Happy Health Systems

VDI Deployment

2015

[David Magnaterra]

3/16/2015

Table of Contents

[Version Control 2](#_Toc318118926)

[Virtualization Plan 3](#_Toc318118926)

1.1 [VDI Design 3](#_Toc318118926)

2.1 [IP Range 4](#_Toc318118926)

[Security 5](#_Toc318118926)

1.2 [NAP 6](#_Toc318118926)

[References 8](#_Toc318118926)

**Version**

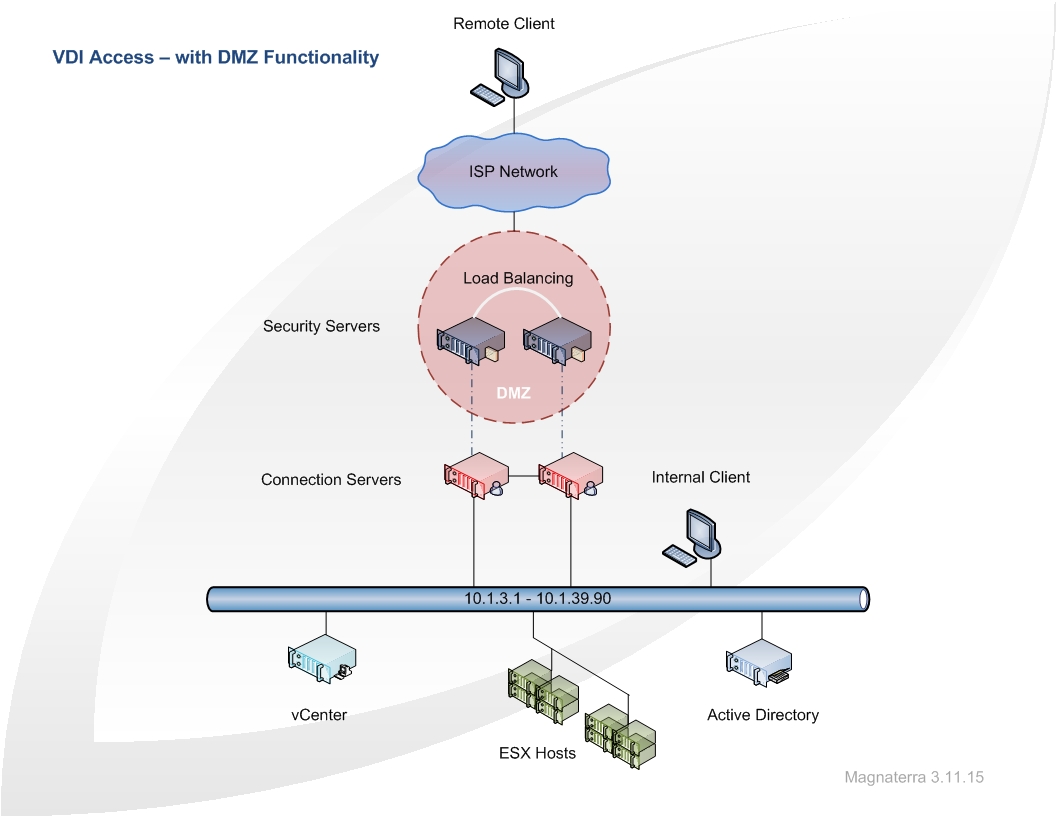
|  |  |  |
| --- | --- | --- |
| Version Number | Deployment Model | Date |
| 1.0 | U05A1 | 03/16/2015 |

# 

**Virtualization Plan**

Happy Health Systems will benefit from two virtual desktop infrastructures (VDI). The first infrastructure consists of access for the branch offices. The clinics, Physician’s offices, and research facility access the network from an Internet Service Provider (ISP). This connects the remote clients to the demilitarized zone (DMZ). The client queries the virtual domain controller in the DMZ, Kerberos generates a ticket. Upon authentication, the connection queries the load balanced view security servers a transaction occurs accessing the view connection servers. The user group membership is applied and vCenter serves the session delivered by the ESX hosts. Diagram 1.1 portrays the two infrastructures.

**1.1 VDI Design**



Internal VDI connectivity is the second infrastructure. Both infrastructures utilize the same vCenter and ESX hosts for session. Internal access connects directly to the local domain controller for authentication first. Upon authentication the load balanced view connection servers are queried for a session provided by vCenter aligned with the ESX hosts. All load-balancing is driven by the Cisco F5 Routers promoting seamless traffic management.

