NEW INFRASTRUCTURE DESIGN

PROPOSAL

Vivian J. Goshashy
NEWVUE HEALTH | SPOKANE, WA

Table of Contents

Executive Summary 2
Summary of Current Issues 3
Proposed Infrastructure and Server Role Design 5
High Availability Plan 7
Hybrid Integration Readiness 9
Infrastructure Diagram 11

Executive Summary

This proposal presents a comprehensive technology modernization plan for NewVUE Health, designed to transform our current IT infrastructure into a secure, reliable platform that supports our healthcare mission and organizational growth. Our solution establishes a modern, cloud-ready foundation that addresses both immediate operational needs and future expansion requirements.

We will implement a robust virtualized environment at our Spokane headquarters using Microsoft Windows Server 2022, featuring eight strategically designed virtual servers deployed in high-availability pairs:

- *Two Domain Controllers for centralized security management, providing secure user authentication, enforcing security policies, and handling DNS/DHCP services*
- *Two File Servers for reliable storage of patient records and department files, along with centralized print services*
- *Two Application Servers to host future healthcare systems including Electronic Health Records (EHR), patient portals, and clinical applications*
- *Two Web Servers to host our clinic website and web-based applications accessible to both staff and patients through browsers*

The infrastructure will implement Organizational Units (OUs) structured to reflect our departments including HR, Administration, and Medical, enabling precise security controls and policy management. This design incorporates hybrid cloud readiness, ensuring seamless future integration with Microsoft Azure cloud services while maintaining our on-premises infrastructure.

This modernization directly supports NewVUE Health's goals by:

- *Ensuring Continuous Operations through redundant server pairs that prevent service interruptions*
- *Meeting HIPAA Compliance with centralized security controls and audit capabilities*
- *Enhancing Patient Care by providing a stable platform for EHR systems and patient portals*
- *Supporting Organizational Growth with a scalable architecture ready for new clinics and services*

This investment creates a future ready technology environment that empowers our staff to deliver exceptional healthcare services while maintaining the highest standards of data security and operational reliability.

Summary of Current Issues

NewVUE Health faces significant IT challenges that directly impact patient care, operational efficiency, and regulatory compliance. The organization currently operates on an outdated peer-to-peer network model that lacks centralized management, creating vulnerabilities across all aspects of our technology infrastructure.

Key Challenges and Proposed Solutions:

Security & Compliance Issues:

- *Current State: Failed HIPAA audit due to lack of centralized access controls, missing patch management, and no auditing system. Patient data is vulnerable with local user accounts on each machine.*
- *Solution: Our proposed two domain controllers will implement centralized Active Directory, enabling enforced security policies, granular access controls, and comprehensive auditing. The Windows Server Update Services (WSUS) on our application servers will provide centralized patch management, while organizational units will ensure department specific security compliance.*

Operational Efficiency Problems:

- *Current State: Manual file sharing configurations, unreliable printing, and new user account creation taking days to configure across multiple machines.*
- *Solution: The two file servers with DFS replication will provide reliable, centralized file and print services accessible from any location. Active Directory automation will reduce new user setup from days to minutes, with Group Policies ensuring consistent configurations across all workstations.*

Scalability Limitations:

- *Current State: The peer-to-peer workgroup cannot support organizational growth, new clinic openings, or integration with external healthcare systems.*
- *Solution: The virtualized environment with eight redundant servers provides immediate scalability. The OU structure supports easy department expansion, while the hybrid-ready design enables seamless cloud integration and future partnership with regional healthcare systems.*

Business Continuity Risks:

- *Current State: No centralized backup systems and single points of failure across all IT services.*
- *Solution: The high-availability pairs for all critical services (domain controllers, file servers, application servers, and web servers) ensure continuous operations.*

- *Automated backup systems on the application servers protect against data loss, while redundant design eliminates single points of failure.*

Modern Healthcare Delivery Gaps:

- *Current State: Inability to support telehealth expansion, patient portals, or secure remote access for field staff.*
- *Solution: The application and web servers provide the foundation for EHR systems, patient portals, and telehealth applications. The infrastructure supports secure remote access capabilities essential for mobile outreach units and future telehealth initiatives.*

This proposed infrastructure directly transforms NewVUE Health from a vulnerable, inefficient operation into a modern, compliant healthcare technology environment capable of supporting current needs while scaling for future growth and innovation.

