Happy Health Systems

Network Infrastructure Alignment and Active Directory Integrations

We will provide a centralize solutions for EMR and clinical applications

2015

[David Magnaterra]

2/10/2015

Table of Contents

[Version Control 2](#_Toc318118926)

[Executive Summary 3](#_Toc318118926)

[Project Scope 4](#_Toc318118926)

[Stakeholders 8](#_Toc318118926)

[Project Requirements 8](#_Toc318118926)

1.1 [Network EMR Topology w/Integration 12](#_Toc318118926)

1.2 [Philips iSite PACS Topology 13](#_Toc318118926)

[IP Addressing and Routing Architecture 13](#_Toc318118926)

1.3 [Network Topology 14](#_Toc318118926)

[Organizational Units 15](#_Toc318118926)

[DNS 15](#_Toc318118926)

[DFS Strategy 16](#_Toc318118926)

[FSRM Strategy 17](#_Toc318118926)

[EFS Strategy 17](#_Toc318118926)

[OU Deployment 17](#_Toc318118926)

1.4 [OU and Container Design 18](#_Toc318118926)

[Domain Models Available 19](#_Toc318118926)

[Administration Design and Logical Plan 20](#_Toc318118926)

1.5 [DNS Architecture 21](#_Toc318118926)

[Windows Server Configurations 21](#_Toc318118926)

[OU Strategy 22](#_Toc318118926)

[2.1 Domain Controllers 23](#_Toc318118926)

[1.6 OU Architecture 23](#_Toc318118926)

[Roles 24](#_Toc318118926)

[Administrative Plan 24](#_Toc318118926)

[Configuration Steps 25](#_Toc318118926)

[Physical Infrastructure 25](#_Toc318118926)

[1.7 Replication Infrastructure 26](#_Toc318118926)

[2.2 Bandwidth Allocation 27](#_Toc318118926)

[Active Directory Lightweight Directory Services (AD LDS) 28](#_Toc318118926)

[Active Directory Federation Services (AD FS) 28](#_Toc318118926)

[Active Directory Certificate Services (AD CS) 29](#_Toc318118926)

[References 30](#_Toc318118926)

**Version**

|  |  |  |
| --- | --- | --- |
| Version Number | Deployment Model | Date |
| 5.0 | **U05A1** | **02/10/2015** |

# 

# Executive Summary

A need has become apparent for centralized data management and consolidation of applications. The goal is to create standardization across the network thus linking the sites and creating a scalable environment with low overhead. The server operating systems and SQL will be promoted to 2008 R2 versions at the Enterprise platform. Licensures for Microsoft, AIX and Linux will be evaluated for the best enterprise solution.

Domain controllers will be accessible by the network nodes upon orientation and business need. Windows Server 2012 R2 will become the standard for all Microsoft server nodes. Enterprise licensing for Windows Server 2012 R2 enables wide use of the new operating system moreover promoting virtualization and integration of new server roles and features. Window Deployment Services will be the vessel for server OS upgrades. This deployment will be systematic addressing domain controls first then DNS, SEP, and DHCP servers. All other application servers will inherit the new versions of the server OS after a database backup. Upon database servers being upgraded, the tables will be indexed to ensure a clean transition.

User workstations will have the option to select between multiple domains upon Active Directory user and group assignment. A DMZ (demilitarized zone) will host various virtual server environments thus providing efficient patient care for Physician and clinics.

The network circuits will be provided by Time Warner. Class C IP addressing will provide the scope the business requires. Various VLANs will identify the site of the Layer 3 switches; this type of switch will enable routing protocols for packet security. WAPS (wireless access points) will be installed at all sites for ease of access and patient contentment. The WAPs will have two channels, one for patient access and another for domain access.

Applications aligned with the standardized network infrastructure will enable seamless upgrades and administration. EPIC applications and derivatives, will liquidate many current applications for reporting. Secure access to the EMR and PACS will be delivered for effective and efficient patient care. Microsoft Office will be deployed to client nodes by Microsoft SCCM scripting. A report will be generated once the client nodes are joined to the domain. PeopleSoft ERP will be deployed from SCCM by group membership to the finance group. Once the user authenticates to the domain controller an unattended installation will be pushed to the user’s computer. Symantec security and Spybot Search and destroy will be encapsulated within the standard Windows 7 x64 image. SCCM imaging will occur by means of network PXE.

**Project Scope**

**Project summary and rationalization**

Larry Macon, CFO of Happy Health Systems, called for the network and application alignment project to support cost with the business needs. Happy Health Systems is a network of hospitals and clinics located in southwest Ohio. We pride ourselves on accurate diagnosis derived by high technological means. A demand for secure confidential information access and sharing generates a new need for a topology change. Secure communication between sites will ensure compliance and data integrity. Patient information will inherit HIPPA compliant securities. The projected budgetary responsibility is 1.5.million dollars. Standardization strategically increases productivity and enhances patient care. The estimated annual support budget is $250,000 which will be drawn from the operational budget. Support is projected to become proficient for the IT systems served to the end users.

**Project Overview**

The undertaking of this project derives from a legacy support parameters and security constraints. The annual cost of legacy systems exceeds $300,000. Maintaining database updates will discontinue upon vendor support constrictions.

**Project Charter**

* Data traffic testing will begin with the current servers to gauge connectivity constraints.
* Volume estimates will be compiled and analyzed.
* Modality entries will be added (PACS).
* Physical nodes will be clustered for redundancy.
* Virtual nodes will utilize vMotion for redundancy.
* High availability servers will be placed at our disaster recovery site for another layer of redundancy.
* Security will be tested.
* Work flow changes will be defined for the department.
* Down time processes will be defined.

**The scope of this project includes and excludes the following items:**

Included

* Format: An Internet portal (Citrix) will provide the remote access point.
* Users: Will be provided Active Directory accounts.
* Users: Will be provided Exchange access.
* Users: Will be provided database access outside of LDAP (iSite, Cerner)
* Users: Will be provided EPIC securities.
* Users: A zero footprint viewer will be integrated into EPIC for access to PACS imaging.
* Update messages: Information regarding updates will be conveyed by email and the home page of the web portal.
* Infrastructure: Server remote upgrades.
* Infrastructure: Workstation remote upgrades.
* Infrastructure: Manual workstation hardware upgrade.
* Infrastructure: Manual workstation software upgrade.
* Infrastructure: Virtual host servers built.
* Infrastructure: VMWare vSphere 5.5 integration
* Infrastructure: Windows 2012 Hyper Visor domain controller cloning.
* Security: All data pulled/pushed from the DMZ will be encrypted with 256 bit SSL.
* Search tools: The end user is provided searching and history features within EPIC, Cerner, and iSite.
* Internet: Access to the web hosted applications must comply with IE8 and IE9 browsers.
* Access: The web portal will be available 24 hours, 7 days a week.
* Support: The network support center will be available 24 hours, 7 days a week.
* Support: Each system will have an on-call administrator available 24 hours, 7 days a week.

Excluded

* Promotion: The web portal will not be promoted to other hospitals.
* Internet: Content and color schemes are not amendable.
* Email: The email usage will be internal Microsoft Exchange.
* Instructions: Instructions will be defined by the facility.

**Approach**

Sequential Processes

* Servers and clients will receive remote OS deployment
* Client workstations will be upgraded and imaged.
* A bi-directional tunnel will be established between clinic sites and servers.
* The physical servers will be clustered with a HA server (high availability) at a disaster recovery site.
* The virtual servers will be redundant by vMotion with a HA server (high availability) at a disaster recovery site.
* Data will be migrations will be completed after hours.
* Databases will be validated.
* The biomedical team will create new entries on all modalities (Radiology PACS) in the network.
* Dry run testing will begin.
* Upon success, the final go-live date will be determined.
* Network naming schemas and architectures will be standardized.

