# Technology Solutions Images - Free Download on Freepik, Picture

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | |
| **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](#_Toc1291210558)

[Project Introduction 2](#_Toc1255684884)

[Network Topology 3](#_Toc1712338464)

[Network Overview 4](#_Toc438761381)

[2. WAN Design 5](#_Toc477438932)

[2. LAN Design 7](#_Toc1188806845)

[3. Site-to-Site VPN Configuration 8](#_Toc587119943)

[9](#_Toc1021537837)

[4. Splunk 9](#_Toc1981651627)

[1. Active Directory & GPO Configuration 13](#_Toc405223791)

[AWS Cloud Infrastructure Deployment Report 30](#_Toc305713162)

[Introduction 31](#_Toc1434821087)

[1. VPC and Subnet Design 31](#_Toc1263944112)

[2. Security Groups configuration 31](#_Toc1886441099)

[3. EC2 Web Server and Autoscaling 31](#_Toc1669783576)

[4. Application Load Balancing 31](#_Toc1792050575)

[5. VPN Configuration (Hybrid Networking) 32](#_Toc739491188)

[6. Routing and Connectivity 32](#_Toc847004517)

[7. Additional Configuration Highlights 33](#_Toc87286676)

[Conclusion 33](#_Toc445718336)

# Project Introduction

With rapid global interconnectivity, the demand for secure and highly available as well as scalable enterprise networks is greater than ever. The Technical Training Institute of BC (TTI) is a market leader in education, operating several campuses in Burnaby, Downtown Vancouver, and Richmond. It has come to our attention that TTI fundamentally needs to update its IT infrastructure in order to serve modern operational and instructional requirements. In response to these concerns, our team of IT consultants crafted a detailed enterprise network design that seeks to revitalize TTI's infrastructure into a scalable, robust, and efficient digital environment.

This case study is based on real-world tendering simulating a consulting project where every student group acts as a separate consulting firm to develop a proposed documentation and implementation network solution. Our design features LAN and WAN connectivity across several sites, remote access, data segmentation, distribution of central control, and high availability clusters. Following the industry best practices, we are supported with Cisco networking, Microsoft Active Directory, secure firewall appliances, and other leading technologies, demonstrating TTI's flexible, practical, and scalable solutions.

Integrating centralized logging through Splunk with Active Directory replication for regionally dispersed sites, implementing high availability for DHCP and DNS, as well as role-based access controls meets functional and security compliance. Our proof-of-concept implementation verifies each technical component and checks the feasibility of the proposed solution in the working enterprise environment.

This report captures the technical reasoning of the design and implementation processes along with the advantages that our architecture would bring to TTI's future business activities. With this effort, we demonstrate applying learned concepts in a collaborative setting designed to simulate real world situations.

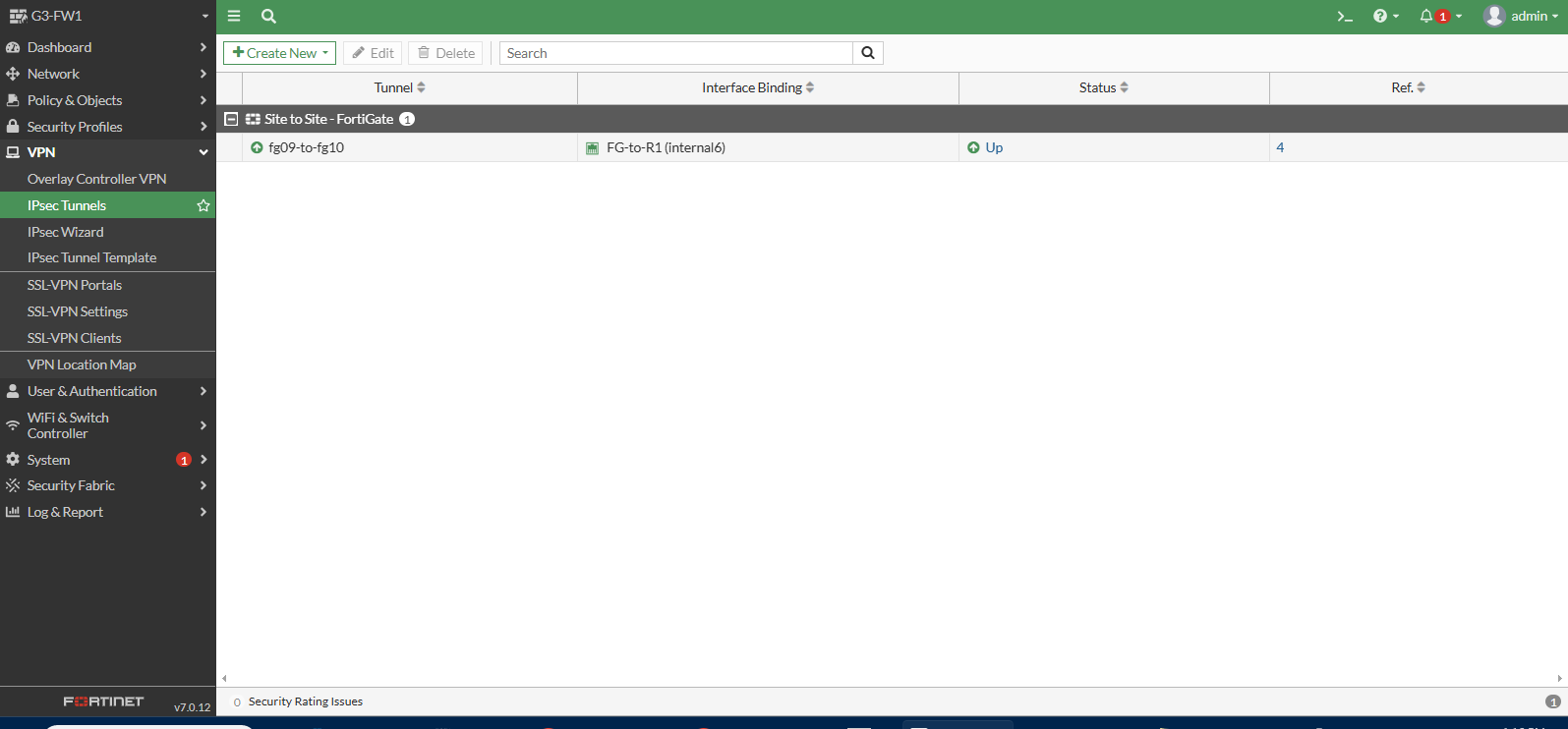
# Network Topology

# Network Overview

#### Site-to-Site VPN Configuration

**Phase 1 Objective**: Establish secure VPN tunnels using FortiGate firewalls between Vancouver and Burnaby.

* FortiGate Group 3 assigned firewalls: Firewall 9 (Vancouver), Firewall 10 (Burnaby)
* Tunnel Interface with IPsec Phase 1/2 configured
* Static routes and security policies defined



### 

#### Splunk

* **Devices**: FortiGate, Cisco Routers
* **VMs Used**:
  + Splunk Forwarder VM
  + Splunk Server VM
* **Log Forwarding**:
  + SNMP and Syslog configured on both firewalls and Routers
  + Logs forwarded to Splunk Forwarder and visible on Splunk Server
* **Dashboards**:
  + Created individual dashboards for each firewall with metrics and event logs

### Project Objectives and Scope

The reason this project exists is to create a resilient, secure and scalable enterprise network infrastructure that optimally and fully serves the academic, administrative, and operational activities in TTI’s multi-campus structure. The design served does both the present needs and the future growth due to persistent availability in uninterrupted access, management, and policy application(audit) throughout all campuses.

Our works includes the design of the Layer 2 and Layer 3 topologies, secure site-to-site WAN access through the BCNET/CANARIE infrastructure, and the Active Directory service integration with DNS, DHCP, GPO, and other IAM services for control and policy enforcement. Moreover, we are implementing a secure Internet Edge with Cisco ASA appliances, VLAN Firewall segmentation for departmental isolation, and central Splunk logging fort real-time monitoring and fault detection.

Each element of the network is realizing high availability and responsiveness such that they are always available and when an outage occurs the services are still maintained and smoothly delivered, sustain TTI's digital operations.

### Problem Statement and Proposed Solution

With its campuses located in Burnaby, Richmond, and Downtown Vancouver, the Technical Training Institute of BC (TTI) is an emerging educational institution that is facing numerous network problems related to expansion, security, and central management. The existing system does not have a cohesive framework to cross regional borders for servicing the network, which results in poorly coordinated and inefficient services at different locations. The absence of a uniform addressing scheme leads to conflicts in IP addresses as well as unproductive and elaborate routing paths. Additionally, TTI's dependence on IPv4 along with legacy security risks due to insufficient segmentation of Local Area Networks (LANs) increases the risk of security breaches and performance bottlenecks. Communication between different sites is erratic and prone to failure; unhindered central directory services stymie the enforcement of important security controls throughout the entire institution.

Motivated by these issues, we developed a network architecture that is modular, secure, and scalable. The architecture incorporates both IPv4 and IPv6 addressing, centralized services with Microsoft Active Directory, and secured WAN communication over BCNET/CANARIE infrastructure. Department traffic will be VLAN segmented, and service availability will be ensured through high-availability solutions such as DHCP failover, redundant domain controllers, and clustering to enable 24/7 operational continuity. Deployment of Cisco ASA firewalls will protect the Internet Edge, and centralized log management will be performed using Splunk for complete environment visibility and alerting. The solution is compliant with TTI’s operational needs while ensuring minimal change will be needed later for cloud integration, ISP transition, or other future requirements.

TTI’s inter-campus communication is one of their priorities and concerns. BCNET/CANARIE, for example, has fiber and copper links between campuses, but they are functioning below their optimal potential in regard to bandwidth, routing security, and path efficiency. We are proposing the construction of additional IPv4-contained cross zonal transport using MPLS Layer 3 VPNs to produce redundancies within the WAN paths with Provider Independence. For this, we will use OSPF or BGP in dynamic routing to allow inter and intra domain route fail over and outage recovery during outages.

Another significant concern is **network segmentation and security**. Currently, different departments (e.g., HR, Finance, Sales) operate within flat broadcast domains, making it easy for threats to propagate. We address this by introducing **VLAN-based segmentation**, where each department is isolated using Layer 2 boundaries, and **inter-VLAN routing is handled at the distribution layer** with ACLs to control access. Rogue device insertion and unauthorized network access are mitigated using DHCP snooping, port security, and centralized control via a secured Network Operations Centre (NOC) located at the Burnaby campus.

The **Active Directory (AD) infrastructure** is another critical element of our proposal. We are deploying a **single-domain, multi-site AD topology** with domain controllers at each campus to ensure local authentication, reduce latency, and maintain service availability in case of link failure. Each campus will have its own Organizational Units (OUs) for servers and workstations, and Group Policy Objects (GPOs) will be used to enforce enterprise-wide security policies. Users will be created for each department, and permissions will follow the principle of least privilege. GPOs will enforce password complexity, restrict USB usage, configure Windows Defender, and map shared drives based on group membership.

**High availability and redundancy** are central to our network services strategy. DHCP will be configured in a failover mode using Microsoft’s DHCP failover feature. DNS will have scavenging enabled, reverse zones created, and all NS records validated. Furthermore, we will implement **Windows Server Failover Clustering** at the Burnaby datacenter. A clustered file server will provide departmental shares (e.g., HR, Finance, AllStaff) with NTFS permissions controlled via AD security groups. This ensures that users always have access to critical files even in the event of hardware or service failure.

To support operational excellence and troubleshooting, we are deploying **centralized logging using Splunk**. All logs from Cisco equipment, domain controllers, and workstations will be forwarded to a Splunk Universal Forwarder, which will then transmit them to a centralized Splunk server. This ensures complete visibility, real-time alerting, and traceability of network activity. Logs will be time-synchronized using UTC from a Stratum-2 public time source and include hostnames to enable easy correlation and incident response.

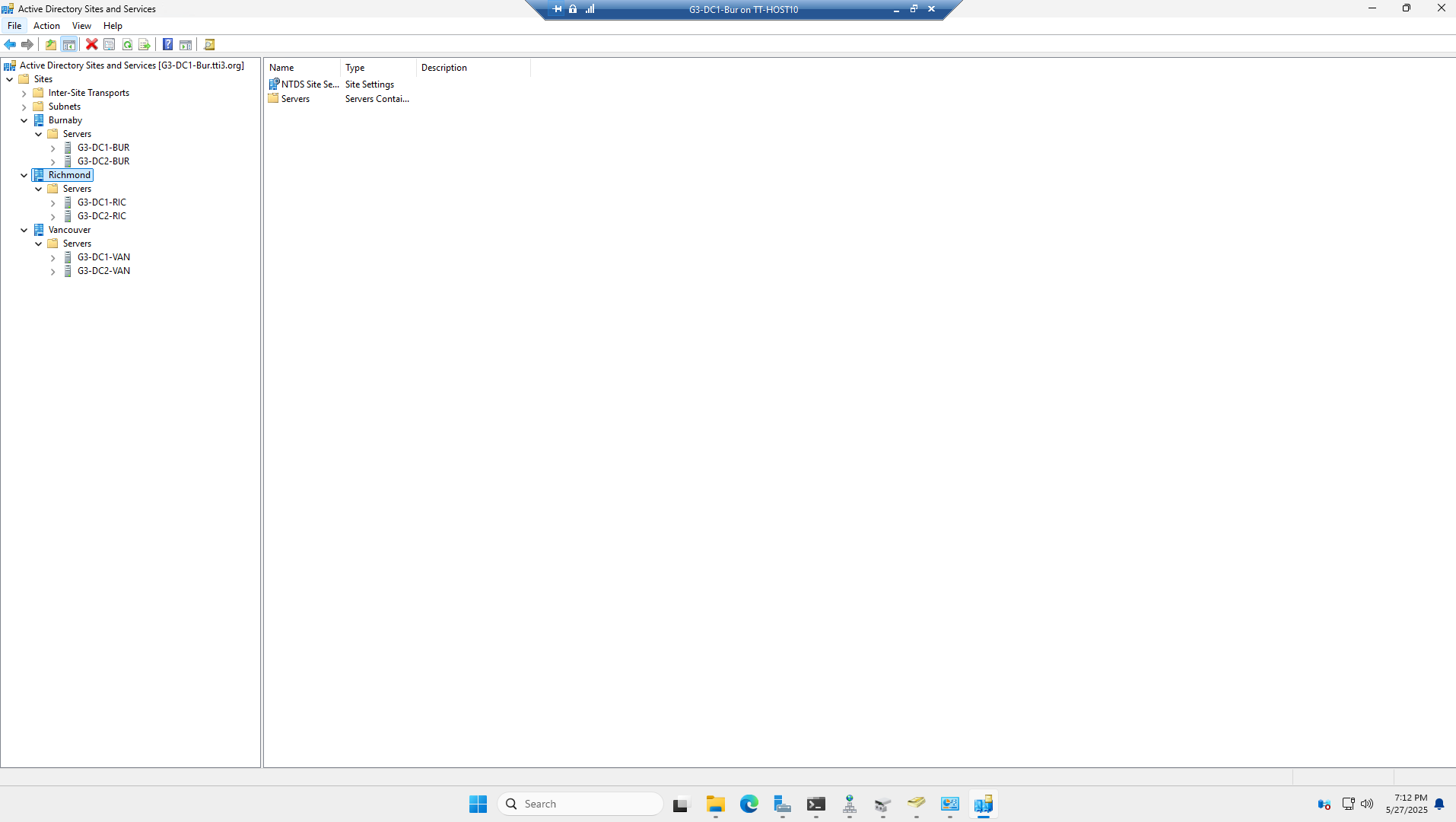
Finally, recognizing TTI’s long-term vision of expanding into the cloud, our design incorporates optional **AWS integration**. This involves extending services like DNS, directory sync, or web application hosting into the cloud using Amazon’s free-tier offerings. This not only provides a scalable testbed for hybrid deployments but also prepares TTI for future cloud transitions while minimizing cost.