Proposed Infrastructure and Server Role Design

Infrastructure Overview
NewVUE Health's headquarters will implement a fully virtualized infrastructure running on a hypervisor cluster consisting of two physical host servers with shared storage. This environment will host eight virtual servers that provide comprehensive IT services with high availability and centralized management.

Virtualization Platform Selection

- *Platform: Microsoft Hyper-V*
- *Justification: Hyper-V is included with Windows Server 2022, providing cost-effectiveness for our nonprofit organization. It offers robust high-availability features, excellent integration with Windows environments, and supports live migration for maintenance without downtime. The platform's scalability allows easy addition of resources as NewVUE grows.*

Server Role Design and Justification

Domain Services Cluster (High Availability Pair)

- *Domain Controllers*
- *Roles: Active Directory Domain Services, DNS Server, DHCP Server*
- *Justification: Deploying two domain controllers ensures continuous authentication services. Combining DNS with AD DS is a Microsoft best practice for optimal performance. DHCP is distributed across both servers in failover mode for redundancy. This separation from other roles maintains security and stability for core identity services.*

File and Print Services Cluster (High Availability Pair)

- *File and Print Servers*
- *Roles: File Services, Print Services, DFS Namespace, DFS Replication*
- *Justification: These servers provide redundant access to critical patient data and departmental files. DFS Replication maintains synchronized copies of data across both servers, while DFS Namespace presents a unified access path to users. Print services are included as they naturally align with file resource sharing.*

Application Services Tier (High Availability Pair)

- *Application Servers*
- *Roles: Electronic Health Record (EHR) System, Patient Portal, Clinical Applications*
- *Justification: Separating applications from infrastructure services isolates resource-intensive workloads. The redundant design ensures critical healthcare applications remain available. This tier can scale horizontally by adding more application servers as needed.*

Web Services Tier (High Availability Pair)

- *Web Servers*
- *Roles: Clinic Website, Web-Based Applications, Remote Access Portal*
- *Justification: Web services are separated from internal applications for security segmentation. This design allows implementing different security policies and SSL certificates. Load balancing between web servers ensures optimal performance for patient and staff access.*

Network Considerations

- *A minimum of 10Gb connectivity between hosts and shared storage*
- *VLAN segmentation to isolate server traffic, user traffic, and future IoT medical devices*
- *Redundant network switches and connections to eliminate single points of failure*
- *Quality of Service (QoS) policies to prioritize clinical application traffic*

Centralized Management and Efficiency Benefits
This design supports centralized management through Active Directory and Group Policies applied to organizational units reflecting departmental structure (HR, Admin, Medical). Role-based access controls ensure least-privilege security while automated policy enforcement reduces manual configuration efforts.

Future Scalability

- *The virtualized environment allows easy addition of CPU, memory, and storage resources*
- *New clinics can be integrated as AD sites with localized domain controllers*
- *The application and web tiers can scale horizontally to support increased load*
- *Hybrid cloud readiness enables burst capacity to Azure during peak demand periods*

This server role design provides a balanced approach to performance, security, and manageability while establishing a foundation that can scale with NewVUE Health's growth and evolving healthcare technology needs.

High Availability Plan

Critical Services Requiring Redundancy

Our high availability plan focuses on four essential service categories where downtime would directly impact patient care and daily operations:

1. *Identity and Access Services (Domain Controllers)*
2. *Data Storage Services (File Servers)*
3. *Healthcare Applications (EHR and Patient Portal)*
4. *Web Presence Services (Clinic Website and Web Apps)*

Implementation Strategy

1. Domain Controllers - Automatic Failover

- *Implementation: Two domain controllers (NV-DC01 and NV-DC02) running Active Directory in a multi-master replication configuration*
- *How It Works: Both controllers actively authenticate users, and replicate changes every 15 seconds. If one server fails, authentication and DNS services automatically continue the remaining server*
- *Failover Process: Completely automatic - users experience no interruption in login access or network connectivity*

2. File Services - Transparent Failover

- *Implementation: Two file servers (NV-FS01 and NV-FS02) using DFS Replication and DFS Namespace*
- *How It Works:*
    - *Files are continuously synchronized between both servers*
    - *Users access files through a single namespace path*
    - *The namespace automatically directs users to the available server*
- *Failover Process: If NV-FS01 fails, users are automatically redirected to NV-FS02 within seconds, with no change required on their end*