Cohesive planning and strategic implementation will enable a prudent outcome.

* **Strengths:** Critical thinking and well trained professionals will provide positive outcomes.
* **Weaknesses** The network bandwidth metrics will need to be analyzed or modified. Administration of systems will be transformed.
* **Opportunities** Aligning the applications and network resources will enable a scalable environment with low overhead. The upgrades and hardware administration will be managed by centralized support hence minimizing system diversification. Patient information will inherit added security therefore enhancing patient care.
* **Threats** The legacy systems may not be able to be fully tested parallel to the go-live. Workstations and print servers will be exchanged during the go-live.
* **Risks** Network failure could stop access. The redundancy will need to be assessed system by system.
* **Constraints** The budget will not stretch to fund unforeseen variables. The team is limited to six members. The timeline is smaller than other site’s metrics.
* **Assumptions** The appropriate tools are available. Each team member is competent in their role. The risk management has been analyzed accordingly. The ROI will exceed the initial investment.

**Stakeholders**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Management Type** | **Role** | **Project Phase** |
| Larry Macon | Capital Budget Allocation | CFO | Phase 1, 2 |
| Dan Johnson | Applications | Manager | Phase 1, 2, 3, 4, 5 |
| Bob Smith | Infrastructure | Manager | Phase 1, 2, 3, 4, 5 |
| Lisa Connell | Clinical Informatics | Physician Liaison | Phase 4, 5 |
| David Magnaterra | Clinical Applications | Trainer | Phase 3, 4, 5 |
| Carl Canter | Infrastructure | Analyst | Phase 2, 3, 4, 5 |
| Durral Kisone | Infrastructure | Workstation Lead | Phase 2, 3, 4, 5 |
| Shane Wackson | Infrastructure | NOS | Phase 2, 3, 4, 5 |
| Justin Walken | Infrastructure | Network Engineering | Phase 2, 3, 4, 5 |
| Greg Courtney | Application | Analyst | Phase 2, 3, 4, 5 |
| Dan Acape | Application | Analyst | Phase 2, 3, 4, 5 |
| Larry Kiser | Application | Analyst | Phase 2, 3, 4, 5 |

**Project Requirements**

**Process**

The budgetary means equate to 55 million dollars capitol allocated for the project. The organization strategies include deployment by October 18, 2014. This is not a tentative date; the fiscal year must prove the EPCI EMR functions due to federal compensation and kickbacks. These kickbacks will negate cost thus enabling the new strategies to take form.

**Organizational Assessment**

Organizational constraints consist of data migration from the legacy Novell infrastructure. A single domain and forest will be executed for the new topology. Email migration from Novell GroupWise to Microsoft Exchange will occur and data validation will transpire as well. All DICOM data from the current databases will migrate to the Philips iSite IBM SAN. VCEs (virtual modules) will incorporate the structured DICOM datasets. A Vendor Neutral Archive (VNA) deployment will allow ownership, cost leverage, and DR capabilities for the proprietary iSyntex (compressed DICOM type) data. ACUO temporal routers will drop a copy on the Philips iSite SAN and the VNA thus providing the preceding capabilities illustrated in diagram 1.2. DNS and DHCP servers will be deployed at the four main facilities. A demilitarized zone (DMZ) will be constructed for remote access and public addressing. Lab datasets will migrate into the Cerner Pathnet Oracle database. Validation will occur upon migration. EPIC 2012 will become the EMR. All data from the prior Carecast EMR will be migrated into the EPIC environment. HL7 feeds will connect both Pathnet and iSite with EPIC illustrated in diagram 1.1.

Infrastructure assets range in operating systems. The current architecture consists of Windows Server 2000, 2003, and 2008. Windows Deployment Services will assist in server upgrades. Philips iSite and EPIC incorporate vendor owned hardware, these system comprise Windows platforms and UNIX architectures. These operating systems will not be a part of the deployment scope as they are supported by the vendor. Client workstations need hardware upgrades to facilitate the applications and the 64 bit upgrade. Moving from an x86 to an x64 platform allows larger use of memory for the workstations. Memory will be upgraded to expand performance. Virtualization of application server will occur for Cerner Pathnet and PeopleSoft. The two systems will become redundant with VMWare vMotion technologies. A HP 3PAR SAN will be attached to all virtual nodes thus providing redundant storage with fiber channel bandwidth approaching 8 Gbps.

**Requirement Management (multi-tier)**

**Network Administration**

* Domain configurations consist of one domain with four domain controller one per hospital. Active Directory will entail user and group administration, DHCP, static IP scopes, site sub netting, DNS replication, and DFS sharing. Group policies will be deployed by SCCM as well as all unattended installer packages. (1/25/2015)
* Remote operating system deployment begins with servers which incorporate Windows Server 2008 or lower. Windows Deployment Services will deliver remote OS upgrades for servers and clients. Client must meet the following specifications to be in the WDS scope: dual core processor, 6 GB of RAM. Any client outside of the scope will be manually imaged by SCCM PXE distribution. (1/27/2015)
* Security will be managed by IPSEC technologies and SSL encryption. All non-LDAP databases will align security measures with standardized protocols. Users, network administrator, systems analyst, and domain administrator securities will be defined. Groups, organizational units and all other containers will be configured for centralize policy management. (2/2/2015)
* Email accounts migration into the Exchange platform will begin. Inbox storage allocation will be standardized. (2/10/2015)
* A parallel network will exist for testing; the current Novell network will coexist with the new Microsoft Server 2012 R2 Active Directory driven environment. After bi-directional connectivity is established, users and groups will be migrated. (2/10/2015)
* Network modifications will begin. The current existing routing and switch environment will be upgraded to a Layer 3 switch environment with F5 routing. (2/10/2015)
* Client Workstations will have to meet a specification of Intel E7600 2 core processors, HP 6000 pro workstations, 6 GB of RAM, Windows 7 x64, and IE 8 browser. (2/1/2015)
* Radiology Diagnostic Workstations will have to meet a specification of Intel Xeon E5620 4 core processors, HP Z800 workstations, 12 GB of RAM, Windows 7 x64, and IE 8 browser. Video will meet a specification of a Barco MXRT-7400 graphic card and a minimum of one Barco Coronis Fusion 6 MP MDCC-6130 monitor coupled with a minimum of one HP LA2405wg monitor. The standards will double the video specifications. (2/5/2015)
* Cutover and deployment will begin after business hours on a Friday. (3/18/2015)

Threshold -----------------------------------------------------------------------------------------------------------------------------