In summary, our proposed network solution for TTI is tailored to meet the institution’s specific needs: secure and redundant WAN connectivity, logically segmented and secured LANs, centralized and reliable directory services, high-availability network infrastructure, comprehensive monitoring, and cloud readiness. It addresses existing pain points while providing the foundation for future scalability and digital transformation.

### **Active Directory & GPO Configuration**

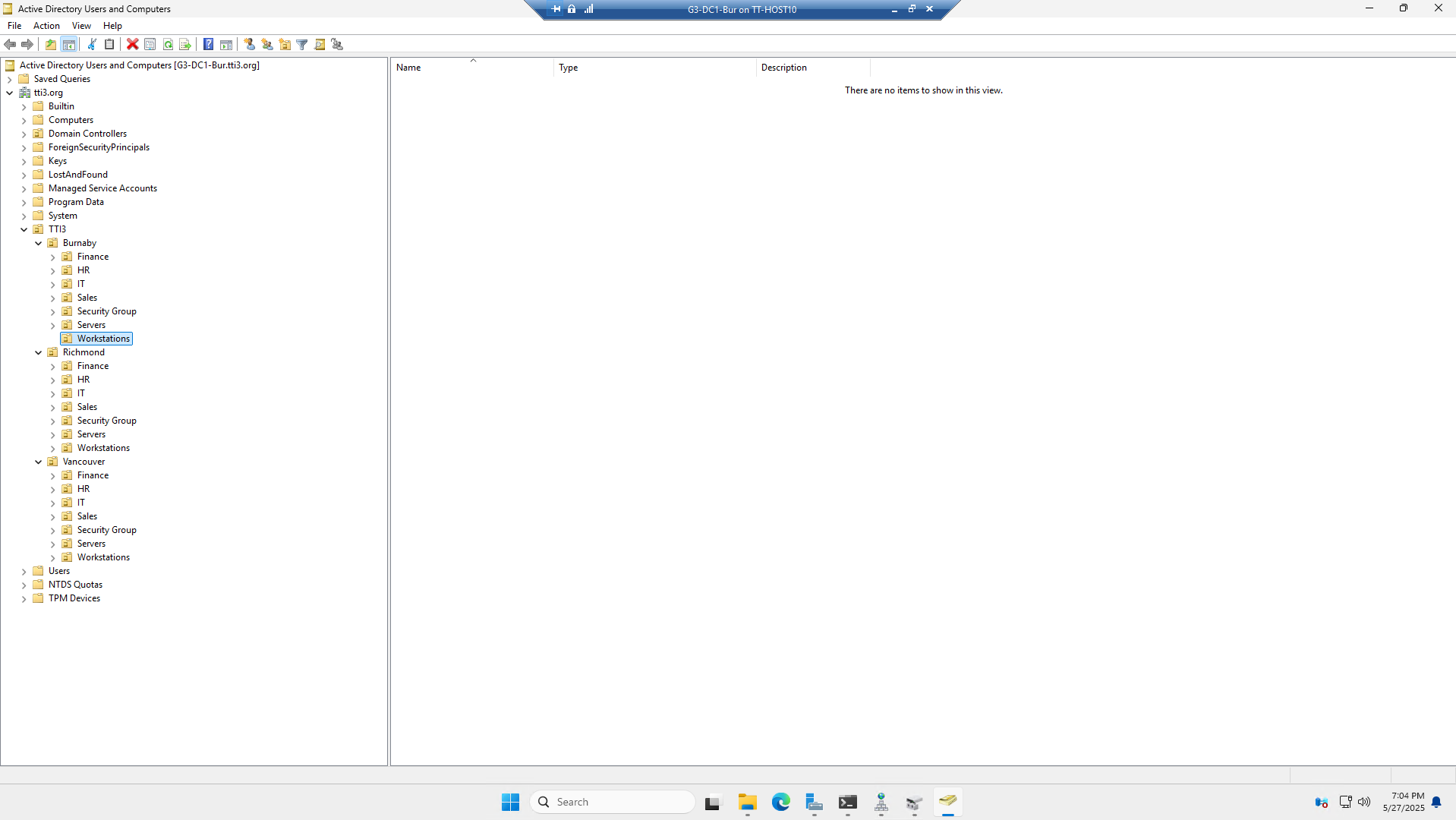
A multiple-site Active Directory (AD) infrastructure was deployed, with domain controllers placed in Burnaby, Richmond, and Vancouver. This design ensures high availability and low latency for authentication and directory services across all campuses. DNS and DHCP roles were assigned to the domain controllers 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**



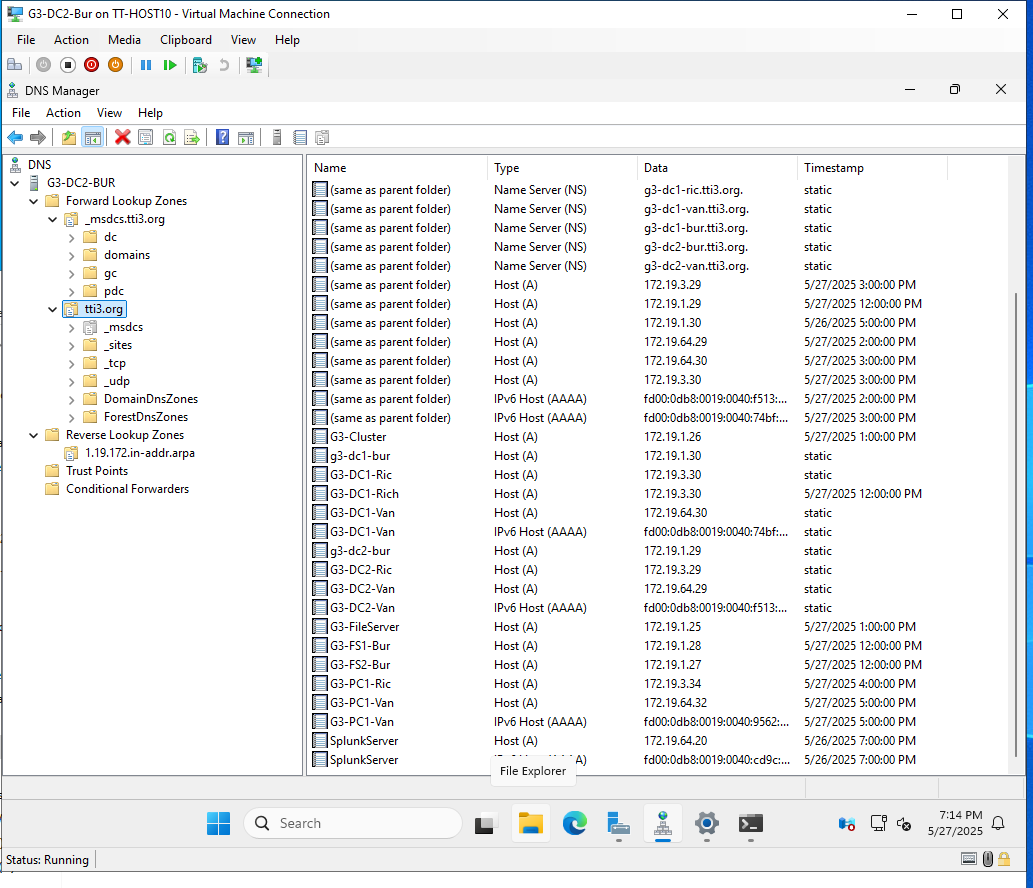
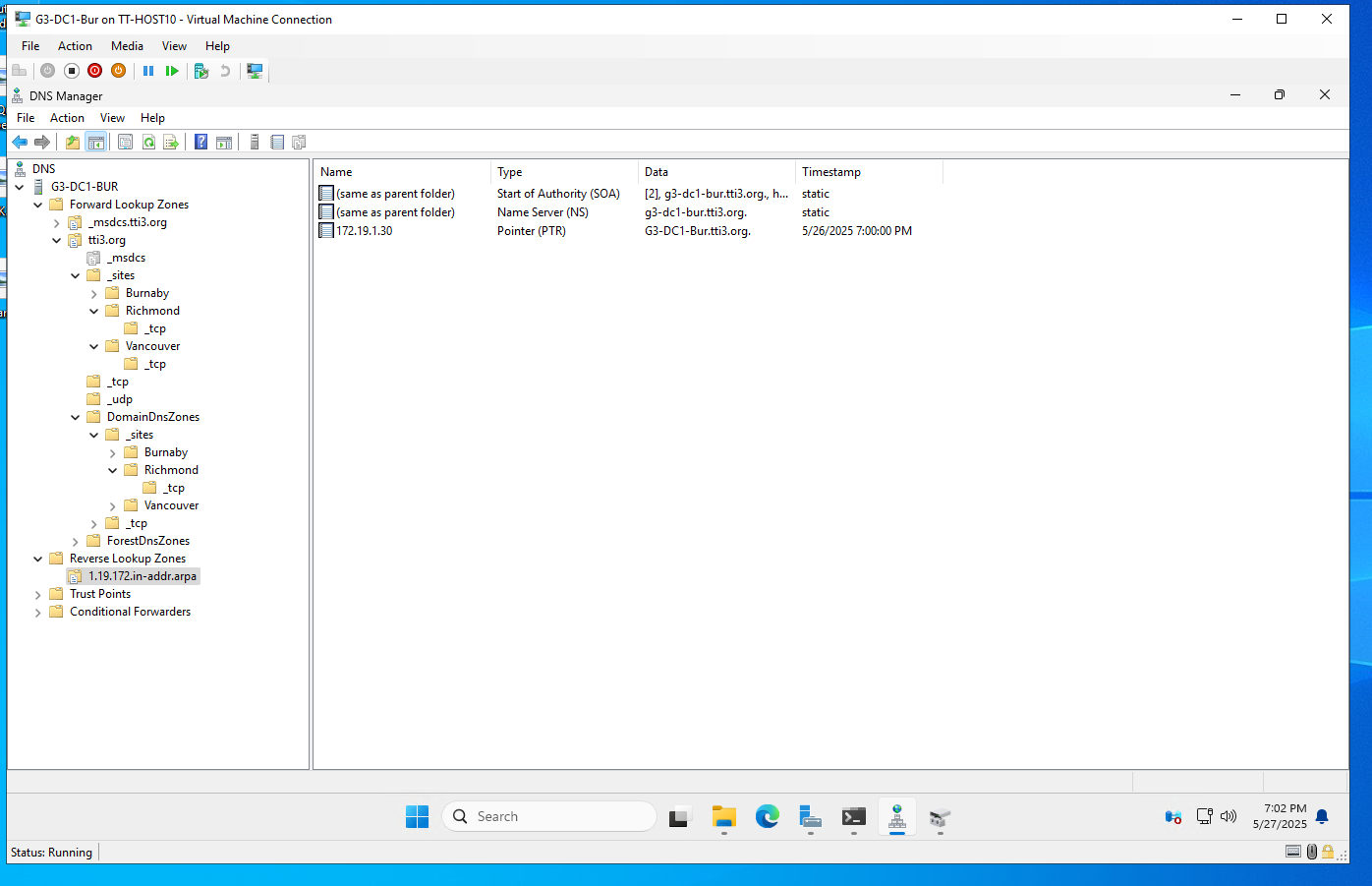
This screenshot demonstrates the successful configuration of Active Directory Sites and Services, showing clearly defined site links between Burnaby, Richmond, and Vancouver. It confirms that inter-site replication is functioning as intended, ensuring both redundancy and efficient replication across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

