NewVue Health Infrastructure Modernization

ON-PREMISES AND HYBRID CLOUD INTEGRATION

Vivian J. Goshashy

IT236 | SERVER ADMINISTRATION FALL 2025

Table of Contents

Executive Summary

Purpose and Scope

The NewVue Health Infrastructure Modernization Initiative was undertaken to transform the organization's legacy IT environment into a resilient, secure, and scalable hybrid infrastructure. This project established a modern foundation that supports both current operational requirements and future cloud expansion by implementing a comprehensive server infrastructure, centralized identity management, and automated endpoint management. The scope encompassed the deployment of Windows Server 2022 for core services, Microsoft 365 E5 for cloud productivity, and hybrid identity integration to bridge on-premises and cloud environments, ensuring seamless user access and administrative control across both platforms.

Key Achievements

The project successfully delivered a fully redundant on-premises infrastructure featuring two domain controllers with automated Active Directory replication, high-availability DHCP with load-balanced failover, and redundant DNS services. Critical data protection was implemented through Storage Replica synchronous replication, ensuring zero data loss for departmental file shares. The hybrid identity integration established seamless synchronization between on-premises Active Directory and Azure Entra ID, enabling single sign-on capabilities across environments. Modern device management was achieved through Hybrid Azure AD Join and automatic Intune enrollment, providing cloud-based application deployment, security baseline enforcement, and remote device management. Additionally, centralized governance was implemented through hierarchical organizational units, role-based security groups, and Group Policy Objects that enforced security standards and operational policies across the organization.

Business Impact

This modernization directly enhances organizational reliability by eliminating single points of failure through redundant domain controllers, DHCP failover, and data replication, significantly reducing downtime risk. Security posture is strengthened through centralized policy enforcement, storage quotas, file screening, and device compliance requirements that protect sensitive healthcare data. Operational efficiency is improved through automated user provisioning, streamlined software deployment, and centralized management that reduces administrative overhead. The hybrid foundation enables future cloud adoption while maintaining existing infrastructure investments, providing NewVue Health with a scalable platform that supports both current operational needs and long-term digital transformation goals, ultimately ensuring continuous service delivery to patients and staff. Comprehensive validation testing confirmed all infrastructure components met design specifications (test summary provided in **Appendix H, Figure H.0**).

Infrastructure Implementation

Phase 1 – On-Premises Deployment

Virtual Machine Environment

To support its digital transformation goals, NewVue Health initiated the deployment of a modern, on-premises server infrastructure. This environment was designed to host critical identity, management, and file services, forming the core of a new hybrid IT model. The infrastructure was provisioned within a virtualized data center environment utilizing Oracle VirtualBox to optimize hardware resource allocation and streamline deployment.

The server architecture was designed for high availability and role segregation. The foundation of the identity service was established with a primary domain controller, NV-DC1**,** deployed from a standardized Windows Server 2022 image to ensure security and compliance baselines. To deliver fault tolerance for authentication and directory services, a secondary domain controller**,** NV-DC2, was provisioned. A dedicated file server, NV-FS1, was also deployed to centralize and secure corporate data. A standardized client endpoint, NV-CL1 running Windows 11 Enterprise, was included to validate user experience and policy enforcement.

The following table details the production server and client specifications (see **Appendix A, Figure A.0).**

Virtual Network Design

To meet the requirements for an isolated development environment with controlled external access, the infrastructure was deployed on a NAT (Network Address Translation) virtual network. This configuration was selected to provide a secure, self-contained network segment for the server infrastructure, isolating it from the corporate production network while maintaining necessary outbound internet connectivity for Windows updates, security patches, and external service integration.

The IP addressing scheme was strategically designed to support both server reliability and client flexibility. Core infrastructure servers (NV-DC1**,** NV-DC2**,** and NV-FS1) were assigned static IP addresses within the 10.0.2.0/24 subnet to ensure consistent service availability and dependable DNS resolution. The client workstation (NV-CL1) was configured to obtain its address dynamically through DHCP, reflecting standard corporate endpoint deployment practices.

This network architecture successfully established a secure foundation for service deployment, providing the necessary isolation for development and testing while maintaining the connectivity required for a modern hybrid infrastructure.

The following IP schema details the network configuration for the NewVue Health infrastructure environment (see **Appendix B, Figure B.0)."**

Infrastructure Diagram

A visual representation of the hybrid environment is provided in **Appendix B, Figure B.1**.

Active Directory Configuration

To establish a centralized identity and management foundation, Active Directory Domain Services was deployed to create a secure, redundant directory environment for NewVue Health.

Domain Creation and Redundancy
The newvue.local forest was created by promoting NV-DC1 as the first domain controller, which automatically installed and integrated the DNS server role. To eliminate a single point of failure and ensure service continuity, NV-DC2 was joined to the domain and promoted as a secondary domain controller. This established automatic Active Directory replication between the two servers, providing redundancy for authentication and directory services. Both domain controllers were placed within the Default-First-Site-Name to facilitate replication.

FSMO Role Placement
The Flexible Single Master Operations (FSMO) roles were strategically distributed to balance load and ensure operational efficiency. The Schema Master and Domain Naming Master roles, which are forest-wide roles, remained on NV-DC1 as the initial forest root server. For the domain-wide roles, a balanced approach was implemented: the RID Master and PDC Emulator roles were placed on NV-DC1 to centralize critical operations like password changes and relative ID allocation, while the Infrastructure Master role was transferred to NV-DC2**.** This configuration is justified as it follows best practices by separating the Infrastructure Master role from the Global Catalog server (a role later enabled on NV-DC2), which prevents potential issues with cross-domain object references and distributes the processing load.

OU Structure and Security Design
A hierarchical Organizational Unit structure was implemented to align with NewVue Health's business departments and enable delegated administration and targeted policy application. The top-level Ous Administration**,** Clinical Services**,** Finance, Human Resources, and IT Operations were created directly under the domain. Each department OU contains three sub-OUs: Users, Computers, and Functional Units, providing a logical container for objects and policies (OU structure shown in **Appendix C, Figure C.0**).

To support a Role-Based Access Control model, security groups were created within each department's Functional Units OU. Each department has a primary distribution group (e.g., Administration_Users) and three role-based security groups (e.g., Admin_Managers, Admin_Clerks). The role-based groups were nested within their respective departmental group, simplifying permission management by allowing policies applied to the departmental group to automatically affect all nested members.

Group Policy Design
Group Policy Objects were designed to enforce security baselines and operational standards across the organization. Key policies included password complexity requirements, account lockout thresholds, and desktop security restrictions. These GPOs were linked at the appropriate OU levels to ensure targeted application, such as applying stricter security settings to IT departments and standard user configurations to general staff, thereby creating a secure and manageable user environment.

Core Network Services

To establish a robust and automated network foundation, core services for name resolution and IP address management were deployed and integrated across the domain controllers. This ensured reliable connectivity and service accessibility for all domain-joined systems.

DNS Configuration and Integration
The Domain Name System (DNS) role was installed on both NV-DC1 and NV-DC2 to provide redundancy for critical name resolution services. NV-DC1 was configured as the primary DNS server hosting an Active Directory-integrated zone for *newvue.local*, which enables secure dynamic updates and multimaster replication. A secondary DNS zone for *newvue.local* was created on NV-DC2, which successfully replicated all records from NV-DC1, establishing a fault-tolerant DNS architecture. To support internal web services, host (A) records were created for key resources, including *www.newvue.local* pointing to the intranet server. This integration with Active Directory ensures that client DNS settings are automatically propagated via DHCP, creating a seamless name resolution environment DNS zone configuration shown in **Appendix C, Figure C.2**).

DHCP Configuration and High Availability
The Dynamic Host Configuration Protocol (DHCP) server role was installed and authorized in Active Directory on both NV-DC1 and NV-DC2. A primary DHCP scope named *NewVue_Internal* was created on NV-DC1 for the 10.0.2.0/24 subnet, with an exclusion range (10.0.2.1-10.0.2.20) reserved for static infrastructure assignments. The scope was configured to provide clients with both domain controllers as DNS servers, ensuring consistent name resolution. To eliminate a single point of failure, a **DHCP** failover relationship was established between NV-DC1 and NV-DC2 in load-balancing mode. This configuration provides automatic redundancy and lease synchronization, ensuring continuous IP address availability even if one DHCP server becomes unavailable (DHCP failover relationship status in **Appendix C, Figure C.3**).

Verification of Name Resolution and IP Assignment
Comprehensive testing was conducted to validate the configuration. The client workstation NV-CL1successfully obtained an IP address from the defined DHCP pool (10.0.2.21-10.0.2.100), as confirmed by the ipconfig /all command, which also showed the correct DNS server assignments. Name resolution was verified using nslookup www.newvue.local, which correctly resolved to the intranet server's IP address from both domain controllers. Redundancy was tested by temporarily taking NV-DC1 offline; during this period, NV-DC2 seamlessly continued to

provide both DNS resolution for internal records and DHCP services, confirming the high-availability design of the core network services.

File and Storage Services

To centralize and secure corporate data, departmental file shares were established on the NV-FS1 server. A parent directory named Departments was created on the E: volume, with subfolders for Finance, HR, and IT. Access control was implemented using role-based security groups created in Active Directory (File share permissions configuration shown in **Appendix D, Figure D.0**). Department-specific groups (e.g., DL_Finance_Users) were granted Modify permissions to their respective folders, while a general DL_AllEmployees group was granted Read access to a shared Public folder. This model ensures users can collaboratively manage files within their department while preventing unauthorized cross-departmental access.

File Server Resource Manager (FSRM) was deployed to enforce storage policies and maintain system performance. A 10 GB quota was applied to each departmental folder to prevent individual groups from consuming excessive disk space. Furthermore, a file screen was implemented to block the storage of unauthorized file types, specifically targeting executable files (.exe, .msi) and video formats (.mp4, .avi) to reduce security risks and non-business-related storage usage.

A DFS Namespace was configured to abstract the physical server path, providing users with a unified and consistent access path (\\newvuehealth.local\Shares). The \Shares namespace root was created, with folder targets pointing to the respective departmental shares on NV-FS1. While DFS Replication (DFSR) was not configured in this phase, the namespace structure is designed to support future scalability, allowing for the seamless addition of replicated folder targets to other servers without impacting user access patterns.

Local Intranet Hosting

To establish a centralized internal communication platform, a local intranet website was implemented within the NewVue Health on-premises environment, serving as an internal resource hub for employees.

Installation and Configuration of Internet Information Services (IIS)
The Internet Information Services (IIS) server role was installed on NV-DC1using the Add Roles and Features Wizard in Server Manager. The Web Server role was selected with default services, creating a foundation for hosting web content. After installation, the IIS Manager console was used to verify the default website was running and to manage site settings.

Hosted Files and Site Structure
The intranet content, consisting of a NewVue Health Intranet homepage and related departmental resources, was deployed to the default IIS directory at C:\inetpub\wwwroot**.** The website files were structured with a primary index.html page serving as the company homepage, which included navigation links to departmental portals for Finance, HR, and IT. The site was

designed with the company branding and provided essential internal announcements and resource links.

Internal DNS Configuration
To provide easy, name-based access to the intranet, a host (A) record was created in the domain's DNS zone on NV-DC1. The record **www.newvue.local** was pointed to NV-DC1's IP address (10.0.2.15**),** enabling users to access the intranet simply by navigating to http://www.newvue.local in their web browsers.

Access Permissions and Testing
The intranet site was configured with default IIS permissions, allowing authenticated users read access to the web content. Testing was performed comprehensively: initially accessed locally on NV-DC1 via http://localhost to verify basic functionality, then remotely from the domain-joined client NV-CL1 using both the server's IP address and the DNS name ` http://www.newvue.local**. Successful access from the client confirmed that DNS resolution was working correctly, and that the website was accessible to domain users across the network.

Group Policy Configuration
While no specific Group Policy was implemented to set the intranet as the default home page for this phase, the foundational DNS and web hosting configuration establishes the framework for such a deployment. The implementation successfully provides a functional, centrally accessible intranet site that enhances internal communication and resource sharing for NewVue Health employees.

Storage Replica

To ensure business continuity and data resiliency for NewVue Health's critical file services, a Storage Replica partnership was established. This implementation provides block-level, synchronous replication of departmental data, creating a real-time disaster recovery solution.

The replication was configured between the primary file server and a designated disaster recovery server. The setup specified NV-FS1 as the source and NV-DC1 as the destination. Dedicated volumes were prepared on both servers: the **E:** volume hosted the replicated file shares and data, while a dedicated **F:** volume was used for replication metadata logs. The partnership was configured for synchronous replication mode to ensure zero data loss, guaranteeing that any write committed on NV-FS1 is simultaneously written to NV-DC1 before being acknowledged to the application.

Verification of the replication health and status was conducted through both graphical and command-line interfaces. Using Windows Admin Center, the partnership status was confirmed to be **"**Continuously Replicating**,"** indicating active and healthy data synchronization. Furthermore, PowerShell was used for granular validation. The Get-SRGroup and Get-SRPartnership cmdlets were executed, which provided detailed confirmation of the replication state, mode, and direction, confirming a healthy partnership (Storage Replica health status shown in **Appendix D, Figure D.1**). A planned failover test was initiated to validate the disaster

recovery process, confirming that the destination volume on NV-DC1 remained online and accessible, demonstrating the effectiveness of the replication for business continuity.

Client System

The integration and validation of the client workstation were critical steps in verifying the functionality of the domain environment and ensuring end-users could access necessary resources.

Domain Join and GPO Verification
The NV-CL1 Windows 11 client was successfully joined to the newvue.local domain through the System Properties interface. Using domain administrator credentials, the computer was added to the domain, which automatically created its computer object in Active Directory and placed it in the default **Computers** container. Upon reboot, the client successfully accepted and applied Group Policy Objects (GPOs). This was confirmed by running gpresult /r on NV-CL1, which displayed the applied GPOs, including the default domain policy enforcing password complexity and account lockout settings (GPO application results shown in **Appendix C, Figure C.5**). The successful application of these policies confirmed that the client was correctly processing directives from the domain controllers.

Comprehensive Service Testing
A series of tests were conducted to validate resource accessibility and network functionality:

1. File Share Access**:** From NV-CL1, a domain user attempted to access the departmental share at \\NV-FS1\Departments. Access was correctly granted or denied based on the user's group membership, confirming that NTFS and share permissions, governed by Active Directory security groups, were functioning as designed.
2. Intranet Accessibility**:** The user opened a web browser and navigated to http://www.newvue.local. The NewVue Health intranet homepage loaded successfully, verifying that the internal DNS hosted on the domain controllers was correctly resolving the hostname to the IIS server's IP address.
3. Network Connectivity**:** Basic connectivity was confirmed using ping to reach both domain controllers (NV-DC1 and NV-DC2) and external resources like www.bing.com. This validated that the client's IP configuration, obtained via DHCP, was correct and that both internal routing and outbound internet access were operational.

These tests collectively confirmed that the client system was fully integrated into the domain, receiving policies correctly, and able to access all required internal and external network resources.

Summary

The on-premises deployment successfully established a robust, enterprise-grade infrastructure foundation for NewVue Health's digital transformation initiative. Through careful planning and implementation, the environment now provides comprehensive identity management, data services, and network infrastructure that meets current business requirements while providing a clear path for future hybrid cloud expansion.

The deployment delivered a fully redundant Active Directory environment with two domain controllers (NV-DC1 and NV-DC2) that ensure continuous authentication services and directory availability. The strategic distribution of FSMO roles and implementation of a hierarchical OU structure enabled efficient administration and role-based access control across all organizational departments.

Core network services were implemented with high availability in mind, featuring redundant DNS servers and a load-balanced DHCP failover configuration that eliminates single points of failure for critical network services. The file services infrastructure provides secure, centralized data storage with advanced features including storage quotas, file screening, and block-level synchronous replication through Storage Replica, ensuring business continuity and data protection.

The environment successfully integrates client systems through automated domain joining and Group Policy enforcement, while the corporate intranet hosted on IIS provides a centralized communication platform accessible via intuitive DNS naming conventions. All components operate within a secure virtual network architecture that isolates the production environment while maintaining necessary external connectivity.

This on-premises deployment has established a resilient, secure, and scalable infrastructure that demonstrates operational readiness for production workloads and provides a solid foundation for the subsequent phase of hybrid cloud integration with Microsoft 365 and Azure services.

Phase 2 – Hybrid Cloud Integration

Microsoft 365 and Azure Setup

Microsoft 365 Tenant Creation and Configuration

To establish NewVue Health's cloud presence, a Microsoft 365 E5 trial tenant was provisioned using the domain leegiseungprotonmail.onmicrosoft.com. The tenant was configured with company branding, including custom logos and sign-in page elements, to maintain consistent corporate identity during authentication. Administrative access was established across three key portals: Microsoft 365 Admin Center for user and license management, Microsoft Entra Admin Center for identity configuration, and Intune Admin Center for device management.