3. Application Services - Load Balanced Availability

- *Implementation: Two application servers (NV-APP01 and NV-APP02) configured in a network load balancing cluster*
- *How It Works:*
    - *Both servers run identical healthcare applications (EHR, patient portal)*
    - *User requests are distributed between both servers*
    - *If one server fails, all traffic automatically routes to the remaining server*
- *Failover Process: Seamless transition with no session loss for users*

4. Web Services - Redundant Web Presence

- *Implementation: Two web servers (NV-WEB01 and NV-WEB02) behind a load balancer*
- *How It Works:*
    - *Both servers host identical web content*
    - *The load balancer monitors server health and distributes traffic*
    - *External DNS points to the load balancer virtual IP address*
- *Failover Process: Automatic detection and rerouting of web traffic if a web server becomes unavailable*

Additional Fault Tolerance Measures

Virtualization Layer Protection

- *Hyper-V Cluster: Both physical hosts configured in a failover cluster*
- *How It Works: If one physical server fails, all virtual machines automatically restart on the surviving host*
- *Benefit: Protection against complete hardware failure*

Storage Redundancy

- *RAID Configuration: Shared storage using RAID 10 for data protection*
- *How It Works: Data is striped and mirrored across multiple disks*
- *Benefit: Continuous operation even if individual hard drives fail*

Network Path Redundancy

- *NIC Teaming: Each server connects to redundant switches via multiple network cables*
- *How It Works: If one network path fails, traffic automatically uses the alternative path*
- *Benefit: Protection against network hardware failures*

Monitoring and Alerting

- *Automated Monitoring: Continuous health checks on all critical services*
- *Alert System: Immediate notification to IT staff if any service fails or shows degradation*
- *Benefit: Proactive response to issues before they impact users*

This comprehensive high availability plan ensures that NewVUE Health's critical IT services maintain continuous operation, directly supporting our commitment to uninterrupted patient care and operational excellence.

Hybrid Integration Readiness

Preparing for Cloud Integration
Our on-premises infrastructure is designed from the ground up to support seamless future integration with Microsoft 365 and Microsoft Entra ID. The foundation we're building will enable a smooth transition to hybrid cloud management without requiring significant reconfiguration.

Identity Synchronization Implementation

Primary Tool: Microsoft Entra ID Connect

- *Installation Location: A dedicated server (NV-SYNC01) separates from our domain controllers*
- *Why This Server:*
    - *Isolates synchronization processes from critical authentication services*
    - *Allows for specialized security hardening focused on external connectivity*
    - *Provides flexibility for maintenance and updates without impacting core AD services*
    - *Ensures optimal performance by dedicating resources to synchronization tasks*

Supporting Tool: ADFix (Active Directory Health Check)

- *Installation Location: Administrative workstations and NV-MGMT01*
- *Why This Tool:*
    - *Identifies and cleans up AD inconsistencies before synchronization*
    - *Ensures user attributes (UPN, email addresses) are properly formatted*
    - *Validates that our AD structure meets Entra ID Connect requirements*
    - *Prevents synchronization errors and configuration issues*

Hybrid Management Preparation

Identity Foundation Readiness

- *UPN Configuration: User Principal Names configured as username@newvuehealth.orgto match our public domain*
- *Attribute Consistency: Ensuring all user objects have required attributes populated (displayName, department, jobTitle)*
- *OU Structure: Organizational Units designed to support Azure AD group-based licensing and policies*

Network Readiness

- *Firewall Rules: Pre-configured to allow outbound connectivity to Microsoft 365 endpoints*
- *DNS Configuration: Public DNS records prepared for hybrid authentication requirements*
- *Certificate Authority: Internal PKI ready to issue certificates for secure hybrid connectivity*

Server Role Integration Strategy

Application Servers (NV-APP01/02)

- *Future Role: Host hybrid workflow services and application proxy connectors*
- *Benefit: Enable secure external access to on-premises applications via Entra ID*

Web Servers (NV-WEB01/02)

- *Future Role: Integrate with Entra ID for external user authentication*
- *Benefit: Secure patient portal access using cloud-based identity management*

File Servers (NV-FS01/02)