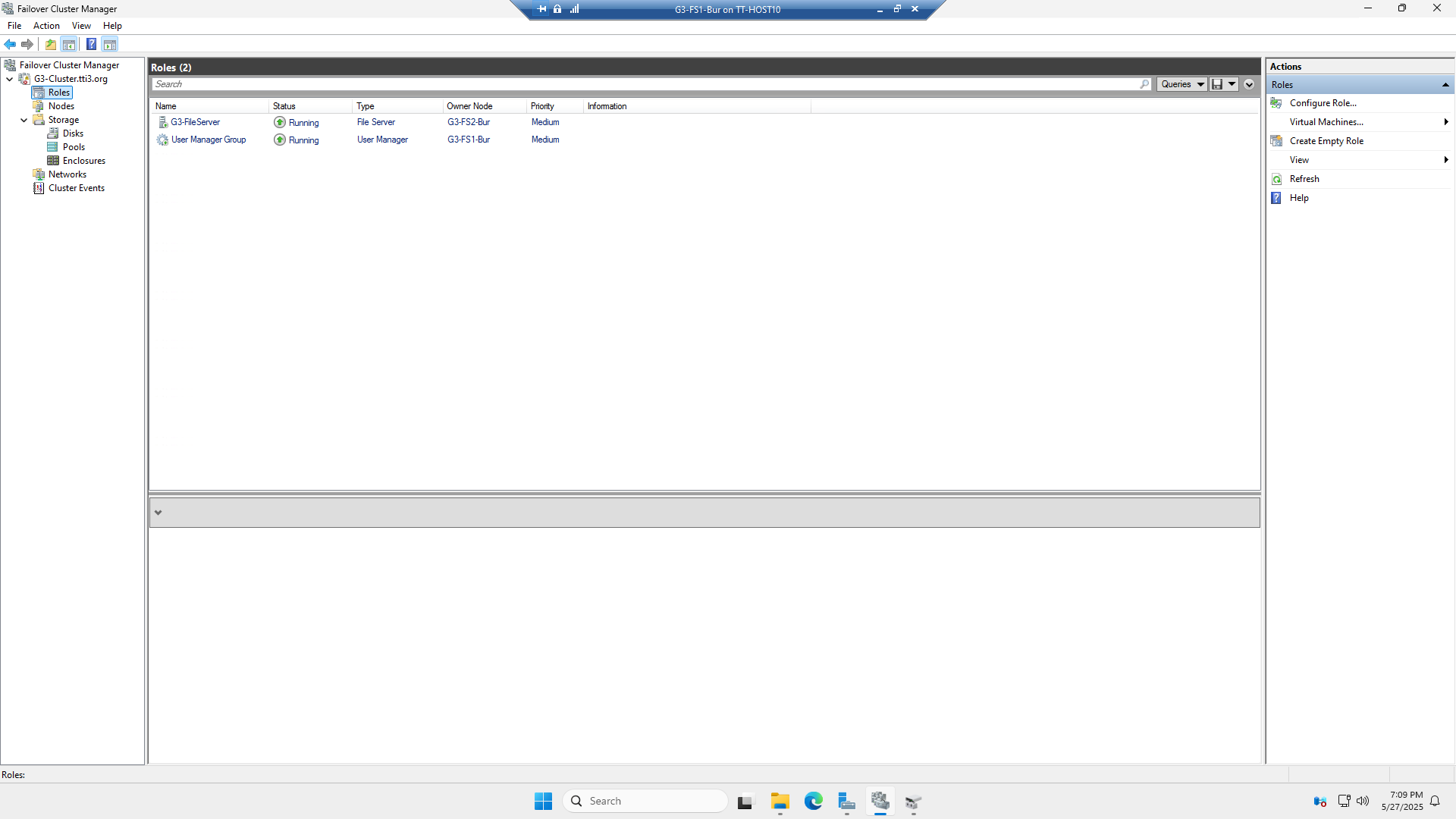
**Burnaby: DNS Configuration**



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.

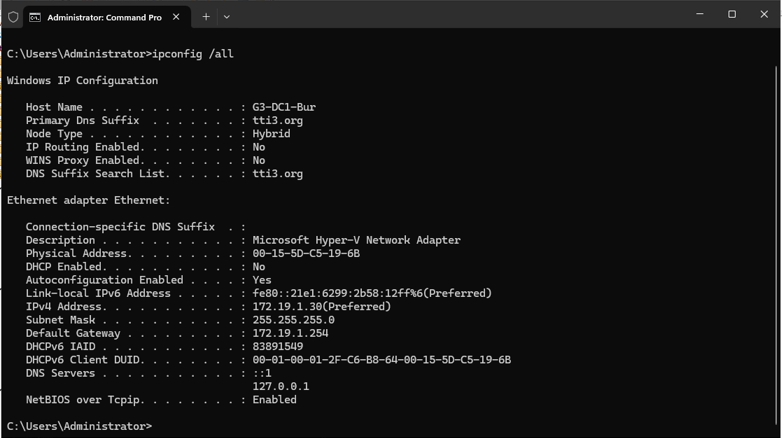
These configurations are essential to ensure reliable name resolution, enable successful domain controller synchronization, and support features such as Group Policy application and secure authentication. Scavenging settings have also been reviewed and configured, helping to automatically clean up stale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

**Burnaby: Cluster Manager – File Server Role**



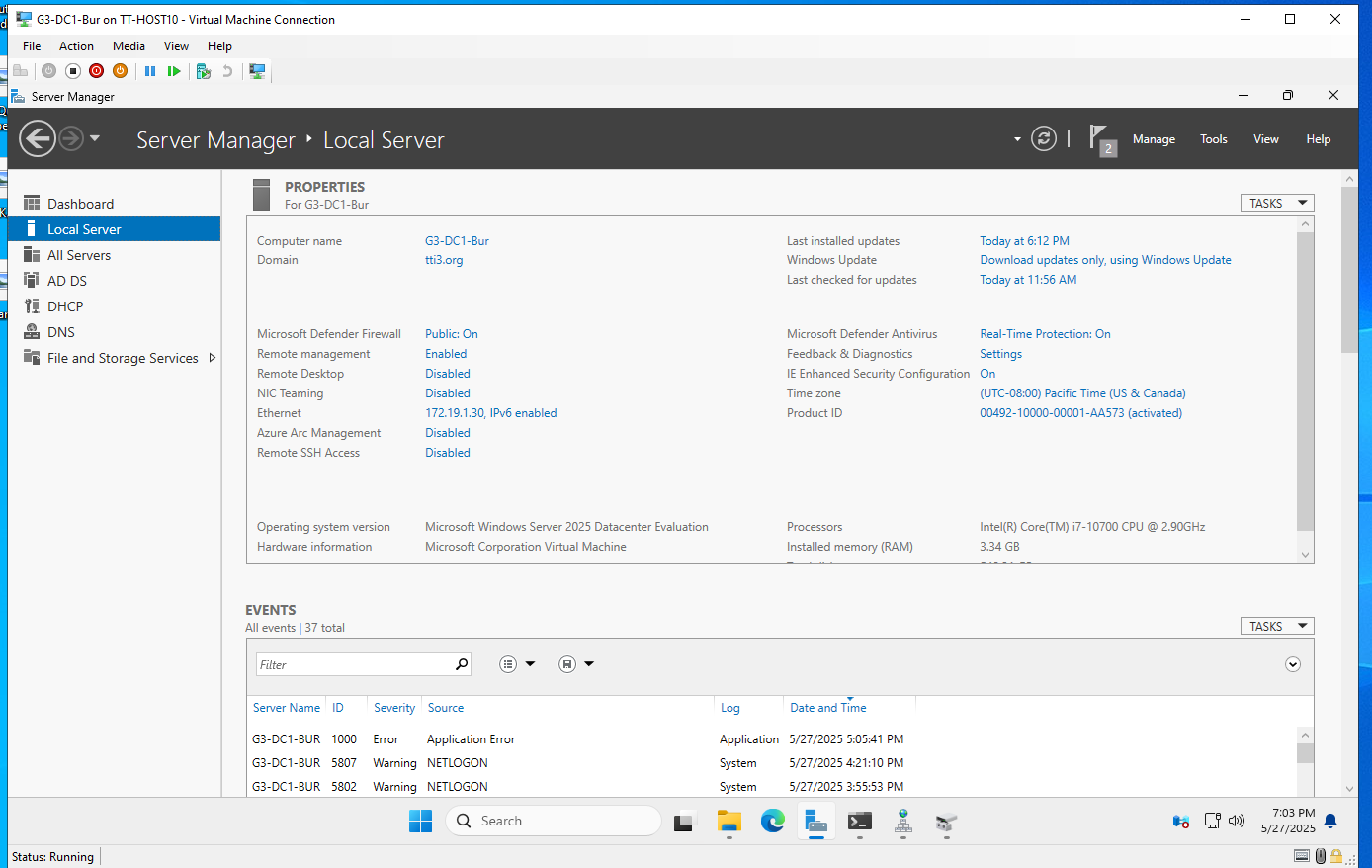
This screenshot verifies the successful deployment of a Windows Server Failover Cluster at the Burnaby datacenter. It shows two active roles — a clustered file server and a user management role — distributed across separate nodes (G3-FS1-Bur and G3-FS2-Bur), confirming high availability. The shared file 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**



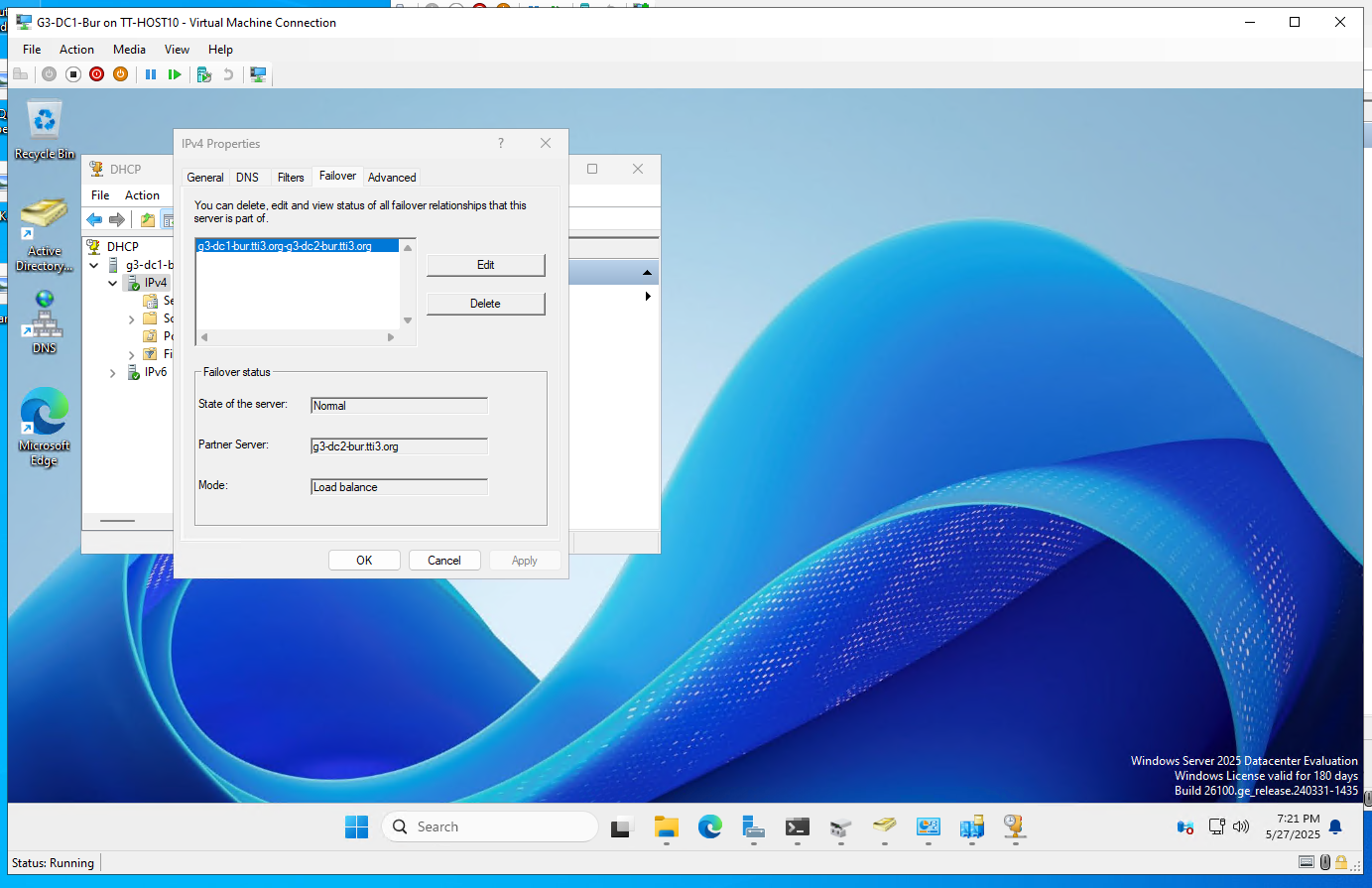
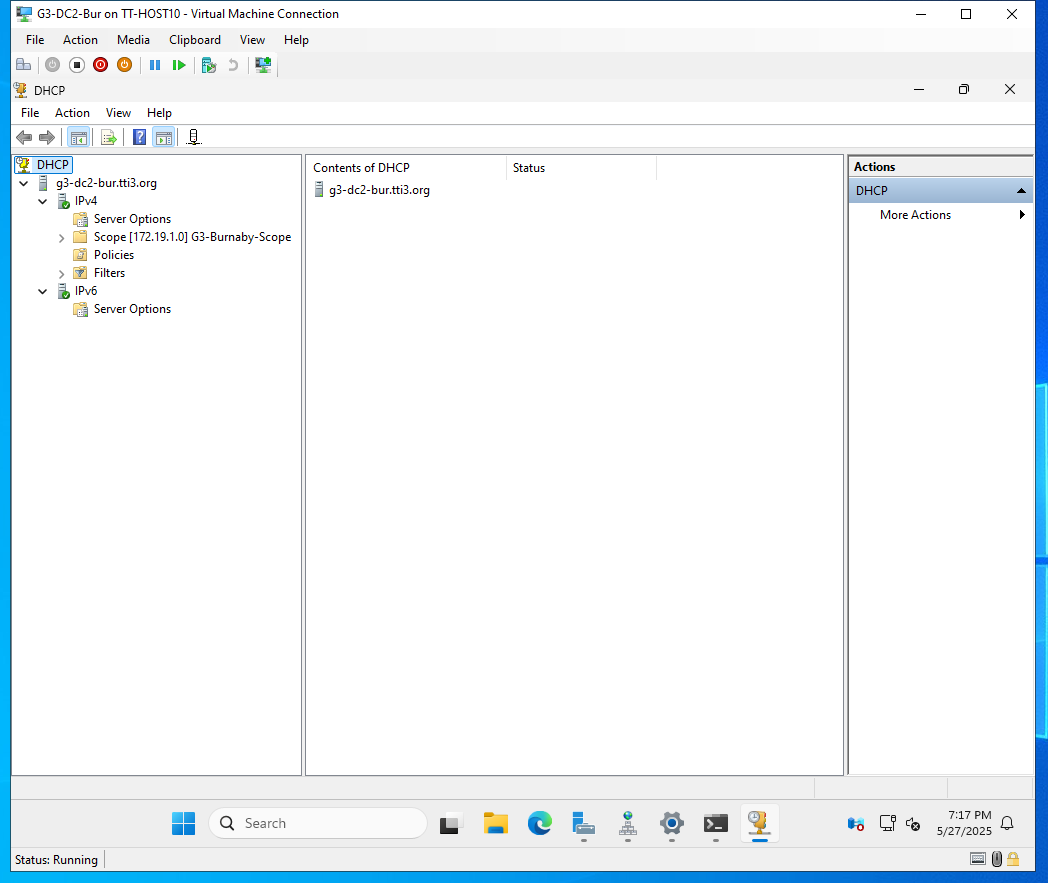
This screenshot shows the result of the ipconfig /all command executed on G3-DC1-Bur. It confirms that the domain controller received its IPv4 address (172.19.1.30) from DHCP, with DNS and gateway information properly assigned. The DNS suffix search list shows integration with the tti3.org domain, and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

