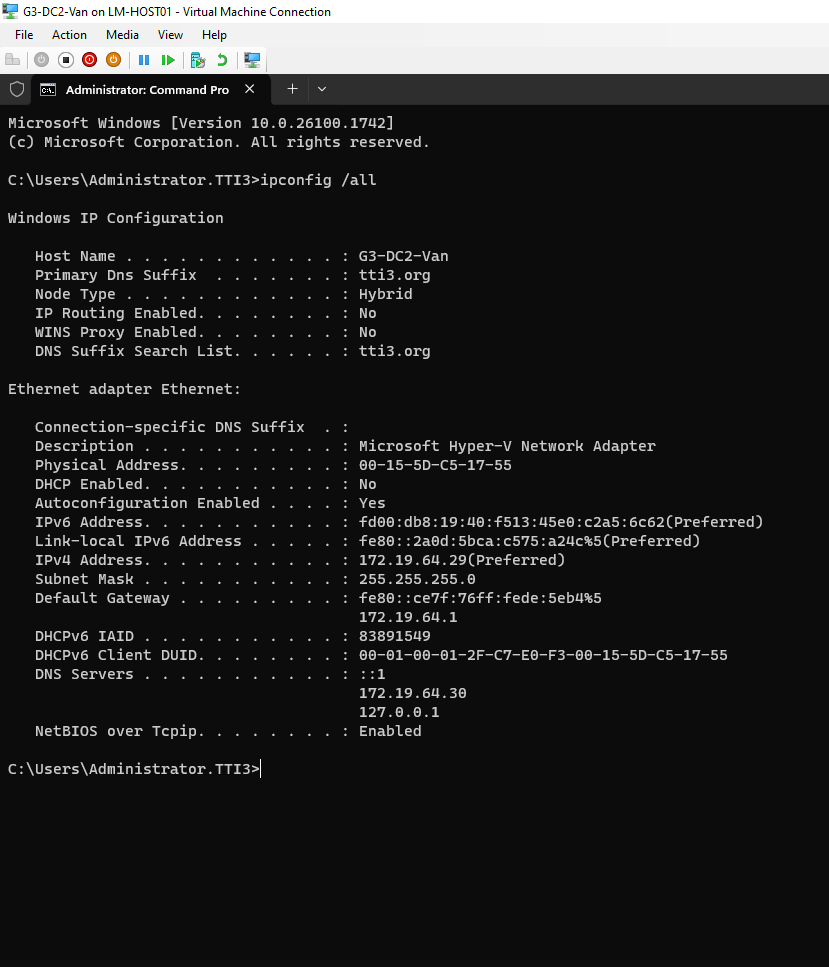
The ipconfig /all result proves that G3-DC1-Van has received a static IPv4 address in the expected subnet (172.19.64.x). DNS is set to local and secondary servers for redundancy, and the domain name and suffix confirm proper binding to tti3.org.