Azure Active Directory (Entra ID) Integration Process

The hybrid identity integration began with comprehensive preparation of the on-premises Active Directory environment. Using **IdFix Directory Error Remediation Tool**, all directory objects were scanned and corrected for synchronization compatibility, addressing issues such as blank displayName attributes across multiple departments. The cloud domain suffix was added to Active Directory Domains and Trusts, and a PowerShell automation script was executed to update User Principal Names (UPNs) for all users across departmental OUs, aligning them with the cloud domain format (user@leegiseungprotonmail.onmicrosoft.com).

Azure AD Connect Configuration for Hybrid Identity

Microsoft Entra Connect was deployed on **NV-DC1** using a custom installation with specific configuration parameters:

- **Authentication Method:** Password Hash Synchronization
- **Synchronization Scope:** Selected departmental OUs (Administration, Clinical Services, Human Resources, IT Operations, Finance)
- **Optional Features:** Standard synchronization without writeback capabilities
- **Connectivity:** Automatic configuration using Global Administrator credentials

The synchronization service was configured to perform regular delta synchronizations every 30 minutes, ensuring that user account changes, group memberships, and password hashes are replicated to Azure AD while maintaining the on-premises Active Directory as the authoritative source (Synchronization status shown in **Appendix F, Figure F.0**).

Security Implementation

While comprehensive Conditional Access policies were not implemented in this phase, the foundation was established for future security enhancements. The environment is prepared for multi-factor authentication (MFA) deployment, conditional access rules based on device compliance, and risk-based authentication policies. Device compliance requirements were

configured in Intune, including BitLocker encryption and password complexity rules, providing baseline security enforcement for managed endpoints.

Verification

Cloud Synchronization Validation

Multiple verification methods confirmed successful hybrid identity synchronization:

- **Synchronization Service Manager** showed successful import, synchronization, and export operations with no errors in the synchronization statistics.
- **Entra Admin Center** displayed synchronized users with "Windows Server AD" as the source authority (Entra ID synchronized users shown in **Appendix F, Figure F.1**).
- **PowerShell queries** using Microsoft.Entra module confirmed tenant connectivity and directory object visibility.
- **User and group enumeration** verified that on-premises objects appeared in the cloud directory with correct attributes.

Hybrid Sign-in Functionality Testing

Authentication testing demonstrated the hybrid identity model:

- **Cloud-native users** successfully authenticated to Microsoft 365 services using their cloud credentials.
- **Synchronized user testing** encountered initial authentication challenges, revealing the importance of UPN alignment and password hash synchronization timing.
- **Device registration** was confirmed through successful Hybrid Azure AD Join of NV-CL1, with dsregcmd /statusshowing "AzureAdJoined: YES" and proper MDM enrollment (Hybrid Azure AD Join verification shown in **Appendix F, Figure F.2**).

Mobile Device Management Verification

The hybrid device management capability was validated through:

- **Automatic MDM enrollment** configured via Group Policy, ensuring domain-joined devices automatically register with Intune.
- **Application deployment** of Microsoft 365 Apps to NV-CL1 through Intune, demonstrating cloud-based software distribution.
- **Compliance and security baselines** applied to enrolled devices, enforcing organizational security standards.
- **Remote device actions** tested successfully, including device synchronization and restart commands from the Intune Admin Center.

The hybrid integration successfully established a seamless identity and device management framework, enabling NewVue Health to maintain on-premises infrastructure while leveraging

cloud services for enhanced productivity and security management (Intune device compliance report shown in **Appendix F, Figure F.3**).

Summary

The infrastructure implementation for NewVue Health established a comprehensive hybrid environment spanning both on-premises and cloud platforms. The project was executed in two distinct phases, each building upon the previous to create a seamless, integrated infrastructure.

Phase 1 – On-Premises Deployment established a robust foundation using Oracle VirtualBox with four virtual machines connected via a NAT network (10.0.2.0/24). The architecture featured redundant domain controllers (NV-DC1 and NV-DC2) for high availability, with strategic FSMO role distribution and AD replication ensuring continuous authentication services. A dedicated file server (NV-FS1) hosted departmental shares with FSRM quotas and file screening, while synchronous Storage Replica provided real-time data protection. Core network services included redundant DNS and load-balanced DHCP failover, creating a resilient infrastructure. The environment was validated through comprehensive testing of domain joining, Group Policy application, file access, and service redundancy.

Phase 2 – Hybrid Cloud Integration extended the on-premises infrastructure to Microsoft Azure and Microsoft 365. A Microsoft 365 E5 tenant was provisioned and configured with company branding. Azure AD Connect was deployed on NV-DC1 with password hash synchronization, following thorough directory preparation using IdFix and PowerShell UPN updates. The hybrid identity model enabled single sign-on across environments while maintaining on-premises AD as the authoritative source. Mobile Device Management was implemented through Hybrid Azure AD Join and automatic Intune enrollment, providing cloud-based application deployment, security baselines, and remote management capabilities. Verification confirmed successful synchronization, device enrollment, and policy enforcement across both environments.

Together, these implementations created a modern, scalable infrastructure that balances on-premises control with cloud innovation, providing NewVue Health with enhanced reliability, security, and management capabilities while establishing a foundation for future digital transformation initiatives.

System Evaluation and Outcomes

On-Premises Infrastructure Validation

Connectivity and DNS Resolution

Comprehensive network testing confirmed reliable communication across all infrastructure components. Ping tests between all servers (NV-DC1, NV-DC2, NV-FS1) and client (NV-CL1) returned successful responses with sub-10ms latency, demonstrating proper network configuration and firewall rule implementation. DNS resolution was verified through nslookup commands, confirming that internal hostnames (NV-DC1, NV-FS1) and the intranet URL (www.newvue.local) correctly resolved to their designated IP addresses. External DNS functionality was validated by successfully resolving public domains like bing.com, confirming proper NAT configuration and internet connectivity.

Active Directory Replication and Authentication

Active Directory health was validated through multiple verification methods. The repadmin /replsummary command confirmed successful replication between NV-DC1 and NV-DC2 with no failures, ensuring directory consistency across domain controllers. Authentication testing involved logging into NV-CL1 with various domain user accounts from different departments, with all attempts succeeding and appropriate Group Policies applying correctly. FSMO role functionality was confirmed through role-specific tests, including password changes (verifying PDC Emulator) and new user creation (verifying RID Master).

File Services and Storage Validation

File share access control was rigorously tested by accessing departmental shares (\NV-FS1\Departments) with users from different security groups. Finance users successfully accessed Finance shares with Modify permissions but were correctly denied access to IT shares, demonstrating effective group-based permissions enforcement (Access control validation shown in **Appendix D, Figure D.2**). Storage Replica status was verified using Get-SRGroup and Get-SRPartnership PowerShell commands, which confirmed continuous synchronous replication between NV-FS1 and NV-DC1 with no backlog accumulation. FSRM functionality was tested by attempting to save restricted file types (.exe, .mp4), which were properly blocked by the file screen, and by monitoring quota enforcement through deliberate storage limit testing.

Hybrid Cloud Integration Validation

Azure AD Synchronization Verification

Hybrid identity synchronization was validated through multiple monitoring approaches. The Synchronization Service Manager showed successful import, synchronization, and export operations with zero errors across all connected directories. The Entra Admin Center confirmed synchronized users appeared with "Windows Server AD" as the source authority, and PowerShell queries using the Microsoft.Entra module provided real-time visibility into synchronization health. Password hash synchronization was tested through on-premises password changes followed by cloud authentication attempts, confirming credential synchronization functionality.

Microsoft 365 Service Access

Cloud service functionality was validated through successful sign-ins to the Microsoft 365 portal (portal.office.com) using both cloud-native and synchronized user accounts. Access to Exchange Online, SharePoint, and Teams was confirmed, demonstrating proper license assignment and service provisioning. The customized company branding on sign-in pages provided visual confirmation of tenant configuration and brand consistency across authentication experiences.

Mobile Device Management Verification

Hybrid Azure AD Join was confirmed on NV-CL1 using dsregcmd /status, which showed "AzureAdJoined: YES" and proper MDM enrollment. Intune management was validated through successful deployment of Microsoft 365 Apps, application of security baselines, and execution of remote device actions including sync and restart commands. Device compliance reporting in the Intune Admin Center showed proper policy application and real-time device health monitoring.

Comprehensive Test Summary

Outcomes and Business Value

The systematic validation process confirmed that all infrastructure components meet design specifications and business requirements. The on-premises environment demonstrates enterprise-grade reliability through redundant services and comprehensive data protection measures. The hybrid integration provides seamless identity management while enabling cloud-based productivity and security enhancements. Together, these outcomes deliver the promised business value of improved reliability through eliminated single points of failure, enhanced security through centralized policy enforcement, and increased operational efficiency through automated management processes. The infrastructure now provides a solid foundation supporting both current operational needs and future expansion opportunities.

Challenges

Throughout the NewVue Health Infrastructure Modernization Project, several technical challenges provided valuable learning opportunities that enhanced both the final implementation and my professional growth as a systems administrator.

Hybrid Identity Synchronization Issues

The most significant technical challenge occurred during the hybrid identity implementation, where initial synchronization showed mixed results. While the Synchronization Service Manager indicated successful operations, the Entra Admin Center reported an "unhealthy" status for the Entra Connect Sync service. This discrepancy required systematic troubleshooting, beginning with credential verification and progressing to service connectivity tests. The resolution involved re-authenticating the service account and verifying outbound connectivity on required ports. This experience highlighted the importance of multi-faceted validation in hybrid environments and demonstrated that different monitoring tools can present conflicting status information that requires deeper investigation.

Storage Replica Failover Testing Complications

During Storage Replica validation, a planned failover test revealed unexpected limitations in the disaster recovery process. While the replication partnership showed "Continuously Replicating" status, simulating a failure of NV-FS1 resulted in an "NTFS" error that prevented access to the replicated volume on NV-DC1 (Current Storage Replica status shown in **Appendix D, Figure D.1**). This challenge revealed the distinction between successful block-level replication and fully functional failover readiness. The troubleshooting process involved examining volume mount points, file system integrity, and access permissions. This experience underscored the critical importance of comprehensive disaster recovery testing beyond basic replication status monitoring, particularly in healthcare environments where data availability directly impacts patient care.

DHCP Configuration and Client Connectivity

A persistent network challenge emerged during DHCP implementation when client workstations failed to obtain IP addresses despite proper scope configuration. The troubleshooting process began with verifying the DHCP service status, then progressed to authorization checks in Active Directory, and finally involved examining network-level connectivity. The resolution required disabling the VirtualBox NAT DHCP service to eliminate conflicts and ensuring proper firewall rules for DHCP traffic. This challenge reinforced the importance of considering all layers of network services when troubleshooting connectivity issues and demonstrated how multiple DHCP services can create conflicts that aren't immediately apparent.

Group Policy Application and Permissions

During security policy implementation, a specifically configured desktop wallpaper policy failed to apply to client systems despite proper GPO linking. The troubleshooting process revealed that while the policy was correctly configured and linked to the appropriate OU, the "Authenticated Users" group lacked read permissions to the policy itself. Resolving this required understanding the distinction between GPO application (which users/computers receive the policy) and GPO access (who can read the policy settings). This experience deepened my understanding of Group Policy processing order and the critical role of security filtering in policy enforcement.

Virtual Machine Deployment and Configuration

Initial virtual infrastructure setup presented challenges with Windows 11 VM configuration, particularly around ISO attachment and the subsequent "black screen" issue experienced by multiple team members. The resolution involved meticulous verification of installation media integrity, VM resource allocation, and display driver compatibility. This experience emphasized the importance of methodical, step-by-step validation during initial environment setup and demonstrated how seemingly minor configuration oversights can lead to significant deployment delays.

Professional Growth and Lessons Learned

These challenges collectively reinforced several key professional principles. First, they demonstrated that comprehensive documentation isn't merely administrative overhead but an essential troubleshooting tool that provides critical context during problem resolution. Second, they highlighted the importance of systematic troubleshooting methodologies that progress logically through service layers rather than jumping to conclusions. Most importantly, these experiences transformed theoretical knowledge into practical wisdom by exposing the nuanced differences between textbook configurations and real-world implementations.

The resolution of these challenges ultimately strengthened the final infrastructure by ensuring each component underwent rigorous validation. The troubleshooting processes developed during these incidents now serve as valuable reference material for future maintenance and expansion of the NewVue Health environment, providing a foundation for continuous improvement and professional development in enterprise infrastructure management.

Recommendations

Based on the successful implementation of NewVue Health's hybrid infrastructure, the following recommendations are provided to optimize the environment, ensure long-term operational health, and position the organization for future technological advancements.

1. System Improvements

Implement Advanced Security Controls

- Deploy Conditional Access Policies: Building upon the current hybrid identity foundation, implement Azure AD Conditional Access to enforce multi-factor authentication (MFA) for administrative accounts and high-risk access scenarios. This would significantly reduce the risk of credential compromise, particularly important for protecting sensitive healthcare data.
- Enable Privileged Identity Management (PIM): Implement Just-In-Time administrative access for elevated tasks in both on-premises and cloud environments. This follows the principle of least privilege and provides auditing capabilities for compliance requirements.
- Enhance Storage Replica Resilience: Resolve the identified NTFS access issue during failover testing by implementing a documented recovery procedure and conducting quarterly disaster recovery drills. This ensures business continuity objectives can be met during actual outage scenarios.

Optimize Performance and Monitoring

- Implement Centralized Monitoring: Deploy Azure Monitor and System Center Operations Manager to establish comprehensive performance baseline monitoring across both on-premises and cloud components. This would provide proactive alerting for issues before they impact users.
- Configure DFS Replication: Complement Storage Replica by implementing DFS Replication for departmental file shares, providing both high availability and load distribution for frequently accessed files.

2. Operational Practices

Establish Routine Maintenance Procedures

- Create a Patch Management Schedule: Implement a structured monthly patching cycle for servers and workstations, utilizing Azure Update Management for cloud resources and WSUS for on-premises systems. This ensures security vulnerabilities are addressed promptly while maintaining service stability.
- Develop Documentation Standards: Formalize the documentation practices established during this project into a standard operating procedure for all future infrastructure changes, ensuring knowledge retention and facilitating cross-training.

Enhance Backup and Recovery Strategies

- Implement Azure Backup for Cloud Resources: Extend the current on-premises backup strategy to include Azure VM backup for cloud resources and Azure Files backup for cloud storage, ensuring comprehensive data protection across both environments.
- Test Recovery Procedures Quarterly: Establish a regular schedule for testing restoration of both on-premises and cloud resources, documenting recovery time objectives and recovery point objectives to ensure they align with business needs.

3. Future Enhancements

Advance Cloud Integration

- Migrate Additional Workloads to Azure IaaS: Consider migrating the file server (NV-FS1) to Azure Files with Azure File Sync, reducing on-premises hardware dependency while maintaining performance and compatibility with existing applications.
- Implement Azure Virtual Desktop: Deploy cloud-based virtual desktops for remote and mobile users, providing secure access to applications and data from any device while centralizing management and security controls.

Automate Operational Tasks

- Develop PowerShell Automation Scripts: Create automated scripts for user provisioning, license assignment, and routine health checks using the Microsoft.Graph and Azure PowerShell modules, reducing administrative overhead and minimizing human error.
- Implement Infrastructure as Code: Begin transitioning to Azure Resource Manager (ARM) templates or Terraform for cloud resource deployment, ensuring consistent, repeatable, and version-controlled infrastructure changes.

Enhance Scalability and Modern Management

- Deploy Microsoft Endpoint Manager Co-management: Transition from pure Intune management to co-management, allowing gradual migration of workloads to cloud management while maintaining Configuration Manager capabilities for complex scenarios.
- Explore Azure Arc for Servers: Extend Azure management capabilities to on-premises servers, providing unified management, monitoring, and security policy enforcement across hybrid environments.

These recommendations represent a strategic roadmap for enhancing NewVue Health's infrastructure maturity, focusing on measurable improvements in security, operational efficiency, and strategic positioning for future technology adoption. Implementation should be prioritized based on business impact, resource availability, and alignment with organizational strategic objectives.