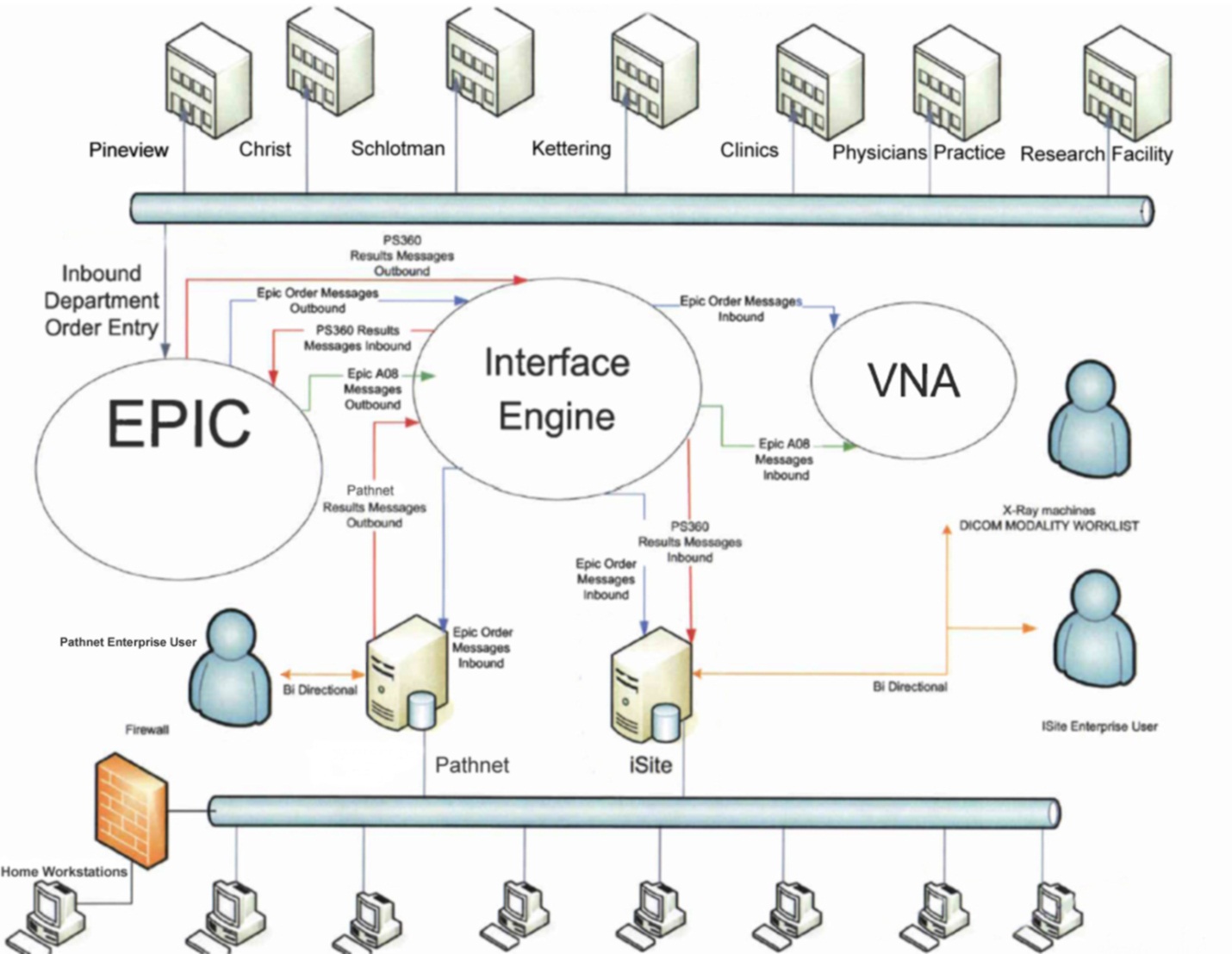
**Application Administration**

* EMR (EPIC) build will be compiled in the CER (test) environment. The design goals consist of HL7 interfaces, SUBI PACS integration, HIS management, Lab result GUIs (by HL7 messages), and PACS results GUIs (by HL7 messages). The integration engine delivering the HL7 messages will be an Ensemble integration engine. This will be the vessel for results and reporting. Groups and users will be linked to Active Directory by LDAP. Administration will be handled by the System Administrators. (3/1/2015)
* Philip iSite 3.6.150 will be the PACS. The archiving will have two DICOM stores. One store will be the SAN provided by Philips, the other store will be an Atmos VNA (vendor neutral archive) solution. The VNA will enable us to gauge the price per stored study with the vendor. Having and owning the information will provide variable leverage with the vendor. BSC (business continuity servers) will be placed at every main hospital for backup access to images these servers will be virtual. Temporal DICOM routers will live at every site for routing images to both iSite and the VNA. Groups and users will be linked to Active Directory by LDAP. Administration will be handled by the System Administrators. Results and reports will be interfaced by the Ensemble integration engine then made available to nurses and physicians. (3/10/2015)
* Cerner Pathnet will track dose and biopsy information. Groups and users will be linked to Active Directory by LDAP. Administration will be handled by the System Administrators. Cerner Pathnet will consist of two host servers carved into virtual servers. The HP 3PAR SAN will be attached to the nodes for redundant storage. Results and reports will be interfaced by the Ensemble integration engine then made available to nurses and physicians. (3/14/2015)
* PeopleSoft (virtual) will be queued to push by SCCM upon user authentication and user group membership. (3/14/2015)
* Workstations will be imaged and tested. The preconfigured systems will be deployed by a team of workstation administrators. (3/14/2015)
* Microsoft office will be deployed to all client workstations by SCCM. An inventory monitor script will run to monitor usage of the MS Office. If the product is not used in 90 days the suite will be uninstalled (a network pull by SCCM) to save enterprise licenses.(systematic upon 3/14/2015 WS deployment)

**Support**

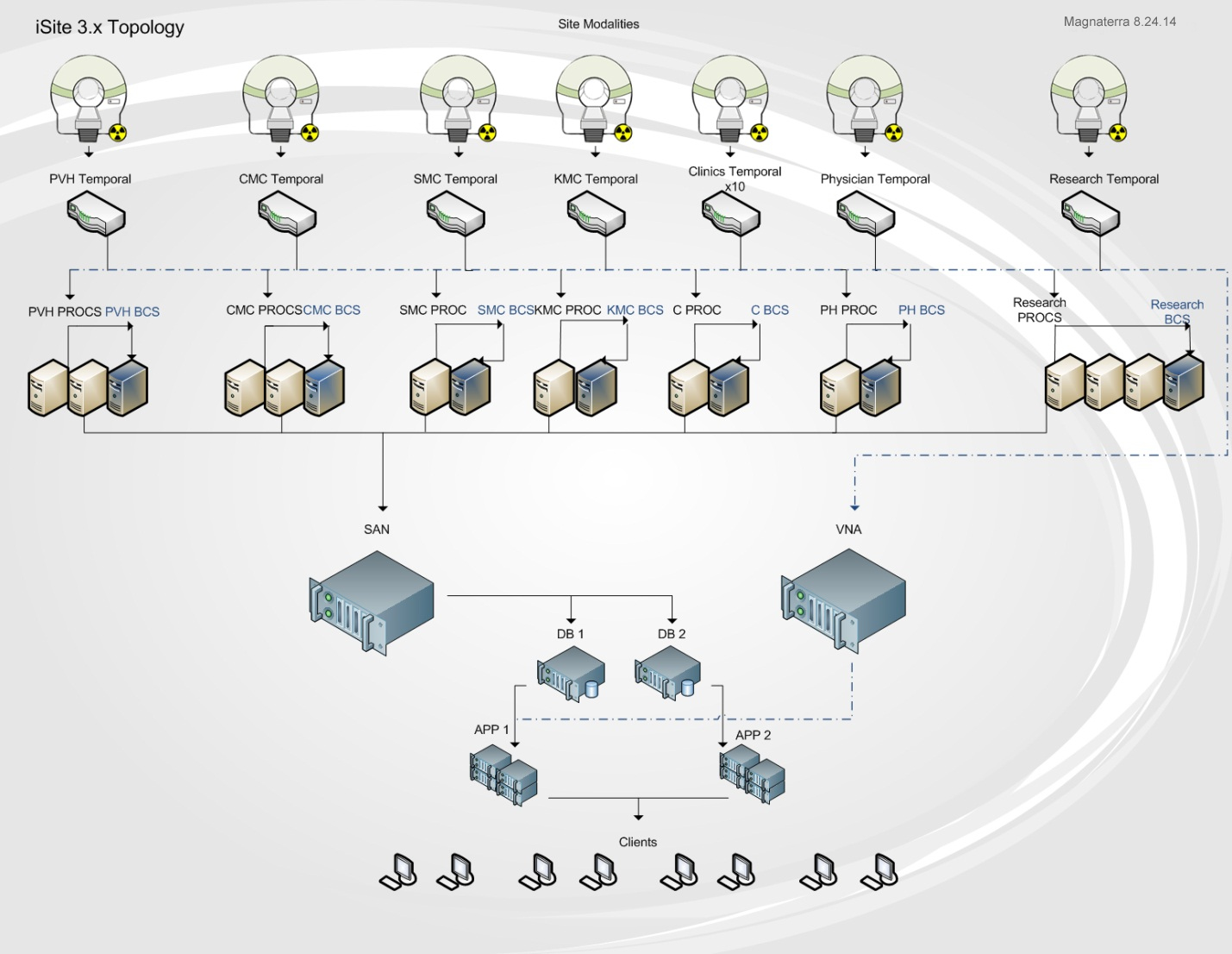
* Customer support models will be analyzed. The goal is to have application support teams, network engineering support, and network administration support 24 hours a day 365 days a year. (3/5/2015)
* Training will begin in a classroom atmosphere. Surveys will be delivered to the users. Additional onsite training will be available based on testing and feedback. (3/13//2015)