### Vancouver: DNS Configuration – DC2 Forward/Reverse Zones



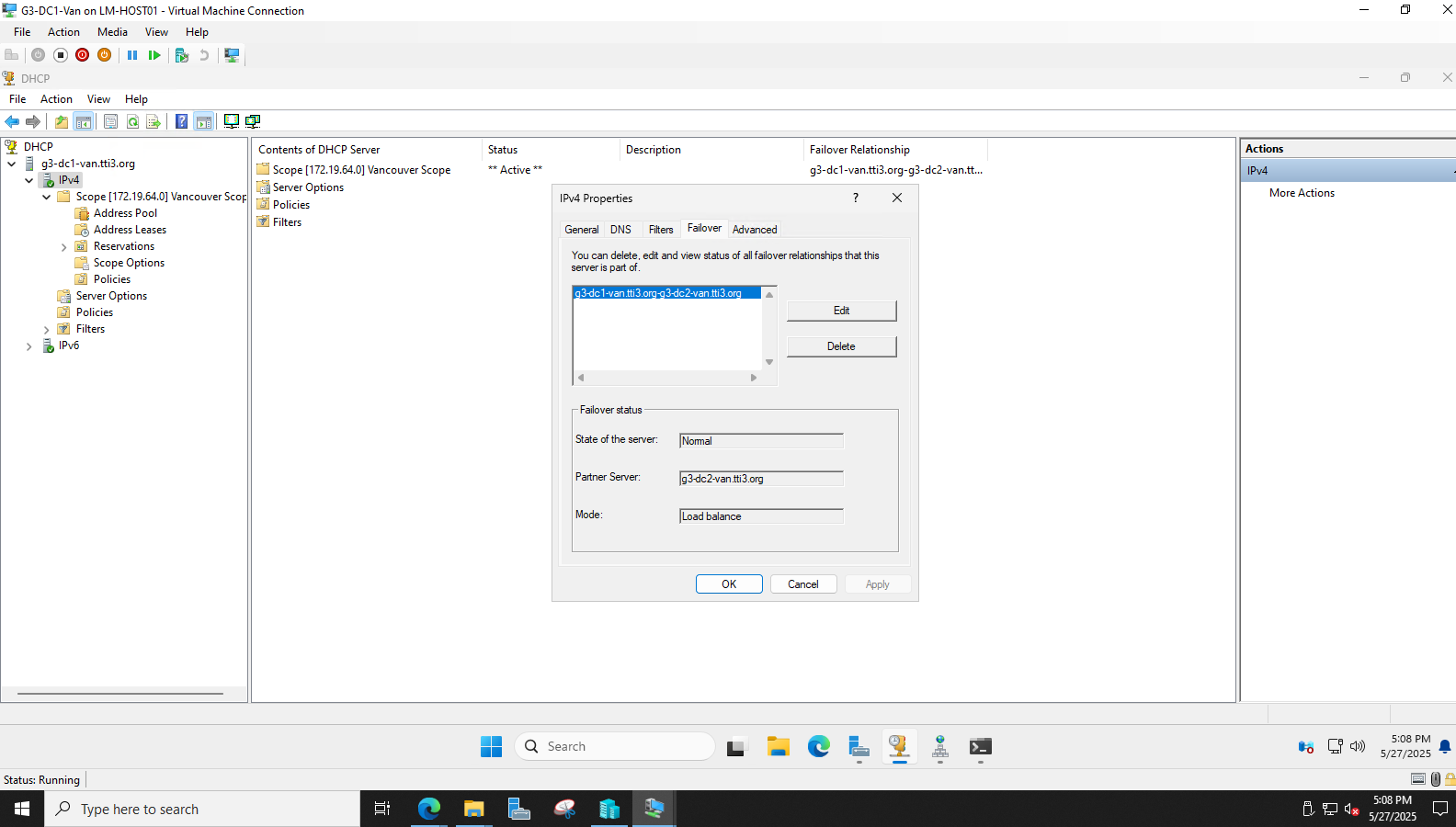
This shows DNS running on G3-DC2-Van, correctly synchronized with forward and reverse zones. NS and PTR entries confirm that records replicate properly between sites. The presence of DCs and member servers from Burnaby and Richmond also confirms inter-site DNS functionality.