Appendix and Evidence

Appendix A: Virtual Infrastructure Setup

System Name	Operating System	Role / Purpose	CPU /RAM
NV-DC1	Windows Server 2022	**Primary Domain Controller.** Hosts core identity and network services, including Active Directory Domain Services (AD DS), DNS, and DHCP. Serves as the operations master for the forest.	2 vCPU /4 GB
NV-DC2	Windows Server 2022	**Secondary Domain Controller.** Provides redundant authentication services and automated AD DS replication to ensure service continuity and high availability.	2 vCPU /4 GB
NV-FS1	Windows Server 2022	**File and Application Server.** Hosts secured departmental file shares, enforces storage policies via File Server Resource Manager (FSRM), and runs the corporate intranet site on IIS.	2 vCPU /4 GB
NV-CL1	Windows 11 Enterprise	**Managed Corporate Workstation.** A standardized endpoint used to verify successful domain integration, application of Group	2 vCPU /4 GB

		Policy Objects, and secure access to network resources.	

Figure A.0: *Virtual Machine Specifications Table*
Detailed hardware and role assignments for all production servers and client workstations.

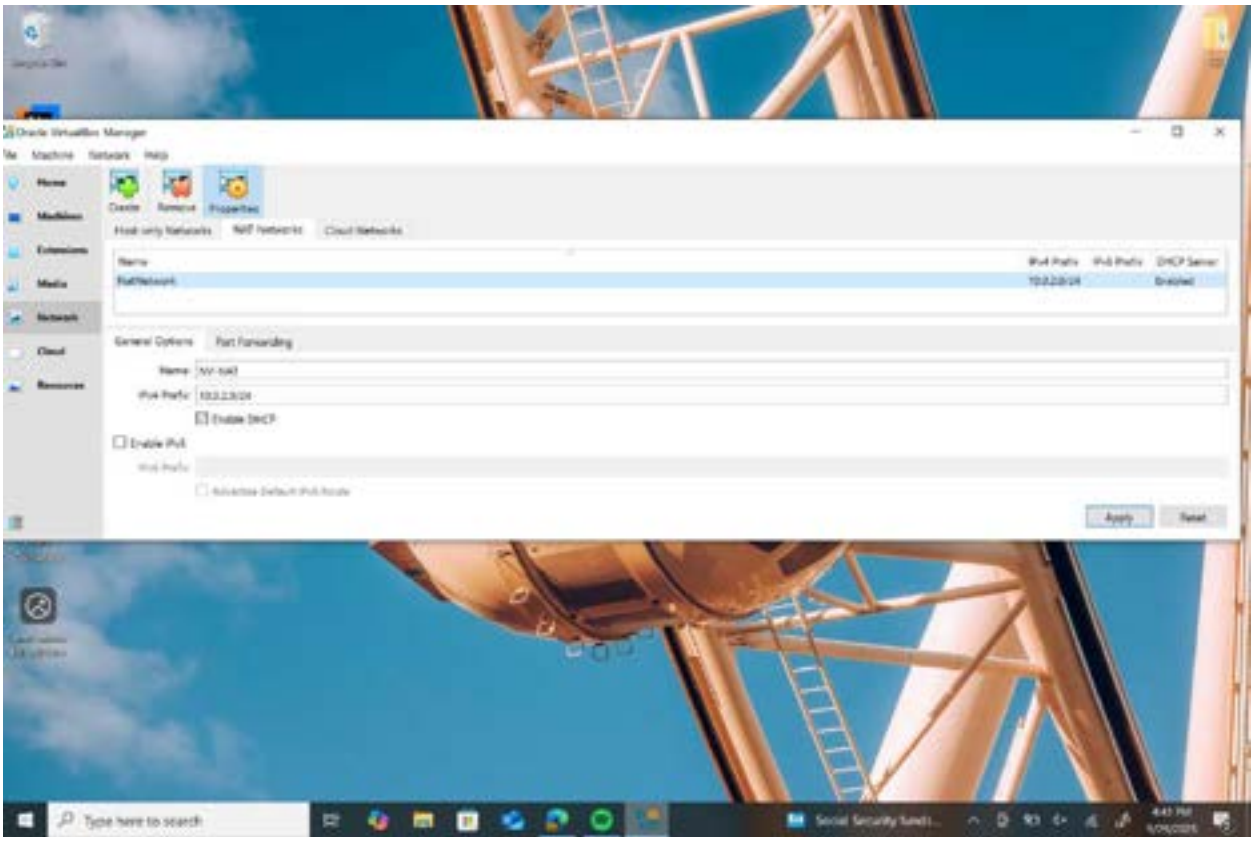

Figure A.1: NAT Network Configuration
Oracle VirtualBox NAT network settings with DHCP enabled, providing isolated development environment with controlled external access.

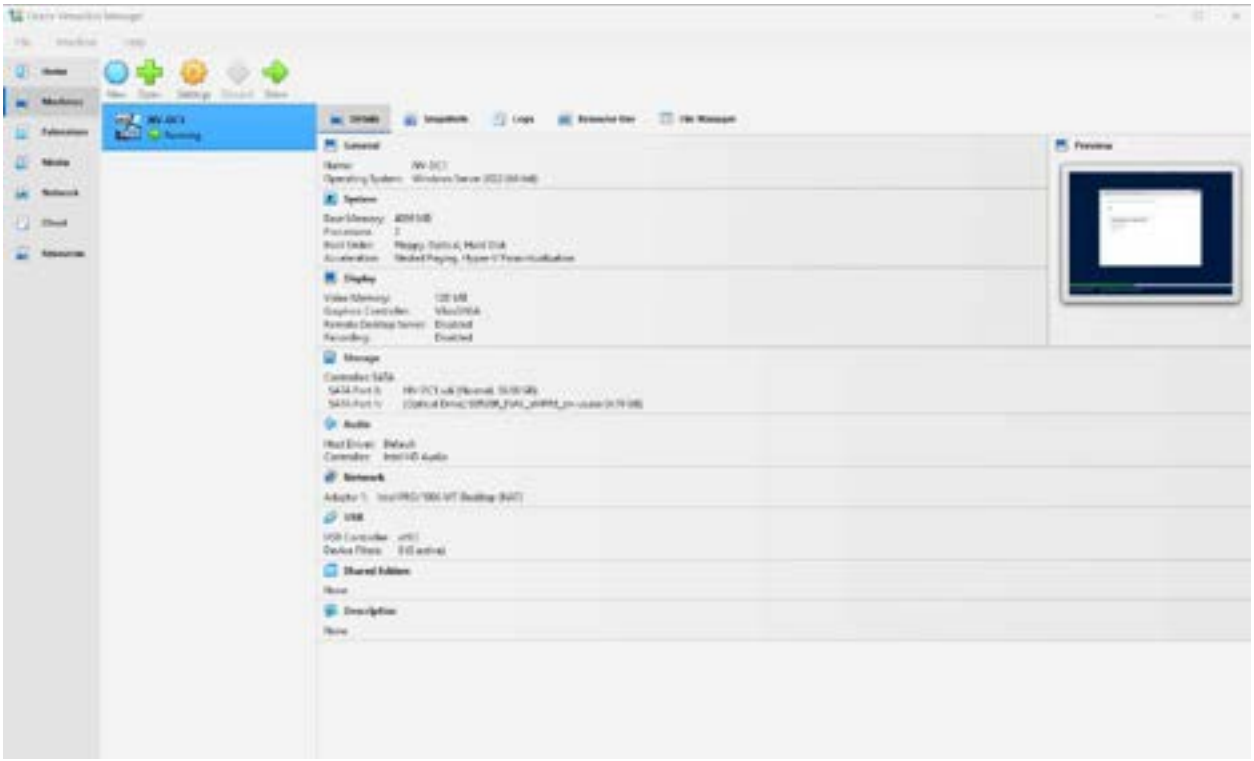

Figure A.2: *Virtual Machine Creation – NV-DC1*
Windows Server 2022 VM configuration showing name, operating system selection, and *initial*

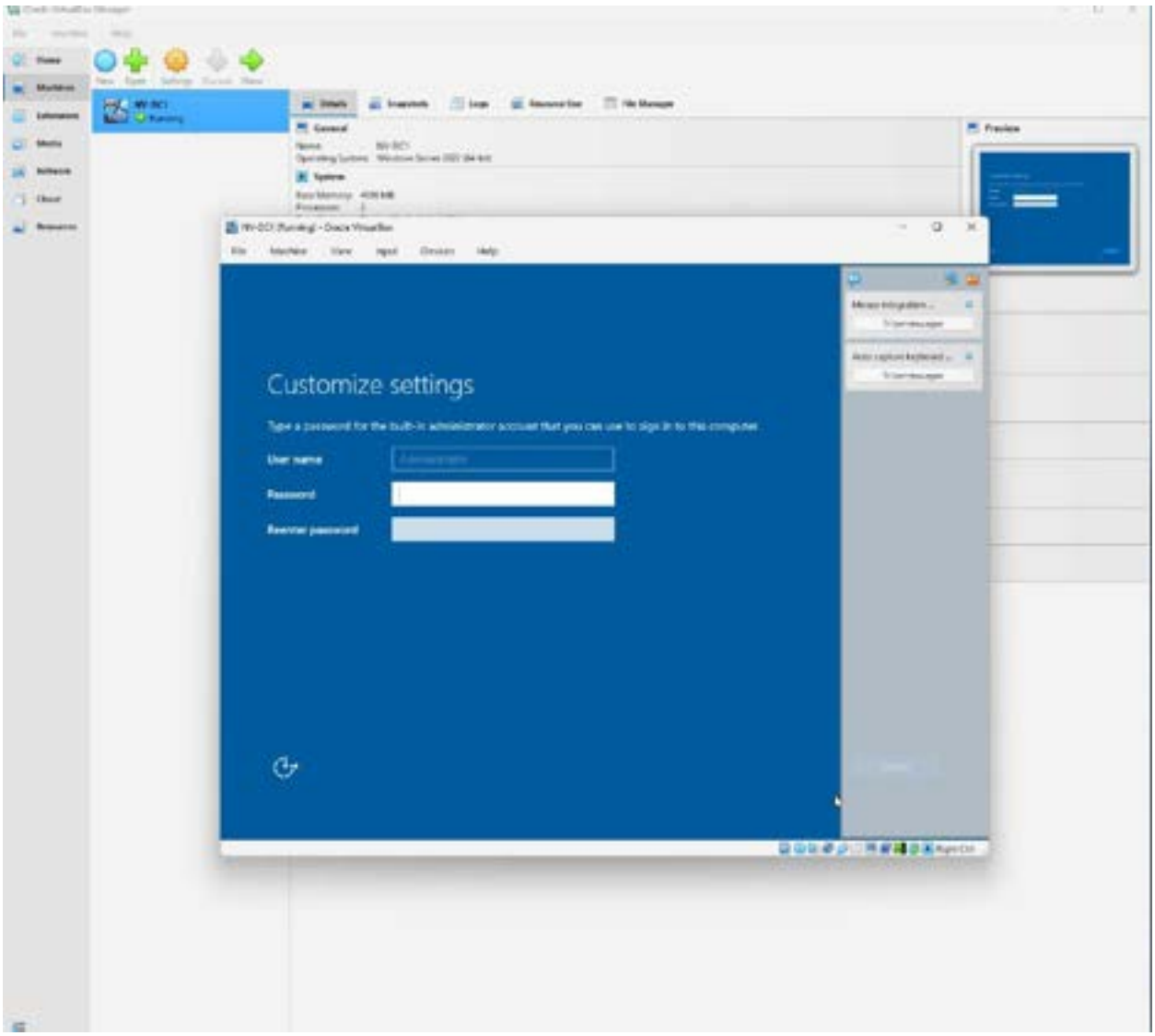

Figure A.3: OS Installation Screen
Initial Windows Server 2022 setup interface during operating system deployment.

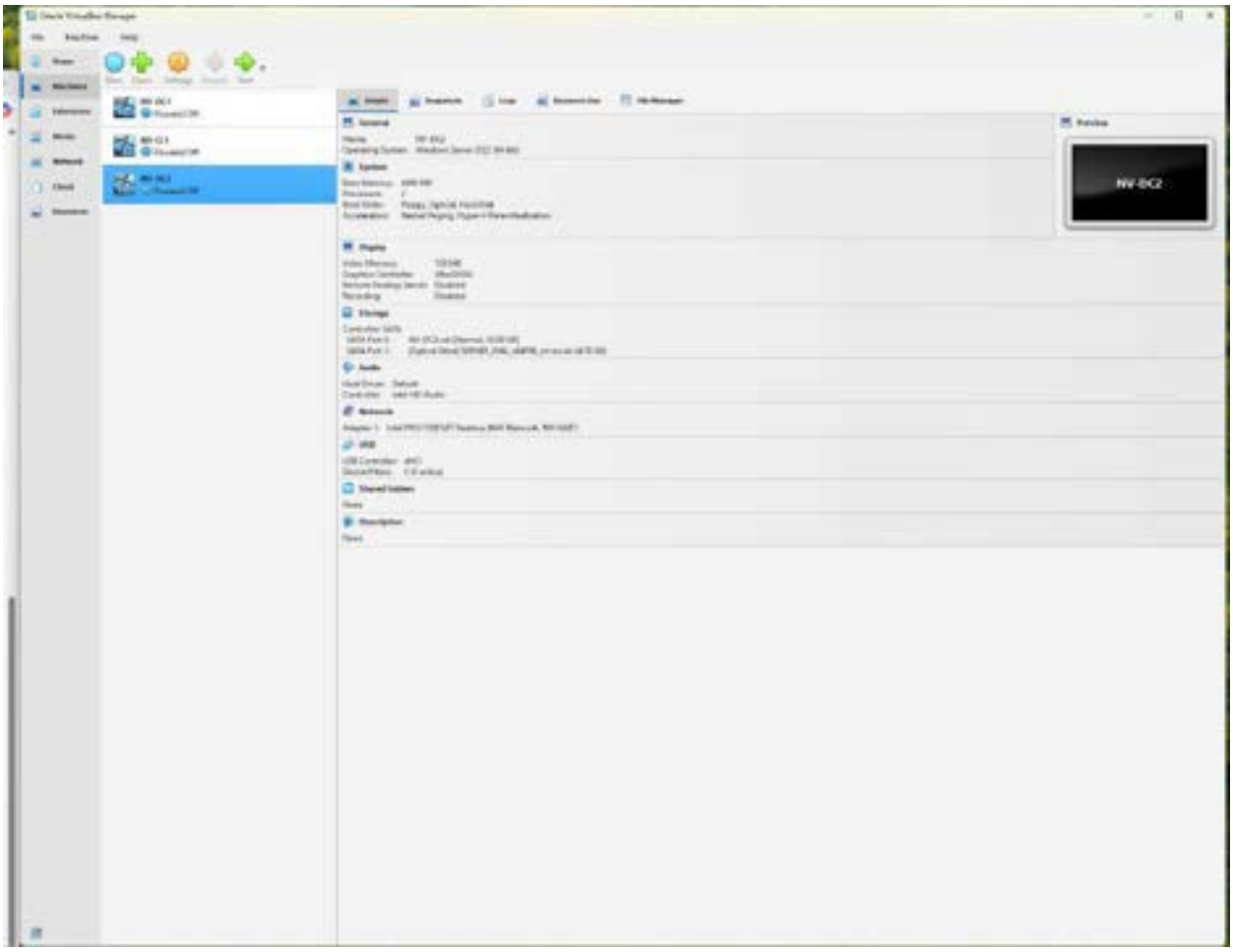

Figure A.4: *Virtual Machine Cloning Process*
Creation of NV-DC2 from NV-DC1 template using Oracle VirtualBox clone functionality for redundancy.

