NetEng Technical Solutions

Liquid Sun Hydro

NETWORK AND SYSTEMS DOCUMENTATION

YASIN GUMUS/JACOB BUSH/DARREN SYLVAIN
NETENG TECHNICAL SOLUTIONS | https://github.com/netengtechsolutions

Table of Contents

Security and Design Rationale 1
Domain Migration 3
The Rationale for Active Directory Migration Method (Live Migration) 3
File Server Migration 4
Active Directory Structure 5
Sites and Services 5
Active Directory Organizational Unit Design 5
DHCP Server Failover 8
Physical Servers and Virtualization 9
The Rationale for Virtualization Solutions 10
Thin Client Solution 11
Server-side Infrastructure (RDS) 11
Client-side Solution 11
The Rationale for Remote Desktop Services and Windows Thin PC 13
Backup Solution 14
VMWare Veeam Backup and Replication Server 14
The Rationale for Veeam Backup and Replication Server 14
Server Disaster Recovery 14
Windows Server Update Services (WSUS) 16
G Suite 17
Acquiring G Suite 17
Configuring G Suite 17
Configuring Google Drive 17
Nagios XI Server Monitor 19
Install Nagios XI 19
Windows Server Monitor Agent 20
Linux Server Monitor Agent 21
SNMP Monitor Configuration 22
Nagios LS Log Server 23
Install Nagios LS 23
Windows Logging Agent 24
Linux logging Agent 24
Windows Deployment Service 25
Configuring WDS 25
Installing Image 26
Firewalls 26
Headquarters 27
Manufacturing 27
Warehouse 27
Network Devices - Management Plane 27
Passwords 27
Memory and CPU threshold notifications 28
Management Access 28
AAA 28
Logging 28
Network Devices - Control Plane 29
Network Time Protocol/NTP 29
Secure Routing Protocols 29
First-hop redundancy protocols/HSRP 29

Data Plane 30
Spanning Tree 30
Disable IP source routing..30
Disable ICMP redirects 30
Disable IP Directed broadcasts..30
VLAN Trunking Protocol/VTP 30
Firewall..31
Filter ICMP..31
Filter IP fragments 31
Filter IP options..31
Filter TTL values 31
Anti-spoofing..31
VoIP..32
Server..32
Phones 32
Wireless 32
Switch/Controller 32
Access Point..32
SSID Standards..32
Certificate Server 32
Security Concerns and Networking Interesting Discoveries..33
Scan Results..33
Security Concerns and Networking Interesting Discoveries..34
Appendix A: Network Diagrams 35
Headquarters - IPv4..35
Headquarters - IPv6 36
Headquarters – Routing..37
Headquarters - Spanning-Tree Protocol/STP 38
Manufacturing Plant - IPv4 39
Manufacturing Plant - IPv6 40
Manufacturing Plant - Routing 41
Warehouse – IPv4..42
Network Time Protocol/NTP 43
Wide-Area Network/WAN 44
Appendix B: Cutsheet 45
Appendix C: Quantitative Risk Analysis 50
Table C.I: Mitigated Results for Residual Risk 50
Table C.II/DIII Residual and Inherent Risk..51
Figure C.I: Inherent Risk, Residual Risk and Risk Tolerance..52
Figure C.II Defense in-depth Analysis..53
Appendix D: Support Documentation and Resources 54
D.I Python Bulk Network Configuration Script..54
E.II Demo of bulknet.py Script 63
E.III Find Non-Ascii Characters..65
E.IV Import Users to Active Directory..66
Pinger Script..73
Appendix E: Scan Results..74
E.I Discovery Scan External 74
E.II Discovery Scan Internal Headquarters 75
E.III Discover Scan Internal Manufacturing..81
E.IV Discovery Scan Internal Warehouse 85

Appendix F: AD & RDP 87
F.I Active Directory Migration 87
F.II File Server Migration 87
F.III Thin Clients - RDS 88
References 92

Security and Design Rationale

The network design and security decisions are based on vendor best-practices and quantitative risk analysis. The main concern for Dominion Greenhouses is the availability of systems and integrity of data. Integrity of data can be ensured with backups, so we calculated only the possible losses due to interruptions in availability and the lost cost of IT staff wages during recovery. To do this we used the frameworks outlined in *How To Measure Anything in Cybersecurity Risk* (Wiley 2016) and *Measuring and Managing Information Risk: A Fair Approach* (Elsevier 2015) which use very broad ranges for estimates of potential losses if a given event were to occur, and runs Monte-Carlo style simulations on the data, calculating losses thousands of times and extracting averages and a bell-curve of likelihood. The concept provided by these frameworks is that if we use values that were are 90% certain are correct, then we can make useful predictions of probabilities of loss for values that are difficult to quantify, such as damage to reputation and the cost of a breach by a specific vector of attack.

The estimates are by nature very large, for example, remote code execution with administrative privileges varies widely depending on the intentions of the actor; but, that large uncertainty still can be used to reduce the uncertainty related to costs of a given event. The upper limit is not infinite, and the bottom limit will not be 0, so even using these large ranges reduces uncertainty and can provide useful results. Douglas Hubbard and Richard Seiersen (Wiley 2016) propose, and what we have done in our simulations, is claim that there is a 90% likelihood that the losses of this compromise (remote admin code execution) range from between approximately $10000-$50000 in this situation. Then we can say that this will happen possibly once every 10 years, so there is a 10% chance of this happening this year. Domain admin credentials can be lost a multitude of ways, so if there is benefit in further disassembling how the credentials are gained and adding them to the framework individually then that is possible, but for the analysis of Dominion Greenhouses we determined that admin credentials will cause the same amount of loss no matter how the credentials were gained, so we did not disassemble this any further and reflected the multiple vectors as events with discrete probabilities but the same loss. An example of some of our values are included in Appendix C.I.

Because Dominion Greenhouses uses the cloud for email and collaboration, does not have any internet-facing services, and uses Cisco ASA internet-facing devices, we determined that the primary vectors of compromise are likely to be malware or social engineering-based. The probabilities are intended to reflect this assumption and the proposed mitigation measures are focused on user education, filtering of web and email traffic at the firewalls, and monitoring for early-detection of post exploitation activity and separation of privileges.

The probabilities and quantitative loss ranges are initially formed from a security baseline deemed appropriate by vendor documentation from Cisco and Microsoft and were customized to be appropriate for Dominion Greenhouses. Some examples of baseline features include authenticating control protocols such as OSPF routing, HSRP, VLAN trucking protocol, Network Time Protocol, implementing access-layer security, inter-branch IPSec VPNs, separation of privileges, and limiting user privileges.

Some of the quantitative effects of mitigations that we tested for feasibility are monthly lunch-and-learns/user education, server monitoring software, Intrusion Detection Systems/Prevention Systems and Web Security Appliances.
It is impossible to measure the cost of compromise within 90% certainty if there is no mechanism to alert IT staff that a compromise has occurred, so we include server monitoring software and some form of host-based IDS/IPS and antivirus software as part of the security

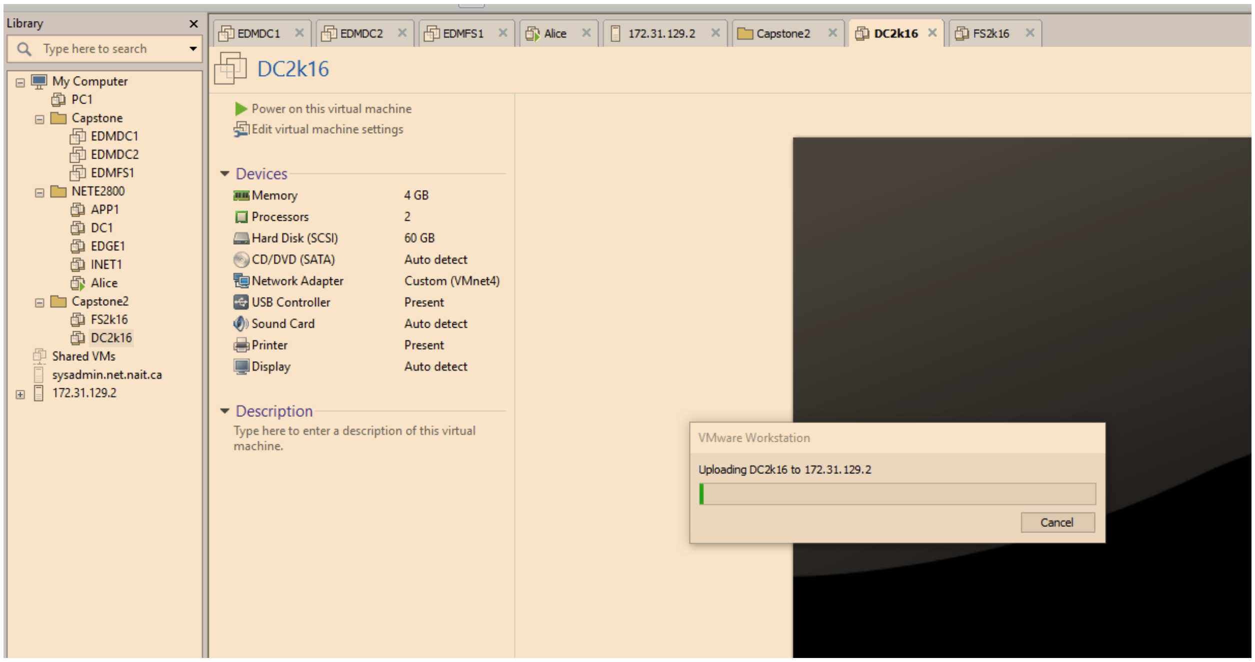
baseline. The only remediation that we propose beyond our baseline is quarterly lunch-and-learns. The graphical annual result lunch and learns is included in the appendix section table C I. Web-based security appliances to filter web traffic result in a very similar residual risk graph. We chose quarterly lunch-and-learns because the cost would be very similar and the results of user training is cumulative and compounding over time, rather than the recurring expense of a solution that steals its benefits back the moment payment stops. More information on the baseline we have created and specific security decisions are included in each configuration section.

The graph in the appendix section graph C I, is the result of the simulations we performed on the data. Concerns for mitigations were formed by the Incident Cost Reduction breakdown from *Measuring and Managing Information Risk: A Fair Approach* (Elsevier 2015), an image of the structure can be found in the appendix section C

Domain Migration

Out-dated server infrastructure in Liquid Sun Hydro Farms requires a thorough upgrading. Existing servers are running Windows 2003 and 2008 with the functional level of Windows 2008. There are two domain controllers (DC) running on Windows 2003 servers with domain and forest functional level of Windows 2008. A file server also runs Windows Server 2003 and will be upgraded to Windows Server 2016.

Active Directory Migration Plan and Implementation
Active Directory migration was implemented after deploying two new Windows 2016 servers. These two servers were then promoted as DCs in our existing domain and replicated from Windows 2003 DC (EDMDC1). After ensuring that Active Directory content was successfully replicated, the Flexible Single Master Operation (FSMO) roles were transferred to the new DC. This made the new Windows Server 2016 the primary DC as it now holds forest-wide and domain-wide master roles. After verifying the current FSMO roles holder and synchronization to the new DC structure in the domain, Windows 2003 DCs are demoted and disconnected from the domain. The last stage of the Active Directory migration was to raise the forest and domain functional level to Windows Server 2016. We performed the live migration on VMware Workstation as our network was not set up at that time. We changed the hardware compatibility to ESXi 6.5 which is the version of ESXi installed on our bare metal server. We then uploaded the new servers to the ESXi server.



Memory	4 GB
Processors	2
Hard Disk (SCSI)	60 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Custom (VMnet4)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

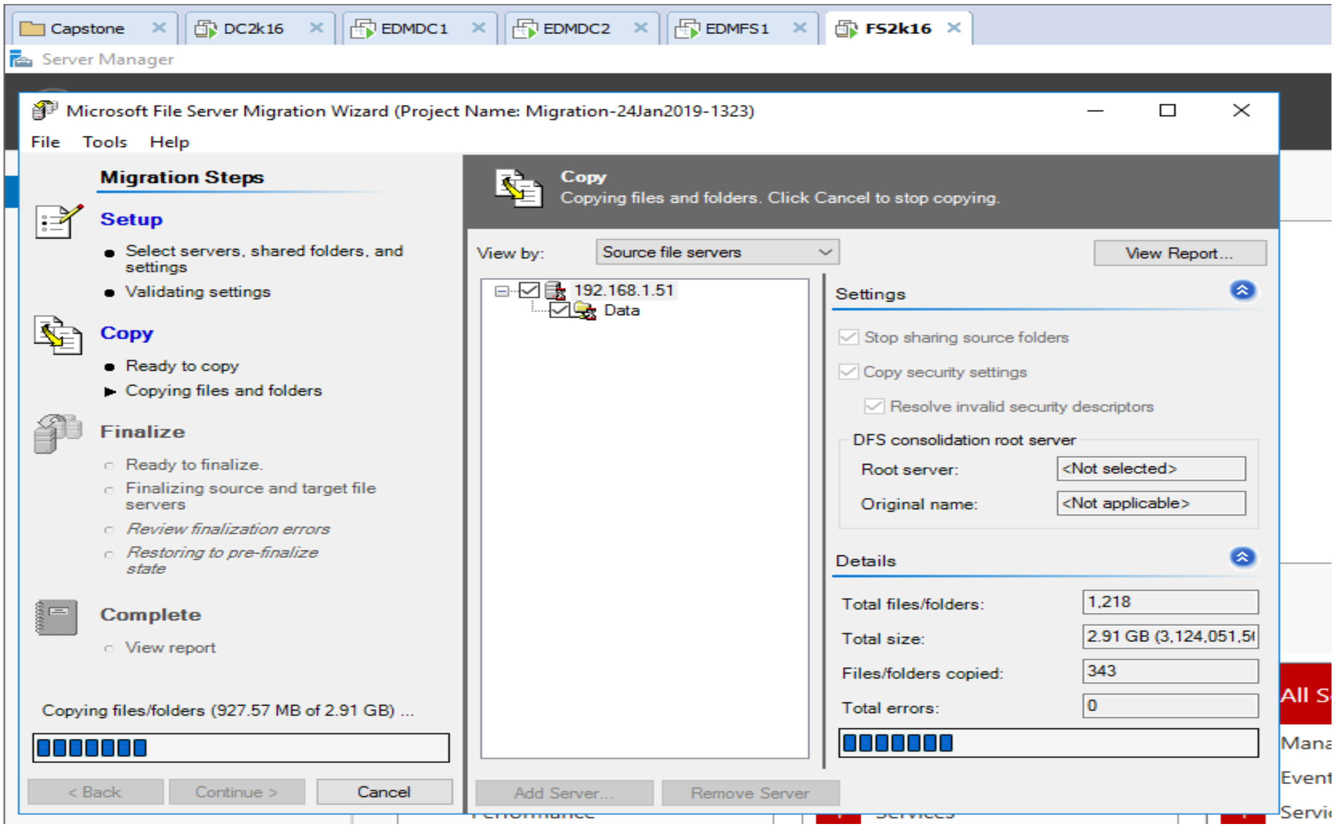
Uploading DC2k16 to 172.31.129.2

The Rationale for Active Directory Migration Method (Live Migration)

It is important that the migration process be performed without any data loss and downtime to the domain services. Therefore, we upgraded our DCs by replicating Active Directory content to the newly created DCs. This live migration method prevented any impairment in migration by providing the advantage of separating the migration and upgrading processes. Moreover, in case of a failure in the migration process we always had the Windows 2003 DCs available as a backup.