### Vancouver: DC2 IP Configuration Validation



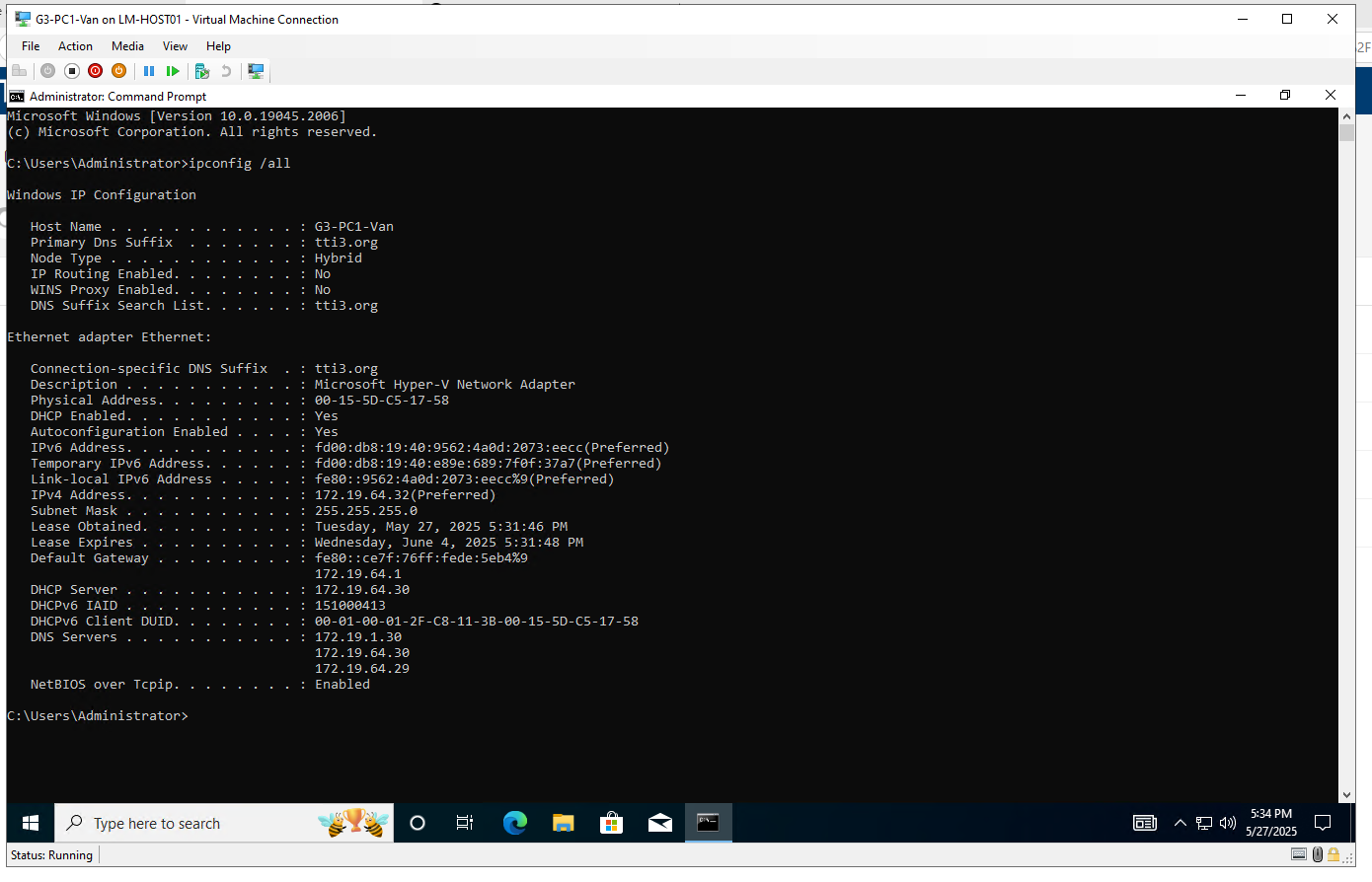
This output validates G3-DC2-Van's address assignment. IPv4 address (172.19.64.x) is correct, and DNS entries point to DC1 and itself for resilience. Domain name suffix confirms domain binding.

### Vancouver: DHCP Scope Failover Verification



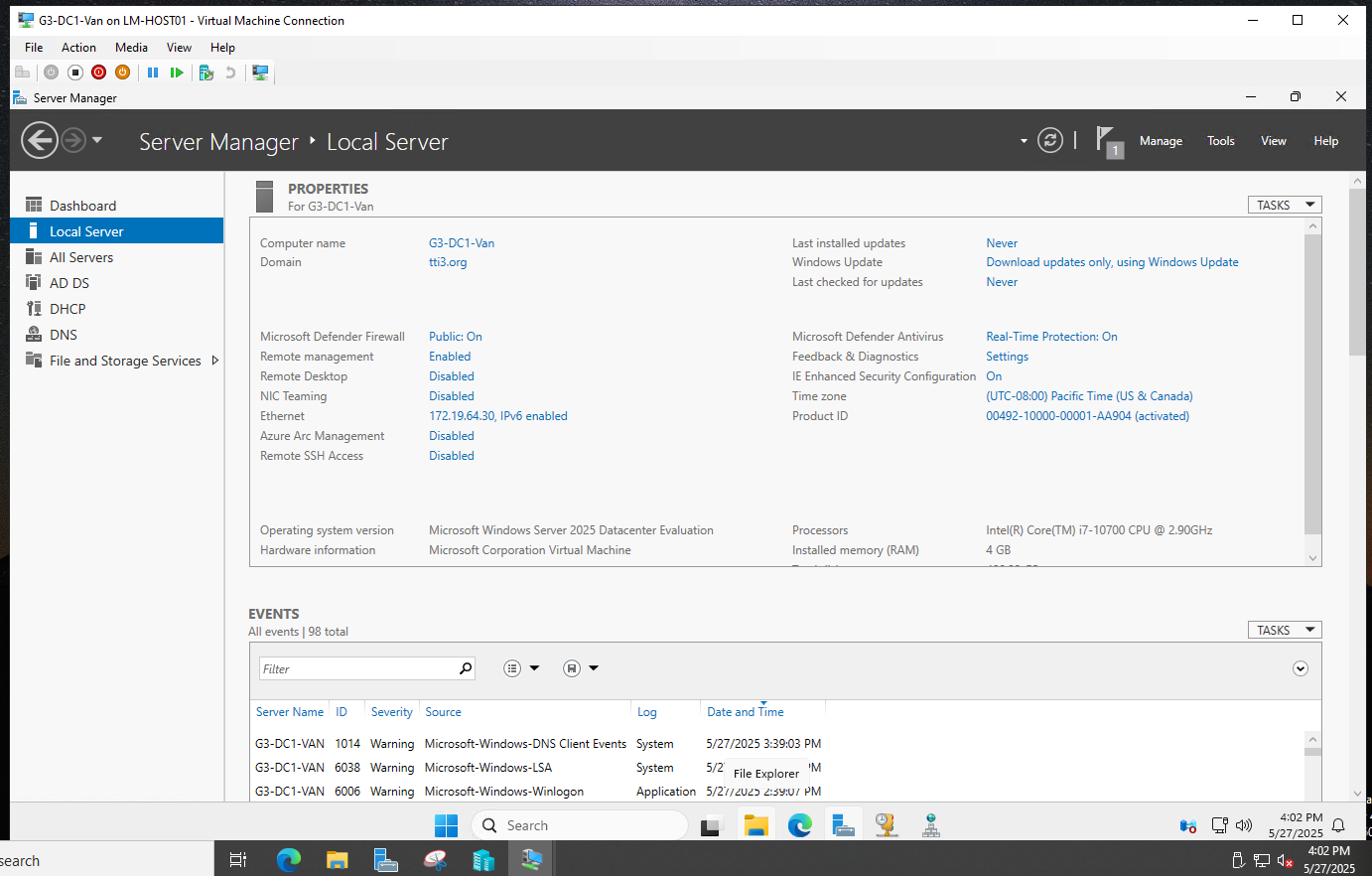
This confirms that DHCP failover has been configured between G3-DC1-Van and G3-DC2-Van in load balance mode. This ensures high availability and fault tolerance for IP address assignments across the Vancouver network segment.