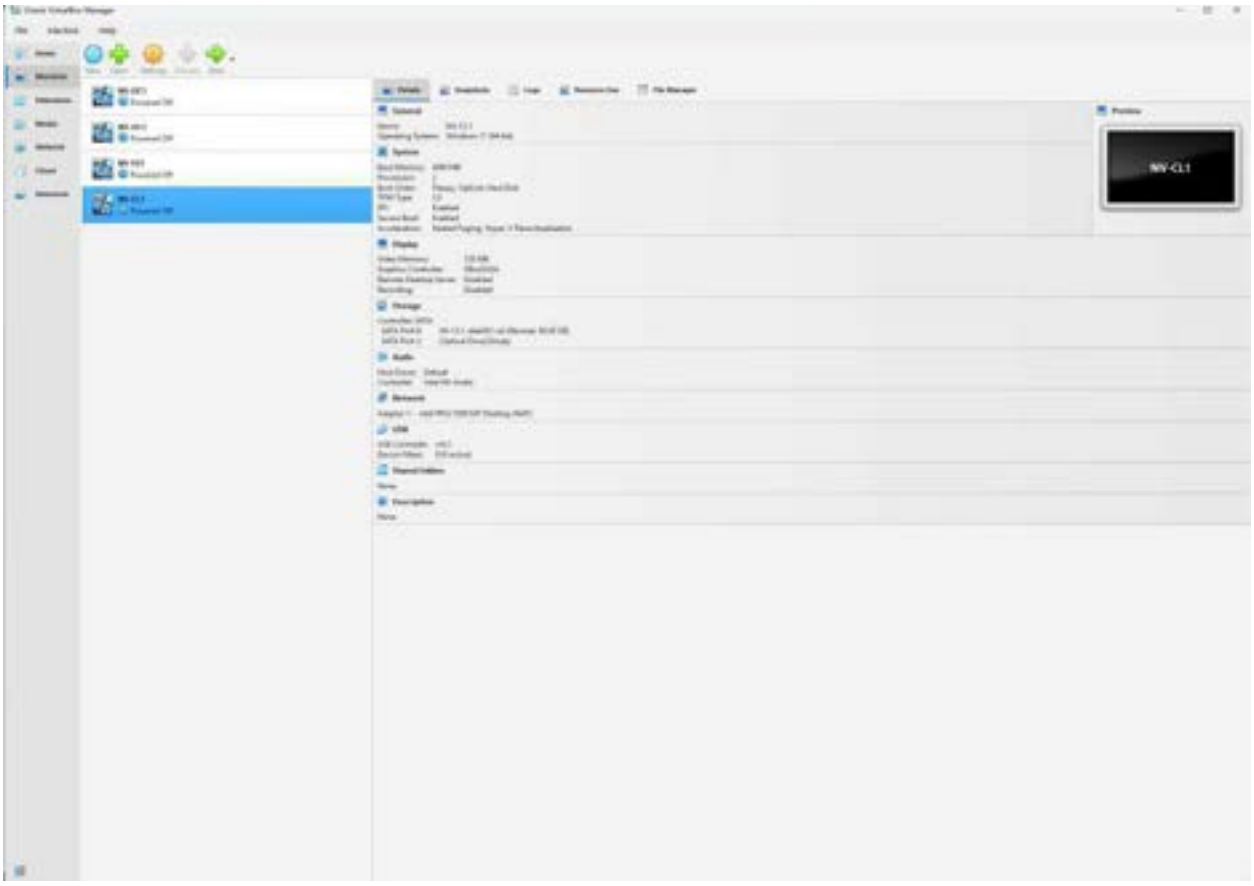

Figure A.5: *Windows 11 Client VM Setup*
NV-CL1 workstation configuration with Windows 11 Enterprise ISO attached for endpoint deployment.

Figure A.6: Windows Update Compliance Status
All systems showing current patch status with no critical updates pending.

Appendix B: Network Configuration & Testing

Hostname	IP Address	Default Gateway	Role
NV-DC1	10.0.2.15	10.0.2.1	Primary Domain Controller (AD DS, DNS, DHCP)
NV-DC2	10.0.2.16	10.0.2.1	Secondary Domain Controller (AD Replication)
NV-FS1	10.0.2.17	10.0.2.1	File Server (FSRM, IIS, Storage Replica)
NV-CL1	DHCP (10.0.2.0/24)	10.0.2.1	Domain-Joined Workstation

Figure B.0: *IP Addressing Schema Table*
Static and dynamic IP assignments for all infrastructure components within the 10.0.2.0/24 subnet.

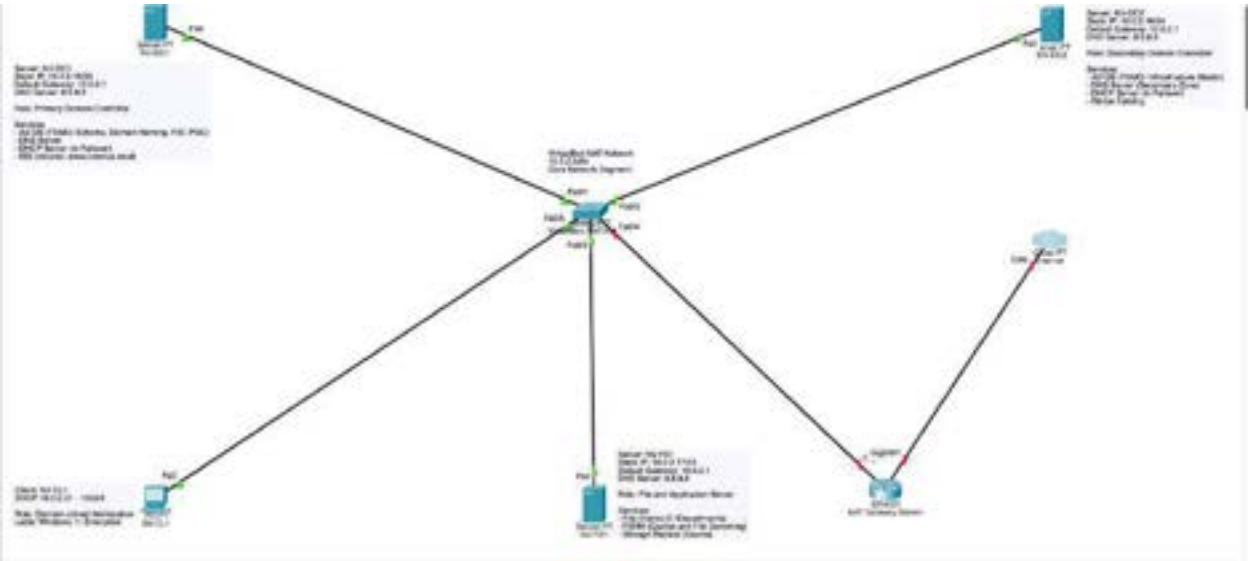

Figure B.1: *Network Infrastructure Diagram*
Visual representation of the hybrid environment showing connectivity between on-premises and cloud components.

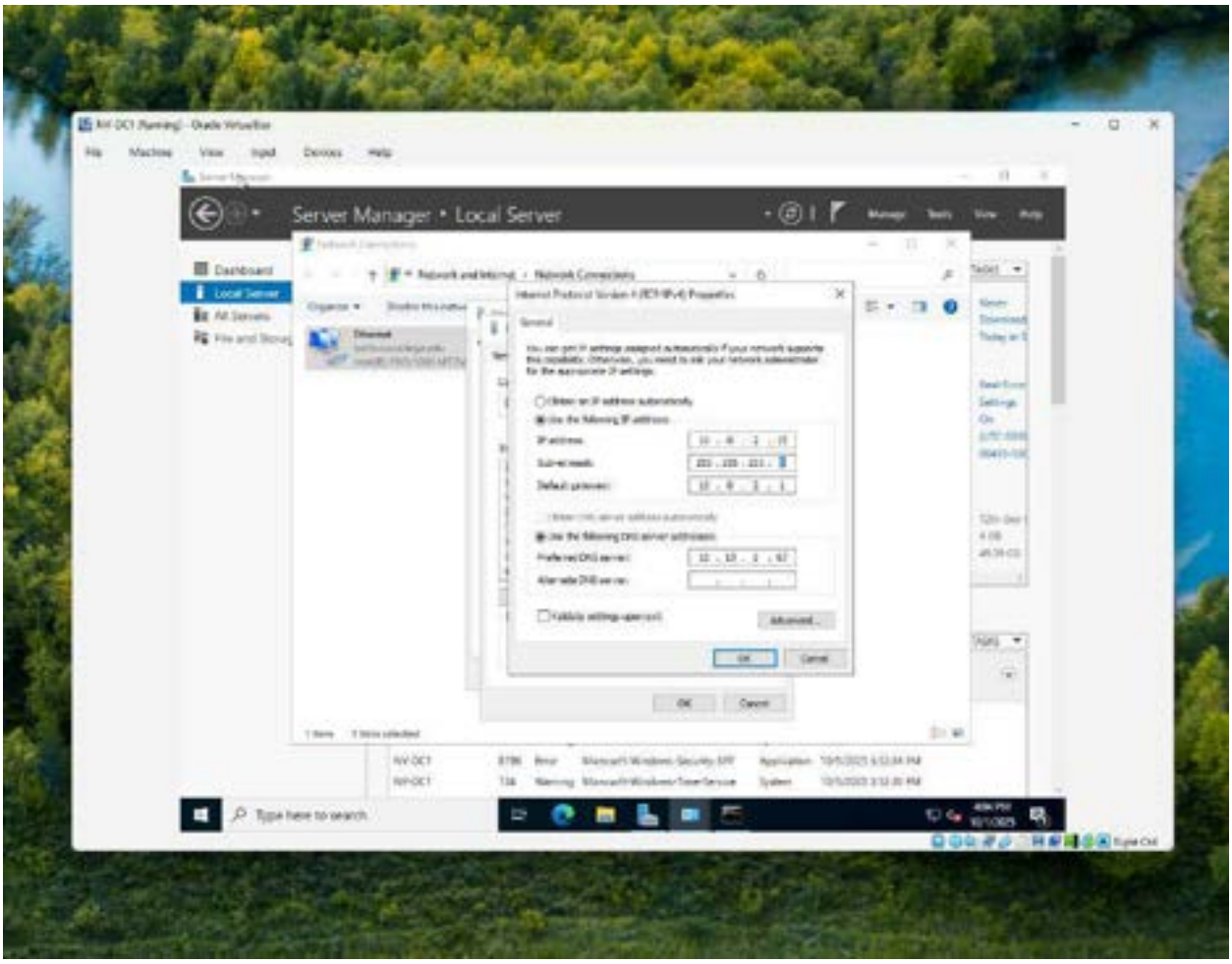

Figure B.2: Static IP Configuration – NV-DC1
Manual IP assignment (10.0.2.15) for primary domain controller ensuring consistent service availability

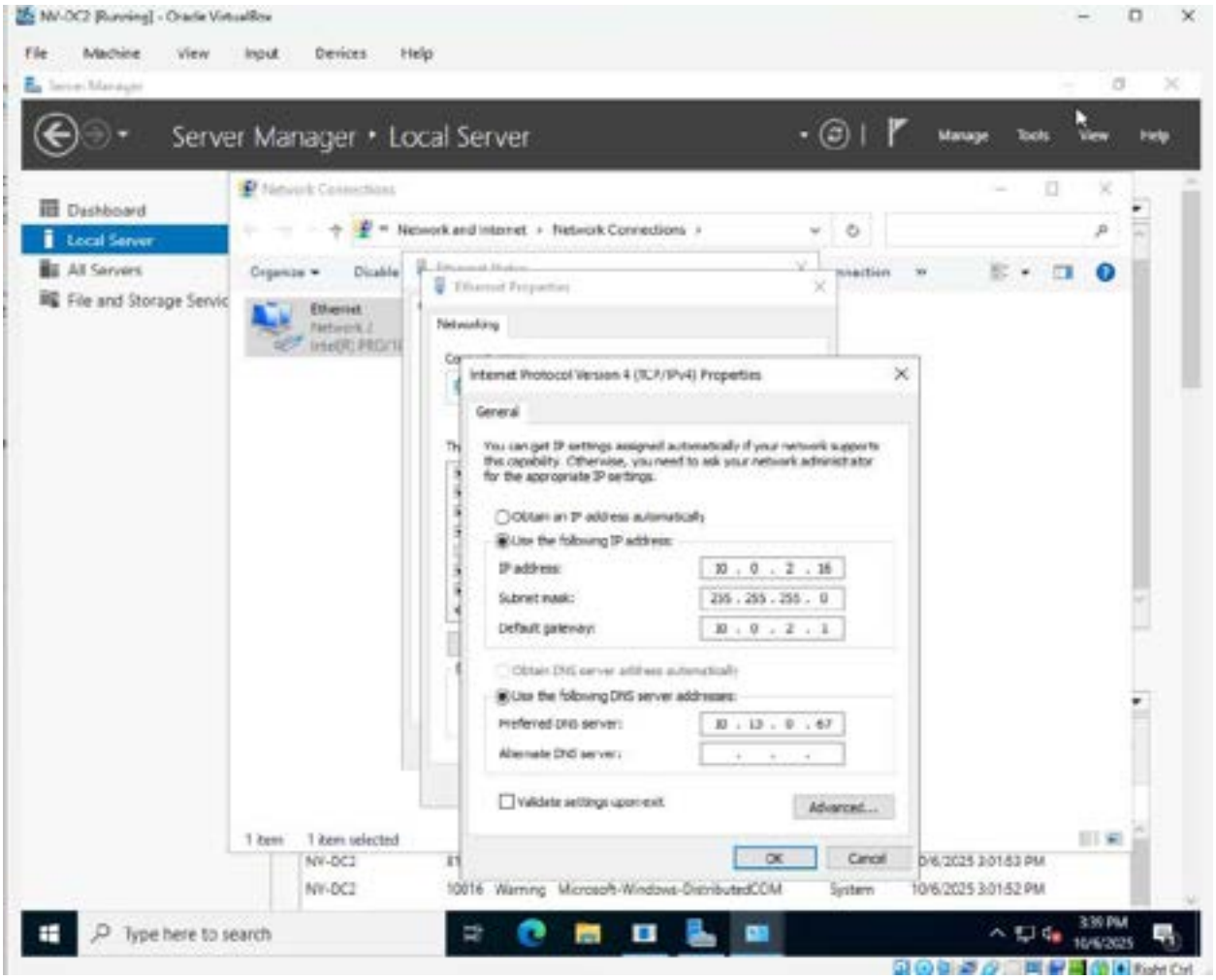

Figure B.3: Static IP Configuration – NV-DC2

Manual IP assignment (10.0.2.16) for secondary domain controller providing authentication redundancy.

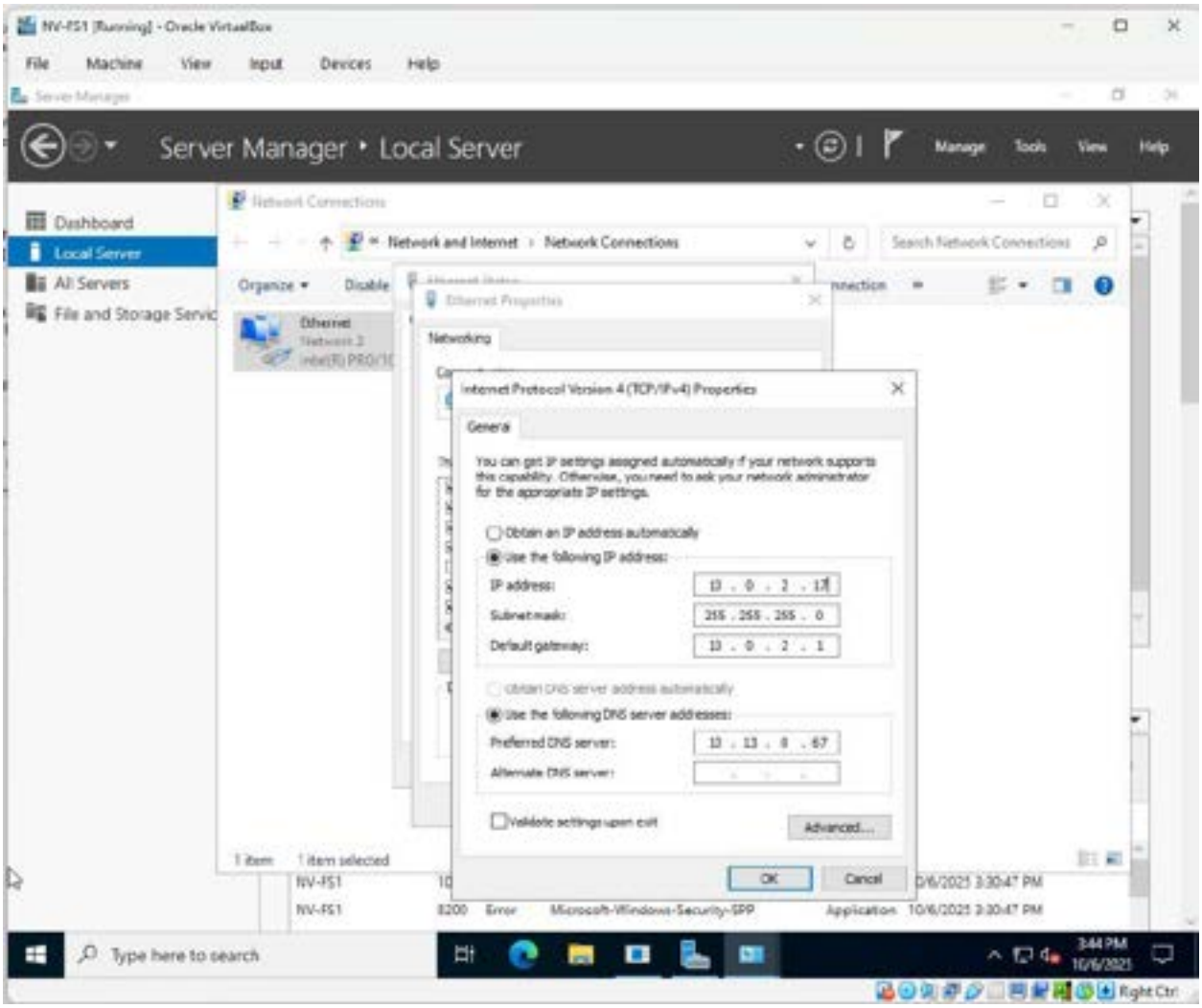

Figure B.4: Static IP Configuration – NV-FS1
Manual IP assignment (10.0.2.17) for file server hosting departmental shares and intranet services.