File Server Migration

File Server is also upgraded by adding a new Windows 2016 server with the File Server role to the domain. Then, the existing files on the server have been moved to the new FS with the use of Microsoft File Server Migration Toolkit. NET Framework Features were installed on the Windows 2003 server to install the Toolkit. To perform the migration with the Toolkit we needed to share the “data” folder on the network.



Microsoft File Server Migration Wizard (Project Name: Migration-24Jan2019-1323)

Copy
Copying files and folders. Click Cancel to stop copying.

Setup
- Select servers, shared folders, and settings
- Validating settings

Copy
- Ready to copy
- ▶ Copying files and folders

Finalize
- ○ Ready to finalize.
- ○ Finalizing source and target file servers
- ○ *Review finalization errors*
- ○ *Restoring to pre-finalize state*

Complete
- ○ View report

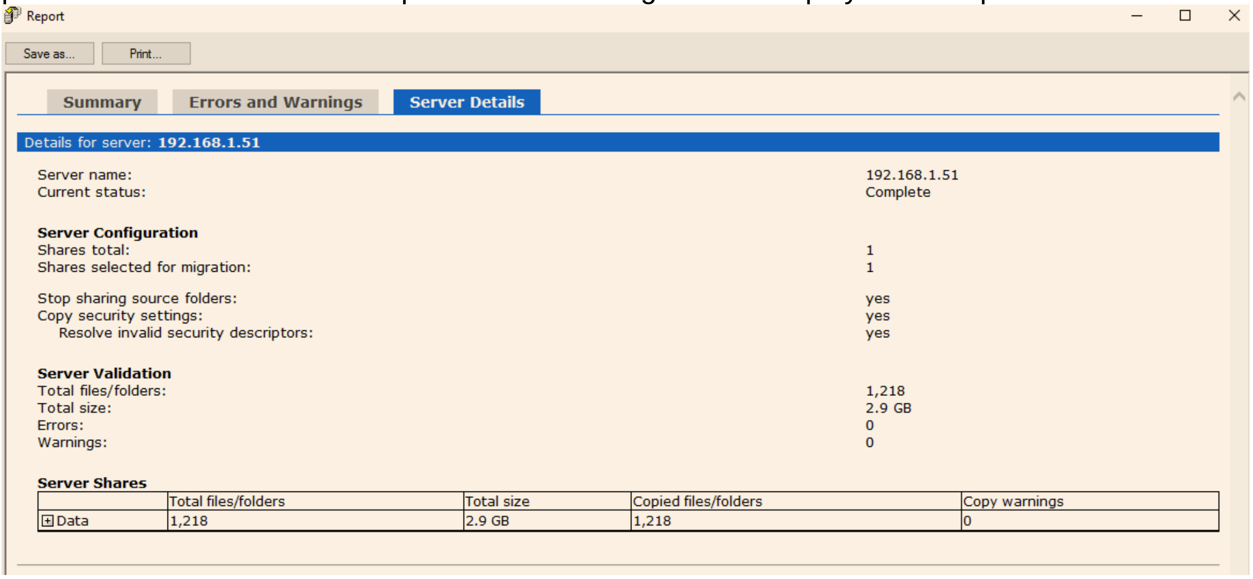
Copying files/folders (927.57 MB of 2.91 GB) ...

☑ Stop sharing source folders
☑ Copy security settings
☑ Resolve invalid security descriptors

DFS consolidation root server
Root server: <Not selected>
Original name: <Not applicable>

Total files/folders: 1,218
Total size: 2.91 GB (3,124,051,5(
Files/folders copied: 343
Total errors: 0

Implementing file server migration with the Microsoft Migration Toolkit allowed us to keep NTFS permissions of the files. The report of our files’ migration is displayed in the picture below.



Details for server: **192.168.1.51**

Server name:	192.168.1.51
Current status:	Complete
Server Configuration	
Shares total:	1
Shares selected for migration:	1
Stop sharing source folders:	yes
Copy security settings:	yes
Resolve invalid security descriptors:	yes
Server Validation	
Total files/folders:	1,218
Total size:	2.9 GB
Errors:	0
Warnings:	0

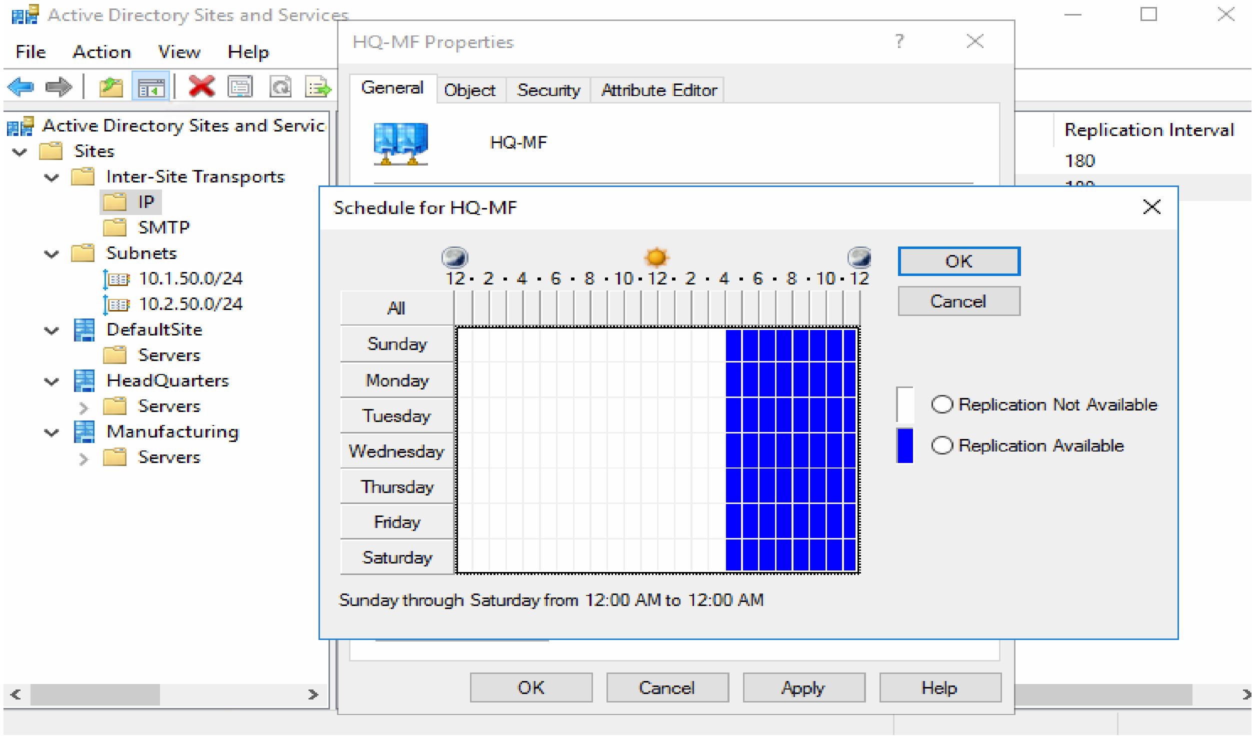
Server Shares

	Total files/folders	Total size	Copied files/folders	Copy warnings
⊞ Data	1,218	2.9 GB	1,218	0

Active Directory Structure

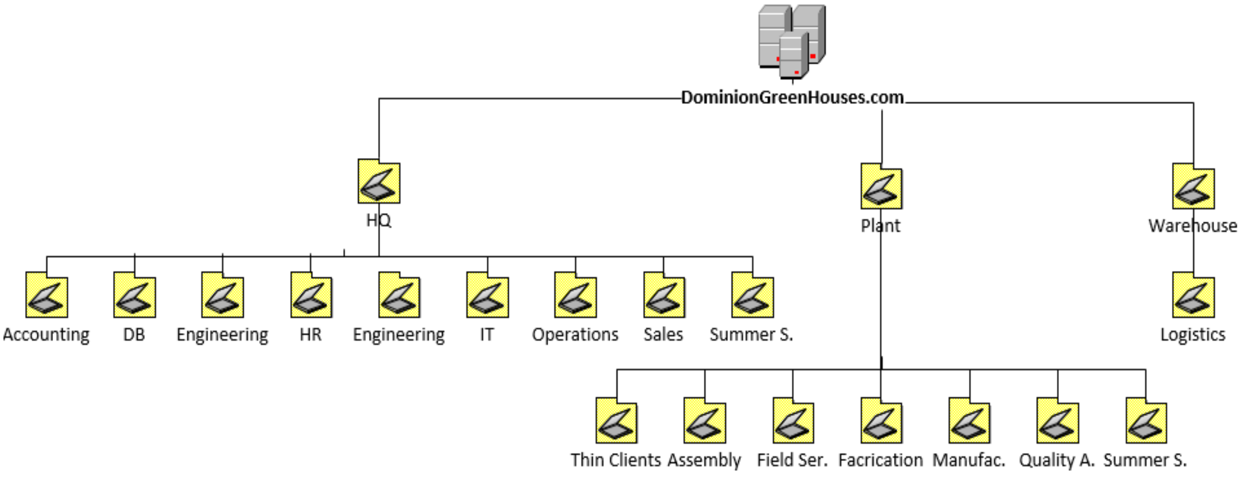
Sites and Services

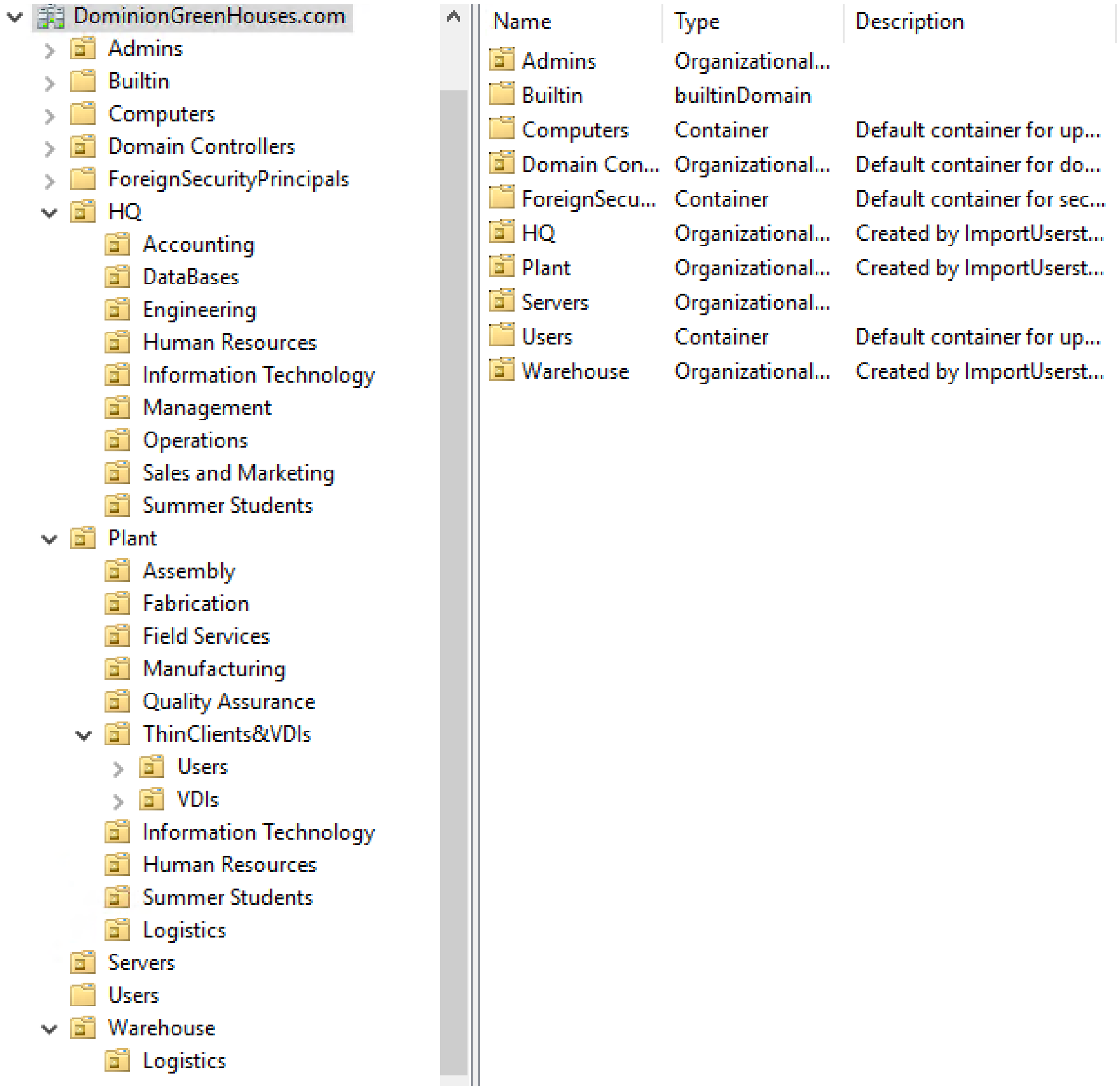
Active Directory Sites and Services are configured for Headquarters and Manufacturing Plant sites and subnets. Replication between HQ and MP is scheduled for non-business hours.