### Vancouver: PC DHCP Lease Verification



A client machine (G3-PC1-Van) has received an IP address from the Vancouver DHCP scope (172.19.64.x). DNS entries and DHCP server values confirm the client is communicating with the correct domain controllers.

### Vancouver: Server Validation – G3-DC1-Van



This Server Manager snapshot shows key configuration details for DC1 in Vancouver: proper domain membership, IP address, OS version, and enabled Windows Defender protection.

### Vancouver: Server Validation – G3-DC2-Van Picture

Similar to DC1, this confirms that DC2 is operational, correctly joined to the domain, and configured with proper security settings and IP information.

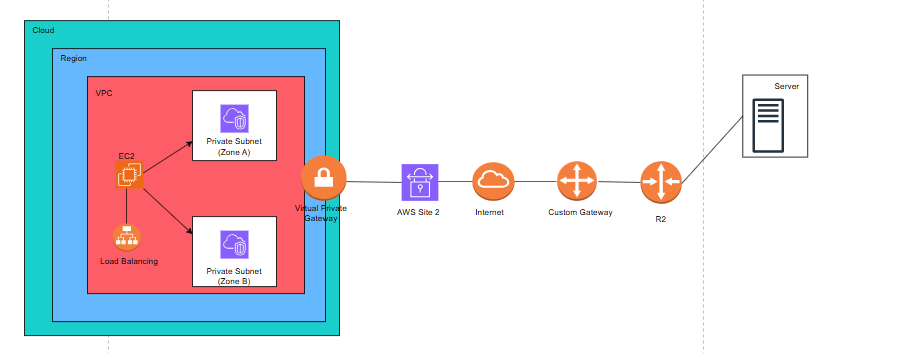
# AWS Cloud Infrastructure Deployment

### Introduction

This report outlines the implementation of a secure, scalable, and highly available cloud infrastructure on **Amazon Web Services (AWS)**. The project was designed to simulate a hybrid enterprise setup by integrating on-premises Cisco infrastructure with AWS cloud services using a Site-to-Site VPN.

The AWS environment includes a **custom VPC**, public and private subnets, EC2 instances launched via an auto scaling group, an Application Load Balancer (ALB), and secure VPN connectivity for hybrid networking.