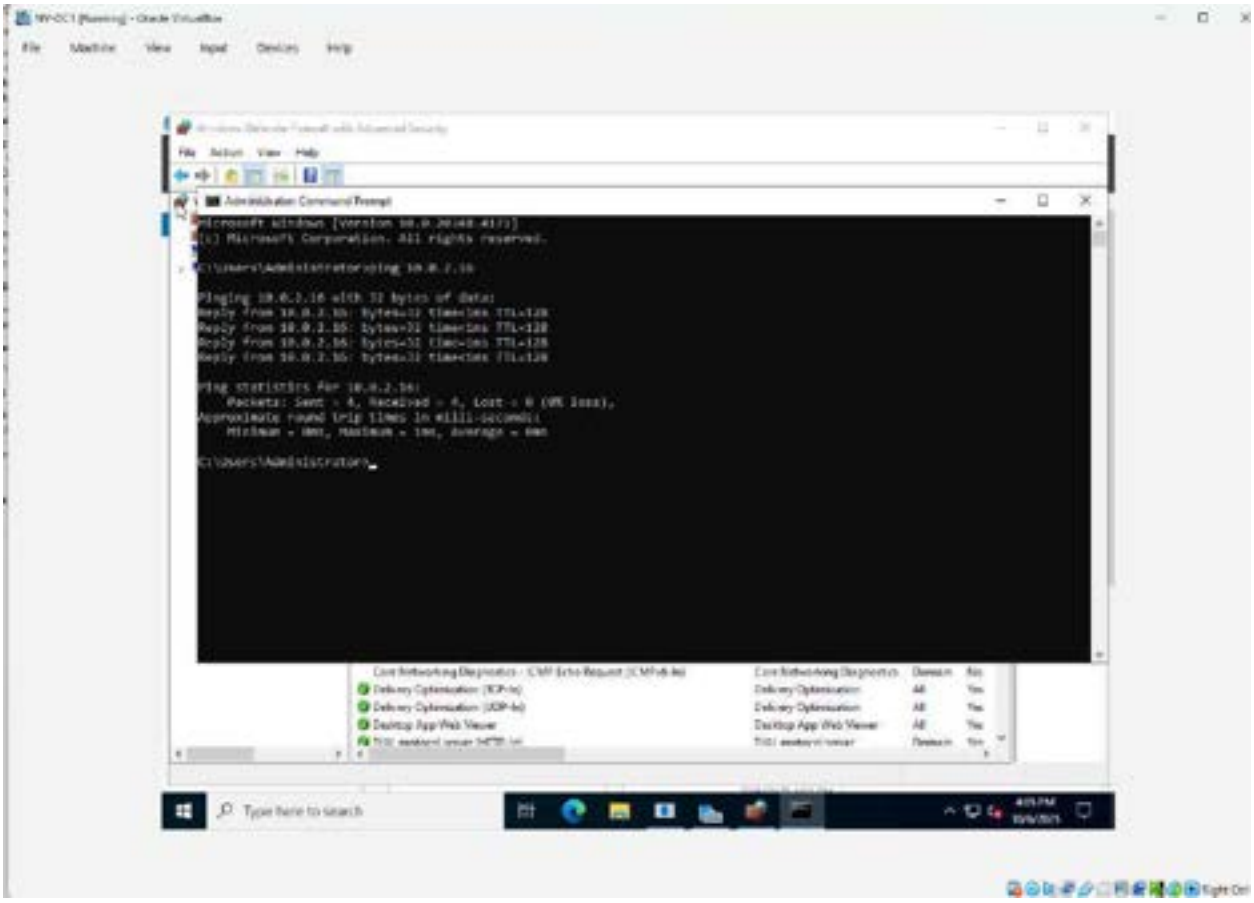

Figure B.5: *Internal Network Connectivity Test – DC to DC*
Ping verification between NV-DC1 and NV-DC2 showing successful communication with sub-10ms latency.

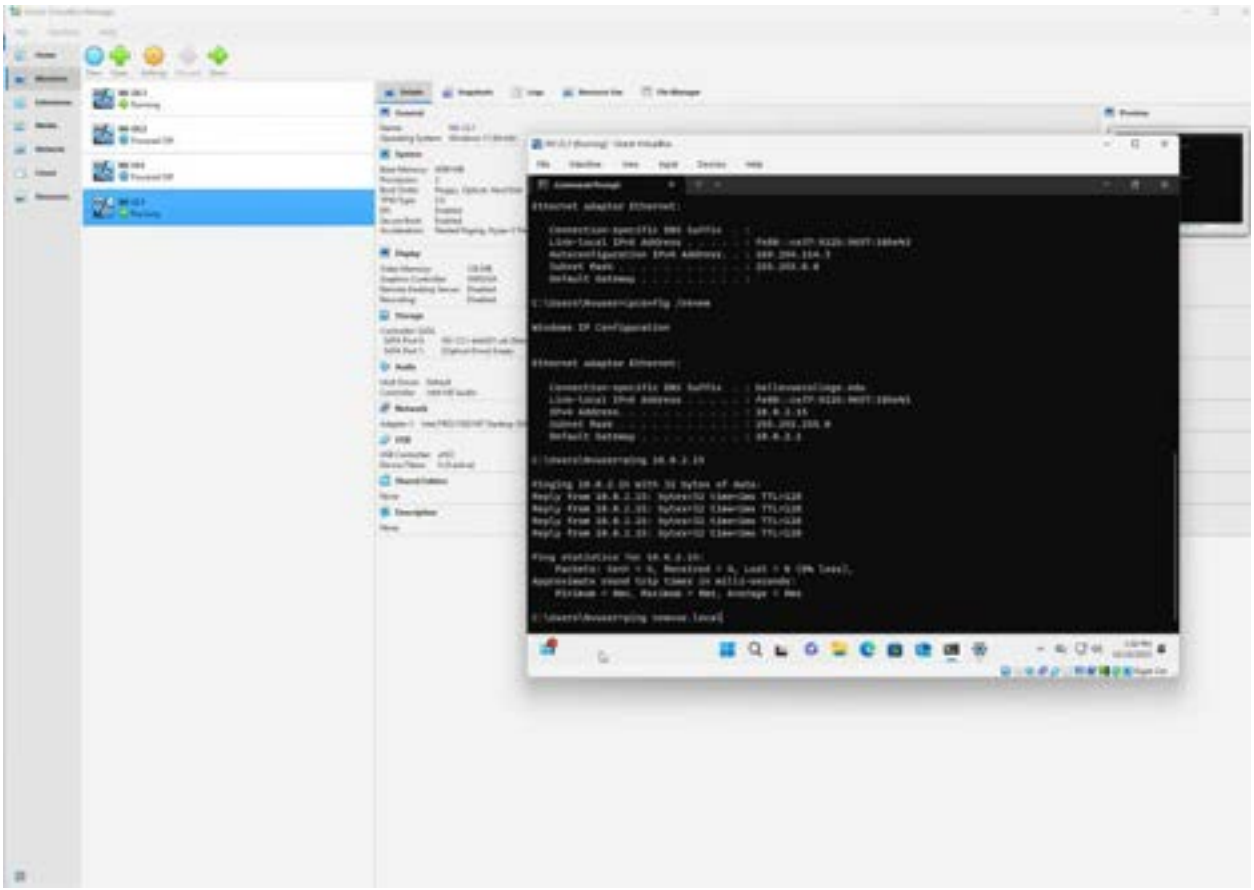

Figure B.6: *Internal Network Connectivity Test – Client to DC*
Ping verification between NV-CL1 and NV-DC1 confirming client-to-server communication.

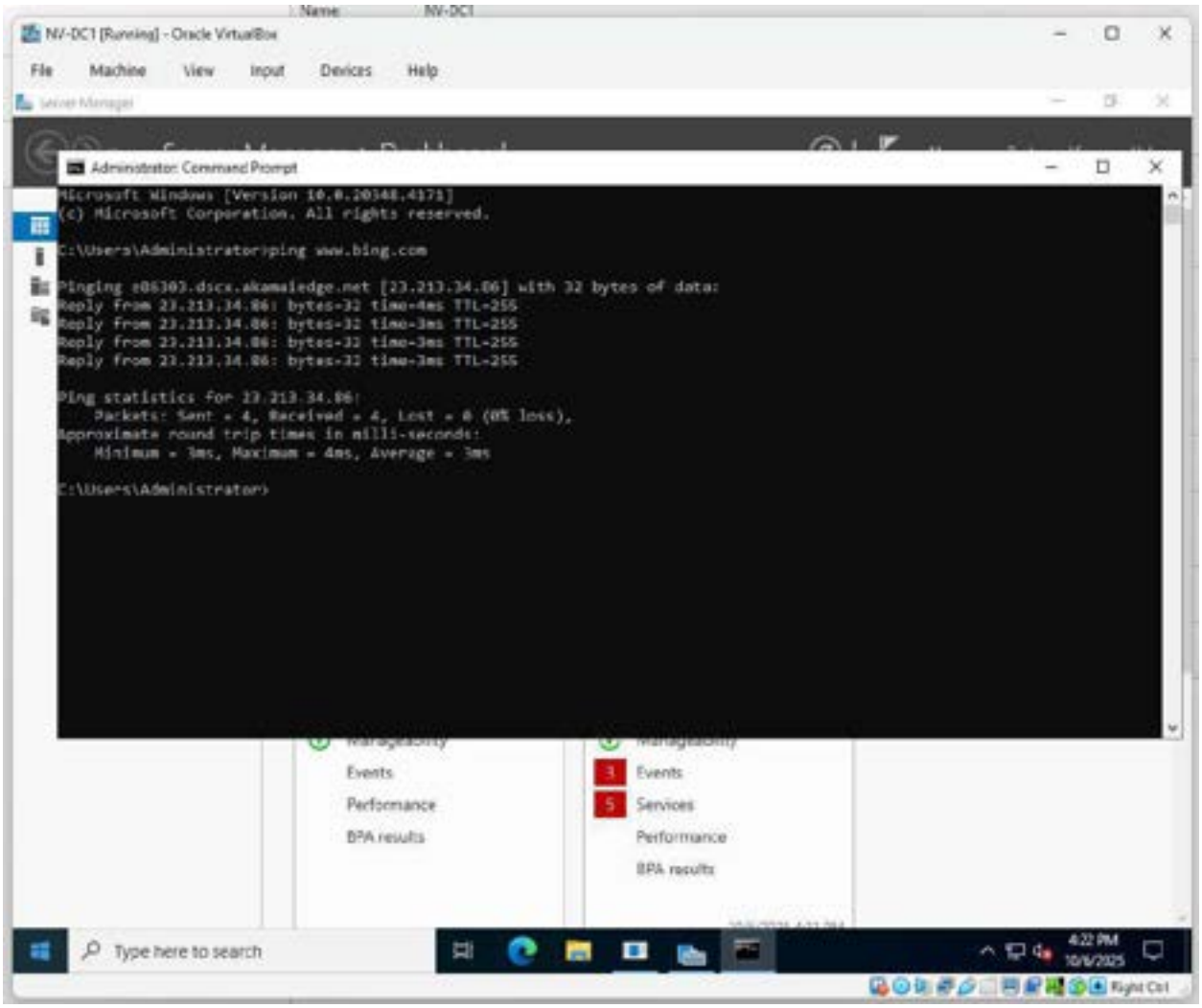

Figure B.7: Internet Connectivity Verification
Successful ping to external domain (bing.com) confirming proper NAT configuration and outbound internet access.

Appendix C: Active Directory & Core Services

Figure C.0: Active Directory OU Structure
Hierarchical organizational unit design aligned with NewVue Health business departments for delegated administration

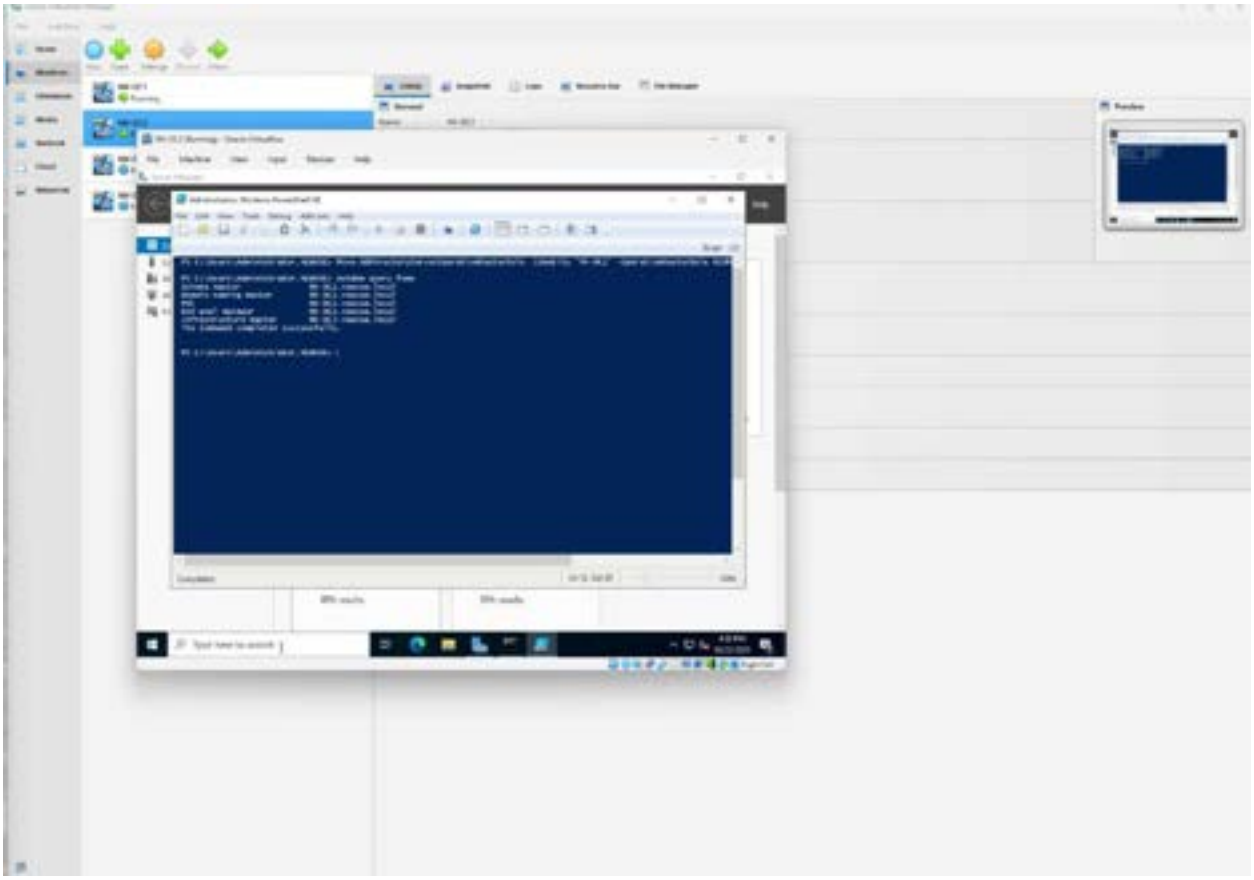

Figure C.1: *FSMO Role Placement Verification*
Output of *netdom query fsmo* showing strategic distribution of Flexible Single Master Operations roles.