**Burnaby: Server Properties**



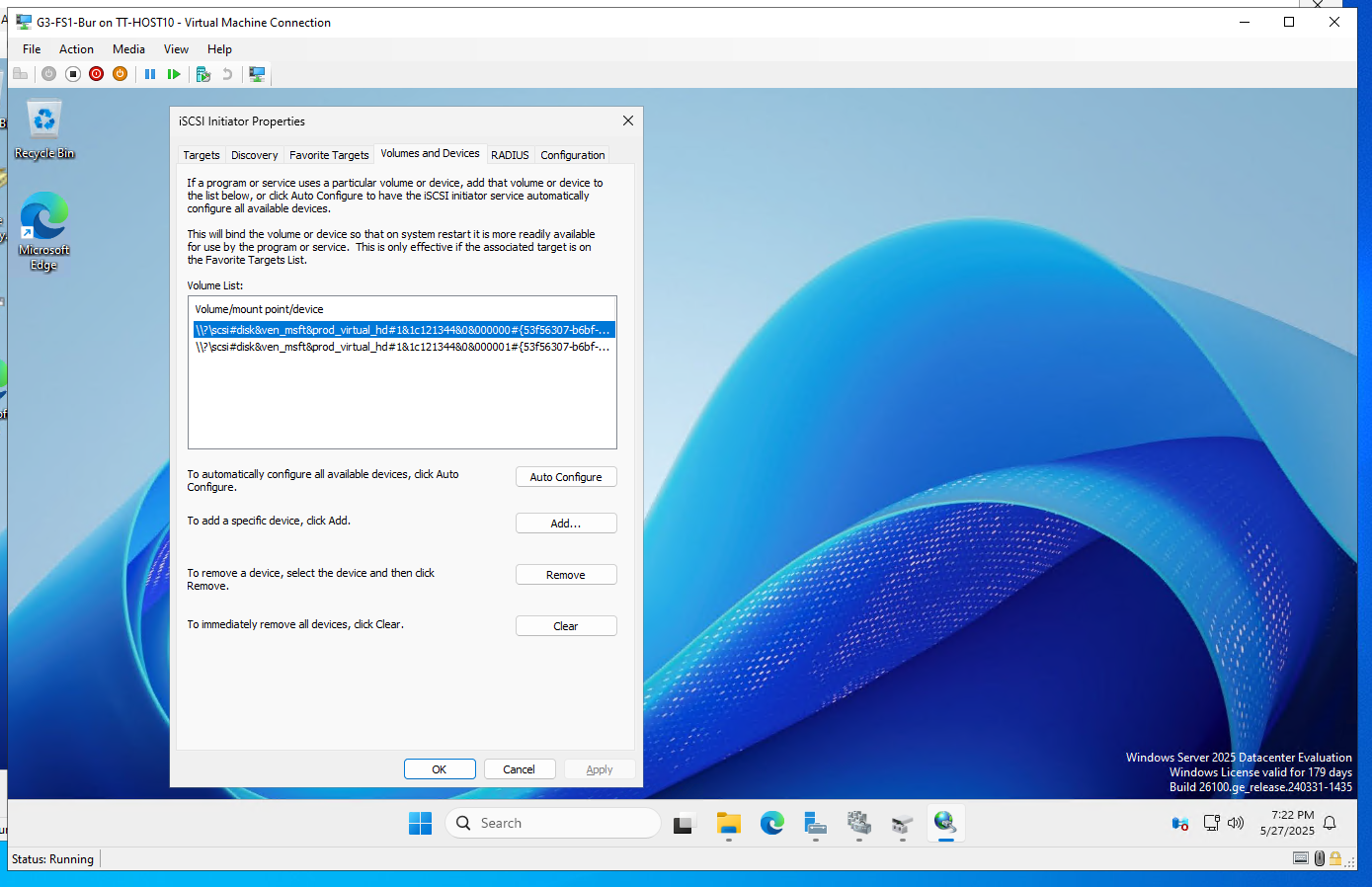
This displays the Server Manager dashboard for G3-DC1-Bur. It verifies that the system is running Windows Server 2025 Datacenter Edition, with domain membership (tti3.org) and real-time protection enabled. Key server roles such as AD DS and DNS are visible, and event logs at the bottom highlight normal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

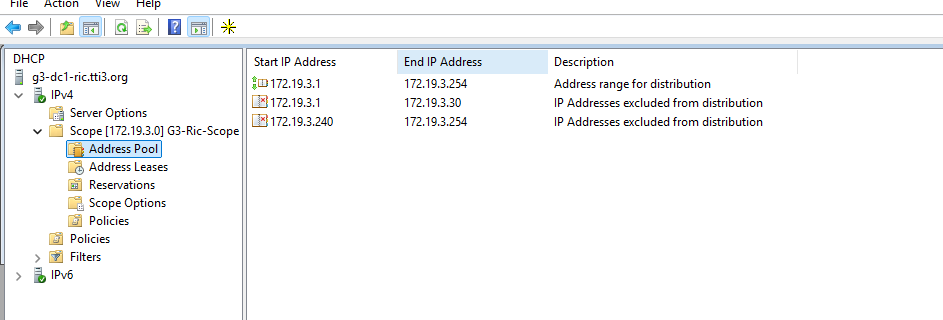
**Burnaby: Cluster Storage Validation – iSCSI Devices**



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.

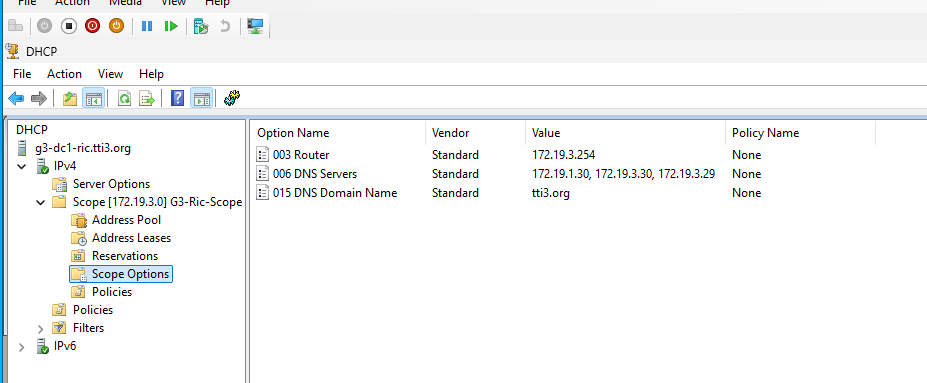
Below is a detailed breakdown of the services validated and implemented in the Richmond site. The configurations mirror Burnaby’s enterprise-grade standards, with emphasis on DHCP scoping, DNS name resolution, GPO enforcement, AD security group structure, and NTFS-based file sharing controls.

**Richmond: DHCP Address Pool and Exclusion Configuration**



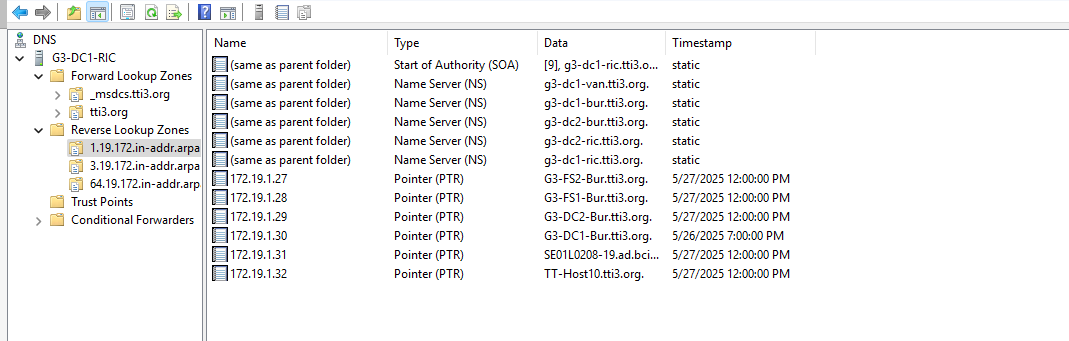
This screenshot shows the DHCP address pool defined on G3-DC1-RIC, which covers the range 172.19.3.1 to 172.19.3.254. Specific exclusions, such as .1 to .30 and .240 to .254, are set aside to reserve addresses for infrastructure devices like servers, routers, and printers. This practice avoids IP conflicts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

**Richmond: DHCP Scope Options**

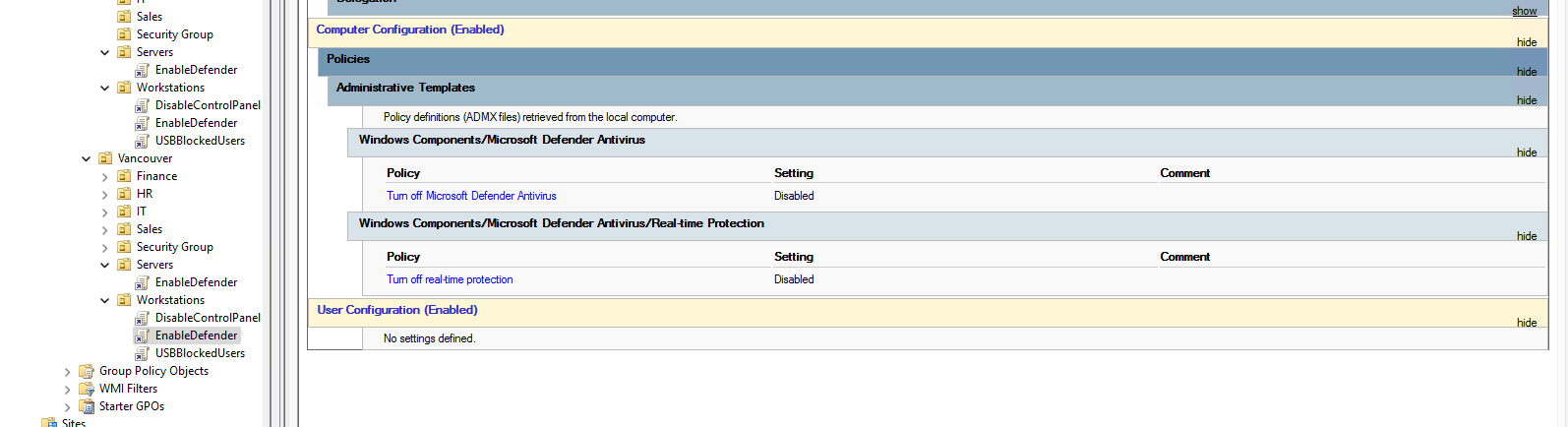


This view from the DHCP console confirms the definition of essential DHCP scope options: the default gateway (router) at 172.19.3.254, DNS servers across sites (172.19.1.30, .29, .30), and the domain name (tti3.org). These options ensure that clients automatically receive network configurations aligned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

**Richmond: Reverse DNS Zone Validation**

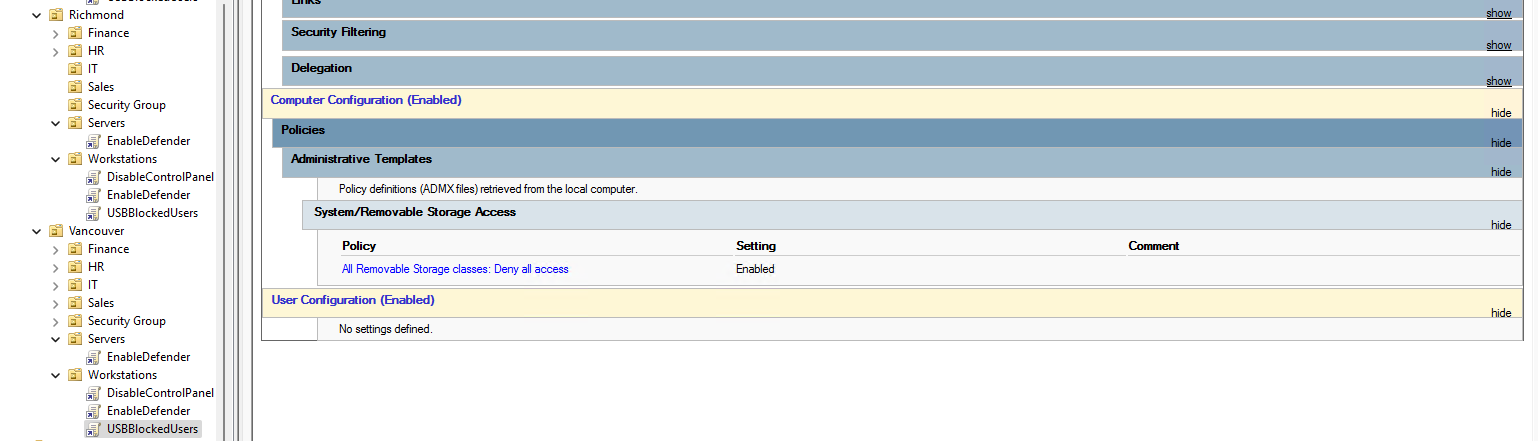
This screenshot from the DNS Manager shows reverse lookup zones configured for Richmond and the broader enterprise. The PTR records confirm that major devices — such as domain controllers and file servers — are resolvable via their IP addresses. This bi-directional resolution supports log auditing, secure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

**Richmond: Defender Real-Time Protection GPO**



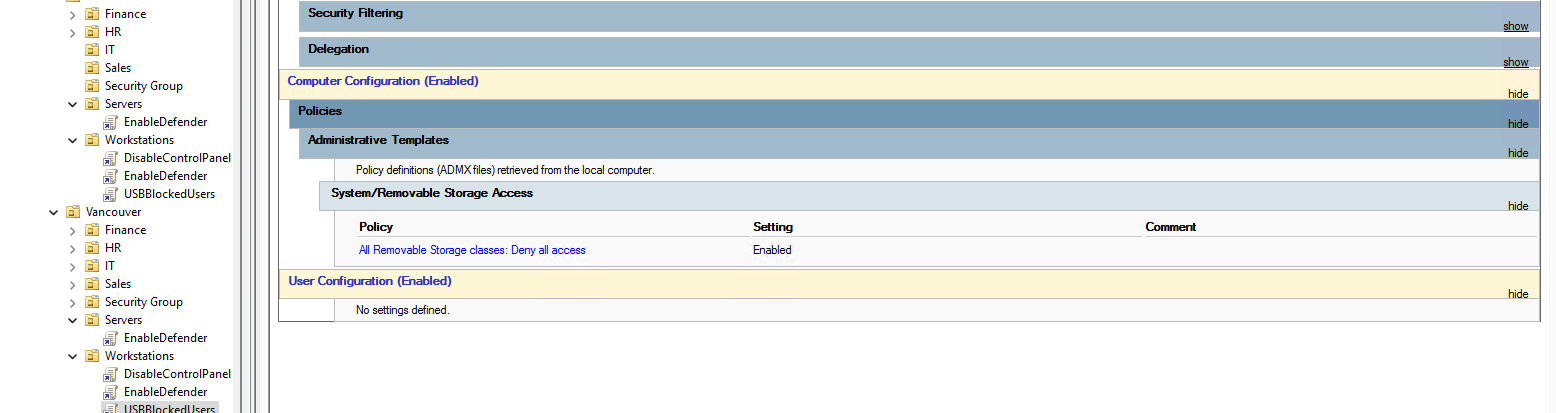
The image shows a GPO applied to Richmond servers that ensures Windows Defender Antivirus, and its real-time protection is enabled. The policies override user settings and prevent tampering, aligning with institutional standards for endpoint protection.