### Topology



### VPC and Subnet Design

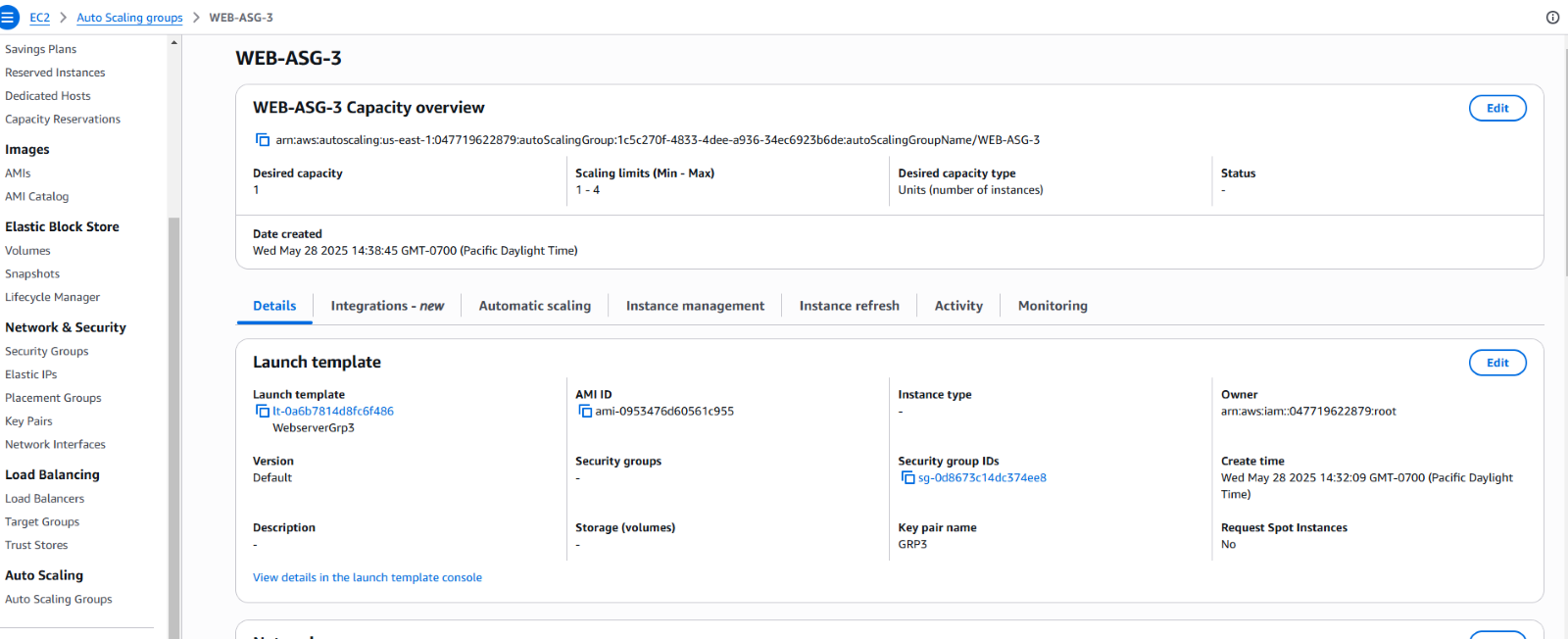
* A custom **VPC** was created with a **10.0.0.0/16** CIDR block. It contains:
* **Public Subnet (10.0.1.0/24)** in **us-east-1a**
* **Private Subnet (10.0.2.0/24)** in **us-east-1b**
* An **Internet Gateway (G3-IGW)** and a **custom route table** (G3-RouteTable) were configured to enable external access for public resources and internal routing for private traffic

### Security Groups configuration

* A **security group (GRP3-SG)** was created with:
* **Inbound Rules**:
  + ICMP (ping) from any IP
  + HTTP (TCP/80) from 10.0.1.0/24
  + SSH (TCP/22) from any IP
* **Outbound traffic**: Fully open by default
* This group was assigned to EC2 instances for controlled access.