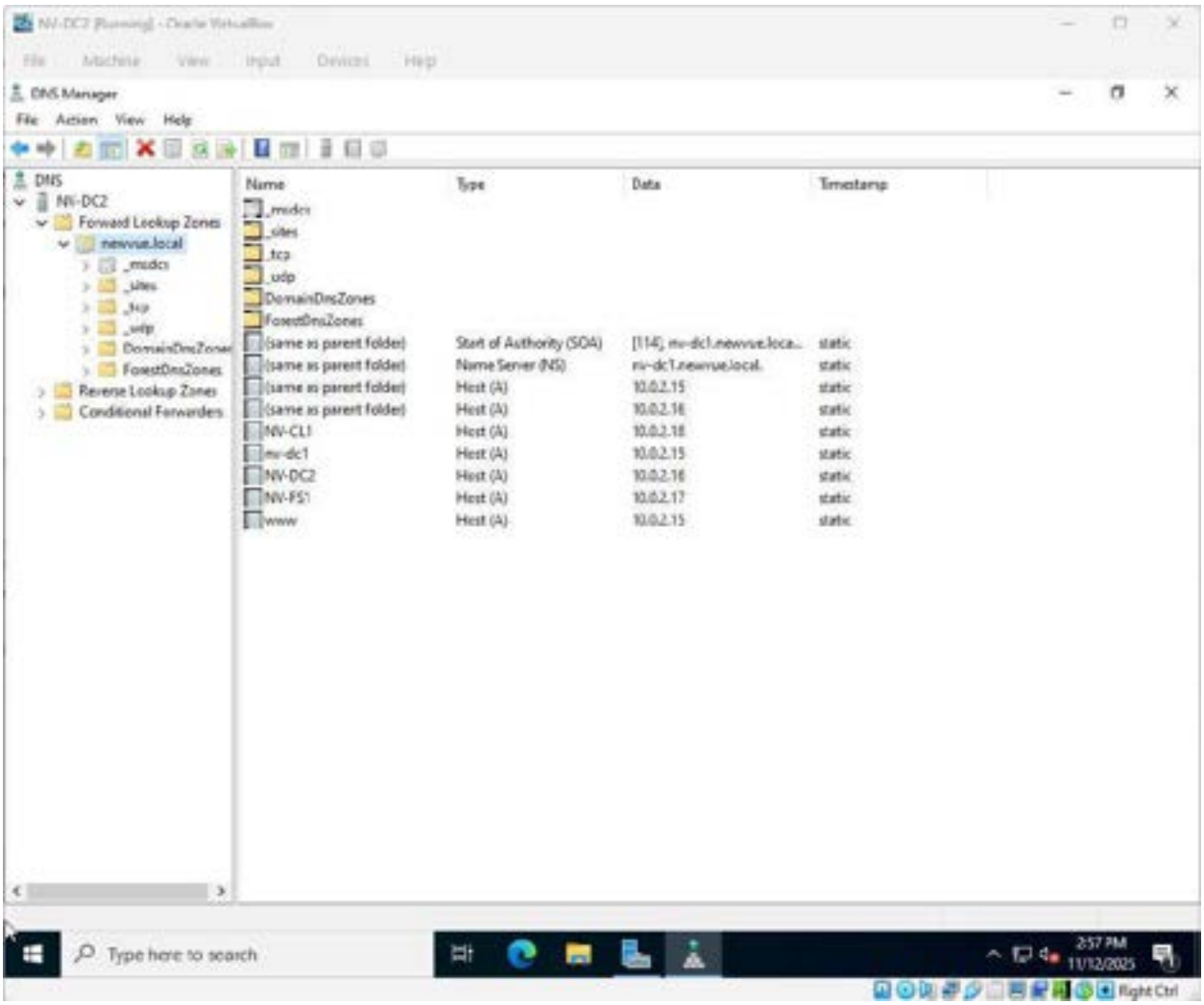

Figure C.2: DNS Zone Configuration
Active Directory-integrated DNS zone for newvue.local showing proper forward and reverse lookup zones.

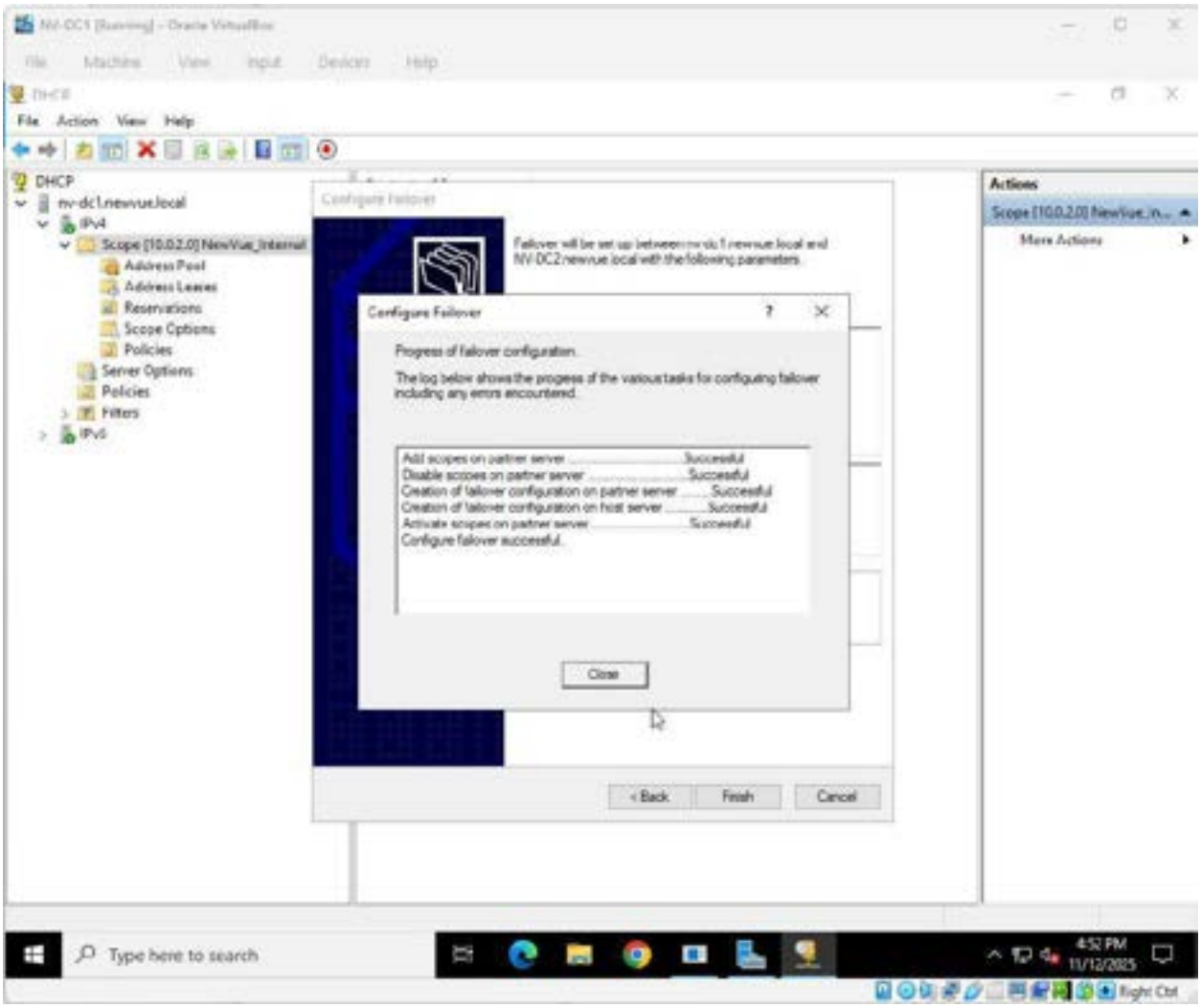

Figure C.3: *DHCP Failover Relationship*
Load-balanced DHCP failover configuration between NV-DC1 and NV-DC2 showing synchronized scopes.

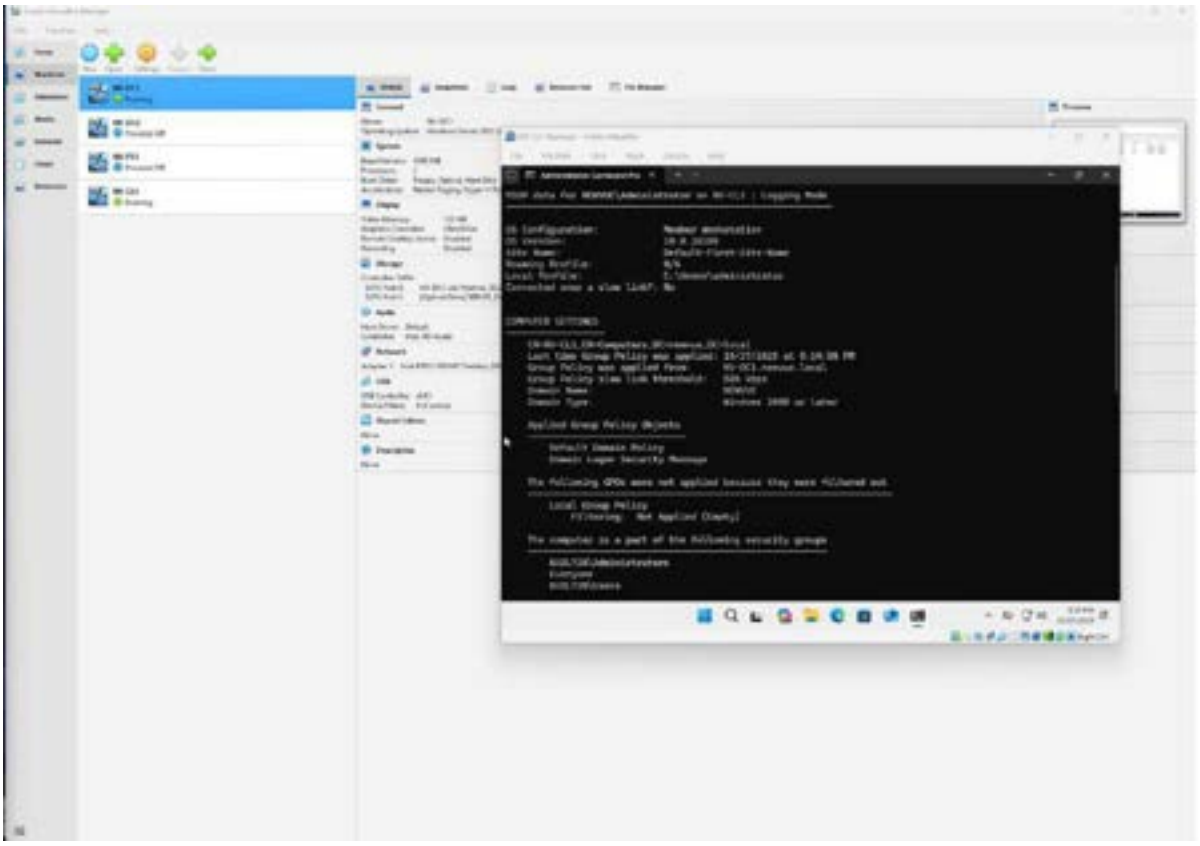

Figure C.5: *Group Policy Application Results*
Output of gpresult /r showing successful application of security and configuration policies to NV-CL1.

Appendix D: File & Storage Services

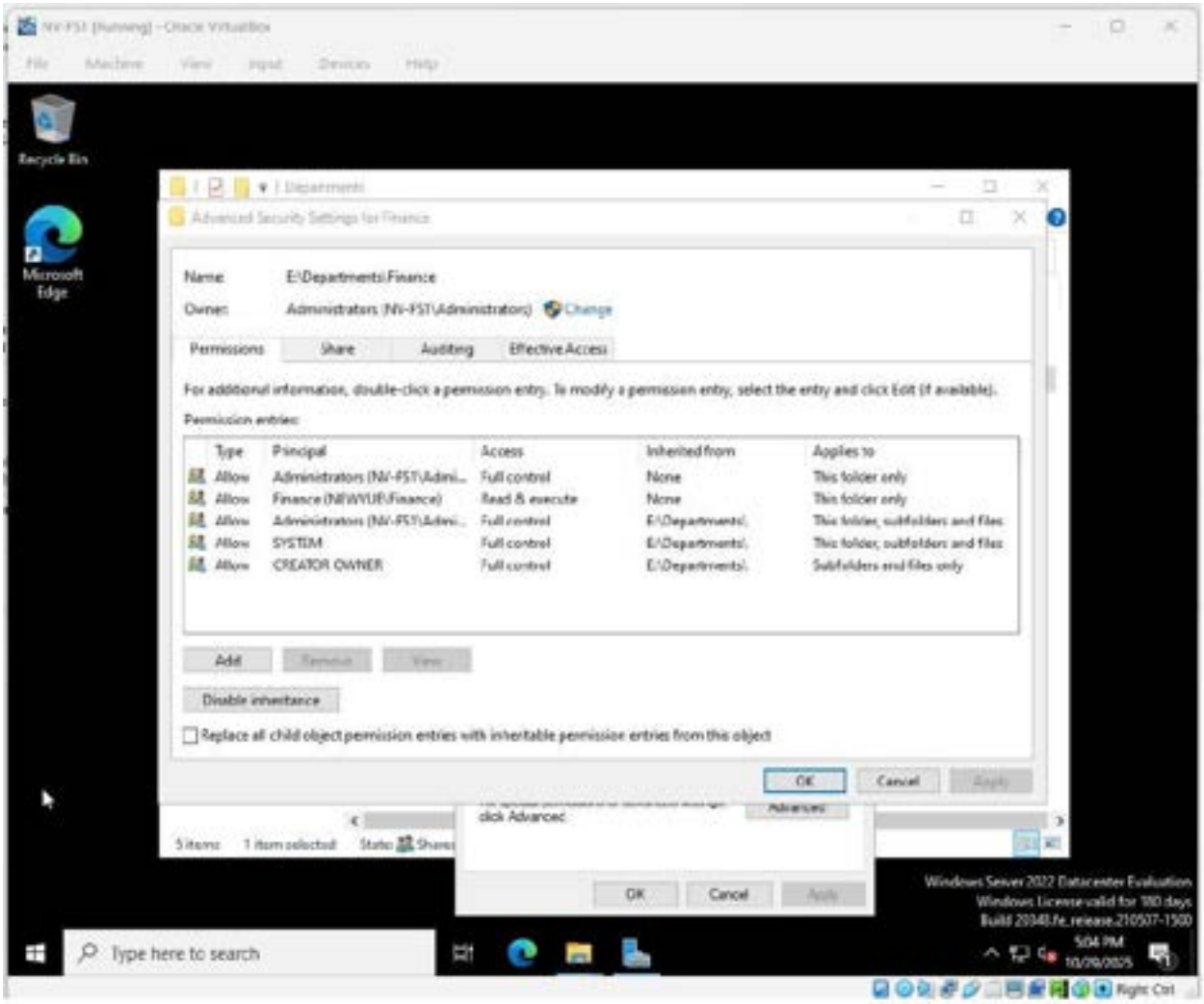

Figure D.0: File Share Permissions Configuration
NTFS permissions dialog showing role-based access control for Finance department share.

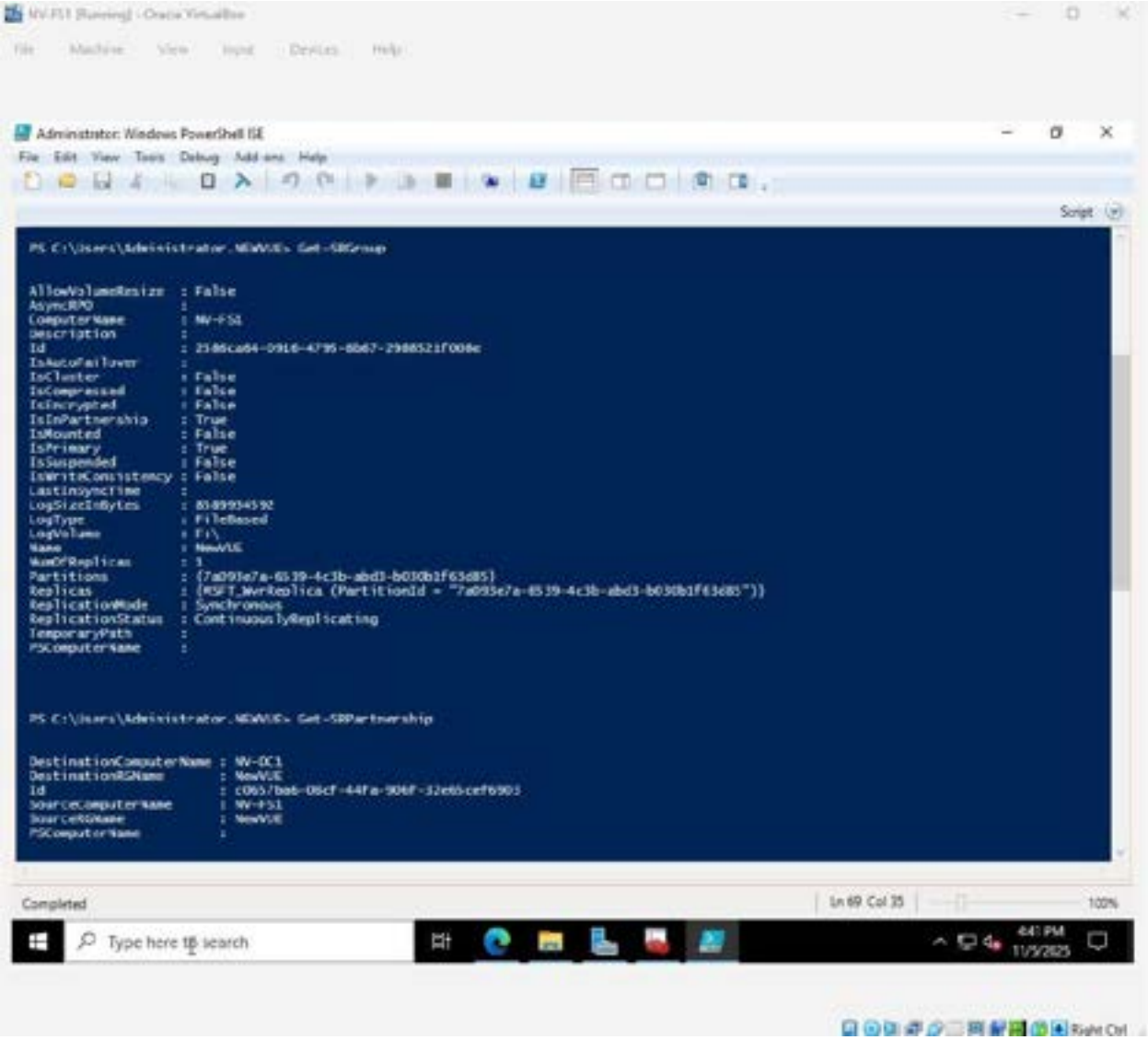

Figure D.1: *Storage Replica Health Status*

PowerShell output of Get-SRPartnership showing continuous synchronous replication between NV-FS1 and NV-DC1.