Sunday through Saturday from 12:00 AM to 12:00 AM

Active Directory Organizational Unit Design



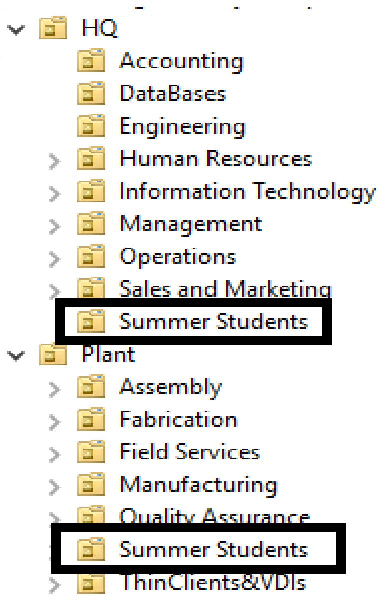


- DominionGreenHouses.com
  - Admins
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - HQ
    - Accounting
    - DataBases
    - Engineering
    - Human Resources
    - Information Technology
    - Management
    - Operations
    - Sales and Marketing
    - Summer Students
  - Plant
    - Assembly
    - Fabrication
    - Field Services
    - Manufacturing
    - Quality Assurance
    - ThinClients&VDIs
      - Users
      - VDIs
    - Information Technology
    - Human Resources
    - Summer Students
    - Logistics
  - Servers
  - Users
  - Warehouse
    - Logistics

Name	Type	Description
Admins	Organizational...	
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
HQ	Organizational...	Created by ImportUserst...
Plant	Organizational...	Created by ImportUserst...
Servers	Organizational...	
Users	Container	Default container for up...
Warehouse	Organizational...	Created by ImportUserst...

Active Directory structure plays very important role when it comes to configuring Group Policy Objects for specific users, groups, departments, and sites in the enterprise. We divided our domain with Organizational Units (OU) for each site. Then, subdivided site OUs into departments.

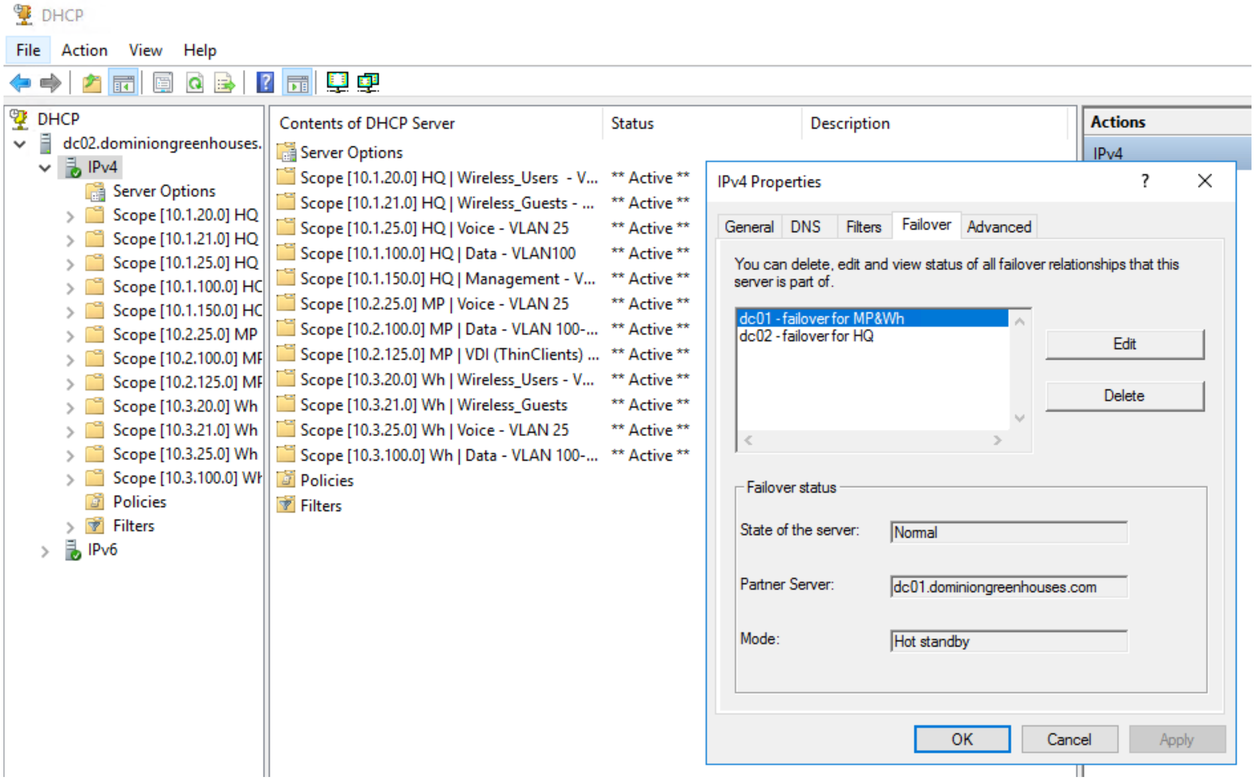
This structure we applied provides us more flexibility and differentiation when we are granting/restricting access, assigning printers, sharing files resources for our users, groups, departments, and sites. Especially, considering that one single user can be categorized into different groups (as specified in the “Employee Names” CSV file), this department structure approach is more ideal than having only site OUs. Organizational Unit structure is also important for file shares on the network for specific departments in different sites.



Although only security groups could have been used to apply GPOs or share files, there are groups that take place in different sites such as Summer Students, Human Resources, and Information Technology.
This means that if we only formed site OUs and were to apply a GPO to Summer Students in the Engineering department, we could not isolate Summer Students in Manufacturing from being included in this GPO because they are all members of the security group. Therefore, our department OUs ease our Active Directory Users and Groups management and provides a more functional structure for GPO implementations. For example, we might wish to apply a GPO and share a folder for Human Resources (HR) users in HQ site. For this reason, we created sub-OUs for each department in each site.

DHCP Server Failover

DHCP Server Service installed on both Domain Controllers to implement failover. The configuration provides each site to get its DHCP assignment from the other site in case of a failure on the site DC. Each failover server is configured as either “Active” or “Hot standby”.



Contents of DHCP Server	Status	Description
Server Options		
Scope [10.1.20.0] HQ | Wireless_Users - V...	** Active **	
Scope [10.1.21.0] HQ | Wireless_Guests - ...	** Active **	
Scope [10.1.25.0] HQ | Voice - VLAN 25	** Active **	
Scope [10.1.100.0] HQ | Data - VLAN100	** Active **	
Scope [10.1.150.0] HQ | Management - V...	** Active **	
Scope [10.2.25.0] MP | Voice - VLAN 25	** Active **	
Scope [10.2.100.0] MP | Data - VLAN 100-...	** Active **	
Scope [10.2.125.0] MP | VDI (ThinClients) ...	** Active **	
Scope [10.3.20.0] Wh | Wireless_Users - V...	** Active **	
Scope [10.3.21.0] Wh | Wireless_Guests	** Active **	
Scope [10.3.25.0] Wh | Voice - VLAN 25	** Active **	
Scope [10.3.100.0] Wh | Data - VLAN 100-...	** Active **	
Policies		
Filters		

IPv4 Properties

General | DNS | Filters | Failover | Advanced

You can delete, edit and view status of all failover relationships that this server is part of.

dc01 - failover for MP&Wh
dc02 - failover for HQ

Edit
Delete

Failover status

State of the server: Normal

Partner Server: dc01.dominiongreenhouses.com

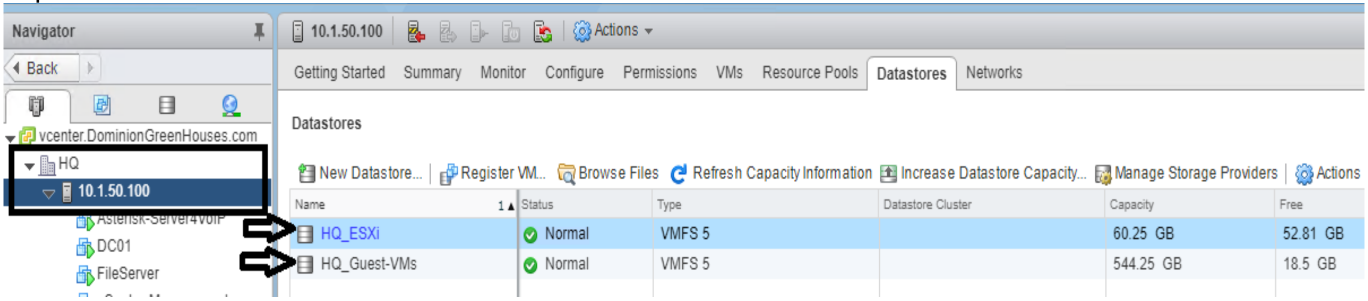
Mode: Hot standby

OK Cancel Apply

The failover configuration above reflects that DC01 which resides in HQ will failover for the subnet scopes in the MP, while DC02 which resides in MP will failover for subnets in the HQ site.To allow DHCP discover messages through broadcast domains routers are configured as relay-agents to relay DHCP messages to both DHCP servers.

Physical Servers and Virtualization

Before we install a virtualization operating system, we configured disk array configuration on the two physical servers we were provided with. We configured the two disks with RAID 1 for virtualization OS, and RAID 5 with the remaining disks for guest VMs. This also enabled to separate OS and Guest VM files.



Datastores

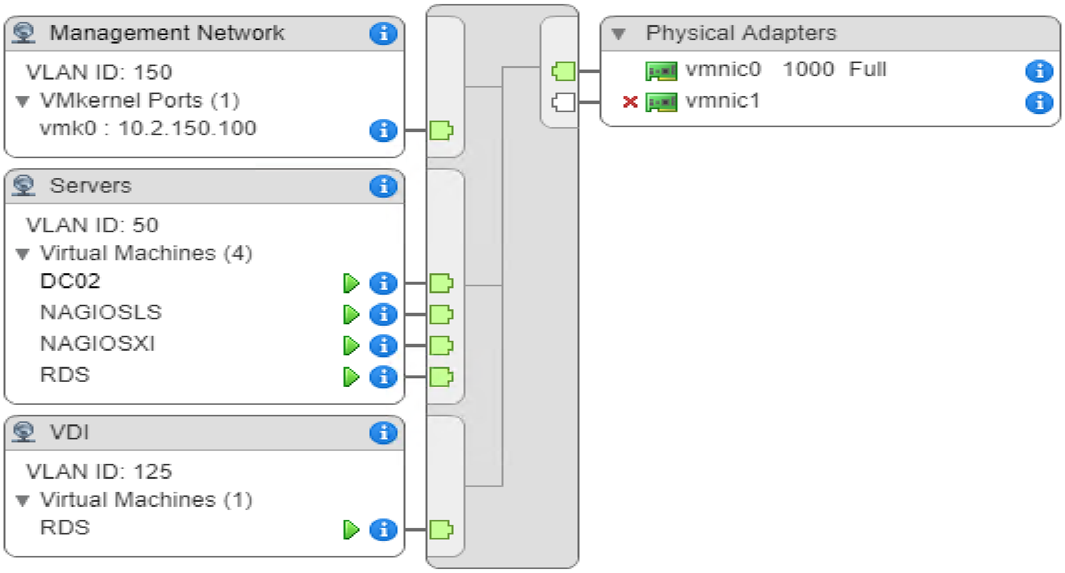
Name	Status	Type	Datastore Cluster	Capacity	Free
HQ_ESXi	Normal	VMFS 5		60.25 GB	52.81 GB
HQ_Guest-VMs	Normal	VMFS 5		544.25 GB	18.5 GB

As a virtualization operating system, we installed type 1 hypervisor VMWare ESXi which will provide both web interface management for each VM, and centralized server management with vSphere vCenter.

Both physical servers are connected and managed via vCenter. The virtual network is configured on vCenter to establish a functional and manageable connectivity between the virtual and the physical network. The server VMs running on ESXi are using VLAN 50 and being tagged in the vCenter with the use of port groups. On the other hand, physical ESXi management adapter is configured to use VLAN 150 which is the management VLAN.

We also configured the following features in vCenter to ease manageability:

- Active Directory Integration and Single sign-on.
- Run-as accounts for each team member (Domain Administrators)
- Library content with operating-systems ISO files.
- VM templates for VM deployment.



Management Network
VLAN ID: 150
VMkernel Ports (1)
vmk0 : 10.2.150.100

Servers
VLAN ID: 50
Virtual Machines (4)
DC02
NAGIOSLS
NAGIOSXI
RDS

VDI
VLAN ID: 125
Virtual Machines (1)
RDS

Physical Adapters
vmnic0 1000 Full
vmnic1

The Rationale for Virtualization Solutions

The goal of using RAID 1 configuration for virtualization OS is that we secure the OS by mirroring the whole disk to another. Since the OS itself does not cover a huge space this disk array configuration was the most ideal choice to ensure our OS can be recovered by using the mirrored disk. For the RAID 5 configuration of the server VMs' disks, other than providing continues recovery if a drive fails, we also aimed for high performance by fast data reading. The choice of type 1 VMWare ESXi virtualization OS makes a variety of different features available for virtualization services:

- Advanced capacity with up to 64 logical processing cores, 256 virtual CPUs for most resource-intensive servers/applications.
- Allows for network traffic shaping
    - Ability to control bust, peak, and average bandwidth.
- Simple backup and restore of VMs.
- Centralized management of the whole server infrastructure. (vSphere)
- Detailed virtual network configurations such as NIC teaming, port groups, VM kernels.

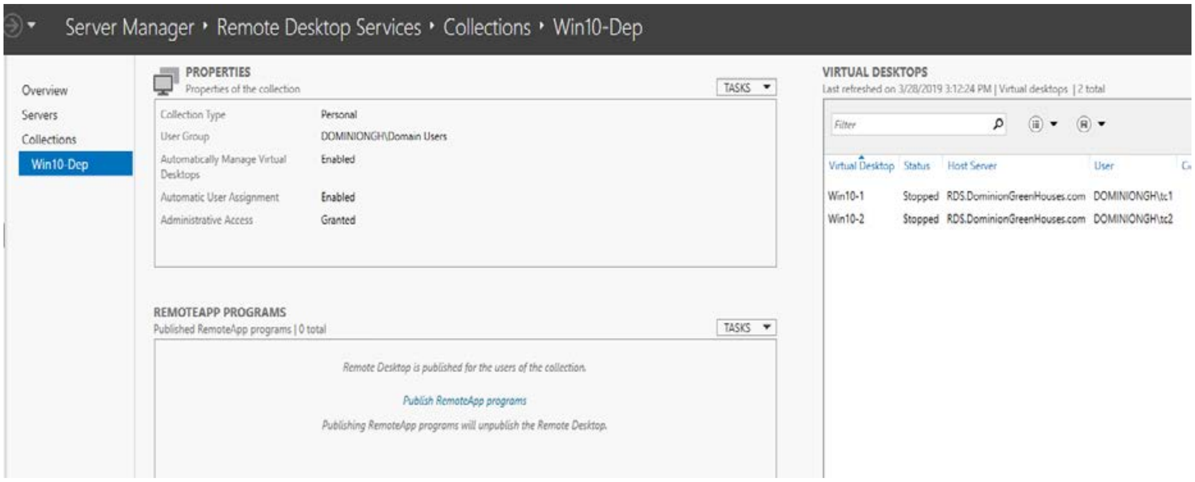
Thin Client Solution

A thin client solution was required to be implemented at the Manufacturing Plan. We approached this implementation with two main components; client-side solution and server-side infrastructure.