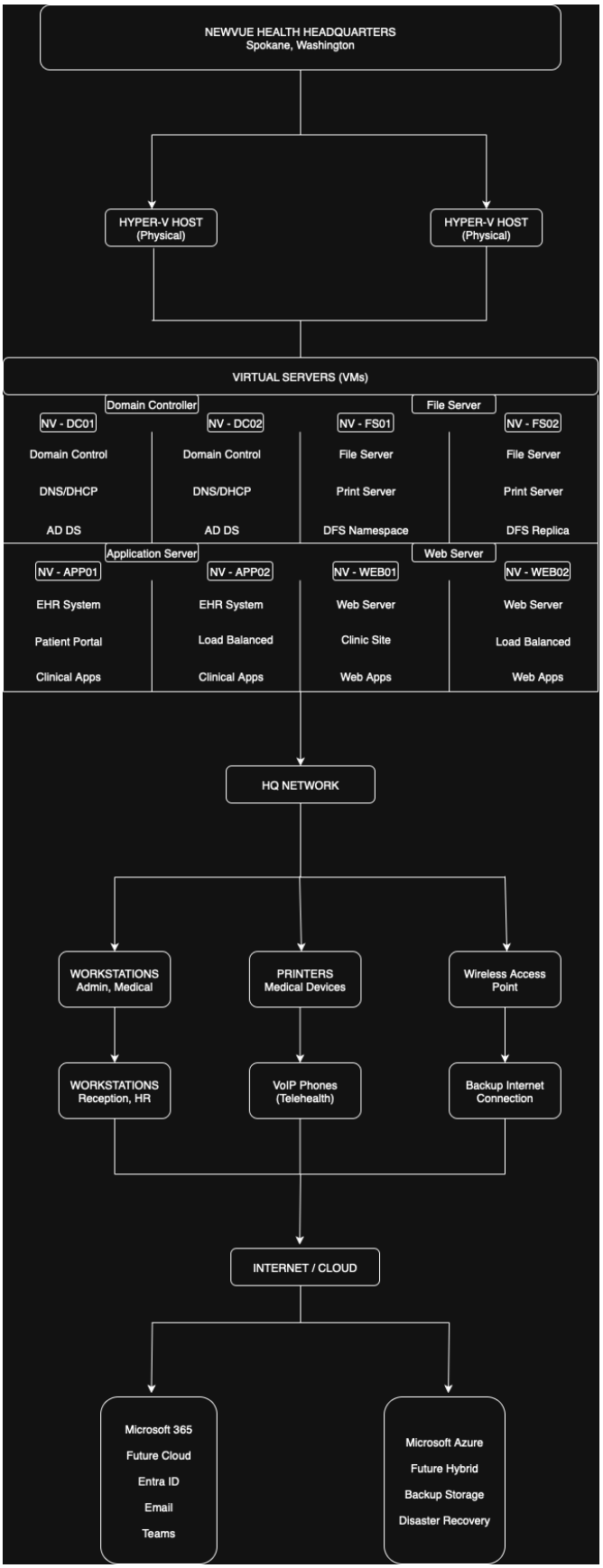
- *Future Role: Azure File Sync compatibility*
- *Benefit: Cloud-tiering capabilities for cost-effective storage management*

Phased Implementation Approach

1. *Phase 1 (Readiness): ADFix cleanup and environment validation*
2. *Phase 2 (Pilot): Entra ID Connect installation with pilot user group*
3. *Phase 3 (Full Sync): Gradual rollout to all users and devices*
4. *Phase 4 (Hybrid Features): Enable MFA, conditional access, and Intune integration*

This preparation ensures that when NewVUE Health is ready to adopt Microsoft 365, we can implement hybrid identity quickly and efficiently, maintaining security and operational continuity throughout the transition.

Infrastructure Diagram


NEWVUE HEALTH HEADQUARTERS
Spokane, Washington
HYPER-V HOST
(Physical)
HYPER-V HOST
(Physical)
VIRTUAL SERVERS (VMs)
Domain Controller
File Server
NV - DC01
NV - DC02
NV - FS01
NV - FS02
Domain Control
DNS/DHCP
AD DS
Domain Control
DNS/DHCP
AD DS
File Server
Print Server
DFS Namespace
File Server
Print Server
DFS Replica
Application Server
Web Server
NV - APP01
NV - APP02
NV - WEB01
NV - WEB02
EHR System
Patient Portal
Clinical Apps
EHR System
Load Balanced
Clinical Apps
Web Server
Clinic Site
Web Apps
Web Server
Load Balanced
Web Apps
HQ NETWORK
WORKSTATIONS
Admin, Medical
PRINTERS
Medical Devices
Wireless Access
Point
WORKSTATIONS
Reception, HR
VoIP Phones
(Telehealth)
Backup Internet
Connection
INTERNET / CLOUD
Microsoft 365
Future Cloud
Entra ID
Email
Teams
Microsoft Azure
Future Hybrid
Backup Storage
Disaster Recovery