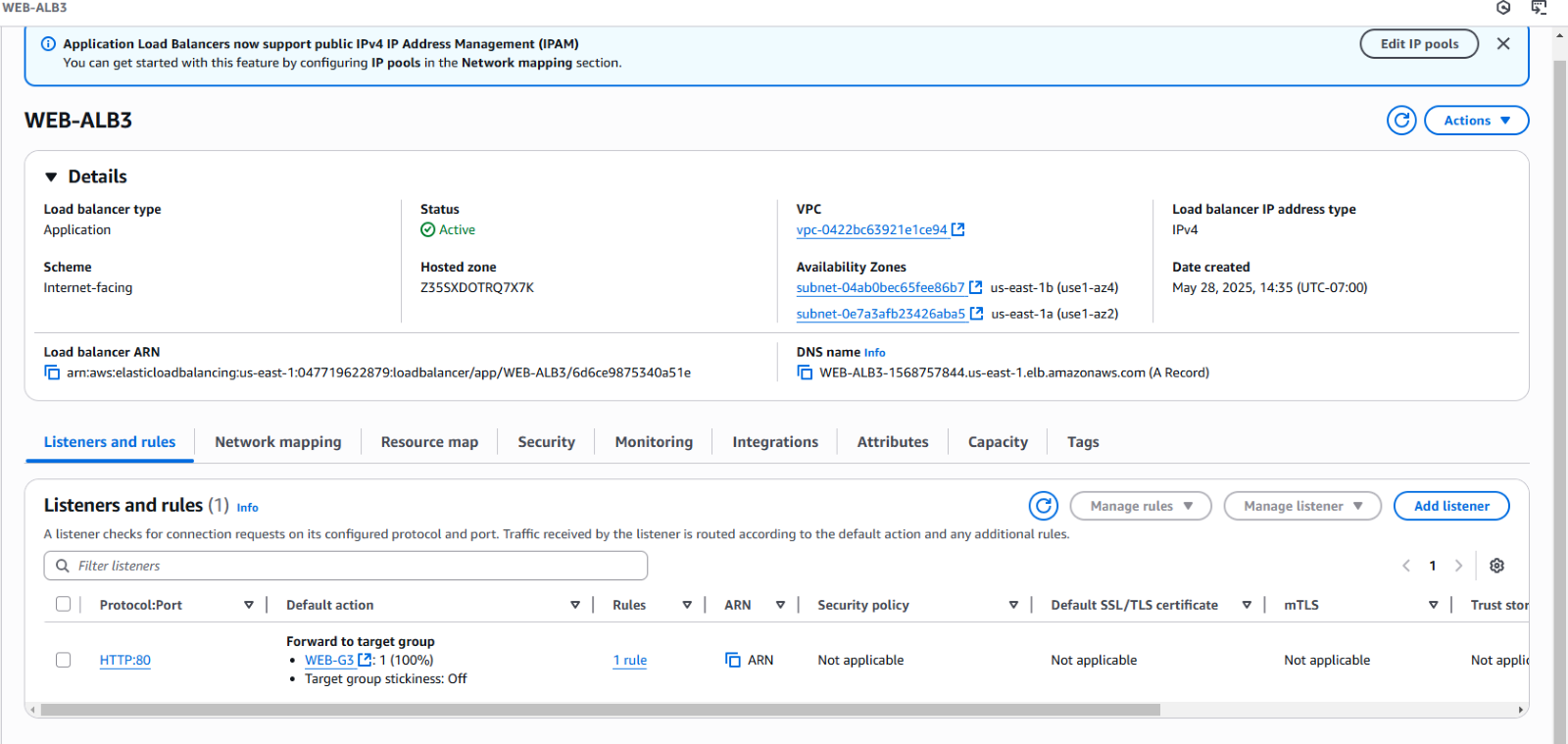
### EC2 Web Server and Autoscaling

* To ensure elasticity and scalability:
* A **Launch Template (WebserverGrp3)** was created to automatically configure EC2 instances as web servers. The script:
* Installs and enables Apache
* Serves a test webpage showing the hostname
* An **Auto Scaling Group (WEB-ASG-3)** was configured to scale between 1–4 instances for flexibility and high availability.



### Application Load Balancing

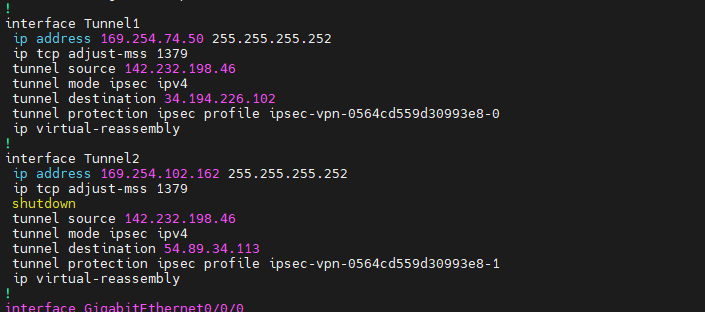
An **Application Load Balancer (WEB-ALB3)** was deployed across two AZs. It listens on **port 80** and routes traffic to a **target group (WEB-G3)** containing Auto Scaling EC2 instances. This setup ensures load distribution and fault tolerance.