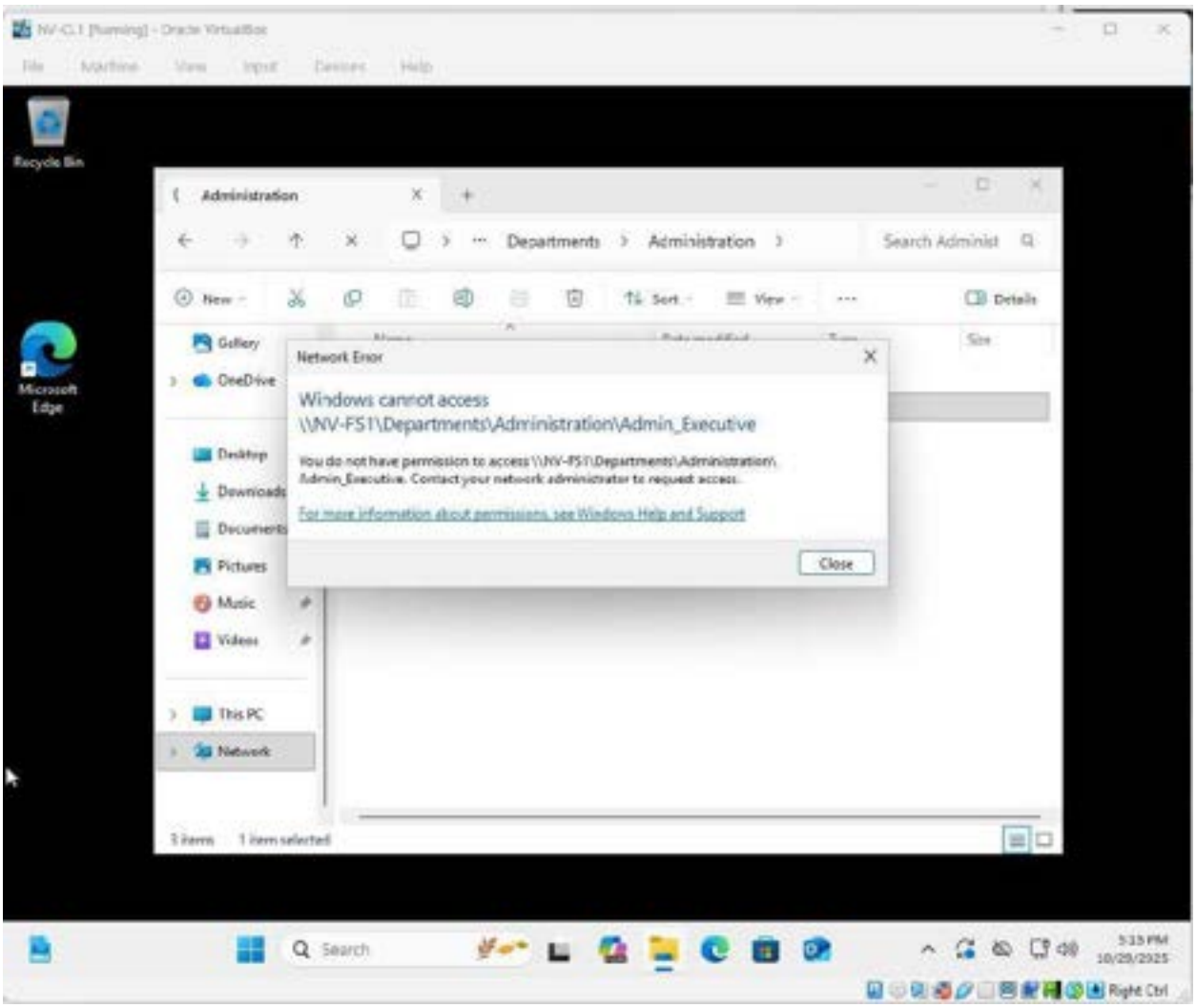

Figure D.2: File Share Access Control Validation
Access denied error when unauthorized user attempts to access Clinical_Services share, demonstrating RBAC enforcement.

Appendix E: Local Intranet Hosting

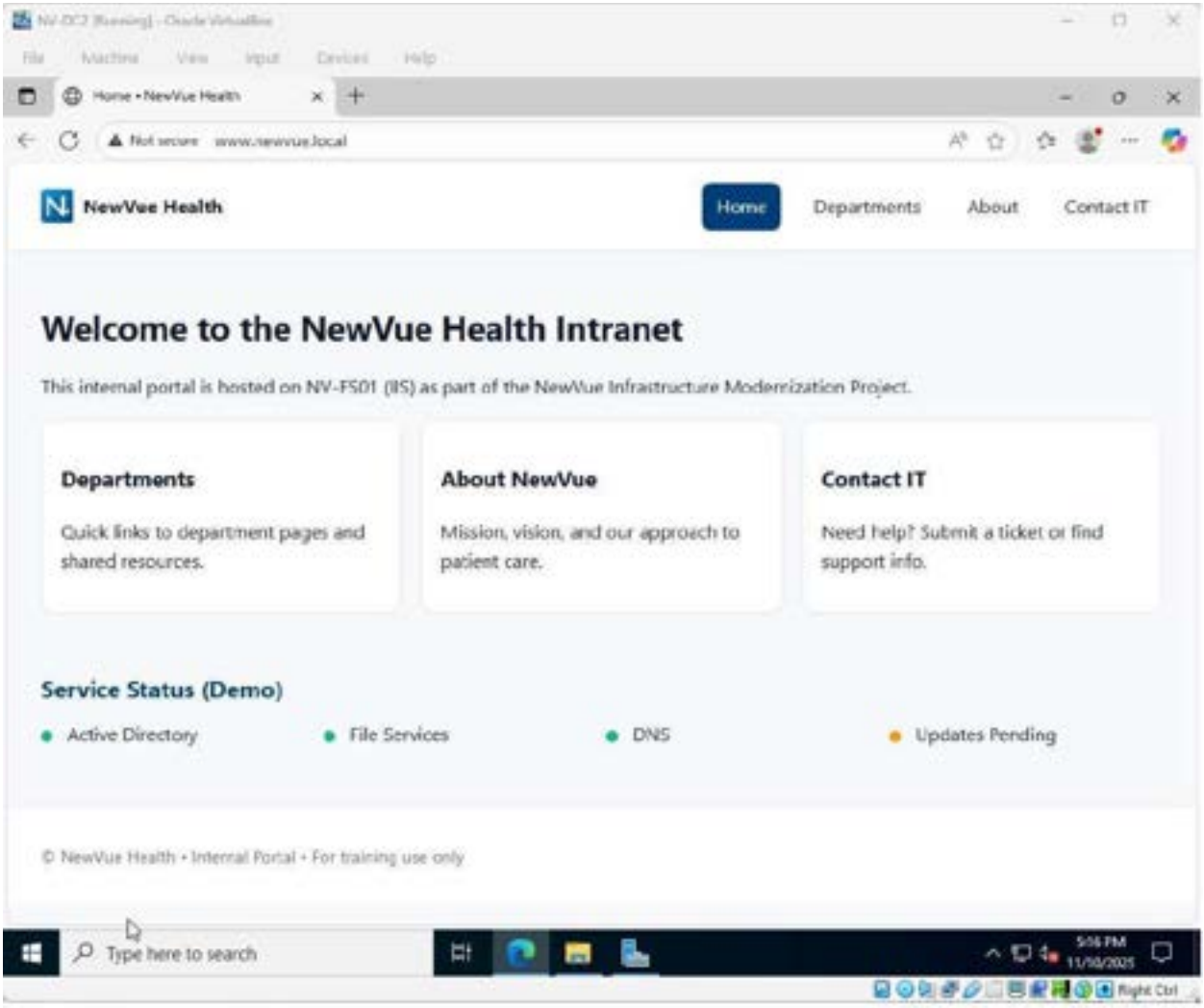

Figure E.0: IIS Default Website Configuration
Internet Information Services Manager showing default website running with proper bindings and authentication settings.

Appendix F: Hybrid Cloud Integration

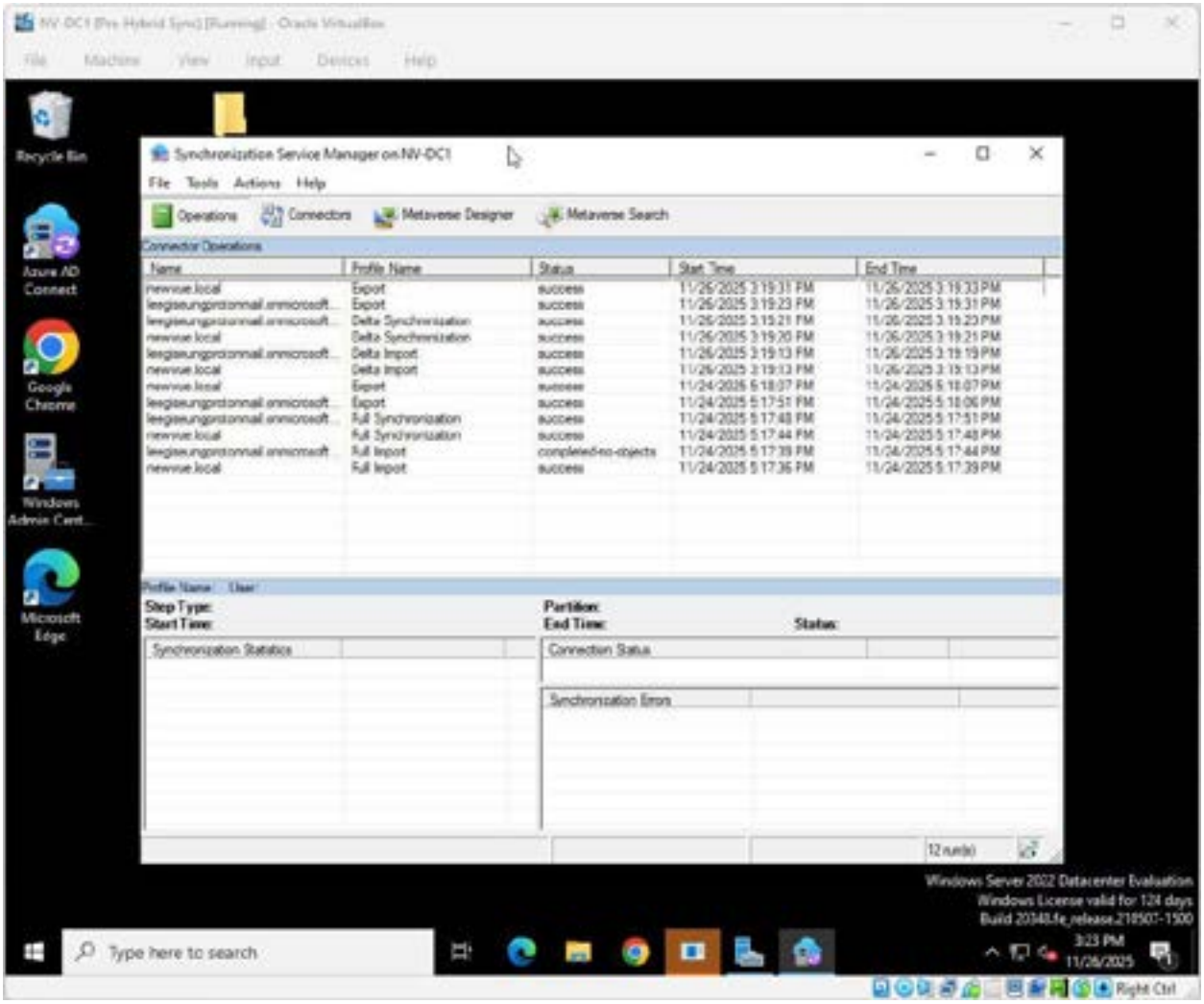

Figure F.0: Azure AD Connect Synchronization Status
Synchronization Service Manager dashboard showing successful import, sync, and export operations with zero errors.

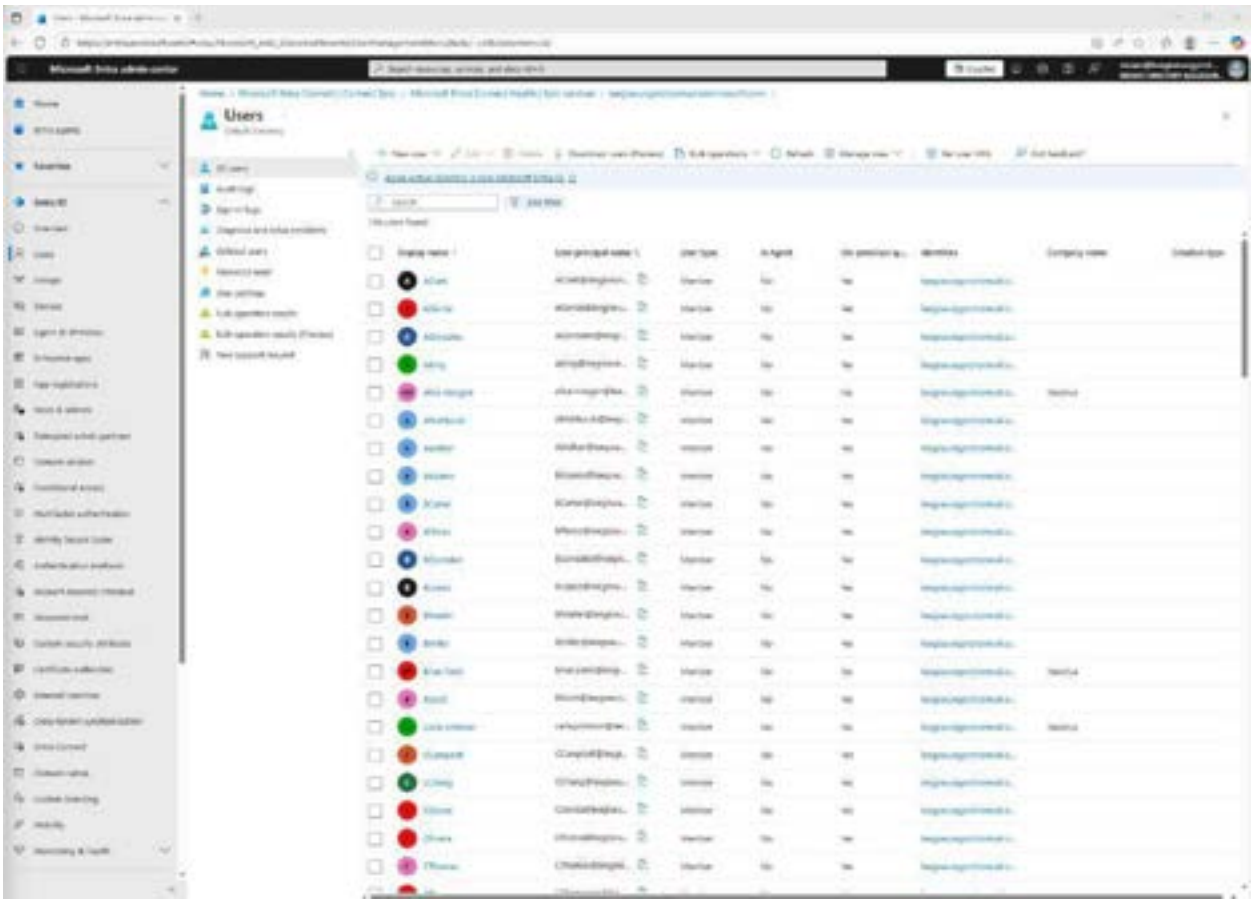

Figure F.1: Entra ID Synchronized Users
Microsoft Entra Admin Center displaying users synchronized from on-premises Active Directory with "Windows Server AD" sourc