**1.1 Network EMR Topology w/Integration**

****

# Radiologist will have preconfigured workstations sent to their homes. Access will connect by token and Cisco Any Connect interfacing. EPIC will not be integrated on these workstations. The Radiologist will need to access EPIC by token through the Citrix SAP. EPIC inherits many security updates thus negating VPN functionality due to constraints. These users will be in the standard VPN and SAP groups; iSite Enterprise and EPIC will also be advertised in the SAP for remote access.

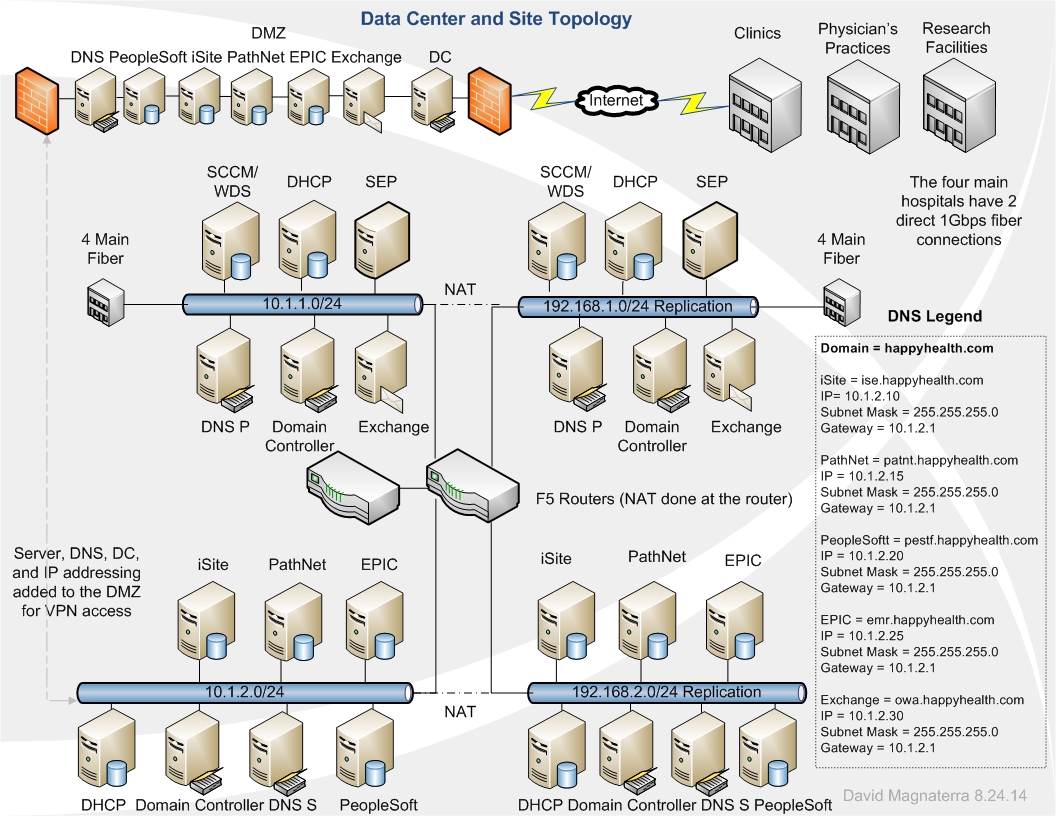
**1.2 Philips iSite PACS Topology**



**IP Addressing and Routing Architecture**

IP addressing will comprise of a Class A scope and a Class C scope. The translation between the two networks will be done by NAT processes on the router. Replication between environments will take place across networks; this will ensure redundancy and enable separate physical networks thus safeguarding the network redundancy.

Clinics, Physician’s practices, and the research facility will apply VPN tunneling for access to the DMZ (demilitarized zone). The DMZ will incorporate iSite Enterprise, PathNet, PeopleSoft, and EPIC. This will enable secure access to the network applications, the Class A private network will NAT for communication to the public networks. The Servers will be added to the DMZ with IIS web hosting and account management. Illustration 1.3 displays the technical overview of the network. The four main hospitals will have two 1 Gbps fiber connections to the datacenter. One connection to the Class A network and one connection to the Class C network therefore providing redundancy. The F5 router will load balance between the two networks dependent upon bandwidth usage and peak hours.

**1.3 Network Topology** 

**Organizational Units**

The design is an object oriented architecture categorizing network resources into containers. Organizational Units (OUs) will contain groups by site definition. Each group will contain users based on roles in the organization. Group policy will be applied at the group level and inherited by the users for standardization and security. Other object will be defined by a naming schema. Computer objects will be organized by a controlled NetBIOS name and managed by site membership. Other devices will have a similar object oriented categories for centralization of network assets.

The OUs will create the foundation for the single domain happyhealth.com. The OUs will manage the geographical diversified sites rather than creating additional domains. The concept is to simplify the administration and provide a scalable optimized infrastructure “It also provides a sense of physical administrative isolation, which some organizations might prefer instead of the logical administrative isolation that can exist when all various object types reside in a common domain” (Posey, 2013). Some Group Policy Objects (GPOs) will be applied to the OU if a site is specified for any change or dry run concerning new technology. Delegation from the OU will be the vessel for management across the various site containers. Naming will be unique in the OUs to promote unique identification of objects moreover normalizing the domain database. Common Names (CNs) for users will be unique as well; this will ensure easy administration for user account creation even though each OU can have has its own CN architecture.

**DNS**

DNS internal placement will consist of primary to secondary nodes. The main datacenter will entertain one primary and on secondary node per network. One WINS node will be placed into each network for NetBIOS resolutions. The CNAME alias will be the record type utilized for all DNS nodes. The DNS resolver will query both the CNAME record and regular resource record. This allows local or remote naming resolutions. Upon network failure, the IP schema can be “flipped” to the stable network e.g. ise.happhealth.com has a native network address of 10.1.2.10. If the 10.1.2.x network fails simply have ise.happhealth.com resolve to 192.168.1.10 thus providing redundancy.