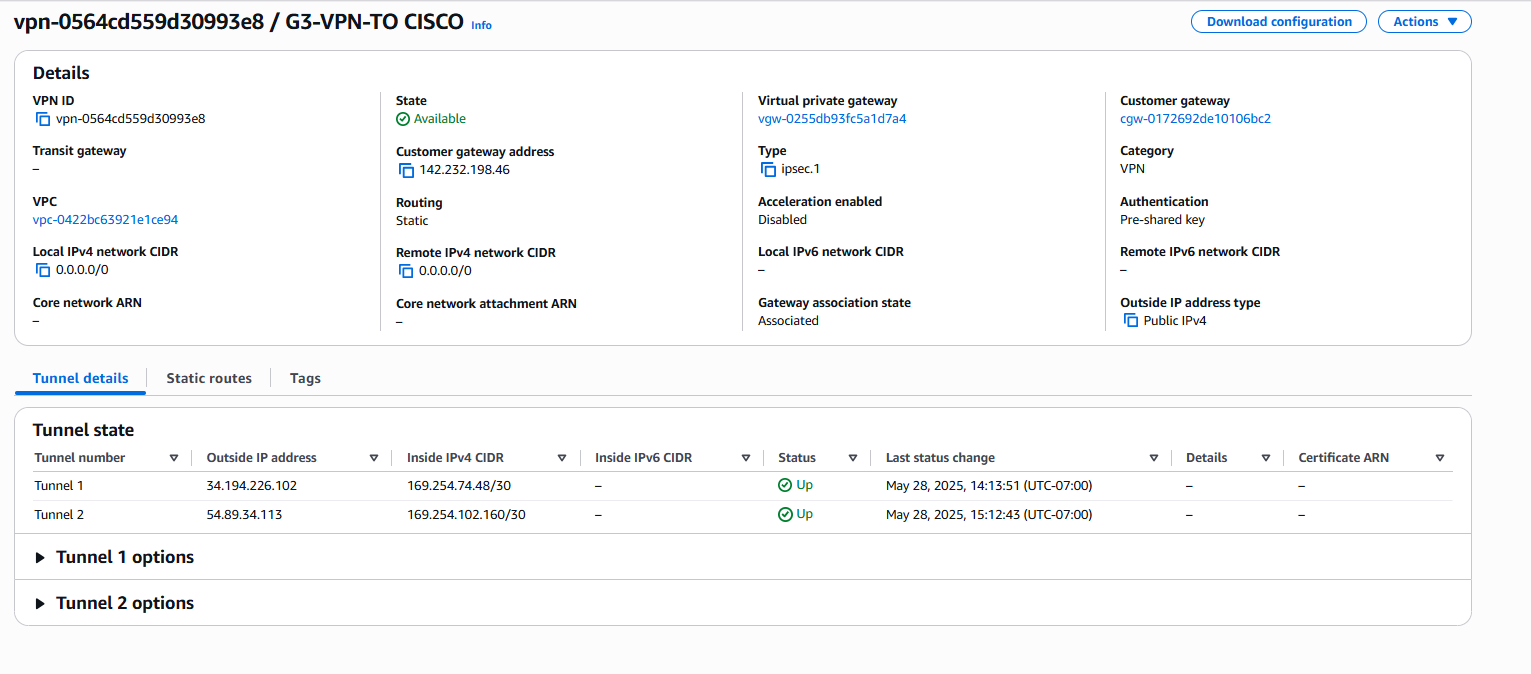


### VPN Configuration (Hybrid Networking)

A **Site-to-Site VPN** was established with static routing between AWS and a Cisco router:

* **VGW:** vgw-0255db93fc5a1d7a4
* **CGW:** cgw-0172692de10106bc2 (IP: 142.232.198.46)
* **Tunnels:**
  + Tunnel 1: 34.194.226.102 ↔ 169.254.74.48/30
  + Tunnel 2: 54.89.34.113 ↔ 169.254.102.160/30