Server-side Infrastructure (RDS)

This is where all the virtual desktop environments and resources reside for each thin client. RDS server is an ideal way to create virtual desktop pools, provide remote access authentication through RD gateway, and control applications running on the virtual desktops. It uses Hyper –V as a virtualization platform; in which a client operating system template is nested and populated within a collection. We set up a virtual network to establish a connection between the nested virtual network and the physical network. This was achieved with virtual network adapters and virtual switches on Hyper -V.

After the virtual network was created and a Windows 10 sysprepped sample was deployed to Hyper -V as a template VM, we deployed our virtual desktop infrastructure by creating a persistent VDI collection. The image below is the overview of the Windows 10 virtual desktop infrastructure collection we created with the Windows 10 template. The VDIs are assigned for specific thin clients users which makes them a persistent VDI to provide users a more specialized desktop environment.


Server Manager ‣ Remote Desktop Services ‣ Collections ‣ Win10-Dep
Overview
Servers
Collections
Win10-Dep
TASKS
TASKS
Filter

PROPERTIES
Properties of the collection

Collection Type	Personal
User Group	DOMINIONGH\Domain Users
Automatically Manage Virtual Desktops	Enabled
Automatic User Assignment	Enabled
Administrative Access	Granted

REMOTEAPP PROGRAMS
Published RemoteApp programs | 0 total

Remote Desktop is published for the users of the collection.

Publish RemoteApp programs

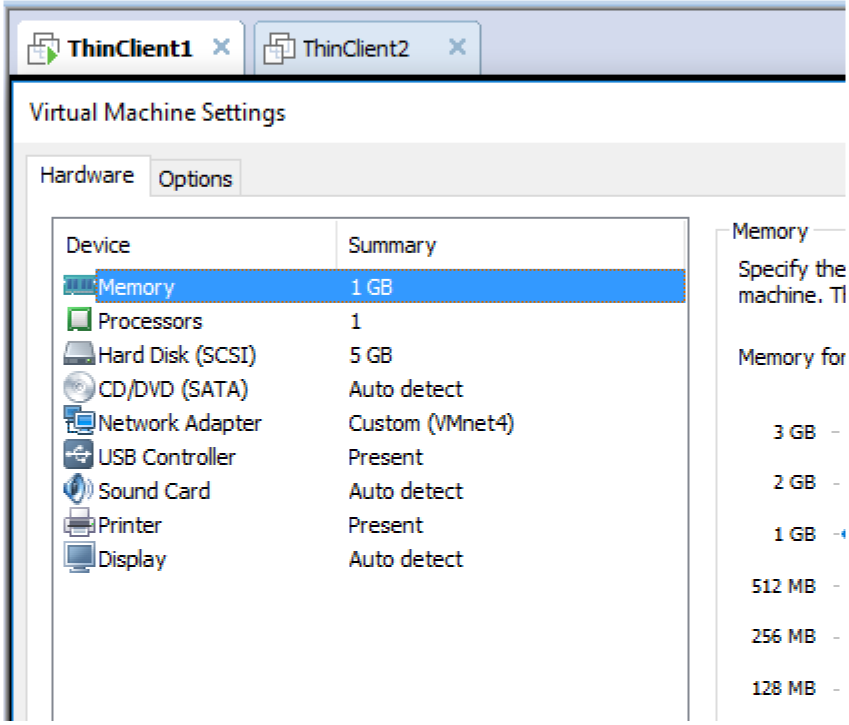
Publishing RemoteApp programs will unpublish the Remote Desktop.

VIRTUAL DESKTOPS
Last refreshed on 3/28/2019 3:12:24 PM | Virtual desktops | 2 total

Virtual Desktop	Status	Host Server	User	C
Win10-1	Stopped	RDS.DominionGreenHouses.com	DOMINIONGH\tc1	
Win10-2	Stopped	RDS.DominionGreenHouses.com	DOMINIONGH\tc2	

Client-side Solution

Since the logic behind the thin client solution is to run all resources on the server-side, the client-side of the infrastructure hardware is reasonably light weight. The main component of the client-side solution is the operating system that provides a remote connection to VDI. The OS we used for this purpose is Microsoft Windows Thin PC - a light-weight version of Windows 7.



Virtual Machine Settings

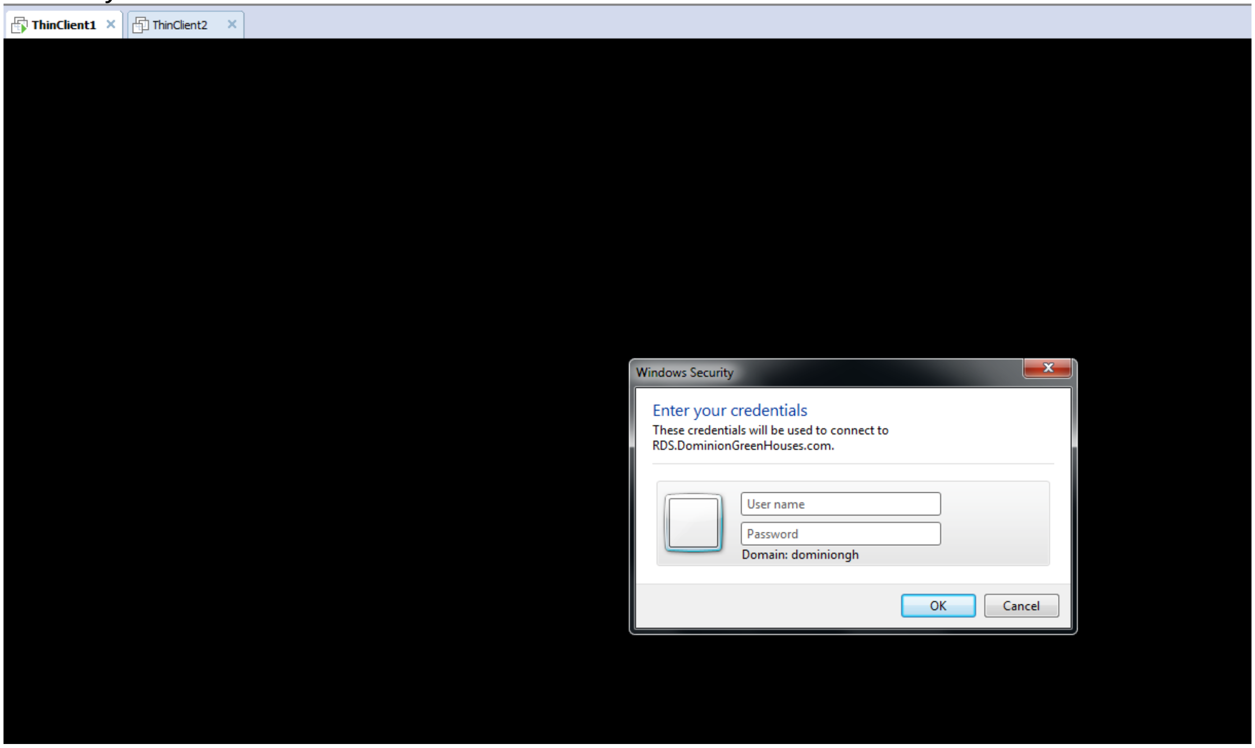
Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	5 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Custom (VMnet4)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Memory

Specify the
machine. Tl

Memory for

We configured Windows Thin PC to RDP at login without displaying a local user login screen or the local desktop with the use of a set of scripts (available in the appendix). Thus, as soon as the client turns on the thin client machine he or she is asked to enter domain credentials by RD Gateway.



Enter your credentials

These credentials will be used to connect to RDS.DominionGreenHouses.com.

User name

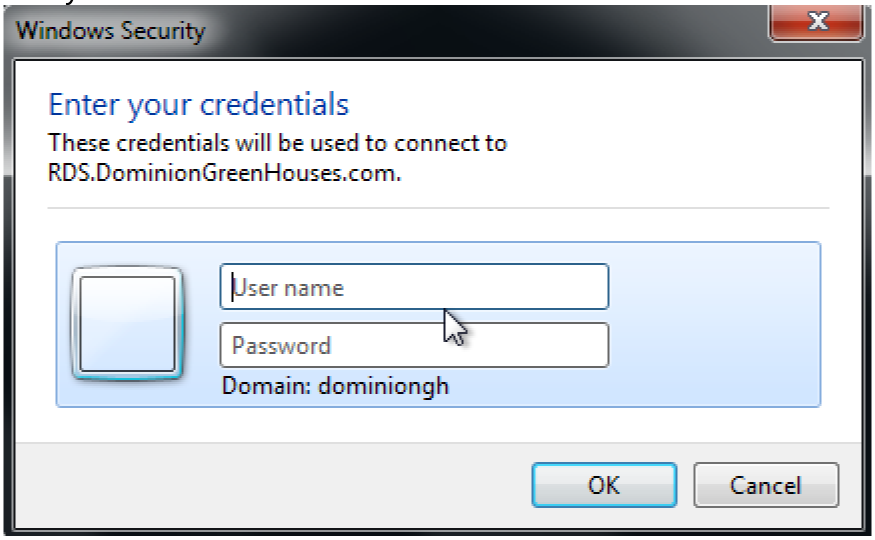
Password

Domain: dominiongh

The Rationale for Remote Desktop Services and Windows Thin PC

RDS is an ideal option for thin clients with its RD Web Access, RD Gateway, RDSH, and RDSM features. These features allow for a secure and functional thin client solution. As a Microsoft Windows service, it collaborates with Active Directory to authenticate thin client users. RD Gateway feature also used to secure remote access to virtual desktop infrastructure. As RD Gateway provides this secure authentication and authorization, it can also be used for private connection over the internet.

Windows Thin PC provides a locked down version of Windows 7 and requires only 5 GB of disk space to be installed. This makes it very efficient to use it as a client-side thin client OS. Windows Thin PC also allowed us to configure it with some scripts so that it can directly RDP into user's VDI at the OS boot-up and prompt for RD Gateway credentials which are integrated with Active Directory credentials.



Windows Security

Enter your credentials

These credentials will be used to connect to RDS.DominionGreenHouses.com.

Domain: dominiongh

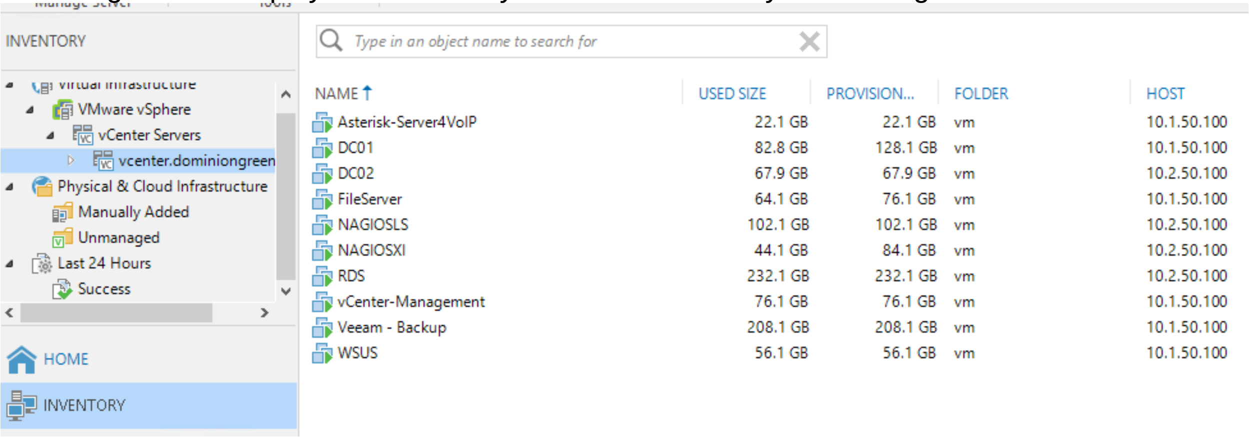
Backup Solution

Natural disasters, hardware failures, cyber-crimes, and user related errors. These are all unpredictable disasters that could strike an enterprise and cause losses on critical business data. For this reason, Dominion Green Houses needs a backup solution to keep its data safe and recoverable when such disasters occur.

VMWare Veeam Backup and Replication Server

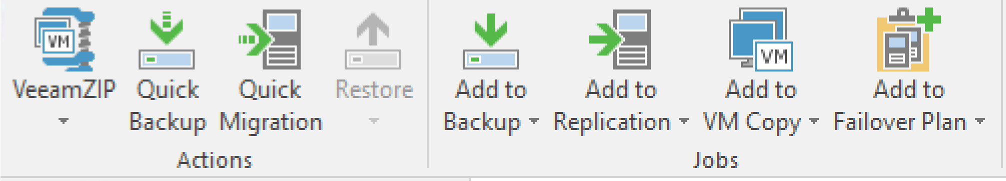
Our product for the backup solution is Veeam Backup and Replication Server which is a VMware product. It is installed on a dedicated Windows Server, and is responsible for all the backup, restore and replication orchestration. Veeam has the ability to perform image-based and storage snapshot backups. We also integrated vCenter with Veeam to create a more practical backup core management infrastructure.

The image below displays the inventory content retrieved by connecting Veeam with vCenter.



NAME ↑	USED SIZE	PROVISION...	FOLDER	HOST
Asterisk-Server4VoIP	22.1 GB	22.1 GB	vm	10.1.50.100
DC01	82.8 GB	128.1 GB	vm	10.1.50.100
DC02	67.9 GB	67.9 GB	vm	10.2.50.100
FileServer	64.1 GB	76.1 GB	vm	10.1.50.100
NAGIOSLS	102.1 GB	102.1 GB	vm	10.2.50.100
NAGIOSXI	44.1 GB	84.1 GB	vm	10.2.50.100
RDS	232.1 GB	232.1 GB	vm	10.2.50.100
vCenter-Management	76.1 GB	76.1 GB	vm	10.1.50.100
Veeam - Backup	208.1 GB	208.1 GB	vm	10.1.50.100
WSUS	56.1 GB	56.1 GB	vm	10.1.50.100

Any virtual machine contained in the inventory is applicable for variety of different processes. Virtual machines can be backed up, replicated, optimized, migrated, and restored.