The Class A IP addressing will be the native or default values. The Class B addressing will only resolve upon network failure. The IP and DNS matching are comprised of the following redundant linkage:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| DNS | IP | IP | Subnet Mask | Subnet Mask | Gateway | Gateway |
| ise.happyhealth.com | 10.1.2.10 | 192.168.1.10 | 255.255.255.0 | 255.255.255.0 | 10.1.2.1 | 192.168.1.1 |
| patnt.happyhealth.com | 10.1.2.15 | 192.168.1.15 | 255.255.255.0 | 255.255.255.0 | 10.1.2.1 | 192.168.1.1 |
| pestf.happyhealth.com | 10.1.2.20 | 192.168.1.20 | 255.255.255.0 | 255.255.255.0 | 10.1.2.1 | 192.168.1.1 |
| emr.happyhealth.com | 10.1.2.25 | 192.168.1.25 | 255.255.255.0 | 255.255.255.0 | 10.1.2.1 | 192.168.1.1 |
| owa.happyhealth.com | 10.1.2.30 | 192.168.1.30 | 255.255.255.0 | 255.255.255.0 | 10.1.2.1 | 192.168.1.1 |

**Authentication**

Domain controllers will employ a ticket system for authentication utilizing the Kerberos protocol. Node identity will be authenticated by the domain controller, the computer objects must be registered in Active Directory otherwise a trust relationship error will occur. Both the node and user need to be an object in the database for authentication. The domain controller will act as an authentication server and forward user credentials to the Key Distribution Center (KDC). Upon arrival, a ticket will be issued and encrypted. The PDC Emulator will process any password changes across the domain. This will manage trusts, GPOs, Time, and distributed file systems (DFS) as well.

**DFS Strategy**

The namespace will be a domain-based replicating approach. Folder structures incorporate a targeted folder containing the shared content. Access to the DFS shares will be scripted to the user’s active directory login (login script). All DFS shares will be on NTFS volumes moreover only sharing Windows based content. Access-based enumeration will be utilized to hide folders and files from users that are not provided permissions for access to the shared content. Windows Server 2008 mode configurations permit access-based enumeration to function across the domain-based namespace. All namespace servers will use Windows Server 2012.

**FSRM Strategy**

File Server Resource Manager (FSRM) quota management for shares will only exploit hard quotas. Each allocated volume entails notifications to the user at 80%, 85%, and 90% retention. Upon 90% retention the administrator will receive an email and an event log will be generated. File screening involves blocking of audio and video for all DFS shares. Executables will be blocked for regular users; administrator will have exclusions denoted within their shared folders. Only active screens will be applied and notification will be sent to both the user and the administrator. Event logs will not be notified.

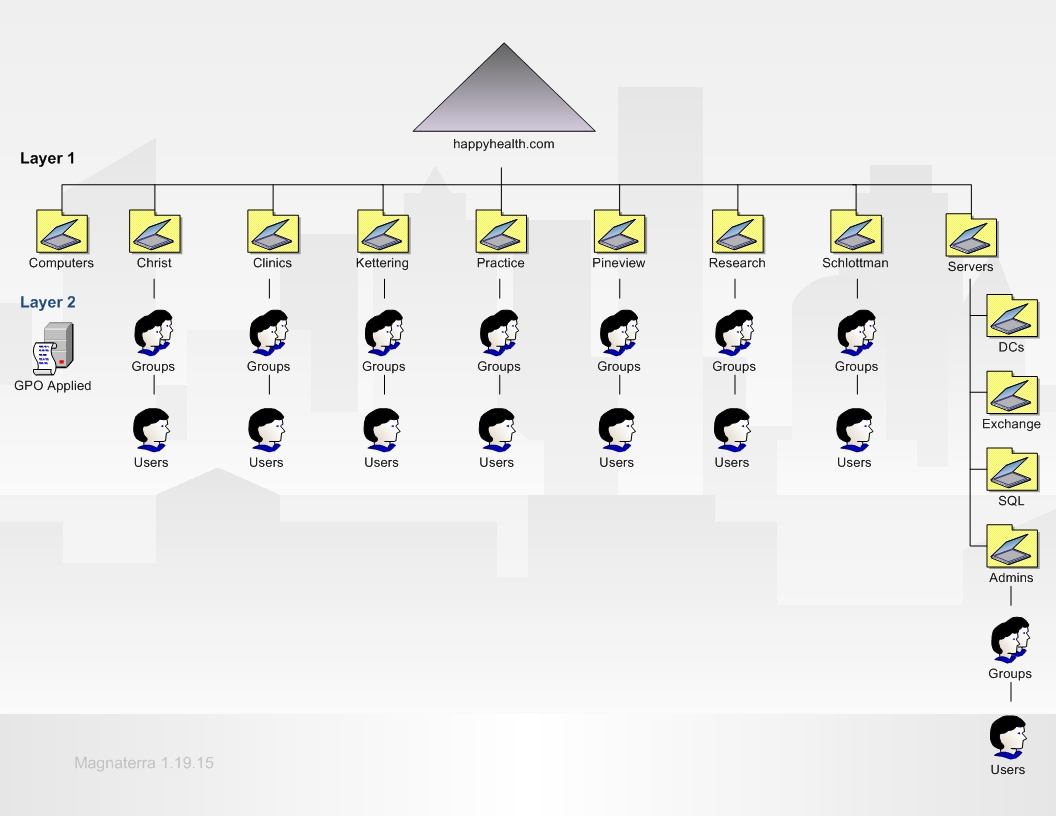
**EFS Strategy**

A knowledge base for IT support and analytics will utilize levels of Encrypted File Systems (EFS). The IT group determines the access to the certificates for folders. The support center will have limited access to much of the content. Domain administrator can break the encryption and network administrators will have access to the database information designated to their IT group. This promotes shared documentation and secures access to the databases’ service account credentialing as well as proprietary information. All mobile devices with Windows 7 incorporate BitLocker. The network image for the mobile devices will begin the hard drive encryption once the device is added to the domain.

**OU Deployment**

The singe domain happyhealth.com will be structured by OU assignment to sites therefore allowing containment of groups and users. OU containers are a part of the layer 1 which encompasses sites, servers, computers, domain controllers, Exchange, SQL, and network administrators. Groups will be defined by the department and contain users by their role in the organization. Layer 2 grouping is the layer where GPOs are applied. Diagram 1.4 exemplifies the distribution of policies and site segmentation across the domain. Notice the server OU, this braches out to separate system administration from the sites and computer objects. Trust relationships are normalized in a single database, all users and computer objects are localized in one domain.

**1.4 OU and Container Design**

****

**AD Structure**

This structure has been compiled to provide a simple and efficient approach for the organization. Simplifying the architecture promotes a scalable environment furthermore optimizing administration across the containers and network nodes. The computers OU incorporates workstations and printer objects. The server OU is branches out into four other OUs. Any server outside of the four OU’s scope will live in the server OU (e.g. DNS, SCCM…). All data is replicated to each domain controller in the single domain promoting low overhead. No global catalog server is necessary as the domain controllers can take the role negating additional nodes. The single domain design allows GPO consistency yet can be applied much like a multi-domain architecture. Auditing is controlled more effectively; the auditing and access control is contained in one domain sponsoring streamlined management of Active Directory. If the business expands, an additional domain can be absorbed and trusts can be developed. Starting in a single domain empowers cost-effectiveness and efficient administration for the project.