The client platform distributed entails Microsoft Window 7 Enterprise Edition and employs HP Flexible Thin Clients (t520-GX). The operating system and applications are managed by Active Directory Group Policy. A user’s group membership determines their associated applications and DFS shares. Hub sites and branch offices utilize the same model (hardware married to GPO) to promote standardization thus optimizing the two infrastructures. IP address distribution is different between the two VDI architectures. The DHCP and routing will be administered once authenticated into the DMZ. Address ranges 10.1.35.1 through 10.1.39.90 will have reservations assigned within the DHCP pool. The external sites will tunnel through the Internet and reach the DMZ therefore accessing the hosted applications and resources. This alternative enables a cost effective solution for support and subtracts network overhead. The table below projects the IP ranges which are dedicated to the sites across the network. The scope of subnets will be routed/forwarded by relay agents. Table 2.1 illustrates the IP range for the VDI clients.

**2.1 IP Range**

|  |  |  |
| --- | --- | --- |
| Site | Scope Subnet | Lease Period |
| Christ | 10.1.3.1 - 10.1.10.254 | **7 Days** |
| Kettering | 10.1.11.1 - 10.1.18.254 | **7 Days** |
| Pineview | 10.1.19.1 - 10.1.26.254 | **7 Days** |
| Schlottman | 10.1.27.1 - 10.1.34.254 | **7 Days** |
| Clinics | 10.1.35.1 - 10.1.36.254 | **Static –RES** |
| Physicians | 10.1.37.1 - 10.1.39.50 | **Static –RES** |
| Research | 10.1.39.51 - 10.1.39.90 | **Static –RES** |

High availability prolongs the infrastructure. The second server used for load balancing also is a Replica instance for the view connection server. Bi-directional replication takes place between the two nodes real time. If on server fails the sister server will continue to function endorsing constant uptime for the environment. Expansion can occur as well; new Replica instances could be added if a need exist. The LDAP directory found on the domain controller in the DMZ and within the internal network govern the access for connections to the vCenter. Virtual Desktop Pools federate various virtual desktops and allow centralized administration denoted by the embedded LDAP directories on the View Connection Server and Replica instances.

**Security**

Security begins with effective account policies. A GPO linked to the domain will enforce Kerberos settings, account lockout policies, and password policies. The group policies will be applied to the organizational unit and in some cases just a group within the organizational unit. Audit policies will review the account policies by triggers. Local policies and right consignments will provide the user no more or no less than they need to perform their job. Local policies for security will incorporate a standardized approach for logon, user desktop, interactive login, and browser based restrictions. Windows provides a firewall and allows advanced security for configuring inbound and outbound rules. The rules can be deployed to the containers globally or locally. Network list and manager polices will be installed to ensure network stability and deter attacks. Unidentified network policies will block unknown networks and network nodes. Identified networks will be blessed and identification of the location will be catalogued. Permission to the identified networks can be managed group policy edits. All virtual desktops benefit from firewall rules certifying access only by the View Connection interface thus confirming all RDP traffic moves through the View Connection Server.

NAP configurations involve DHCP as the gateway. The network access protection will be enabled on the scope. Scope options will be configured to limit access to the nodes which do not operate within the defined parameters. HTTPS connectivity with NAP employs SSL security for connections. Non-compliant clients will be filtered and access will be limited. These windows configuration will be implemented for HTTPS and standard DHCP access. HTTPS access will deliver synonymous NAP configurations; the only difference is the DMZ firewall configurations. NAP governs the remote desktop (RD) gateway as well. The health check of the client querying the gateway will have policy enforcement and group association concerning the remote desktop users. If NAP is unavailable restricted access will be applied. Active Directory account access and Exchange email will be provided, DFS shares will be offline until NAP is available portrayed in diagram 1.2.

**1.2 NAP**



Restriction for applications and control of the application will be identified and managed. Public Key Policies will perform tasks such as automatic certificate enrollment, generate certificate trust lists, administer data recovery agents, and form trust relationships with the certificate authority. Software restriction management will occur to block unapproved software. All new software will be a part of a process called change control. A committee will meet every week to evaluate and approve new software. All other components will be blocked on the domain. Application control policies will inherit AppLocker policies. The software restriction policies and AppLocker policies will work in tandem across the network.

**References**

Microsoft.com. (2011). Virtualization: The Benefits of VDI. Retrieved March 12, 2015 from

<https://technet.microsoft.com/en-us/magazine/dn170431.aspx>

Rouse, Margaret. (2012). Microsoft Network Access Protection (NAP). Retrieved March 2015, from <http://searchconsumerization.techtarget.com/definition/network-access-protection-NAP>

Vmware.com (2013) Design Considerations for Increasing VDI Performance and Scalability with Cisco Unified Computing System. Retrieved March 12, 2015 from <http://www.vmware.com/files/pdf/partners/pure-storage/VMware-increase-vdi-performance-whitepaper.pdf>