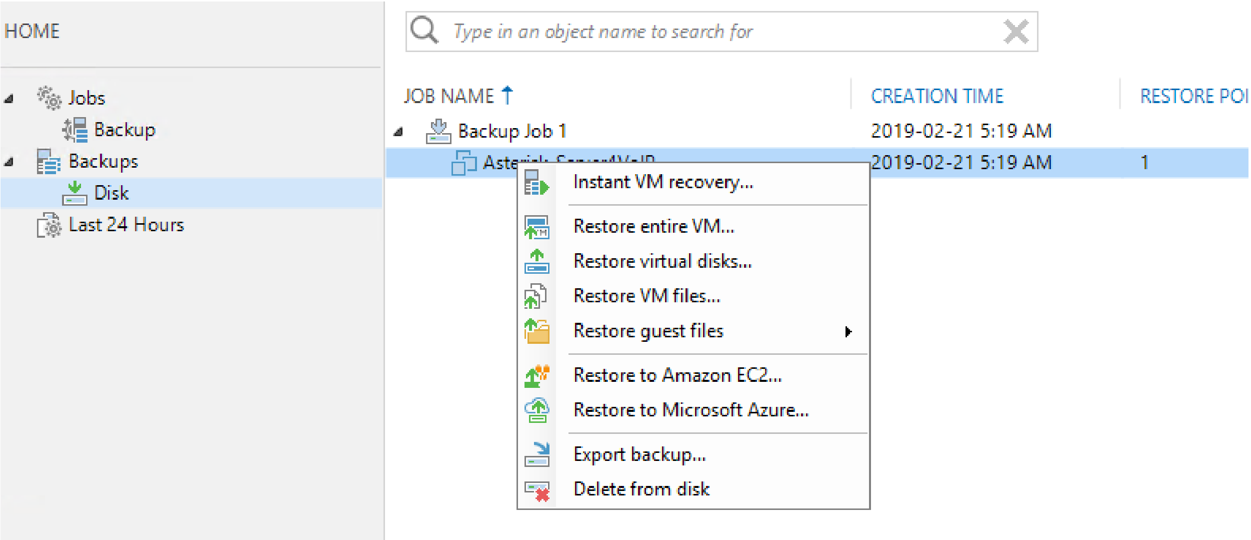


The Rationale for Veeam Backup and Replication Server

Veeam Backup Server meets our backup and restore needs with its features described above. The simplicity with its backup and restore implementations also appeals to our enterprises considering the low number in our IT team. Another exceptional feature of Veeam that suits our needs is that it provides different paths when it comes to recovering from a disaster in the server infrastructure.

Server Disaster Recovery

This section describes our recovery plan when the unthinkable occurs to the server infrastructure. Our Veeam Backup Server runs on-site and is used to back-up all of our infrastructure VMs. It is also used for file-level backup on our File Server. The restore options listed below will help guide us with our recovery implementation.



JOB NAME	CREATION TIME	RESTORE POI
Backup Job 1	2019-02-21 5:19 AM	
Aste	2019-02-21 5:19 AM	1

1. DCs
   a. Deploy a new server replica from a running DC on the domain.
   b. Restore from the application-aware backup.
   c. Recover from off-site backup.

2. File Server
   a. File-level recovery: restoring of files that has been damaged, lost, or corrupted.
   b. Restore the whole VM from the Veeam Backup Server.
   c. Recover from the off-site backup.

3. VDIs
   a. Create a new virtual desktop in the existing collection.
   b. Deploy a new collection.
   c. Restore VM from Veeam.

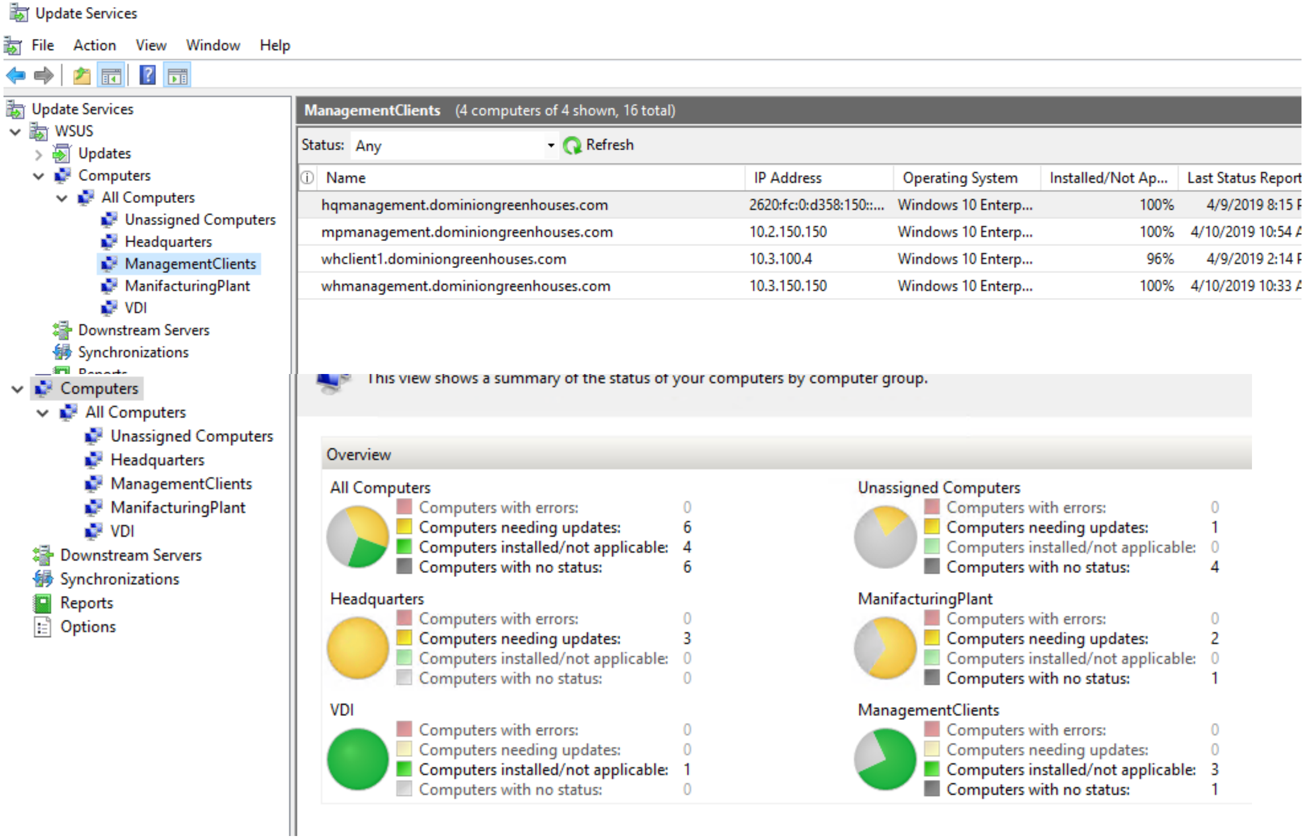
4. WSUS Server
   a. Restore VM from Veeam.

5. Print Server
   a. Restore VM from Veeam.

While DCs, File Server and RDS Server restore options can vary according to disaster's severity, the VDIs, WSUS, and Print Server are lightweight servers that can easily be restored with their Veeam backup.

Windows Server Update Services (WSUS)

Enterprise networks require to be updated with a neat update distribution. We deployed a WSUS server on a dedicated server in Headquarters to manage the distribution of updates. Following the "Windows Update Services" role installation on the dedicated server, we also needed to configure a GPO for computers in the domain to receive its updates from the WSUS server. Computers are categorized into groups and synchronized with WSUS server.



ManagementClients (4 computers of 4 shown, 16 total)

Status: Any

Name	IP Address	Operating System	Installed/Not Ap...	Last Status Report
hqmanagement.dominiongreenhouses.com	2620:fc:0:d358:150::...	Windows 10 Enterp...	100%	4/9/2019 8:15 P
mpmanagement.dominiongreenhouses.com	10.2.150.150	Windows 10 Enterp...	100%	4/10/2019 10:54 A
whclient1.dominiongreenhouses.com	10.3.100.4	Windows 10 Enterp...	96%	4/9/2019 2:14 P
whmanagement.dominiongreenhouses.com	10.3.150.150	Windows 10 Enterp...	100%	4/10/2019 10:33 A

This view shows a summary of the status of your computers by computer group.

Overview

All Computers

🟥 Computers with errors:	0
🟨 Computers needing updates:	6
🟩 Computers installed/not applicable:	4
⬛ Computers with no status:	6

Unassigned Computers

🟥 Computers with errors:	0
🟨 Computers needing updates:	1
🟩 Computers installed/not applicable:	0
⬛ Computers with no status:	4

Headquarters

🟥 Computers with errors:	0
🟨 Computers needing updates:	3
🟩 Computers installed/not applicable:	0
⬛ Computers with no status:	0

ManifacturingPlant

🟥 Computers with errors:	0
🟨 Computers needing updates:	2
🟩 Computers installed/not applicable:	0
⬛ Computers with no status:	1

VDI

🟥 Computers with errors:	0
🟨 Computers needing updates:	0
🟩 Computers installed/not applicable:	1
⬛ Computers with no status:	0

ManagementClients

🟥 Computers with errors:	0
🟨 Computers needing updates:	0
🟩 Computers installed/not applicable:	3
⬛ Computers with no status:	1

G Suite

G Suite is Google's application as a service offering. Allowing customers to use Google's services with their domain name. Included in G Suite is: Gmail, Google Calendar, Google Drive, Google Docs, Google Slides, Google Sheets, and Google Admin to administrate the ladder. Gmail is Google's email application, allowing a customer to use their domain name as the email address. Google Docs, Slides, Sheets are Google's word processing applications designed around live editing and collaboration. These are comparable and mostly backwards compatible with the Microsoft’s word processors. Google drive is Google's file system, that will allow users and administrators to organizes and set permissions on documents in the drive. An administrator can also use Google Admin to create, delete and manage user accounts. Google provides extensive logging with the business edition of G suite. The enterprises edition of G suite will provide additional security features to prevent sensitive data from being leaked. Google also offers a SLA of 99.9% for all G Suite products. G Suite also ensures its customers that everything is backed up with a disaster recovery plan.

Acquiring G Suite

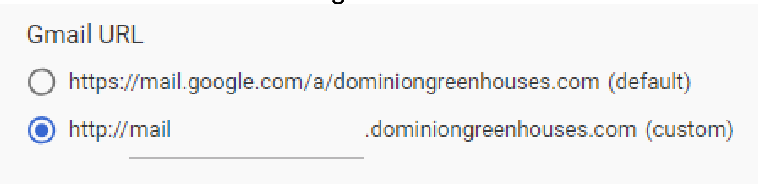
To acquire G Suite, first an administrator needs to create a Google account. Next purchase or transfer the domain you wish to configure with G Suite to Google domains. In this document, our customer’s domain name is dominiongreenhouses.com.

- In Google domains under the ‘email’ tab select get custom email address and select G Suite.

- Choose which level of G suite you require and how many users you wish be active. Will be charged according to how many “active users” you have on G Suite.
- Your first G Suite account will be an administrative account this account can access the G Suite admin console.
- To login to the admin console go to admin.google.com.

Configuring G Suite

- Next in the admin console, go to the Company profile section to ‘personalization’. Upload a logo of the customers company.
- Next go to ‘legal and compliance’ tab. Have a lawyer look at the terms and accept.
- Next go to ‘custom urls’ tab. Edit the Gmail, calendar, Drive, sites, and groups URLs. Such as mail. Such as mail.dominiongreenhouses.com for Gmail.



Gmail URL

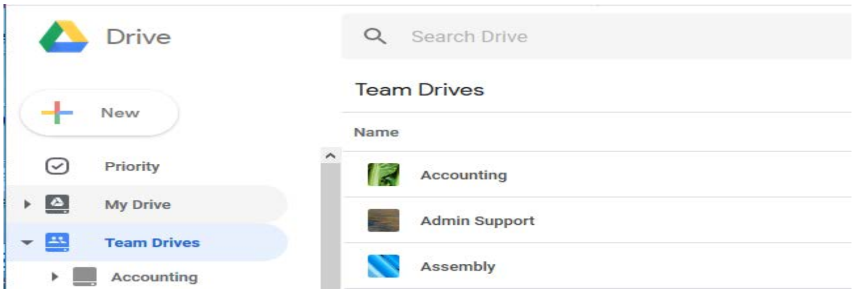
○ https://mail.google.com/a/dominiongreenhouses.com (default)

● http://mail .dominiongreenhouses.com (custom)

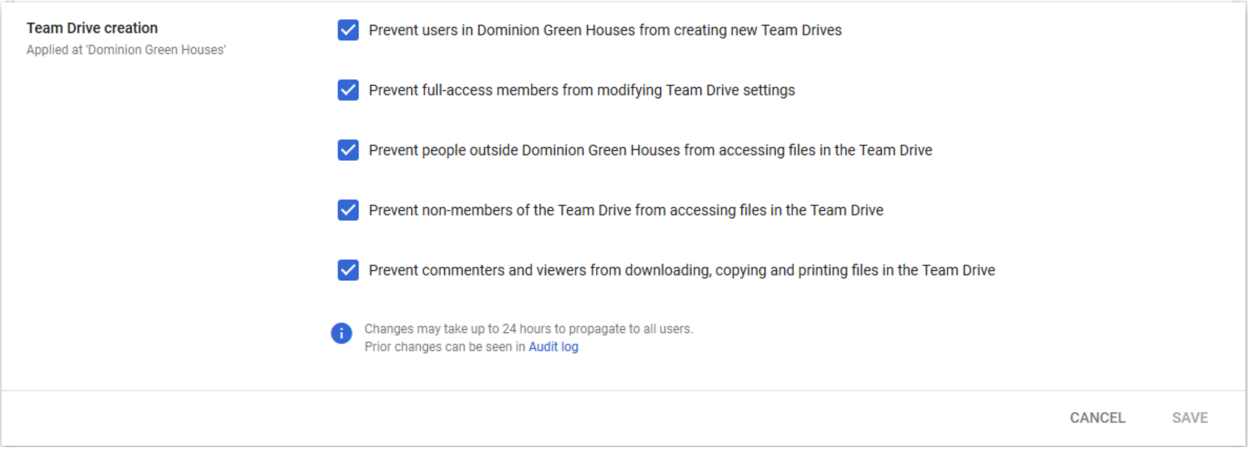
- Next we need to import users in the Google admin console select the users tab. In the users tab hover over the yellow plus button and select bulk upload users. Download the CSV template as it is used to facilitate the bulk upload. Note: Be sure to have the appropriate number of active users available for the upload.