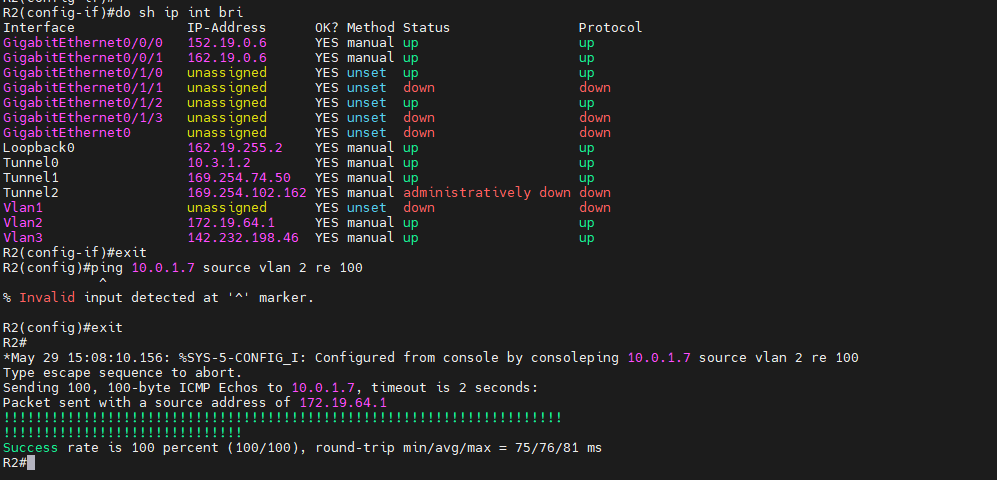
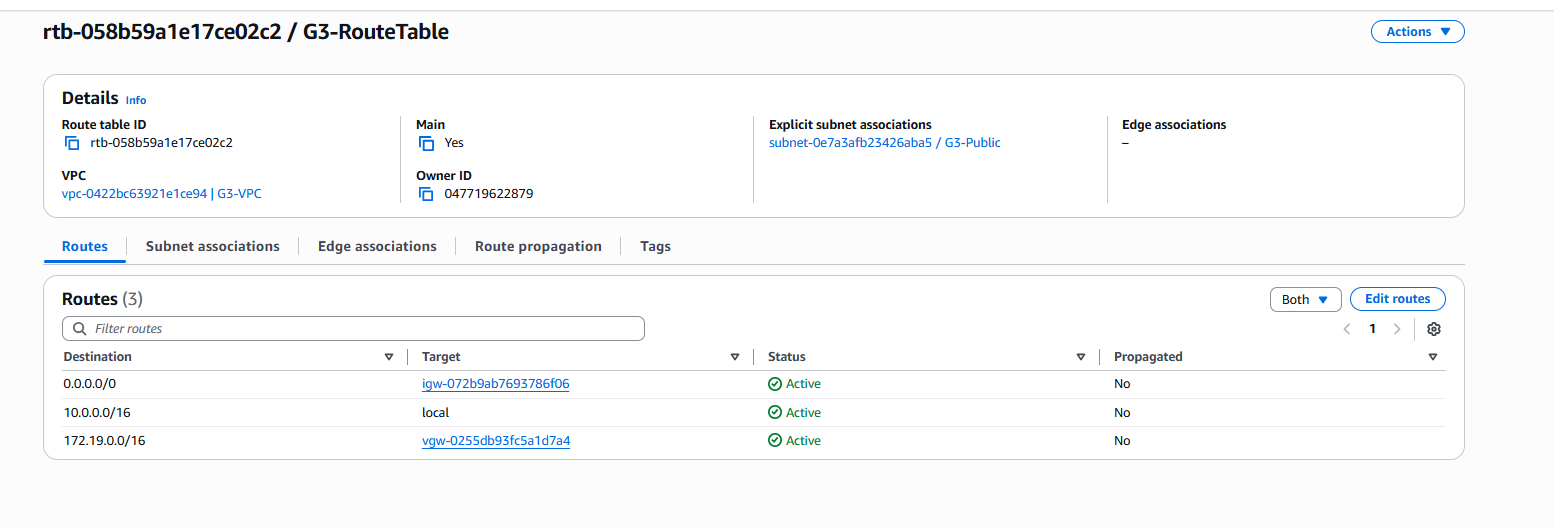


**IPsec/IKEv1** settings with pre-shared keys were configured on the Cisco side using **AES, SHA, and DH Group 14**. Both tunnels were successfully tested using ping.

### Routing and Connectivity

The **route table** includes:

* A default route (0.0.0.0/0) to the Internet Gateway for public access.
* A local route for intra-VPC traffic.
* A route to the **VPN-connected network** (172.19.0.0/16) via the VGW for Cisco LAN integration.



On the Cisco router, **static routes** were added for the AWS subnets, pointing through each tunnel interface for redundancy and failover.

### Additional Configuration Highlights

* **Custom DHCP option set** used for internal DNS resolution.
* DNS resolution and hostname assignment were configured at the VPC level.
* Tunnel lifecycle control and logging were set to default values.
* The **principle of least privilege** was followed for all access and key assignments.

### Conclusion

This AWS infrastructure project successfully simulates a **hybrid enterprise cloud environment**. It includes high availability through load balancing and auto scaling, secure network access via VPN, and follows best practices in VPC design and service isolation.

This deployment ensures scalability, fault tolerance, and secure connectivity between AWS cloud and on-premises resources, laying the foundation for a robust enterprise architecture.