**Domain Models Available**

The single domain model delivers simplified administration by allowing domain controllers to replicate easily and become a global catalog server as well. Auditing and access control can be managed with ease from the singular structure. GPO application is deployed to the groups contained by the OU. A multi-domain model utilizes two or more domains. Trust relationships are designed four ways: one-way, two-way, transitive, and non-transitive. One-way trusts are a single trust relationship and non-transitive. Two-way trusts work within the forest generated by the root domain tree married to the additional domains, these trusts are transitive.

Replication across multiple domains can become complex. Each domain deploys domain controllers with a global catalog. Between the two domain controllers, schema and configuration data replicates, various subsets between the two domains replicate as well. The information is replicated to the other domain controllers within each domain. Domain trees contain the domains, an additional domain added to the tree takes on a child role to the root domain. Trees can be separated within the forest container sharing the logical structure as the top-level container of objects. Each domain in a multi-domain design contains other containers ultimately containing objects.

**Administration Plan and Logical Design**

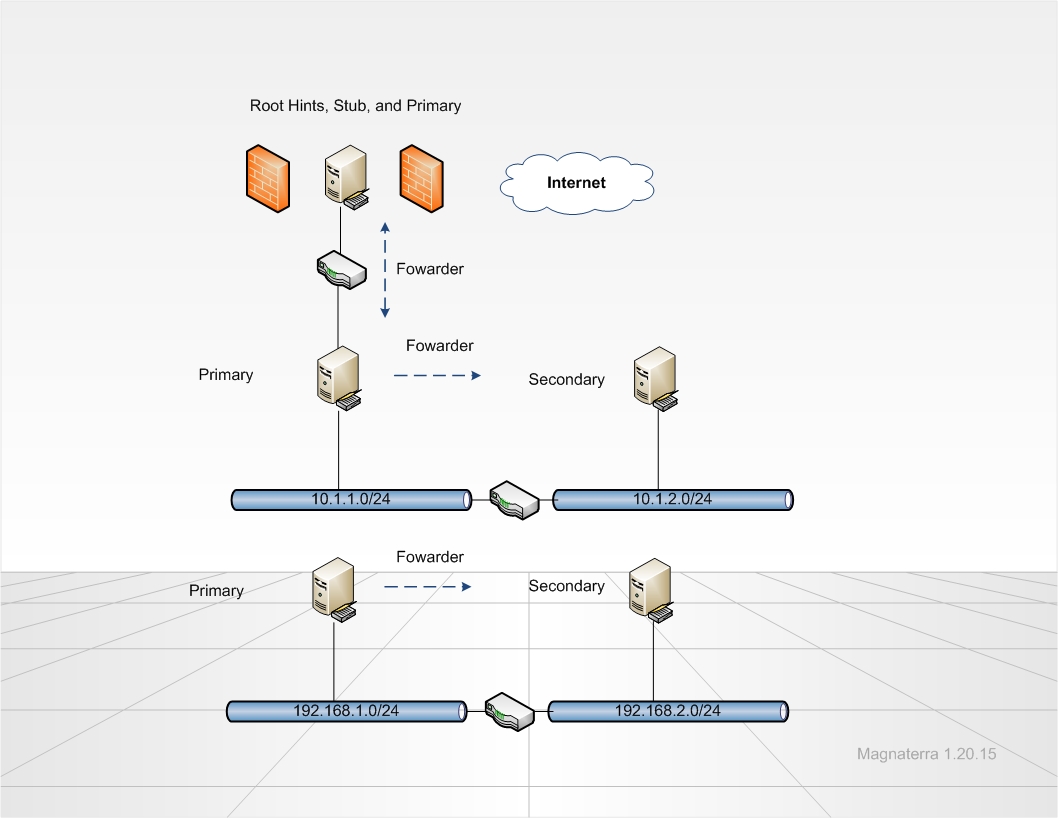
Best practices defined my Microsoft will be followed for all tasks. Workstation managments will be policy-based and applied to the centralized OU containing the computer objects. Effective DFS caching alignment with load will enable efficient management of clients thus providing constant access to shares across the network. Using the single domain model minimizes excessive network resources both hardware and management of Active Directory. Group policy begins at the layer 2 tier illustrated in the preceding diagram (1.4). Users will inherit GPOs from their group membership. All designs will be thoroughly tested prior to cutting over from the Novell architecture.

The demilitarized zone (DMZ) will incorporate a domain controller acting as a global catalog. Clinics, physician’s practices, and the research facility will authenticate by tunneling though the Internet. Each site will have IP and DNS values added to the crypto-domain promoting access to Active Directory and network resources. The ISP for the outlying sites will add our information into their crypto-domain generating the handshake. These users and computers will be added into their OU and function as they are within the backbone.

The configurations in Windows Server 2012 will entail an extension of resources into the DMZ. The DNS build will not be Active Directory integrated. A root server will be incorporated into the DNS node within the DMZ. Within the server management console external forwarding will be done internally. Internal conditional forwarding will occur from the primary DNS servers to the secondary DNS servers. Each DNS server will have a stub interface built to refer requests. Diagram 1.5 projects the design for the flow of replication. Dynamic updates within zones will be enabled because the DNS topology is a primary to secondary interaction across the network. The interfaces listening for the DNS request will be set manually to provide security from DNS poisoning.

Strategic placement within the DMZ will enable efficient resolution and reverse lookup capabilities for the remote sites. Utilizing primary and secondary DNS servers will provide redundancy of the “master record”. If the lookup value is not within the primary record the secondary server will utilize zone transfers on a separate connection to better provide effective record retrieval.

**1.5 DNS Architecture**



**Windows Server Configurations**

MSDN library delivers many feasible approaches know as Infrastructure Planning and Design Guides “The series is a collection of documents that leads the reader through a sequence of core decision points to design an infrastructure for Microsoft products. It also provides a means to validate design decisions with the business to ensure that the solution meets the requirements for both business and infrastructure stakeholders” (MSDN, 2012). Windows Systems Center utilities sanction many tangible resources for deployment and monitoring Active Directory features. The Infrastructure Planning and Design guides (IPDs) create the roadmap for integrating new abilities available in the 2012 architecture. Operations manager IPD assists with the plan by outlining best practice processes for the structure and logical design. Security can be enhanced by employing the data protection manager IPD for archiving and data recovery strategies. A valuable guide for deploying a new infrastructure is the Active Directory domain services IPD. Adding the tactics from this service encourages effective application of panning prior to implementation. All web-based applications will be managed by Internet Information Services (IIS). The associated guide illustrates know issues with resource alignment and illuminates hosting schemes.