**Richmond: USB Blocking GPO Enforcement**



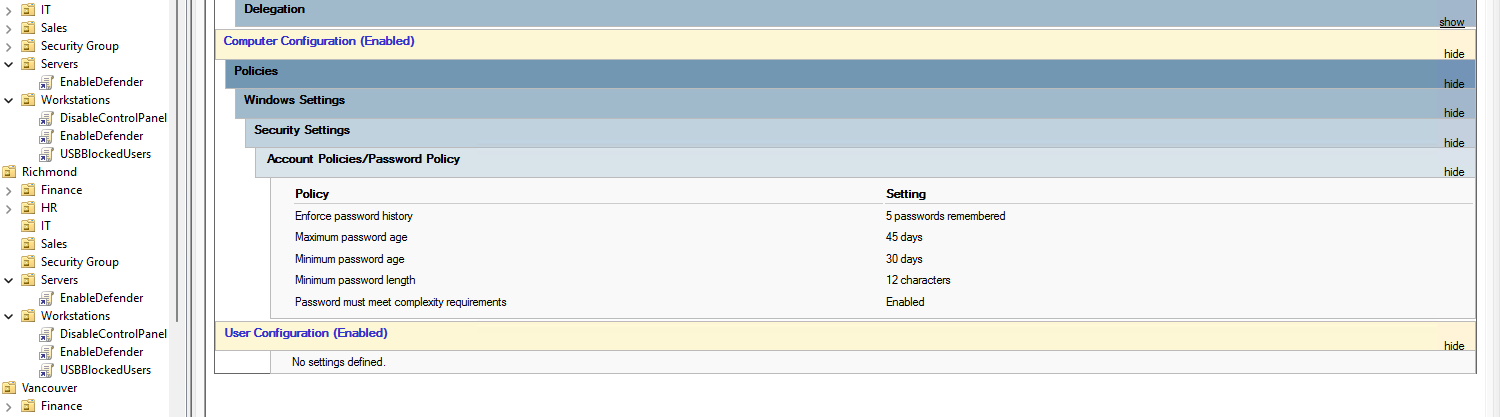
This policy blocks access to all removable storage systems. Applied to the Richmond Workstations OU, it ensures that unauthorized USB devices are not recognized, reducing risk of data leaks or malware infections.

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



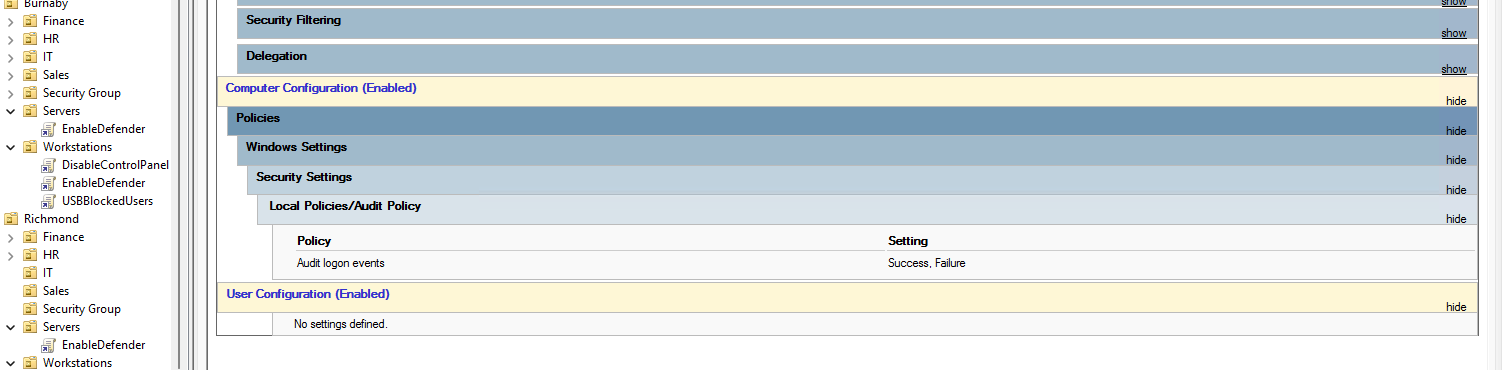
This Vancouver-side is used to compare enforcement across sites. It validates that identical USB blocking policies are consistently deployed to Workstations OUs across all campuses, reinforcing policy uniformity and centralized control.

**Richmond: Password Policy GPO Settings**



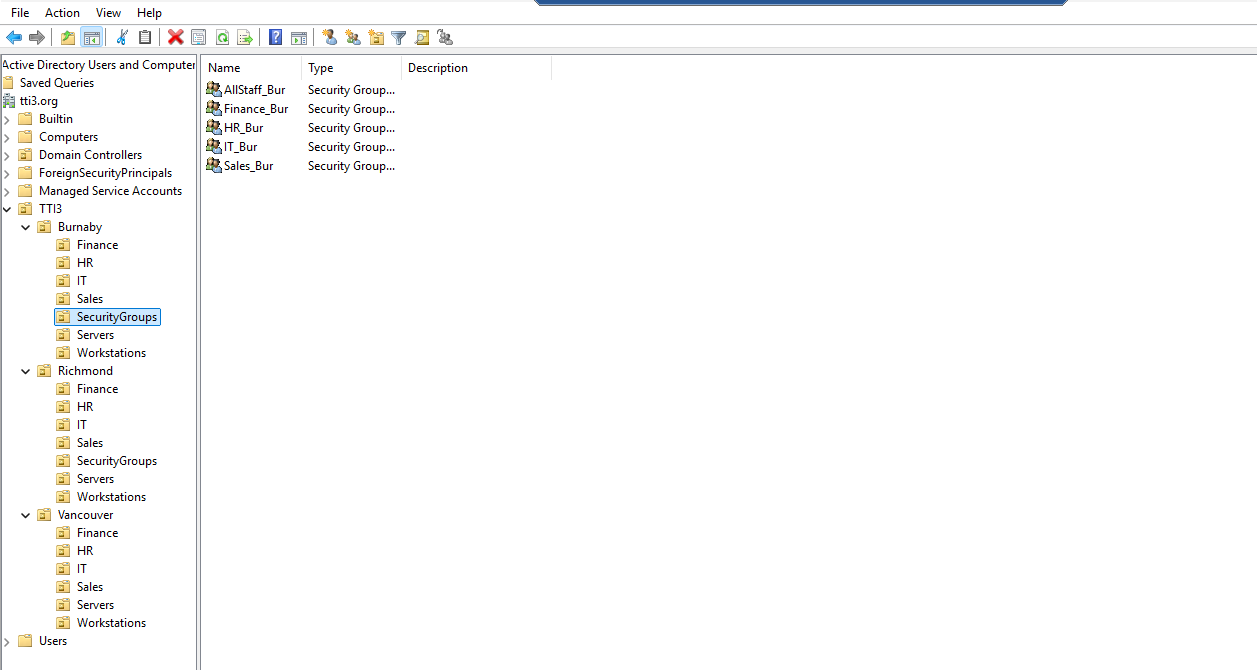
This image shows the Password Policy settings applied to all Richmond users. The GPO enforces password history (5 remembered), maximum/minimum age, complexity requirements, and minimum length. These controls are essential for domain security and compliance.

**Richmond: Audit Policy Enforcement GPO**



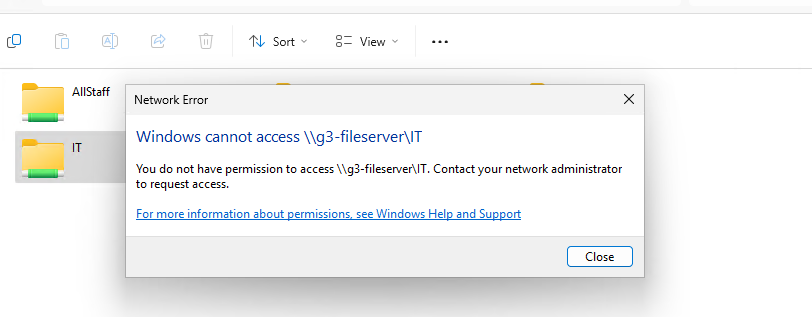
This confirms that a GPO is in place to log both successful and failed logon attempts. This level of auditing is critical for accountability, forensic analysis, and threat detection.

**Richmond: AD Organizational Units – GPO Scoping**



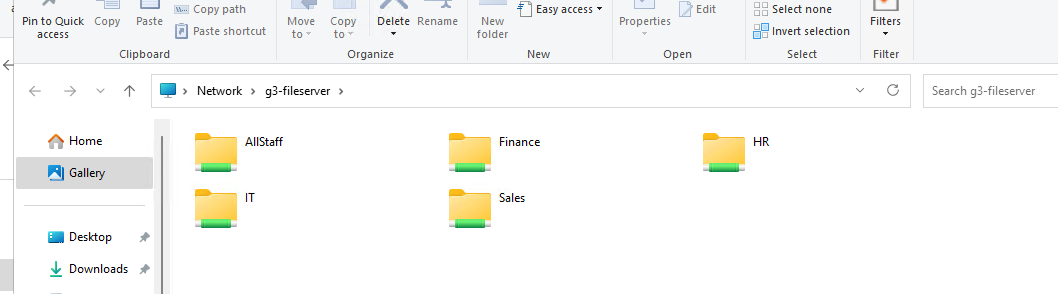
The OU structure is shown again here from the Richmond perspective. It demonstrates how servers, workstations, and departments are logically grouped, enabling site-specific GPO targeting. OUs like USBBlockedUsers or EnableDefender illustrate role-based access control and policy delegation.

**Richmond: NTFS Permissions Enforcement via Security Groups**



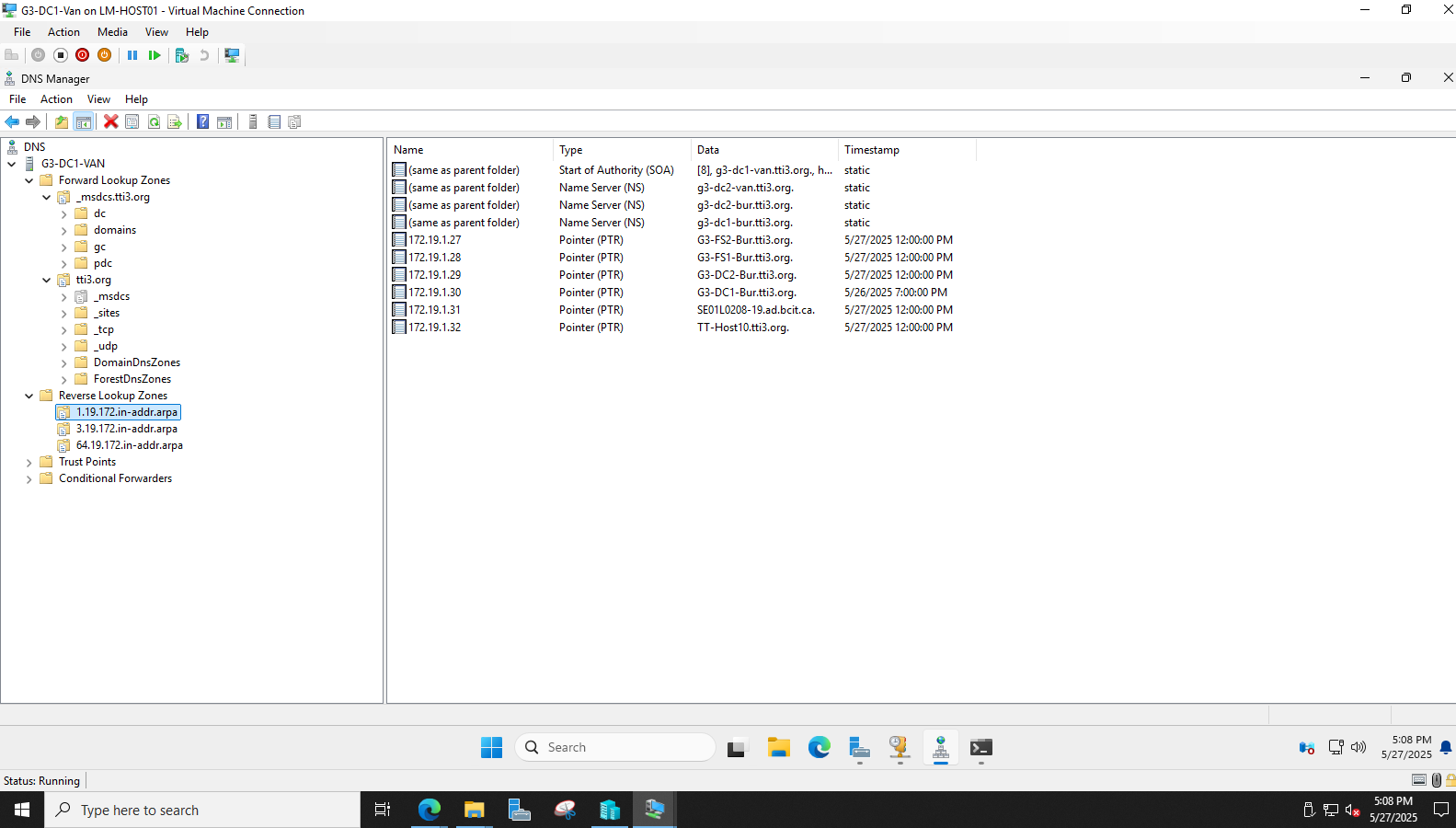
This screenshot validates NTFS file permission enforcement. The user receives a denial message when attempting to access the IT share ([\\g3-fileserver\IT](file:///\\g3-fileserver\IT)) without proper group membership. Access is controlled via AD security groups mapped to departmental shares, ensuring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