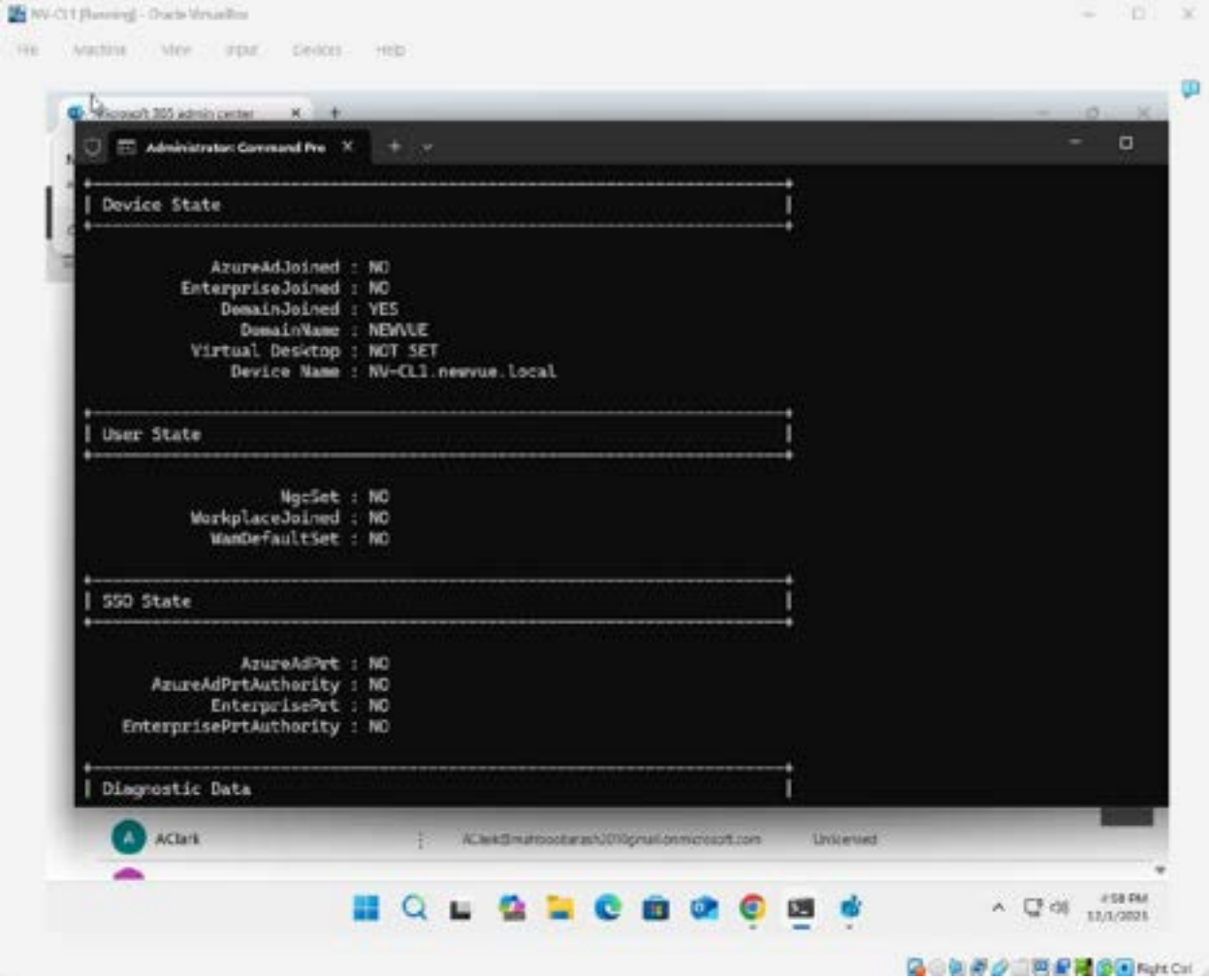

Figure F.2: Hybrid Azure AD Join Verification
Output of dsregcmd /status *showing device registration status and Azure AD join configuration.*

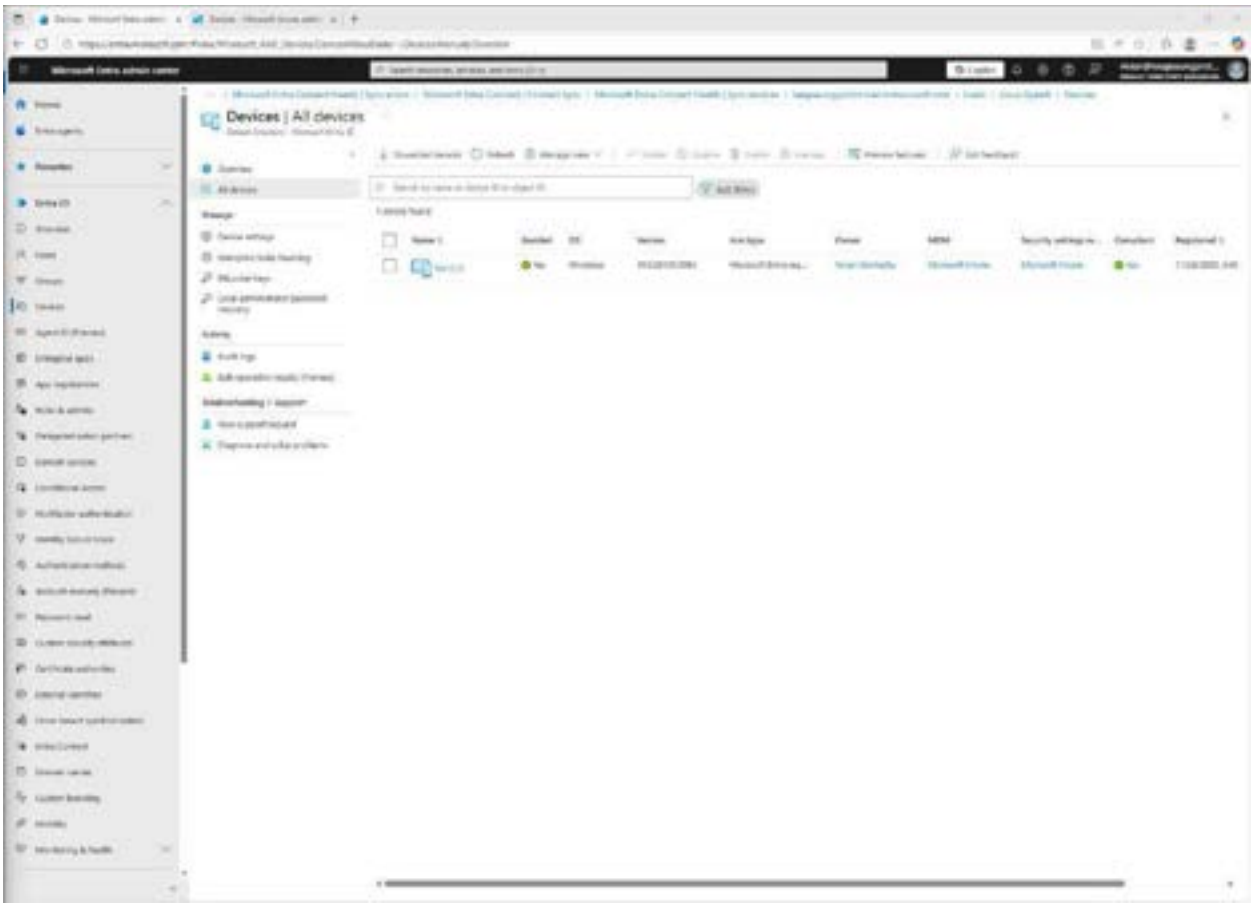

Figure F.3: *Intune Device Compliance Report*
Microsoft Intune Admin Center showing NV-CL1 compliance status with applied

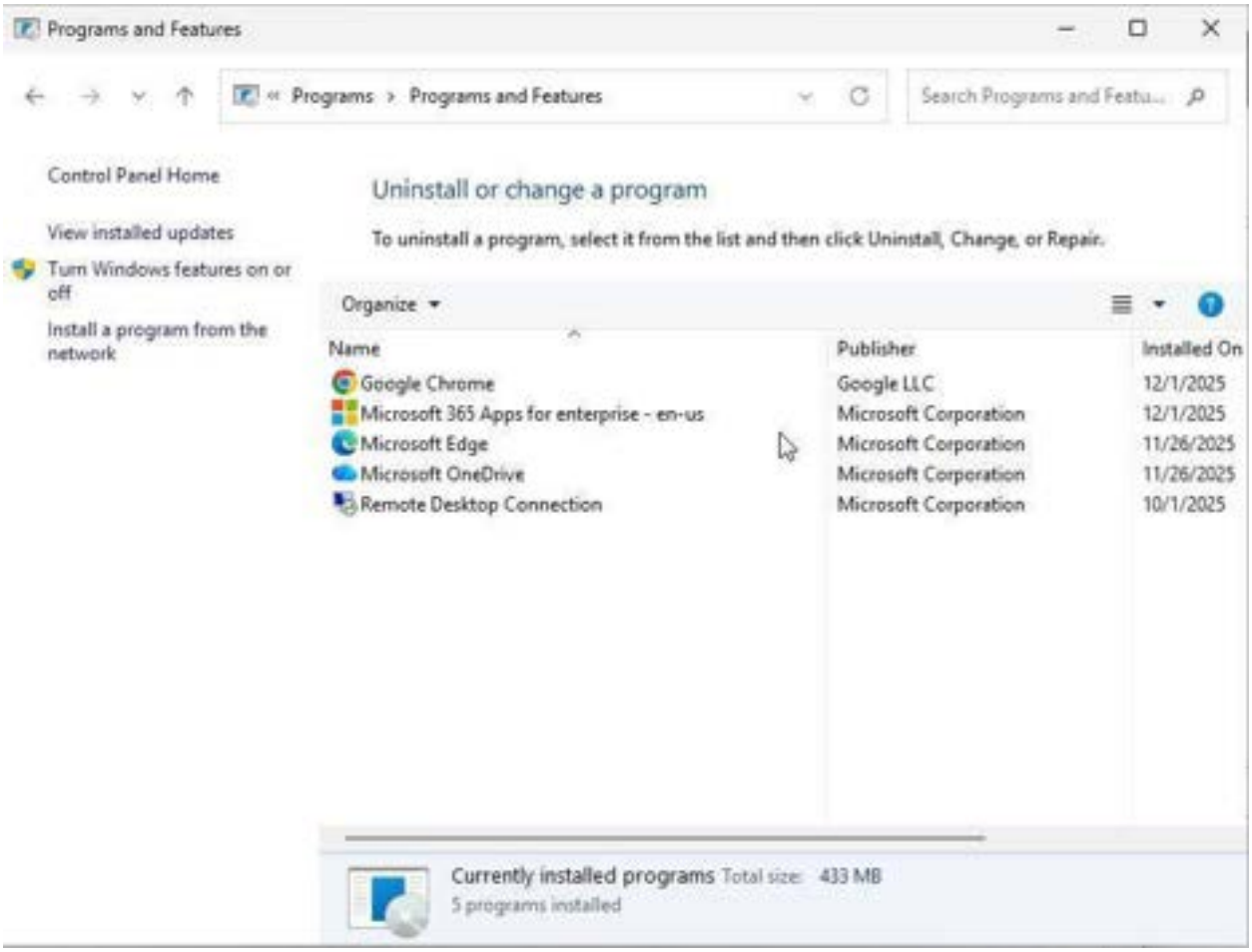

Figure F.4: *Microsoft 365 Apps Deployment*
Successful installation of Microsoft 365 Apps via Intune demonstrating cloud-based software distribution.

Appendix G: Security & Compliance Evidence

Figure G.0: *BitLocker Encryption Status*
BitLocker management interface showing encryption active on NV-CL1 as required by Intune compliance policy.

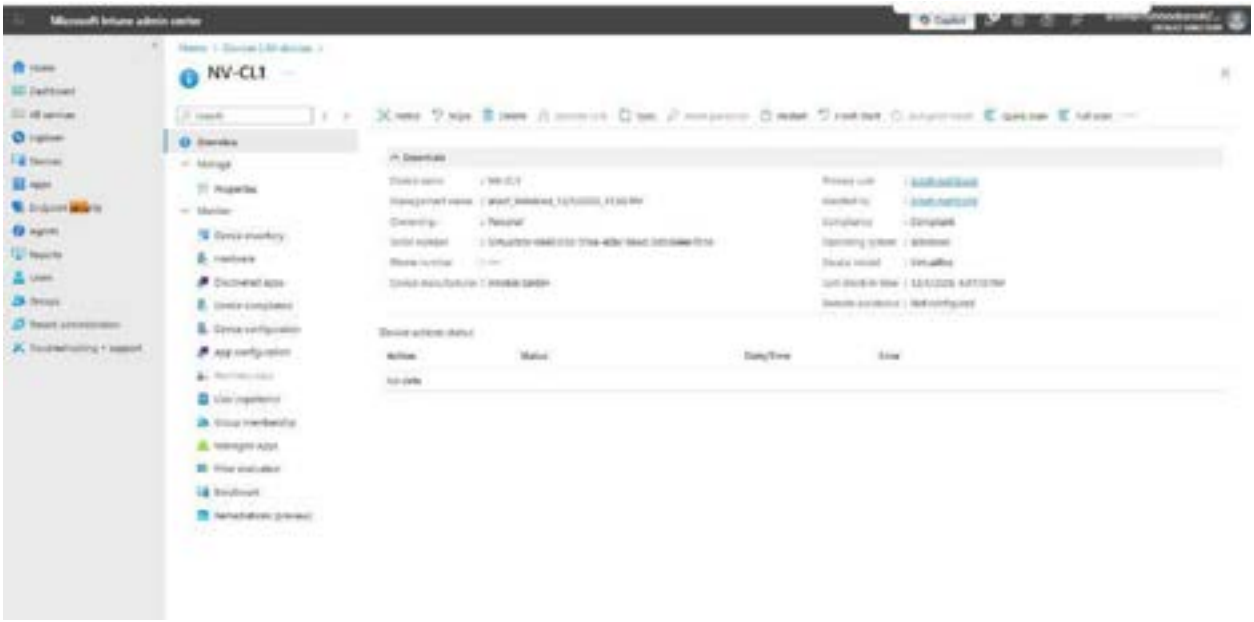

Figure G.1: *Security Baseline Compliance*

Intune device configuration profiles showing applied security settings and compliance status

Appendix H: System Validation Summary

Test Category	Methodology	Result	Validation Confirmed
Network Connectivity	Ping tests between all systems	100% success rate <10ms latency	Proper IP configuration and firewall rules
DNS Resolution	nslookup for internal/external domains	Correct IP resolution for all queries	DNS server configuration and forwarders working
AD Replication	Repadmin / replsummary	No failures, consistent replication	High availability authentication services
File Share Access	Cross-department access attempts	Proper allow/deny based on group membership	Effective RBAC and permission enforcement
Storage Replica	Get-SRPartnership PowerShell	Continuous replication, zero backlog	Data redundancy and business continuity
Azure AD Sync	Synchronization Service Manager	Success across all operations	Effective hybrid identity integration
Hybrid Sign-in	Cloud authentication with synced users	Successful access to M365 services	Password hash synchronization working
Device Management	Intune enrollment and policy application	Compliant status, apps deployed	Modern endpoint management operational

Figure H.0: Comprehensive Infrastructure Test Summary

Consolidated results from all validation tests performed across on-premises and hybrid cloud components.

References and Professional Presentation

Microsoft. (2023). *Active Directory Domain Services overview*. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Microsoft. (2024). *What is Azure Active Directory?* Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

Microsoft. (2024). *What is Azure AD Connect cloud sync?* Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/hybrid/whatis-cloud-sync

Microsoft. (2023). *DHCP failover*. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-failover

Microsoft. (2023). *File Server Resource Manager overview*. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/windows-server/storage/fsrm/fsrm-overview

Microsoft. (2024). *What is Microsoft Intune?* Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Microsoft. (2023). *Storage Replica overview*. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/windows-server/storage/storage-replica/storage-replica-overview

Microsoft. (2024). *What is DFS Namespaces?* Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/windows-server/storage/dfs-namespaces/dfs-overview

Microsoft. (2023). *What is Internet Information Services (IIS)?*Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/iis/get-started/introduction-to-iis/introduction-to-iis-architecture

Microsoft. (2023). *Group Policy overview*. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/windows-server/identity/group-policy/group-policy-overview