Configuring Google Drive

Google Drive is Google's file system. To configure G Suite we will create Team Drives and configure permissions using groups. Groups are also mail enabled, and will allow you to send emails to an entire department.



- In the Admin Console go to the Groups Page.
- Select the blue create groups text to open the create group page.
- Enter a name and an email address for the group.
- Next you will be sent to the permissions page for the group that was just created. Select the Restricted group permissions template. This security template will prevent normal member accounts from adding users and other administrative privileges.
- Next we need to create Team Drives for each department. In Google drive right click on team drive, and Select the rainbow colored 'new' button. Enter a name for the department. Once the team drive has been created right click on the new drive, and select add members. Add the group we created to the team drive with the contributor permissions. This will allow members who are part of the team drive access to all the files in the team drive, without allowing them to delete files they did not create.
- Lastly we need to set permissions in Google drive so not to allow a user to create a team drive. In the admin console go to the Apps tab. Select G Suite. Select Drives and Docs. Once there; click on sharing settings. Under the Dominion Green Houses OU (The root OU) Select Team Drive creation. Select all the boxes and click save. Now users and even the administrator will not be able to create a new team drive.



Team Drive creation
Applied at 'Dominion Green Houses'

☑ Prevent users in Dominion Green Houses from creating new Team Drives

☑ Prevent full-access members from modifying Team Drive settings

☑ Prevent people outside Dominion Green Houses from accessing files in the Team Drive

☑ Prevent non-members of the Team Drive from accessing files in the Team Drive

☑ Prevent commenters and viewers from downloading, copying and printing files in the Team Drive

Changes may take up to 24 hours to propagate to all users.
Prior changes can be seen in Audit log

Nagios XI Server Monitor

Originally I was to configure Solarwinds server monitor for the DominionGreenHouses Domain; However, I ran into compute resource problems, as Solarwinds attempted to eat all the CPU resources on an ESXi server. Therefore, our team decided to switch to using Nagios XI. Nagios XI is a Linux based server monitor. This will allow an administrator to know in real time the status of the servers and network devices in an organization. This way an administrator can more easily anticipate a server or network problem, or react in real time when a problem occurred. Nagios XI only uses 2GB of RAM and provides a versatile and usable web console.

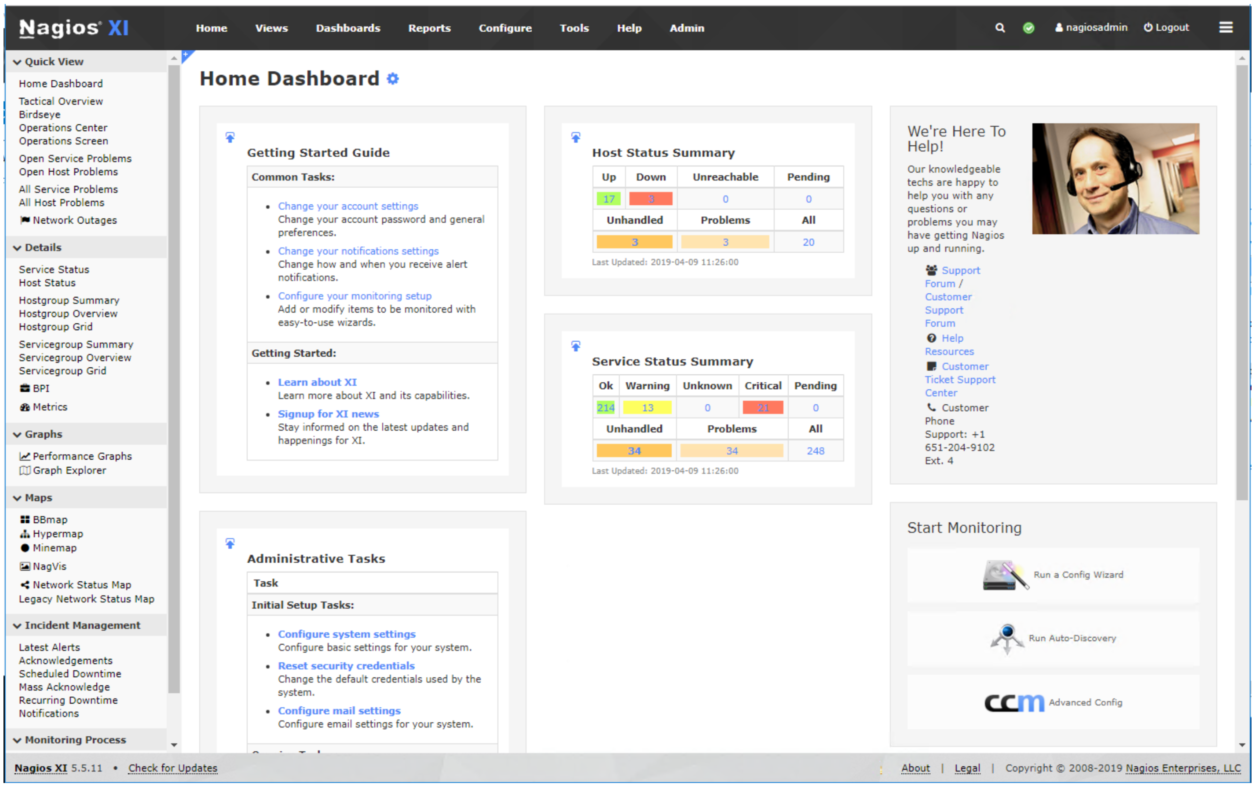
Install Nagios XI

Nagios provides a trial VM as an .ova template for ESXi. We can deploy this template into ESXi using vSphere.

- Login to the vSphere web client with an administrative account.
- In the navigator window, right click on the vSphere server. Select deploy OVF template…
- The deploy OVF template wizard will start. Select the nagiosxi-5.5.11-64.ova file and deploy it into the appropriate ESXi server.
- Rename the Nagios XI server in vSphere to NAGIOSXI
- Once the template has been deployed login to the Nagios XI server by using the default admin password presented in the login banner.
- Once logged in change the default password.
- The default networking configuration for the Nagios XI template is set to DHCP. Change the adapter settings to give the Nagios XI server a static address by editing the network adapter file: /etc/sysconfig/network-scripts/ifcfg-ens33.
- Add the following lines to the file
  - IPADDR = 10.2.50.45
  - NETMASK = 255.255.255.0
  - GATEWAY = 10.2.50.254
  - BOOTPROTO = static
- Next we need to configure the DNS address for the Nagios XI server. Edit the /etc/resolv.conf file.
- Add the following lines
  - nameserver   10.1.50.50
  - nameserver   10.2.50.50
- Restart the Nagios XI server so the new network settings can be applied, and the server can acquire the correct date and time.

Next we can configure Nagios of start monitoring a Windows server. We will need to deploy an agent and get the agent’s password to start monitoring the server.

- Use the web browser to login to the Nagios XI web client using the servers IP address (10.2.50.45).
- Once connected to the web client the installation screen will appear. Input a new admin password and install the server. Once Installation is finished you will be brought to the Nagios XI dashboard.



Home Dashboard

Getting Started Guide

Common Tasks:

- Change your account settings
  Change your account password and general preferences.
- Change your notifications settings
  Change how and when you receive alert notifications.
- Configure your monitoring setup
  Add or modify items to be monitored with easy-to-use wizards.

Getting Started:

- Learn about XI
  Learn more about XI and its capabilities.
- Signup for XI news
  Stay informed on the latest updates and happenings for XI.

Administrative Tasks

Task

Initial Setup Tasks:

- Configure system settings
  Configure basic settings for your system.
- Reset security credentials
  Change the default credentials used by the system.
- Configure mail settings
  Configure email settings for your system.

Host Status Summary

Up	Down	Unreachable	Pending
17	3	0	0
Unhandled	Problems		All
3	3		20

Last Updated: 2019-04-09 11:26:00

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
214	13	0	21	0
Unhandled		Problems		All
34		34		248

Last Updated: 2019-04-09 11:26:00

We're Here To Help!

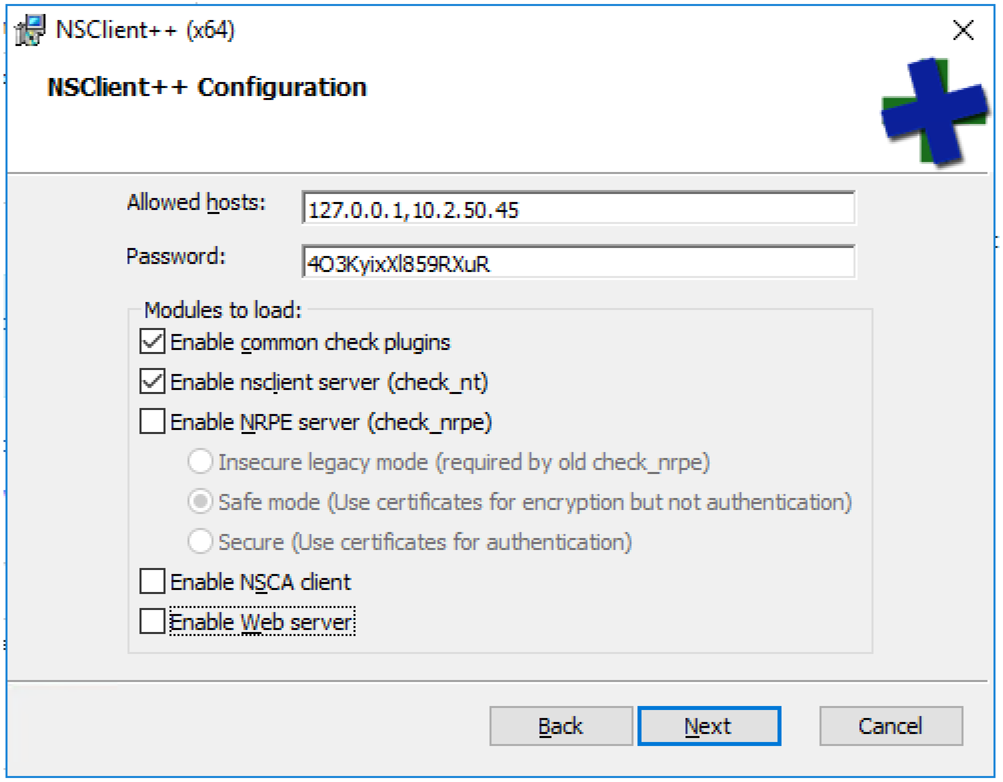
Our knowledgeable techs are happy to help you with any questions or problems you may have getting Nagios up and running.

Support Forum / Customer Support Forum
Help Resources
Customer Ticket Support Center
Customer Phone Support: +1 651-204-9102 Ext. 4

Start Monitoring

Windows Server Monitor Agent

- Logon to the Nagios XI web client. On the top bar of the Nagios XI dashboard select Configure. Next select ‘run a configuration wizard’ under the ‘start monitoring now’ tab. Next scroll to the bottom of the ‘select a wizard’ page. At the bottom of the page you will find the ‘Windows server’ wizard; select the ‘Windows server’ wizard.
- Under the Windows server information section, enter an IP address of the Windows server you with to monitor. Select next.
- Now we are in step 2 of the wizard. If your Nagios XI server was configured with DNS, the host name field under the Windows server details section will auto propagate with the correct FQDN name of the IP address.
- Under the ‘Windows agent’ download the 64-bit Agent. Copy the file to the server you selected in the previous step. The agent is named NSClient++
- Now on the Windows server, launch agent installer wizard. Select typical install.
- In the wizard under ‘allowed hosts’ enter the IP address of the Nagios XI server (10.2.50.45). Copy the password under the password field and past it in the ‘agent password’ fluid under the ‘Windows agent’ section in the configuration wizard in the Nagios XI web client.
- Go back to the Windows server and in the agent install wizard under the ‘modules to load section’ mark the check boxes ‘enable common check plugins’ and ‘enable nsclient server (check_nt)’. Finish the agent wizard using the defaults.



NSClient++ (x64)

NSClient++ Configuration

Allowed hosts: 127.0.0.1,10.2.50.45

Password: 4O3KyixXl859RXuR

Modules to load:

☑ Enable common check plugins
☑ Enable nsclient server (check_nt)
□ Enable NRPE server (check_nrpe)
○ Insecure legacy mode (required by old check_nrpe)
● Safe mode (Use certificates for encryption but not authentication)
○ Secure (Use certificates for authentication)
□ Enable NSCA client
□ Enable Web server

- Now go back to the Nagios XI server. Under the ‘performance counters section select the logon errors counter.
- Finish the Nagios wizard using the defaults.
- Nagios will give you a success message if the Nagios server can reach the Windows server successfully.

Linux Server Monitor Agent

- Logon to the Nagios XI web client. On the top bar of the Nagios XI dashboard select Configure. Next select ‘run a configuration wizard’ under the ‘start monitoring now’ tab. Next scroll to about halfway down the ‘select a wizard’ page. Halfway down the page you will find the ‘Linux server’ wizard; select the ‘Windows server’ wizard.
- Under the Windows server information section, enter an IP address of the Linux server you with to monitor. Under Linux distribution select the correct version of Linux you are using. Select next.
- Now we are in step 2 of the wizard. If your Nagios XI server was configured with DNS, the host name field under the Windows server details section will auto propagate with the correct FQDN name of the IP address.
- Under the Linux agent section open the ‘agent install instructions’. Alternatively you can reach then at http://10.2.50.45/nagiosxi/config/.
- To download the agent from the Nagios XI server, logon to the Linux server selected above and enter the following commands.
    - cd /tmp
    - wget https://assets.nagios.com/downloads/nagiosxi/agents/linux-nrpe-agent.tar.gz
- Once the agent has downloaded use the following commands to initiate the agent install.
    - tar xzf linux-nrpe-agent.tar.gz
    - cd linux-nrpe-agent

  - ./fullinstall
- Near the end of the Linux server agent install. The installer will prompt for to IP address of the Nagios XI server. It wants the IP address in slash notation. (10.2.50.45/24)
- Now that the agent is installed on the Linux server. Go back to the configuration wizard on the Nagios XI server. Finish the Nagios wizard using the defaults.
- Nagios will give you a success message if the Nagios server can reach the Linux server successfully.