**Richmond: Departmental File Shares Verification**



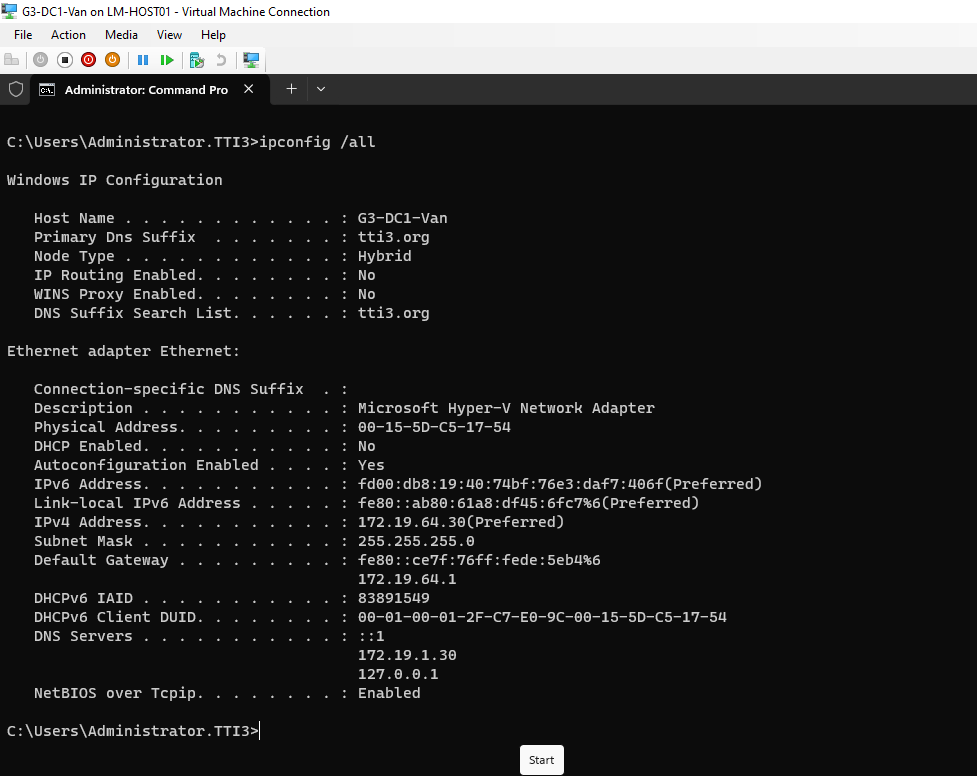
This screenshot shows the shared folders hosted on the clustered file server g3-fileserver. The shared directories — AllStaff, Finance, HR, IT, and Sales — represent mapped network drives accessible by staff based on their group memberships in Active Directory. Each share is assigned NTFS permissions 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**



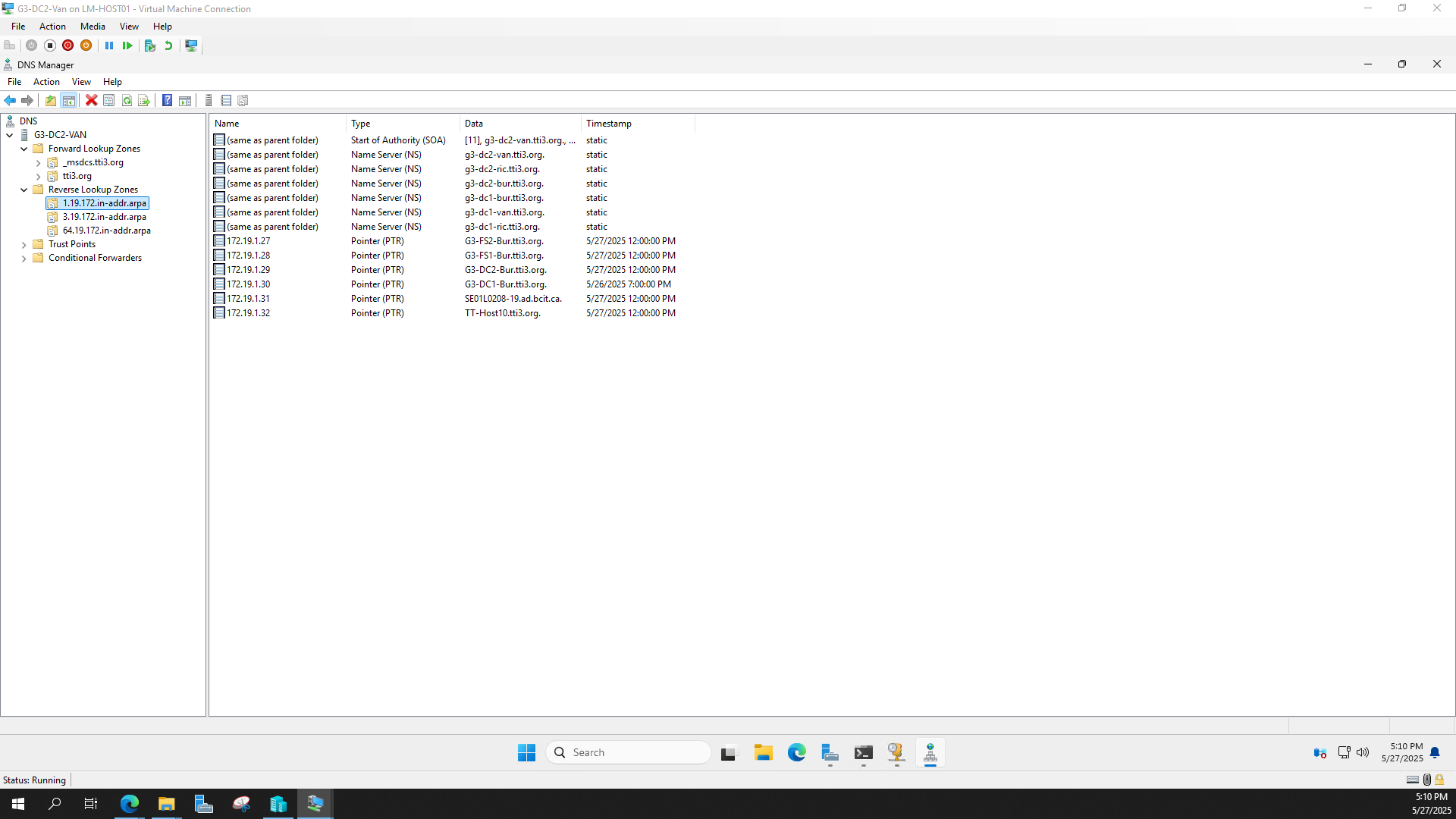
This shows the successful configuration of forward and reverse lookup zones. The presence of authoritative SOA and NS records confirms integration with the domain (tti3.org). PTR records also demonstrate proper reverse resolution for IPs assigned to local resources, supporting troubleshooting, and name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

**Vancouver: DC1 IP Configuration Validation**



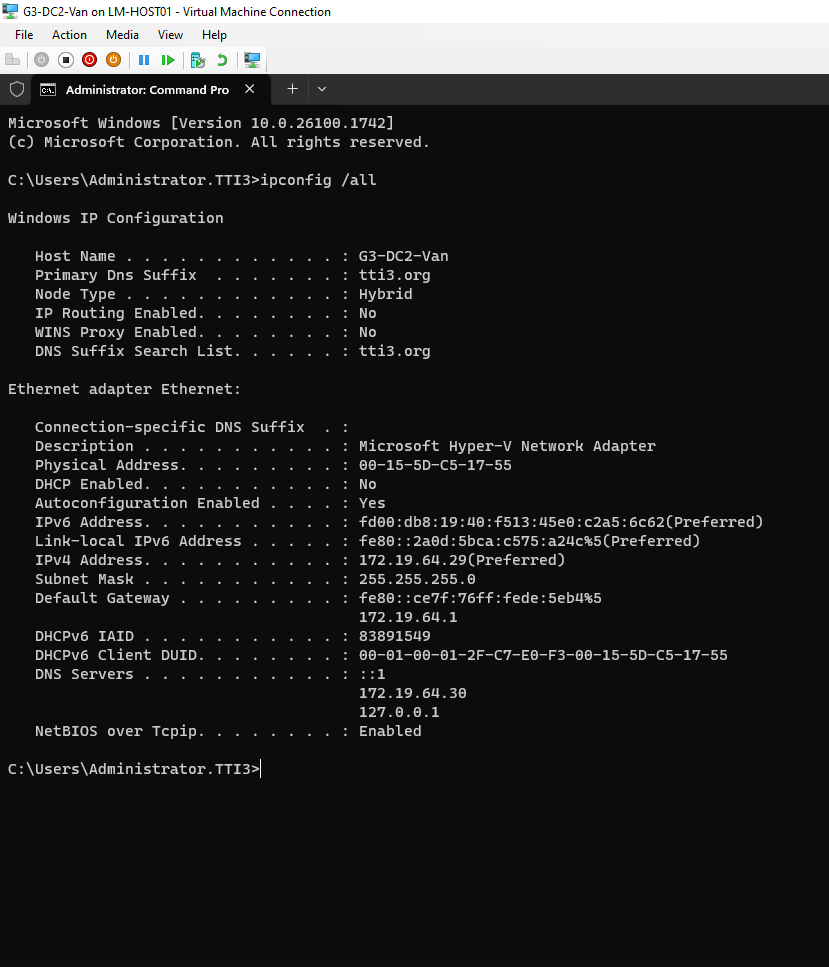
The ipconfig /all result proves that G3-DC1-Van has received a static IPv4 address in the expected subnet (172.19.64.x). DNS is set to local and secondary servers for redundancy, and the domain name and suffix confirm proper binding to tti3.org.

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



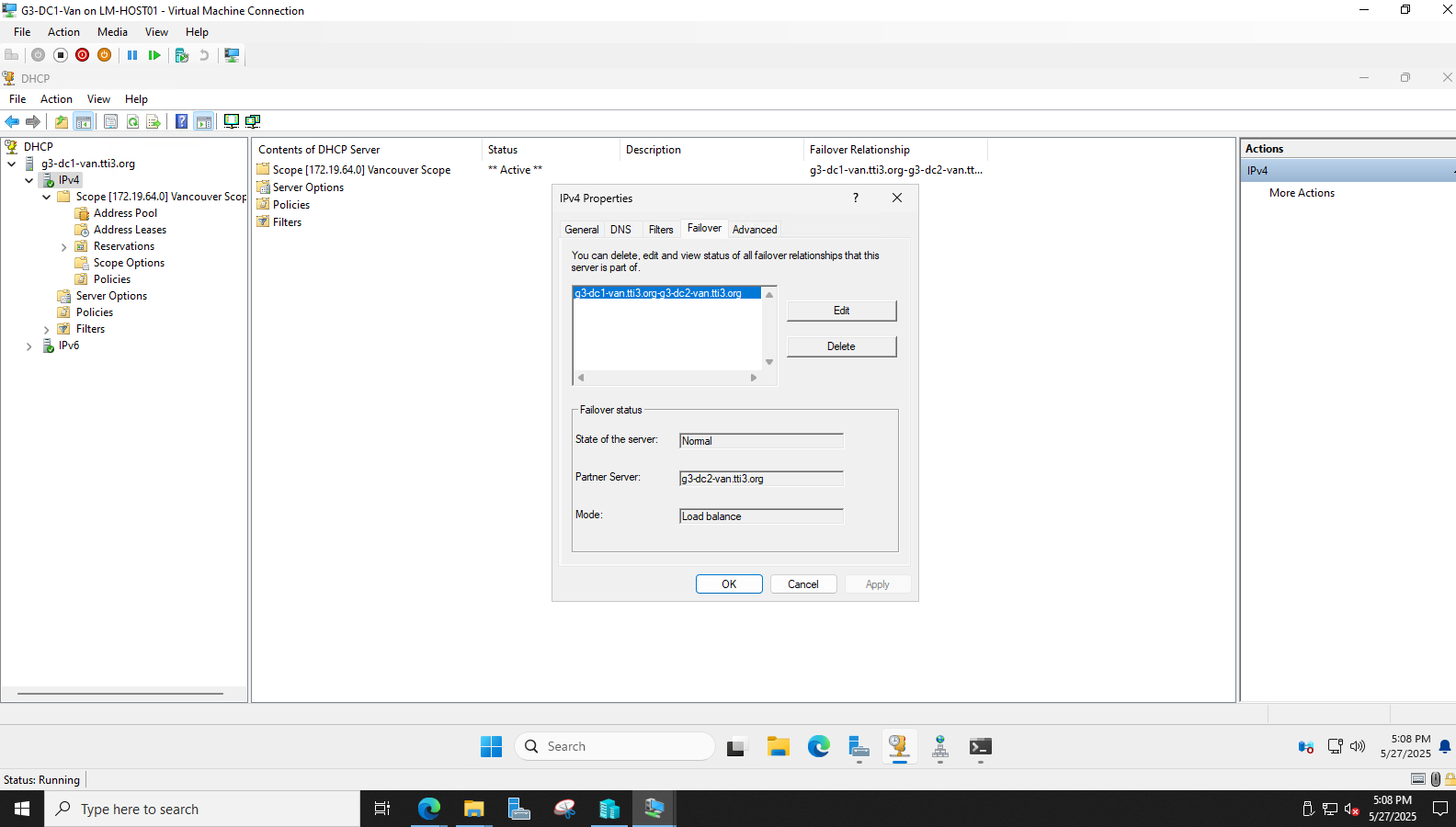
This shows DNS running on G3-DC2-Van, correctly synchronized with forward and reverse zones. NS and PTR entries confirm that records replicate properly between sites. The presence of DCs and member servers from Burnaby and Richmond also confirms inter-site DNS functionality.