**OU Strategy**

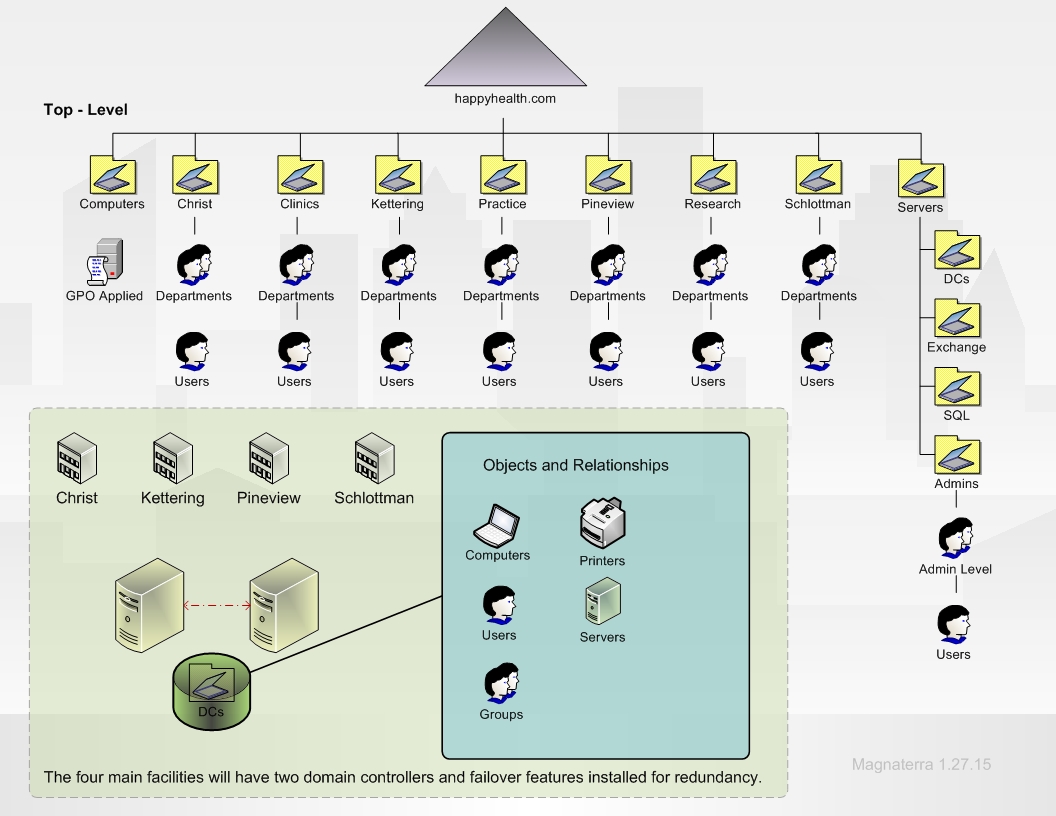
The single domain design relies upon strategic OU object management and the relationships between objects must be persistent. The OUs are the top-level within the HHS domain. Domain controllers ensure replication across the sites projecting a time to live (TTL) value set at two minutes. The four main hospitals incorporate a set of domain controllers utilizing the Microsoft failover cluster manager feature. A virtual IP address will manage the clustered domain controllers. Two identical domain controller servers will reside physically at each main facility. OU management can occur most effectively by accessing the domain controller and OU dedicated to the site. The domain controller cluster naming is demonstrated in table 2.1 below.

Each department associated to the sites are grouped and contained within the OUs. Group objects are organized by site to act like a child domain with two-way transitive trusts. The domain controllers at the main sites will have the directories replication cycle synchronized with the OU object moreover negating manual updating of objects. Strict replication consistency will be imposed for the inbound domain controller normalizing objects in the database. Effective management of objects will ensure seamless replication. Diagram 1.6 exemplifies the structure between the OUs and the domain controllers within the infrastructure.

**2.1 Domain Controllers**

|  |  |  |  |
| --- | --- | --- | --- |
| Site Name | VIP Node | Primary Node | Passive Node |
| Christ | DCWPAPP001V1 10.1.3.3 | DCWPAPP001P1 10.1.3.1 | DCWPAPP001P2 10.1.3.2 |
| Kettering | DCWPAPP002V1 10.1.11.3 | DCWPAPP002P1 10.1.11.1 | DCWPAPP002P2 10.1.11.2 |
| Pineview | DCWPAPP003V1 10.1.19.3 | DCWPAPP003P1 10.1.19.1 | DCWPAPP003P2 10.1.19.2 |
| Schlottman | DCWPAPP004V1 10.1.27.3 | DCWPAPP004P1 10.1.27.1 | DCWPAPP004P2 10.1.27.2 |

**1.6 OU Architecture**

****

**Roles**

Departments divide the users into factions. Using the dispersed OU design enables the naming to be localized in the OU container. This can prevent conflicts with user names and identities yet best practice will be followed and user ID will not be simulated. The groups can have the same name as another group as long as they are not in the same OU. The finance department (group) can be name finance in the OU (or site) they belong to. Deployment of GPOs concerning MSI packages are applied to the OU for computer objects. Group Policies for Active Directory objects trickle down from the OU; they can be global or local to an object. Servers will have the same process yet SCCM will manage the software pushes across the OUs. This allows more condensed reports and auditing. The administrators will be segmented into three groups.

This first administrator is the domain administrator, this role has unrestricted access and rights to all network systems. This role will be embedded in all client and server network images. The second administrator is the desktop support container. This role replicates the local administrator on a workstations, the only additional access is the ability to add a computer object as a member of the domain. The final administrator group is the application administrators. These users have local administrator rights to specific servers. This is role cannot add objects to the domain.

**Administrative Plan**

The server OU illustrated in diagram in 1.5 and 1.6 identify a nested approach for server computer objects. The child OUs allow a structured model and entertains ACL delegation across the contained objects in the admins OU moreover applying effective management of the administrator roles. The group containers absorb the brunt of the group policies and access control. Separating the OUs by site permits separation of group policies thus allowing geographical centralized management of ACLs and GPO applications. Computers OU is completely separate for direct object management concerning policies applied to the client workstation; the objects can be standardized across the domain. The local machine policies and security groups will be applied to the OU for these objects.

**Configuration Steps**

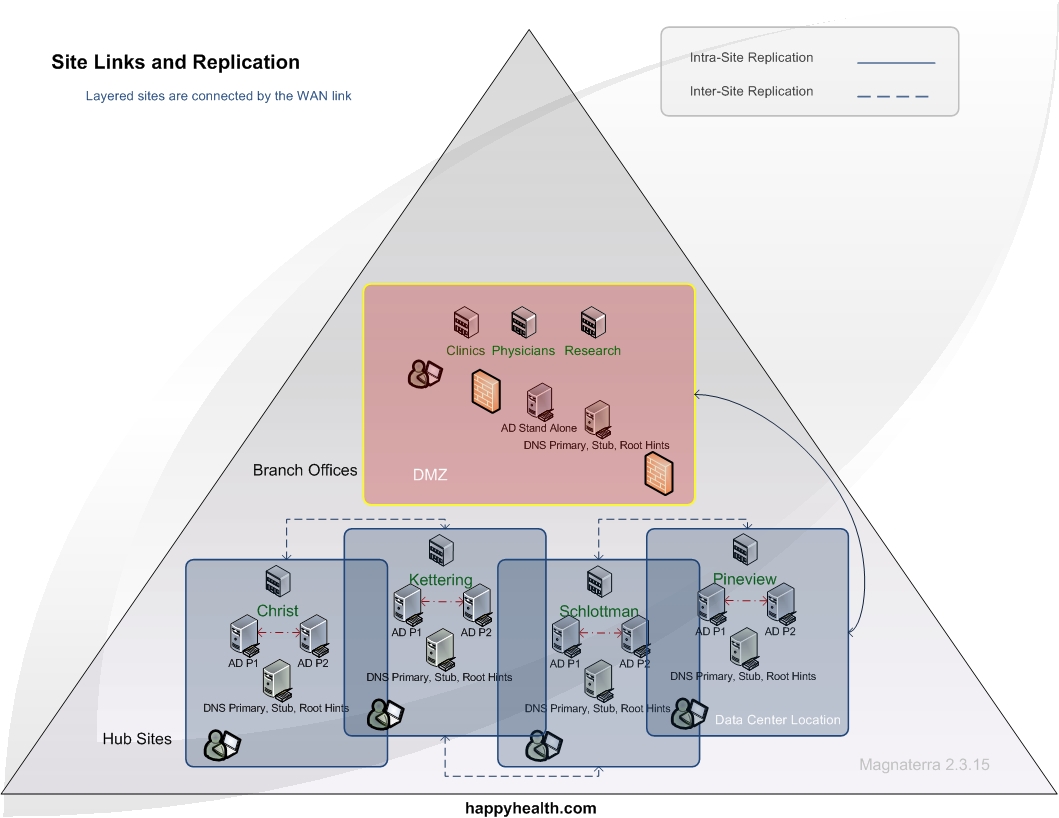
The first step to configure groups and OUs is to develop a scope for the design. The user types must be identified and the policies need to fit the groups association by role and location. Computers in the domain will have a standardize build concerning desktop, browser, and profile policies. Some computers will be a part of an exclusion scope due to custom designs related to the Radiology department. Administration will be centralized and delegate by group policy; metrics and auditing will be analyzed to refine settings.