SNMP Monitor Configuration

- Nagios can also acquire SNMP data from the networking devices in dominion green houses. To enable SNMP requires a basic configuration on each networking device.
- For a cisco switch or router, input the command.
  - snmp-server community Trogdor RO
- For an ASA firewall, input the commands.
  - snmp-server host outside 10.2.50.45 poll community Trogdor version 2c
  - snmp-server community Trogdor
  - snmp-server enable traps syslog
- Logon to the Nagios XI web client. On the top bar of the Nagios XI dashboard select Configure. Next select ‘run a configuration wizard’ under the ‘start monitoring now’ tab. Next scroll to the bottom of the ‘select a wizard’ page. At the near the bottom of the page you will find the ‘network switch / router’ wizard; select the ‘network switch / router’ wizard.
- Under the ‘router/switch information’ section enter the management IP address of the switch. Also enter the ‘snmp community’ string as entered in the networking devices. Select next.
- Accept the defaults and complete the wizard.
- Nagios will give you a success message if the Nagios server can reach the networking device successfully.

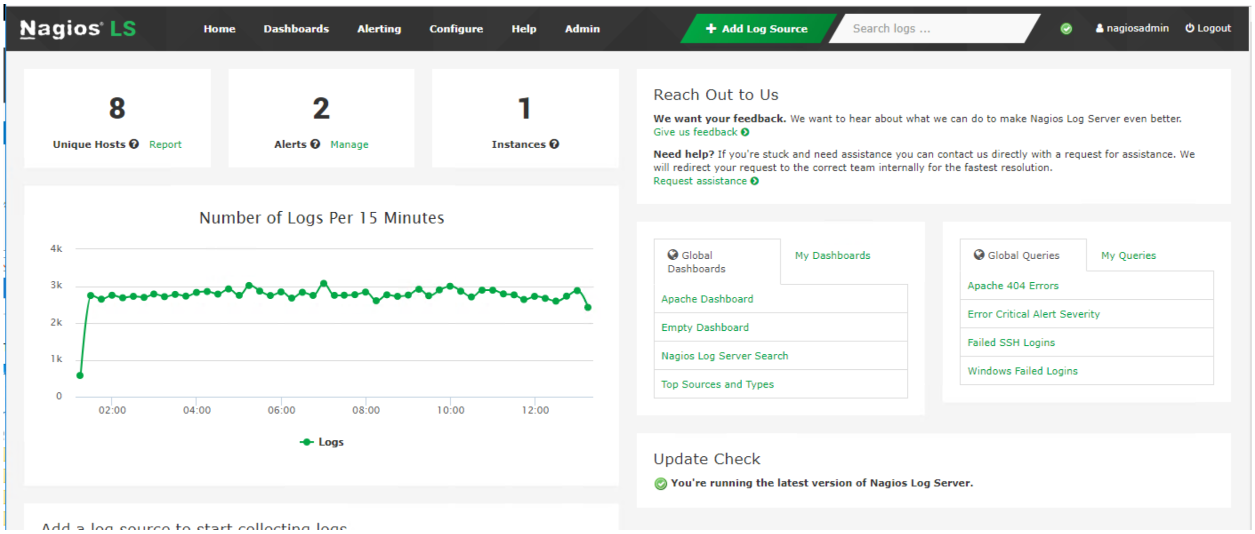
Nagios LS Log Server

A log server provides a centralized location for system logs. Like a server monitor an administrator can receive alerts; however, more importantly a log server can help you find out the cause of downtime. Allowing an administrator to find a solution to downtime caused by crash, is far more cost effective then temporarily fixing a problem by restarting the server. Nagios log server will accumulate logs, then allow an administrator to filter the logs to show only what they need to see.

Install Nagios LS

Nagios provides a trial VM as an .ova template for ESXi. We can deploy this template into ESXi using vSphere.

- Login to the vSphere web client with an administrative account.
- In the navigator window, right click on the vSphere server. Select deploy OVF template…
- The deploy OVF template wizard will start. Select the nagioslogserver-2.0.7-64.ova file and deploy it into the appropriate ESXi server.
- Rename the Nagios LS server in vSphere to NAGIOSLS
- Once the template has been deployed login to the Nagios LS server by using the default admin password presented in the login banner.
- Once logged in change the default password.
- The default networking configuration for the Nagios LS template is set to DHCP. Change the adapter settings to give the Nagios LS server a static address by editing the network adapter file: /etc/sysconfig/network-scripts/ifcfg-ens33.
- Add the following lines to the file
  - IPADDR = 10.2.50.55
  - NETMASK = 255.255.255.0
  - GATEWAY = 10.2.50.254
  - BOOTPROTO = static
- Next we need to configure the DNS address for the Nagios LS server. Edit the /etc/resolv.conf file.
- Add the following lines
  - nameserver 10.1.50.50
  - nameserver 10.2.50.50
- Restart the Nagios LS server so the new network settings can be applied, and the server can acquire the correct date and time.



Reach Out to Us

We want your feedback. We want to hear about what we can do to make Nagios Log Server even better.
Give us feedback

Need help? If you're stuck and need assistance you can contact us directly with a request for assistance. We will redirect your request to the correct team internally for the fastest resolution.
Request assistance

Update Check

You're running the latest version of Nagios Log Server.

Add a log source to start collecting logs

Windows Logging Agent

- Logon to the Nagios LS web client. On the top on the dashboard select the green '+ add log source' button.
- Under the 'add log source' section select Windows.
- In Windows under the 'getting started' section select the green text labeled 'NXLog CE'. This will download the logging agent. Copy this agent to the Windows server you wish to monitor.
- Launch the log server agent installation wizard.
- Accept the EULA and click install.
- The wizard will be finished but we still require additional configuration.
- Back on the Nagios log server under 'configuration setup' copy the contents of the script by selecting the green 'select all' button.
- Back on the Windows server, run notepad as a administrator.
- Navigate to the C:\Program Files (x86)\nxlog\conf\nxlog.conf file and replace the old script configuration with the new script from the Nagios LS server. Save the nxlog.conf file.
- Next open the command prompt as administrator. Use the command 'net start nxlog' to start the logging agent.
- Back on the log server, the dashboard should count an additional 'Unique source' if the agent is working properly.

Linux logging Agent

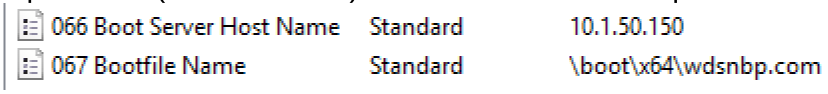
- Logon to the Nagios LS web client. On the top on the dashboard select the green '+ add log source' button.
- Under the 'add log source' section select Linux.
- Copy the contents of the script by selecting the green 'select all' button.
- Go to the Linux server you wish to add to the log server, and paste the script. This script will download, install, and configure the log server agent.
- Back on the log server, the dashboard should count an additional 'Unique source' if the agent is working properly.

Windows Deployment Service

Windows Deployment service (WDS) is window servers O.S. Deployment server. A deployment server is useful since you can install an O.S remotely, with no USB stick is required. Additionally a multicast transition can be setup so multiple O.S's can be installed over the network at the same time. This ability will allow an admin to save time, and the organization money.

Configuring WDS

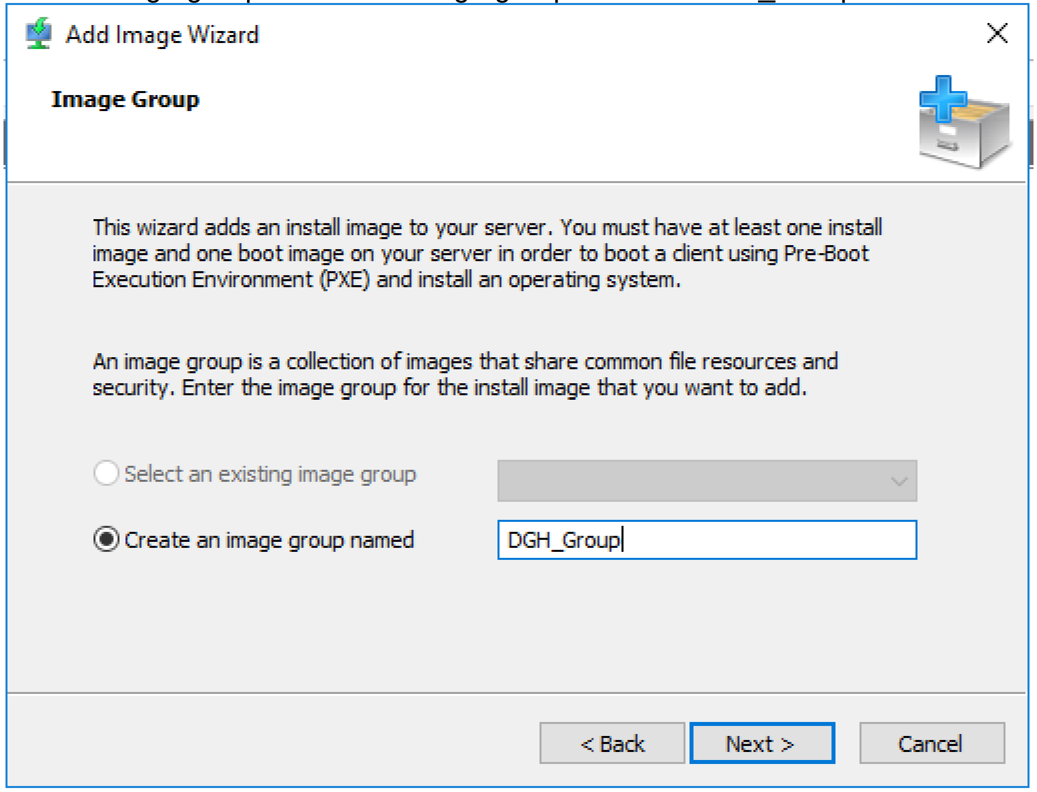
- To allow a host to boot over the network requires a DHCP server. If requires create a DHCP server for your clients. Once you have configured a DHCP server, set the following scope options. Note: option 066 is the IP address of the WDS server.
    - Option 066 (Boot Server Host Name) Value: 10.1.50.150
    - Option 067 (Bootfile Name) Value: \boot\x64\wdsnbp.com



066 Boot Server Host Name	Standard	10.1.50.150
067 Bootfile Name	Standard	\boot\x64\wdsnbp.com

- Next add an additional disk partition to the windows server that will have WDS installed. This partition will be used to store O.S images for deployment.
- Copy a Windows 10 .iso file that you with the WDS server to deploy and mount the disk to the D: drive.
- Next install the WDS role on Windows server by starting the 'add roles and features' wizard and selecting 'Windows Deployment Services' under the Server roles section.
- Launch the WBS GUI. Next we need to configure the WBS server to work on the domain. Under servers, right click on the local deployment server and select 'configure server'.
- The Windows deployment services configuration wizard will launch and will present a checklist that should be completed before proceeding. This list is the following.
    - The server a member of a domain.
    - The network has a DHCP server with option 066 & option 067 configured.
    - DNS is configured on the network
    - The server has a separate partition for O.S Images.
- If the above list has been completed, click next in the Windows deployment services configuration wizard.
- Under the 'install options' page. Select 'Integrate with Active Directory', click next.
- Under 'remote installation folder location' Change the path to the new disk partition that was created for O.S. Images. You will need to create a new folder. Click next.
- Under PXE server initial settings select 'Respond all client computers (known and unknown). This was an administrator can perform a new install. Click next.
- Under 'operation complete' make sure the 'add images to the server now' check box is marked. Finish the wizard.
- The 'add image wizard' should automatically start. Under 'image file' browse to the windows 10 .iso file that should be mounted in the D: drive. Navigate to 'sources' folder. Click next.

- Under ‘image group’ create an image group named. “DGH_Group”. Click next.



Add Image Wizard

Image Group

This wizard adds an install image to your server. You must have at least one install image and one boot image on your server in order to boot a client using Pre-Boot Execution Environment (PXE) and install an operating system.

An image group is a collection of images that share common file resources and security. Enter the image group for the install image that you want to add.

○ Select an existing image group

● Create an image group named: DGH_Group

- Finish the ‘add image’ wizard.
- Now the image is installed on the WDS server; however, a domain admin account will not have permissions to install the image. Meaning when the installer prompts for an privileged account, a domain admin will not have the appropriate privileges to perform the install.
- In the main WDS GUI, navigate to the ‘install images’ folder and select the DGH_group image group that was created above.
- Right click on the image in the image group, select properties.
- Under the ‘user permissions’ tab, add the domain admins group. Give the domain admins full control permissions. Apply the changes and click Ok.
-

Installing Image

- To install the image to a client computer, launch the computer into a network boot by pressing f12 was the BIOS performs it’s POST. The computer should get a DHCP address and find the WBS server from the DHCP options. Once the WBS server is found by the client press f12. The client will download the boot image and launch the WBS ‘Windows Setup’ wizard.
- Select the appropriate keyboard layout. Click next.
- When prompted, enter the appropriate domain\username and password.
- Select the Appropriate Operating system. Click next.
- Select the disk on the client. Click next.
- Now the O.S will be deployed and installed on the Client.

Firewalls

- Explicit allows followed by deny any
- Site-to-site VPNs between branches

- Static IP forwarding to internal management hosts

Headquarters

- Deny SSDP on outside interface – lots of Simple Service Discovery packets on VLAN 1 (IPv4)
- Allow external access to the Headquarters Management Host from trusted external IP addresses (IPv4)
- Allow External Management of the ASA from trusted external IP addresses (IPv4)
- Allow Nagios server from Manufacturing to send snmp requests to the outside interface of the firewall (IPv4)
- Allow Manufacturing Management Host and Warehouse Management Host full access to the Headquarters network (IPv4/v6)
- Allow Manufacturing internal network and Warehouse internal network access to Headquarters server subnet (IPv4/v6)
- Allow manufacturing firewall external IP and Warehouse firewall external IP access to Headquarters Fileserver for logging.
- Allow Manufacturing and Warehouse Wireless AP subnets access to the Headquarters Wireless controller.
- Deny everything else.