**Vancouver: DC2 IP Configuration Validation**



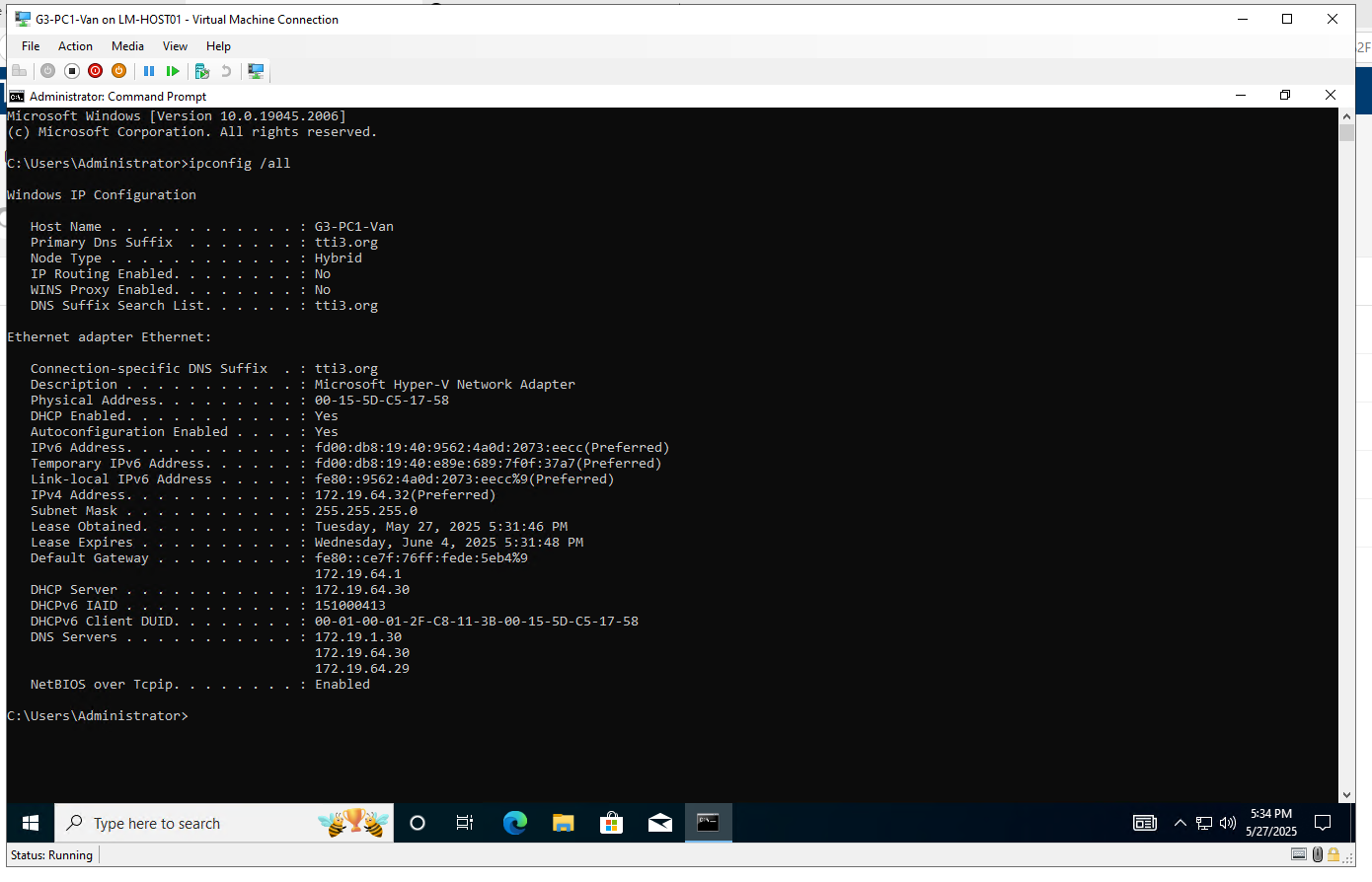
This output validates G3-DC2-Van's address assignment. IPv4 address (172.19.64.x) is correct, and DNS entries point to DC1 and itself for resilience. Domain name suffix confirms domain binding.

**Vancouver: DHCP Scope Failover Verification**



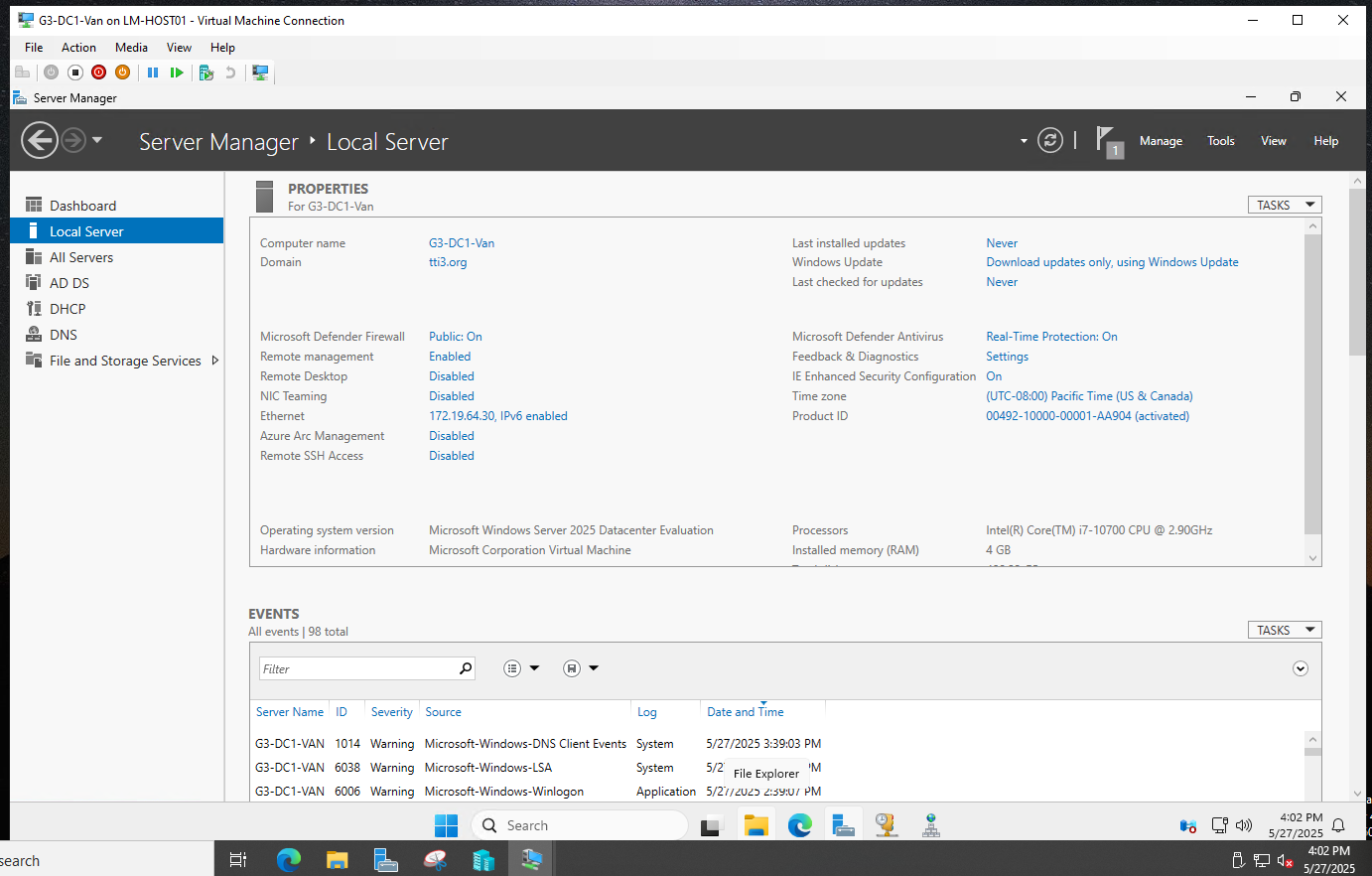
This confirms that DHCP failover has been configured between G3-DC1-Van and G3-DC2-Van in load balance mode. This ensures high availability and fault tolerance for IP address assignments across the Vancouver network segment.

**Vancouver: PC DHCP Lease Verification**

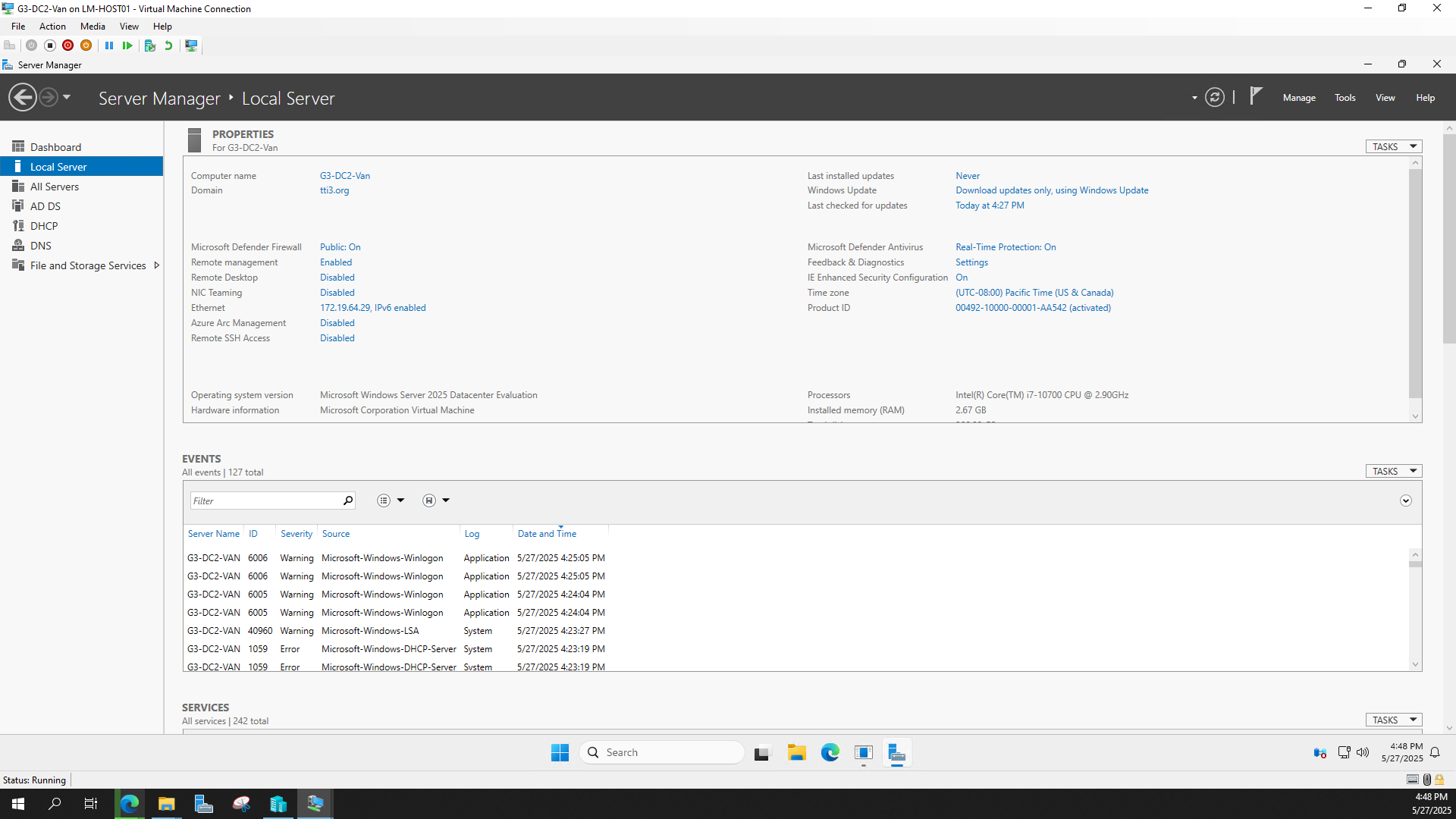


A client machine (G3-PC1-Van) has received an IP address from the Vancouver DHCP scope (172.19.64.x). DNS entries and DHCP server values confirm the client is communicating with the correct domain controllers.