Network infrastructure designs will be planned to facilitate the OU scheme by employing strategic DNS placement across the domain. The Novell security groups will be evaluated and a new model will be built from the Novell environment though delegation tactics will be revised. The group policy management console (GPMC) is the vessel for full management of GPOs across the domain “Try not to over think the design, rather logically consider how you want to delegate and how you want to deploy GPOs” (Melber, 2012). Domain administrators will import and export, create redundancy, search, and configure reporting for the GPOs in this console. Scripting MSI deployment will also occur in the GPMC, unattended installs will be executed by group in the computer OU.

**Physical Infrastructure**

Happy Health Systems will incorporate a replication strategy which employs separation between the hub sites and the branch offices. The hub sites include the four main hospitals: Christ, Kettering, Schlottman, and Pineview. These sites are connected by the WAN link and utilize bi-directional Inter-Site replication. When the objects are generated on the destination domain controller it will then stipulate the source domain controller for the next site. Replication TTL equates to two minutes across the domain for these sites moreover providing a systematic schedule for the replication married to the cost value for routing. Diagram 1.7 clarifies the cost value routes for replication. The clinics, Physician’s offices, and research facility (branch offices) utilize Intra-Site replication. This promotes a one-way connection for the nodes connecting by VPN to the DMZ “The secure connection across the internetwork appears to the user as a private network communication—despite the fact that this communication occurs over a public internetwork—hence the name virtual private network” (MSDN, 2001). Knowledge Consistency Checker (KCC) manages this replication and allows speed to be optimized for the replication. This process is generated from the bi-directional design established within the data center at the Pineview site.

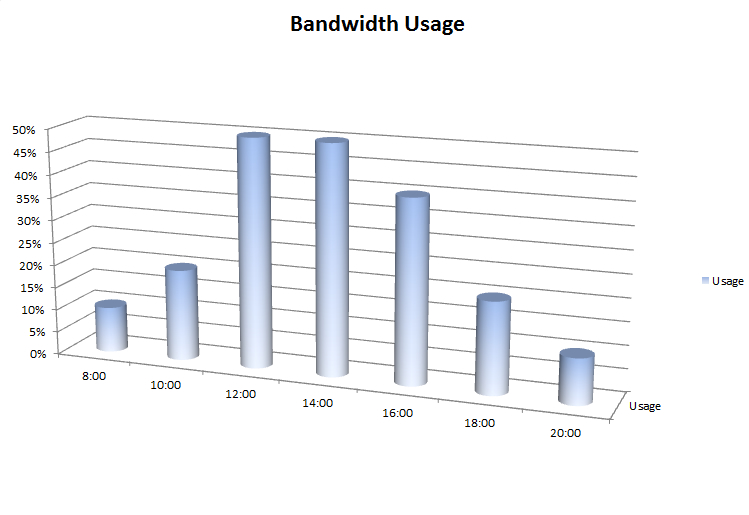
**1.7 Replication Infrastructure**



The Inter Site Topology Generator (ISTG) applies replication over a bridgehead server, these roles are added to the domain controllers in the hub sites. The domain controller at Christ Hospital owns the ISTG role; the role can be moved upon the ISTG becoming offline. When a domain controller becomes online the domain controller at Christ Hospital communicates through the standard replication process; this allows the Intra-Site replication to be current when objects are modified in Active Directory.

Best practice for the branch offices commits replicas of Active Directory information to the infrastructure. The centralize hub sites deliver constant stabilized connectivity over the WAN link to ensure downstream replication for the branch offices. This is considered in the design, each hub site has two one Gbps fiber connections with the WAN promoting object association across the domain. The new infrastructure will increase bandwidth thus facilitating effective connectivity . Chart 2.2 projects the new metrics moreover solidifying the allocation.

**2.2 Bandwidth Allocation**

****

Windows Server configurations are optimized due to the centralized administration of the domain. The single domain architecture allows less hardware and subtracts management of resource domains. Implementing policy-driven object management consents scalable control for system administrators. DFS deployment helps manage storage and sharing yet keeps the components federated. Security in the Windows network also derives from the server configurations. Integrated public key infrastructure (PKI) provides a hand shake with the certificate authority (CA) binding the trusts with the user objects and then indorses validation. Each hub site and the stand alone domain controller in the DMZ will act as a global catalog, every hub site and DMZ will have a DNS server acting as a primary, root hints, and stub for the network. Additional Primary and Secondary DNS servers will reside in the main data center as well as the disaster recovery site.

**Active Directory Lightweight Directory Services**

The Active Directory Lightweight Directory Services (AD LDS) LDAP directory solution will reside on all domain controllers. Philips iSite and EPIC will benefit from this solution concerning authentication. Replication traffic will be reduced by applying this strategy due to the parallel replication directory for the two heavily used applications. Each AD LDS instance will replicate between sites to ensure efficiency. Application data will be stored in AD LDS allowing the Active Directory Domain Services (AD DS) to handle other tasks consequently negating schema changes as well.

**Active Directory Federation Services (AD FS)**

Active Directory Federation Services (AD FS) will be executed within the DMZ. Users will have the single sign-on (SSO) functionality when accessing the resources regarding the branch offices. Once the user authenticates with the domain controller a token will commit the hand-shake promoting federated access to the application moreover the databases. This feature will also be initiated for remote access married to Citrix. Home users will toggle a URL to the Citrix portal; the users will have access to applications based on group membership. Upon access the SSO capabilities will be executed derived from authenticating with the domain controller in the DMZ.

**Active Directory Certificate Services (AD CS)**

Active Directory Certificate Services (AD CS) will issue the certificates to users in a few ways. Certificate Authorities (CAs) issue the certificate to the Active Directory objects and services in the domain. All Internet Information Services (IIS) access will utilize the IIS version 6 administrative tools to generate signed certificates separating internal web-based systems from the AD CS.

**References**

Melber, Derek. (2012).Crash Course in Active Directory Organizational Unit Design. Retrieved January 2015, from <http://www.windowsnetworking.com/articles-tutorials/windows-server-2008/Crash-Course-Active-Directory-Organizational-Unit-Design.html>

MSDN. (2001). Active Directory with Virtual Private Network and Demand Dial Deployments. Retrieved February 2015, from <https://msdn.microsoft.com/en-us/library/bb727069.aspx>

MSDN. (2014). Infrastructure Planning and Design. Retrieved January 2015, from <http://msdn.microsoft.com/en-us/library/cc196387.aspx>

Posey, Brien. (2013).Simplicity Is Key when Deploying Active Directory. Retrieved January 2015, from <http://redmondmag.com/Articles/2013/01/01/Active-Directory-Your-Way.aspx>

TechNet. (2010). Establishing an Active Director Deployment Strategy. Retrieved January 2015, from <http://technet.microsoft.com/en-us/library/cc755990(v=ws.10).aspx>