**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**  


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 Report**

### **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.

### **1. VPC and Subnet Design**

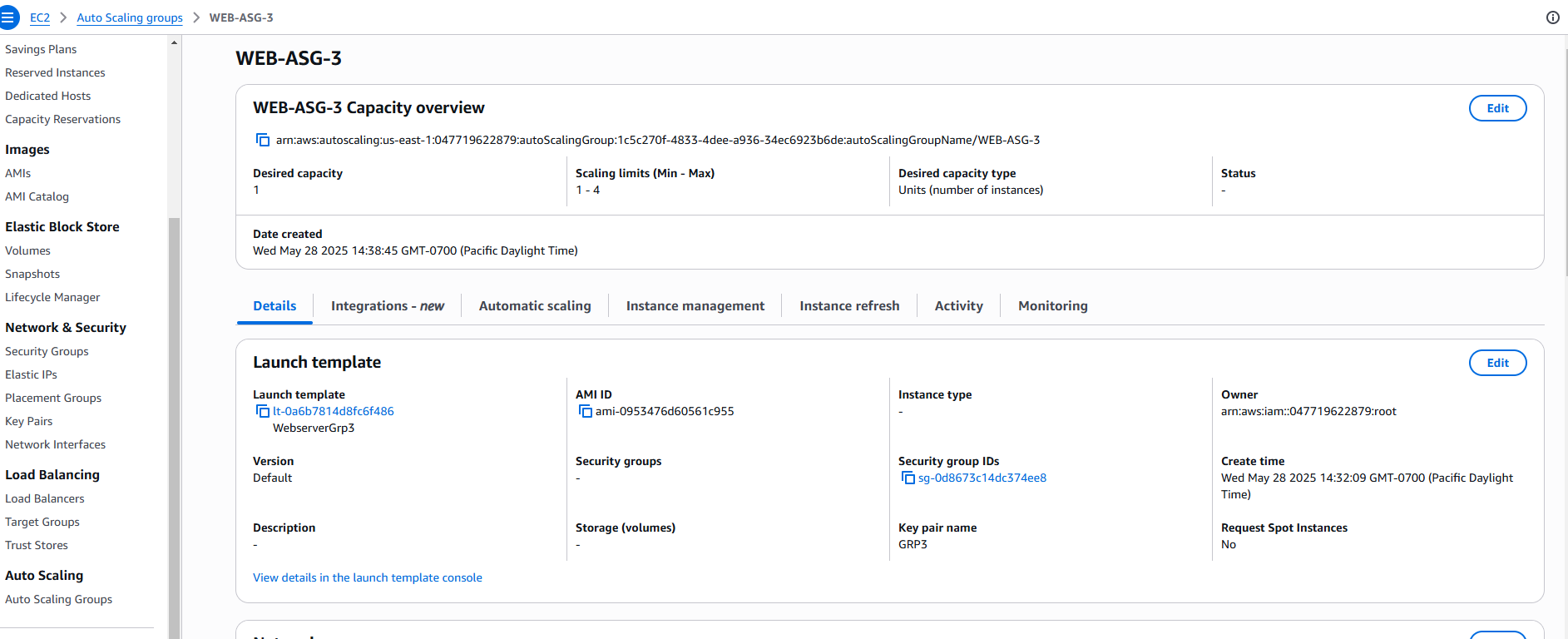
* A custom **VPC** was created with a **10.0.0.0/16** CIDR block. It contains:
* **Public Subnet (10.0.1.0/24)** in **us-east-1a**
* **Private Subnet (10.0.2.0/24)** in **us-east-1b**
* An **Internet Gateway (G3-IGW)** and a **custom route table** (G3-RouteTable) were configured to enable external access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

### **2. 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.

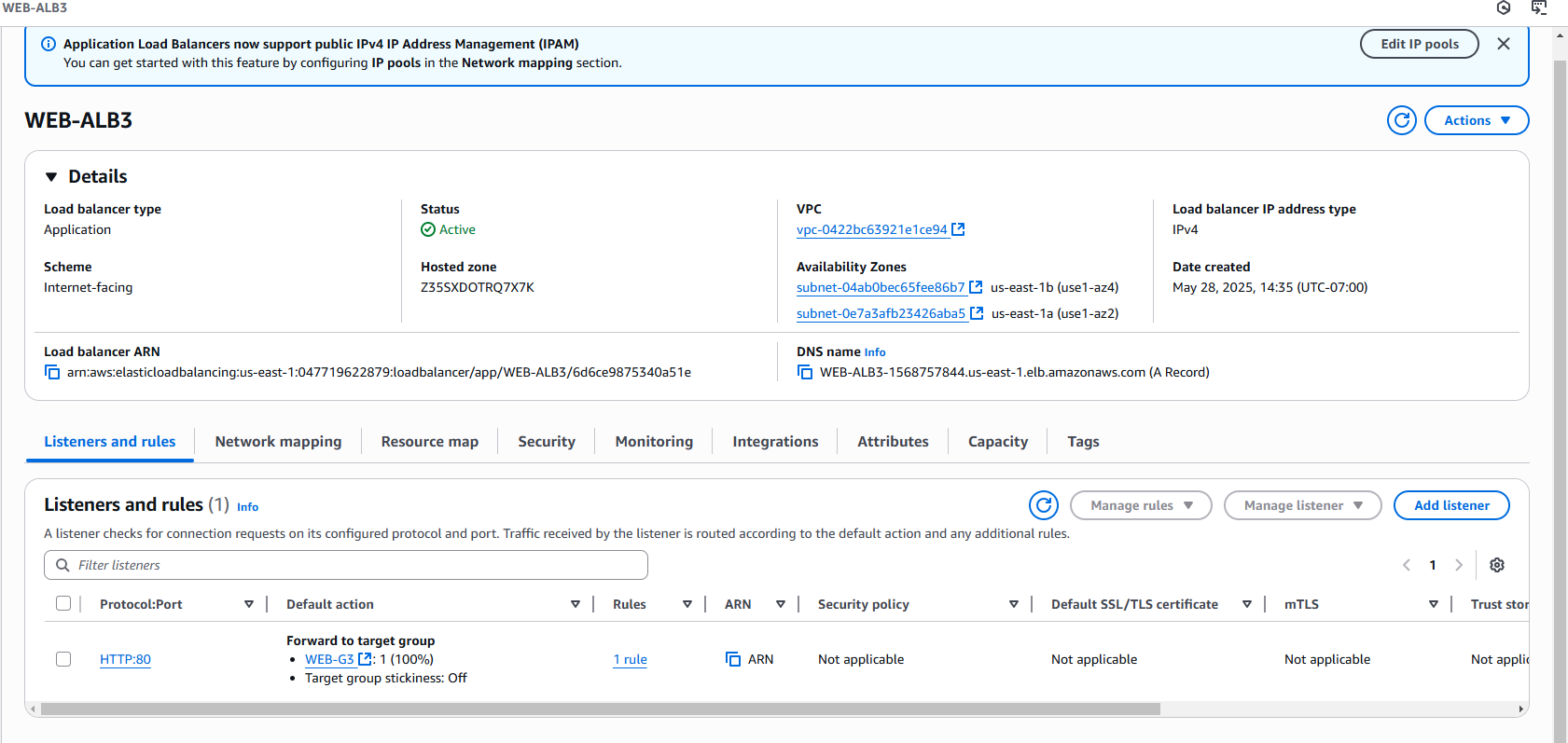
### **3. EC2 Web Server and Autoscaling**

* 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.



### **4. Application Load Balancing**

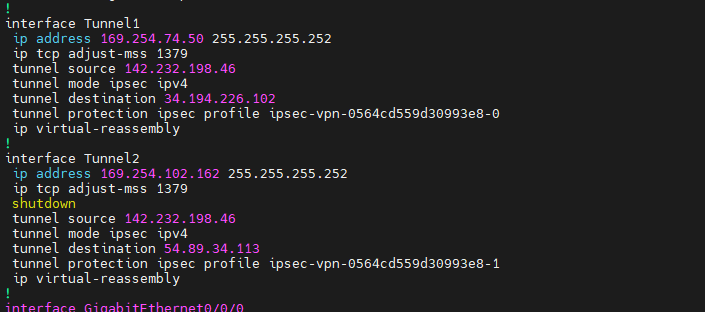
An **Application Load Balancer (WEB-ALB3)** was deployed across two AZs. It listens on **port 80** and routes traffic to a **target group (WEB-G3)** containing Auto Scaling EC2 instances. This setup ensures load distribution and fault tolerance.

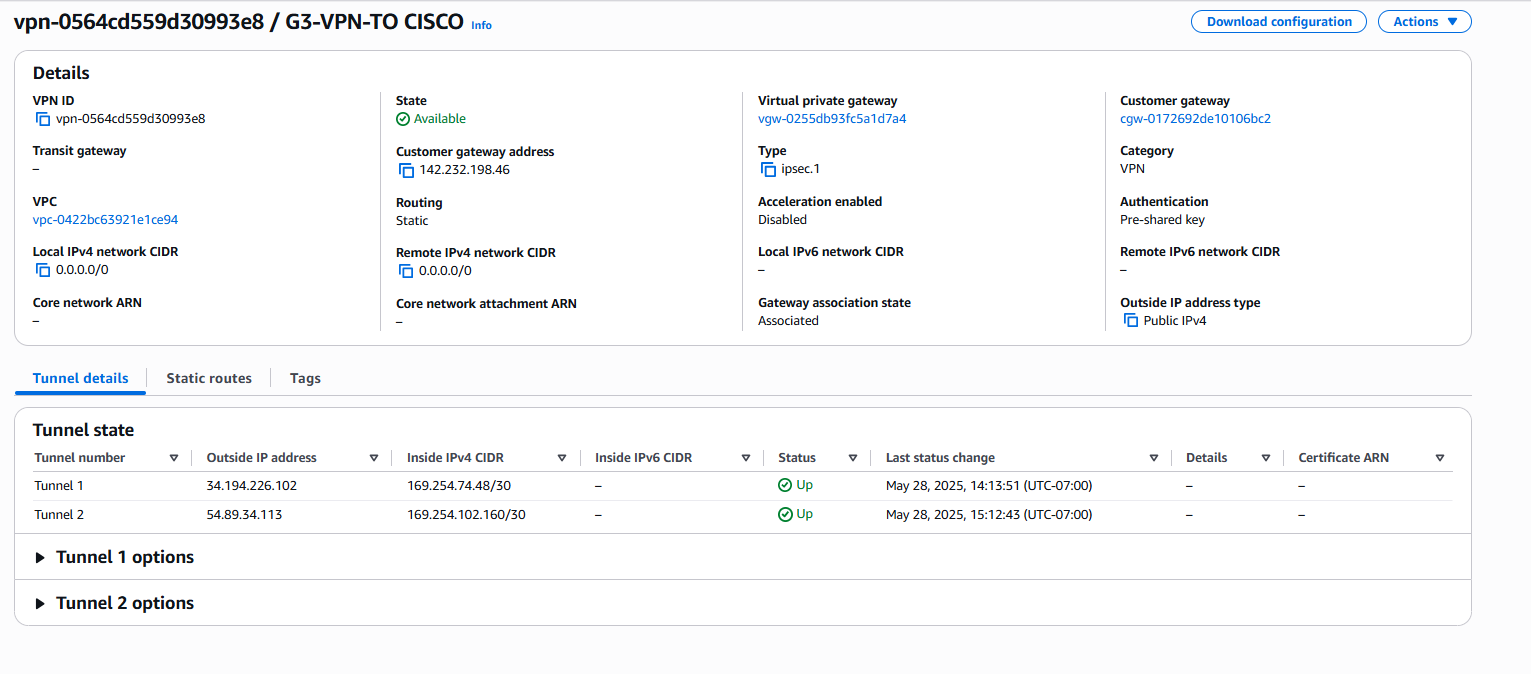


### **5. VPN Configuration (Hybrid Networking)**

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



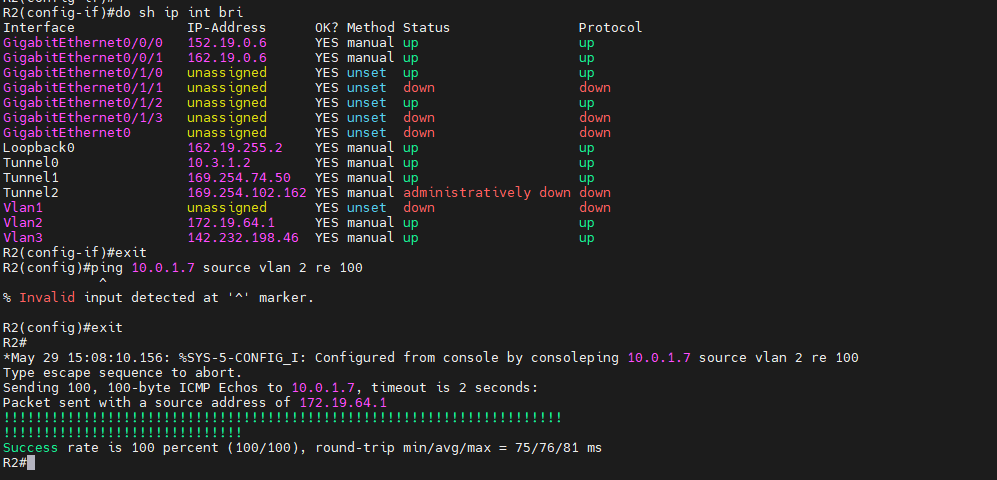
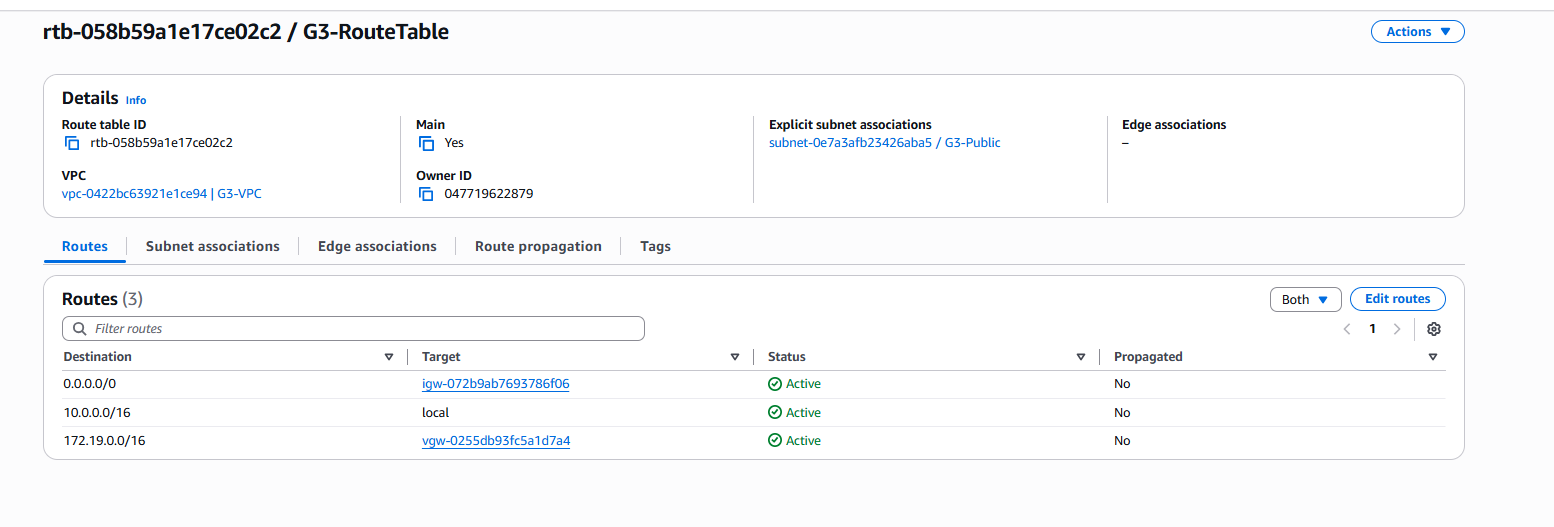


**IPsec/IKEv1** settings with pre-shared keys were configured on the Cisco side using **AES, SHA, and DH Group 14**. Both tunnels were successfully tested using ping.

### **6. 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.

### **7. 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.