Manufacturing

- Deny SSDP on outside interface – lots of Simple Service Discovery packets on VLAN 1 (IPv4)
- Allow Headquarters internal network and Warehouse internal network access to Manufacturing server subnet (IPv4/v6)
- Allow External Management of the ASA from trusted external IP addresses (IPv4)
- Allow Headquarters Management Host and Warehouse Management Host full access to the Headquarters network (IPv4/v6)
- Allow external access to the Manufacturing Management Host from trusted external IP addresses (IPv4)
- Deny anything else

Warehouse

- Deny SSDP on outside interface – lots of Simple Service Discovery packets on VLAN 1 (IPv4)
- Allow Headquarters Management Host and Manufacturing Management Host full access to the Warehouse network (IPv4/v6)
- Allow External Management of the ASA from trusted external IP addresses (IPv4)
- Allow external access to the Warehouse Management Host from trusted external IP addresses (IPv4)
- Allow Nagios server from Manufacturing to send snmp requests to the outside interface of the firewall (IPv4)
- Deny anything else

Network Devices - Management Plane

Passwords

- Password vault created on management stations (Keepass)

- Passwords on network devices hashed with '*enable service password-encryption*'
- Using bulknet.py sent show command to all devices to confirm it was present: *show run* | *include service password-encryption*
- The output of bulknet.py is included in the appendix section D I, because it is used to configure and confirm many network configurations.

Memory and CPU threshold notifications

- Enabled SNMPv3 notifications for 80% CPU utilization and follow-up notification when utilization drops below 70% at 5 second interval.
- Set the process entry limit and size of the history table for CPU utilization statistics to 40% and CPU history size of 300 seconds.
- Tested with bulknet.py command
  show run | *include process cpu threshold type total rising interval 5 falling 70 interval 5*
  show run | *include process cpu statistics limit entry-percentage 40 size 300*

Management Access

- SSH version 2 only
  Tested with bulknet.py : *show run* | *begin line vty*
- Control access to VTY and TTY lines with access lists and firewall configurations
  Tested with bulknet.py while checking SSHv2 only access
  also *show run* | *begin ip access-list extended MANAGEMENT*
- Warning banners
  Tested with bulknet.py: *show run* | *include banner login*

AAA

- Local AAA used. Users can be added, removed or modified with the Python script found on NetEng Tech Solutions GitHub page. This removes the necessity of a dedicated AAA server while still providing some separation of privilege.
  - Administrator *Trogdor* created with privilege 15
    Tested with bulknet.py: *show run* | *include username*
  - Read-only user *MONITOR* created with privilege 0

Logging

- Network device configurations are logged to the file server at Headquarters using TFTP protocol
  - Logs to C:\tftp on FileServer

Network Devices - Control Plane

Network Time Protocol/NTP

- Highly-available NTP configuration that uses Stratum 1 NIST NTP server and a redundant hierarchy as illustrated in appendix diagram, appendix Section A..
- NTP uses password-protection for internal NTP communications but. Communications from Stratum 2 devices to the Stratum 1 device at NIST are not authenticated in this implementation but should be in production.
- Tested with bulknet.py: *show ntp associations* and *show ntp status*

Secure Routing Protocols

- OSPF is used for IPv4 and IPv6 routing
- All IPv4 OSPF is authenticated for all areas
  Tested with bulknet.py: *show ip ospf neighbors* and *show ip ospf interfaces*
- IPv6 OSPF is authenticated everywhere. OSPF gateway border routers do not form neighborships with the any routers besides each other. Area 0 communications/neighbor-negotiations with the NAIT VLAN1 network (Area 0) do not allow for authentication.
  Tested with bulknet.py script: *show ipv6 ospf neighbors* and *show ipv6 ospf interfaces*
- As illustrated in the network diagrams in the Appendices, each location is its own OSPF area. The firewall at each location acts as the Area Border Router connecting each area to Area 0 (NAIT VLAN1) which is the Internet Service Provider/ISP network and is unmanaged by Liquid Sun Hydro Farms.
  Tested interface areas with bulknet.py: *show ip ospf interfaces* and *show ipv6 ospf interfaces* while checking authentication.

First-hop redundancy protocols/HSRP

- Hot-Standby Routing Protocol/HSRP is secured by using pre-shared-keys for authentication between standby peers.
  Tested with bulknet.py: *show run* | *include standby*
- HSRP standby configurations are placed on each VLAN. Because OSPF does not support per-VLAN interface costs the HQ-D-SW2 and MP-D-R1 Multi-layer switches/MLS are used as the primary HSRP router for all IPv4 with priority and preempt configured along with tracking for the upstream interface to automatically decrement the priority of the router is the upstream link fails.
- For IPv6 HSRP MP-D-R2 is likewise has priority, preempt and uplink state tracking for automatic failover. HQ-D-SW1 does not allow for separate HSRP instances for IPv4 and IPv6, so OSPF metrics were tuned to have HQ-D-SW1 will take over as default gateway for both IPv4 and IPv6 if default gateways on network clients are set to use HQ-D-SW1 (FE80::11 or 2620:fc:0:d358:x::250).

Data Plane

Spanning Tree

- Spanning-tree favors the same routers (HQ-D-SW2 and MP-D-SW2) as HSRP for routing efficiency. See Appendices for STP detail.
  Tested with bulknet.py: *show spanning-tree*

Disable IP source routing

- IP source routing allows packets to specify the route that they should take. Disabled on all network devices.
  Tested with bulknet.py: *show run* | *include no ip source-route*

Disable ICMP redirects

- ICMP redirects allows the router to alert the sender of suboptimal paths. Disabled on all network devices.
  Configured and tested manually with *no ip redirects* interface command and *show run*

Disable IP Directed broadcasts

- Allows traffic to be routed to the broadcast address of a different subnet than it originated from. Disabled by default on the devices in this network.
  Tested with bulknet.py: show run | include directed

VLAN Trunking Protocol/VTP

- VTP is disabled on access ports.
  Tested with bulknet.py: *show run*
- VTP is authenticated using pre-shared keys
  Tested with bulknet.py: *show vtp status* | *include MD5 digest*
- Native VLAN is changed to VLAN 2 and VLAN 1 is shutdown.
- Unused ports are shut
  Tested with bulknet.py: *show ip interface brief* | *exclude administratively down*

Firewall

- Configured with explicit permits and deny all.
  Tested with NMAP scanning from ISP/VLAN 1 network. Scan results included in the appendix Section E.

Filter ICMP

- ICMP is dropped from all untrusted networks.

Filter IP fragments

- Web services on cloud. Cloud service provider responsibility.

Filter IP options

- Web services on cloud. Cloud service provider responsibility.

Filter TTL values

- All traffic from untrusted networks is dropped. TTL values for trusted networks is not a concern.

Anti-spoofing

Access Control Lists

- Configured to restrict traffic to devices

Port security

- Unused ports administratively disabled
  Checked with bulknet.py: *show ip int bri*
- Added descriptions to all used ports
- Trunks do not negotiate. All trunks configured manually.
- Native VLAN on all switches changed from default VLAN1 to VLAN2.

BPDU Guard

- Configured on all access ports.

VoIP

Server

- CentOS/Asterisk-FreePBX Server used
- Users are added manually

Phones

- Statically configured with VLAN 25
- Get addresses through DHCP

Wireless

Switch/Controller

- The Cisco 3650 controller functions by tunneling all traffic from the Access Point to the controller over the Management VLAN (in this case VLAN 222/Wireless APs) so the switchport on the Cisco 3650 is left as an access port on VLAN 222/Wireless APs VLAN. The Access Points are directly connected to the Cisco 3650 in this case to provide Power-over-Ethernet/PoE but due to the Controller/AP tunneling the APs do not have to be directly connected to the switch and Manufacturing and the Warehouse locations can use the controller at Headquarters.

Access Point

- Access points are joined to the controller by DHCP pool 'AP' which provides dynamic addresses to access points, DNS resolution at DC01 (Headquarters) and DC02 (Manufacturing) provide the domain-name DominionGreenHouses.com and the address of the controller with DHCP option 43.
  - DHCP option 43 is f104.0a01.defe
    - f1: indicates hex string follows
    - 04: that the address following is 4 bytes
    - 0a01.defe :10.1.150.254

SSID Standards

- Trogdor_Guest
  - WPA2/Auth(password protected)
  - ACLs configured to allow only traffic to ISP network, applied on distribution switch downlink interfaces to access layer
    Tested manually from device connected to Trogdor_Guest network
- Trogdor_Employee
  - WPA2/802.1x Authorization (Integrated with Active Directory)
  - ACLs configured to allow only traffic to ISP network
    Tested manually from device connected to Trogdor_Employee network

Certificate Server

- The certificate server role was installed on DC01 with Simple Certificate Enrollment Procedure/SCEP and Web Authorization capabilities to allow network devices to receive certificates through SCEP and management stations to add the Certificate Server's certificate to their trusted certs to get rid of SSH certificate errors when management stations are configuring network devices.

Security Concerns and Networking Interesting Discoveries

- Greenbone Security Assistant vulnerability scanner uncovered that the VoIP phones allow Telnet traffic and remote Telnet login with admin password, allowing remote admin access to the VoIP phones. In production we would change the default admin password.
- Grandstream Firmware update 1.0.1.97 disables the Telnet function by default, a more sane default.
- Could have used dot1x for authentication to Active Directory with the VoIP phones
- To deny wireless subnet access to the internal network ACLs had to be placed outgoing on HQ-D-SW2 on the downlinks, routed port to HQ-D-SW1 and links to the ESX/Server subnet. Standby negotiations cannot happen over the routed port between HQ-D-SW1 and HQ-D-SW2 so the traffic would have to go to the access layer and back up to the distribution layer if the distribution switches were to be standby neighbors. This would provide high-availability only in the event of an HQ-D-SW2 uplink failure because wireless relies on HQ-D-SW2 and the wireless controller. In this configuration ACLs would have to be placed on access ports on HQ-A-SW1 and HQ-A-SW2 on all operational ports. We chose to sacrifice high-availability for security and placed all of the ACLs on HQ-D-SW2 outgoing on ports that should not forward wireless traffic.
- QoS was not implemented, if quality of voice deteriorates we would have to implement QoS.
- ASA5505 does not support high-availability redundant gateways.
- OSPF does not support per-sub-interface costs.
- Asterisk High severity vulnerability

Scan Results

Discovery scans of the complete internal subnet were completed from each internal management host to verify the inventory of devices on each network. Once discovery scans were completed, each device was vulnerability scanned using OpenVAS. Updates and reconfigurations were applied where applicable, and another scan was executed to confirm that the patches had fixed the vulnerabilities. The results are included in the appendix Section E. The main unmediated vulnerability of concern is a remote code execution vulnerability on the Asterisk server that operating system and module updates has not fixed.

The following suggestions would remove the medium severity vulnerabilities:

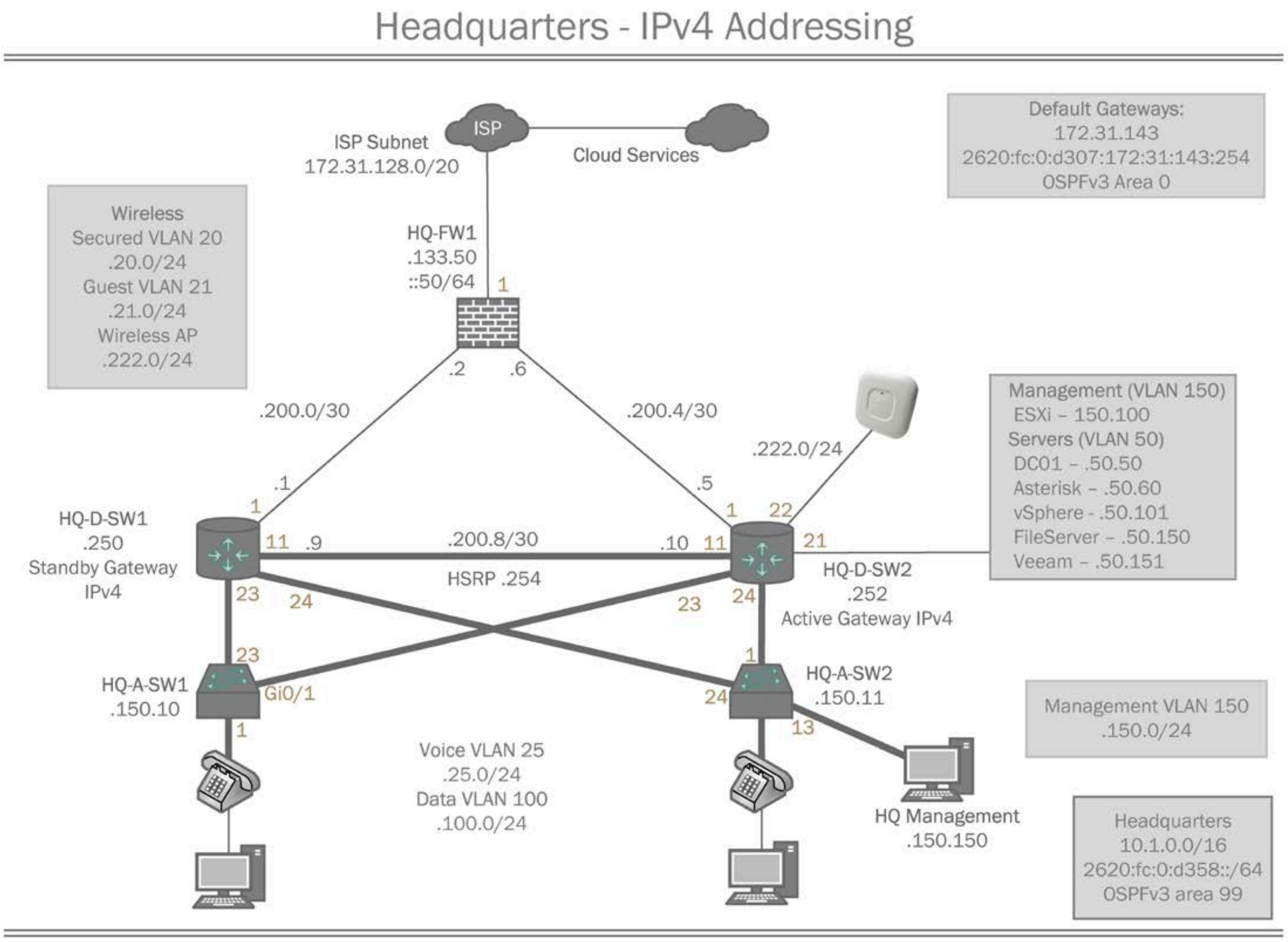
- Disable weak encryption, Diffie-Helman and hashing algorithms on network devices, clients and servers
- Disable HTTP on network devices
- Disable TRACE http method on Asterisk Server
- Filter traffic to 49664/tcp, 49668/tcp, 49684/tcp, 49688/tcp, 49695/tcp, 49699/tcp, 55725/tcp to alleviate DCE/RPC recon attacks.
- Disable Telnet on VoIP phones.

Security Concerns and Networking Interesting Discoveries

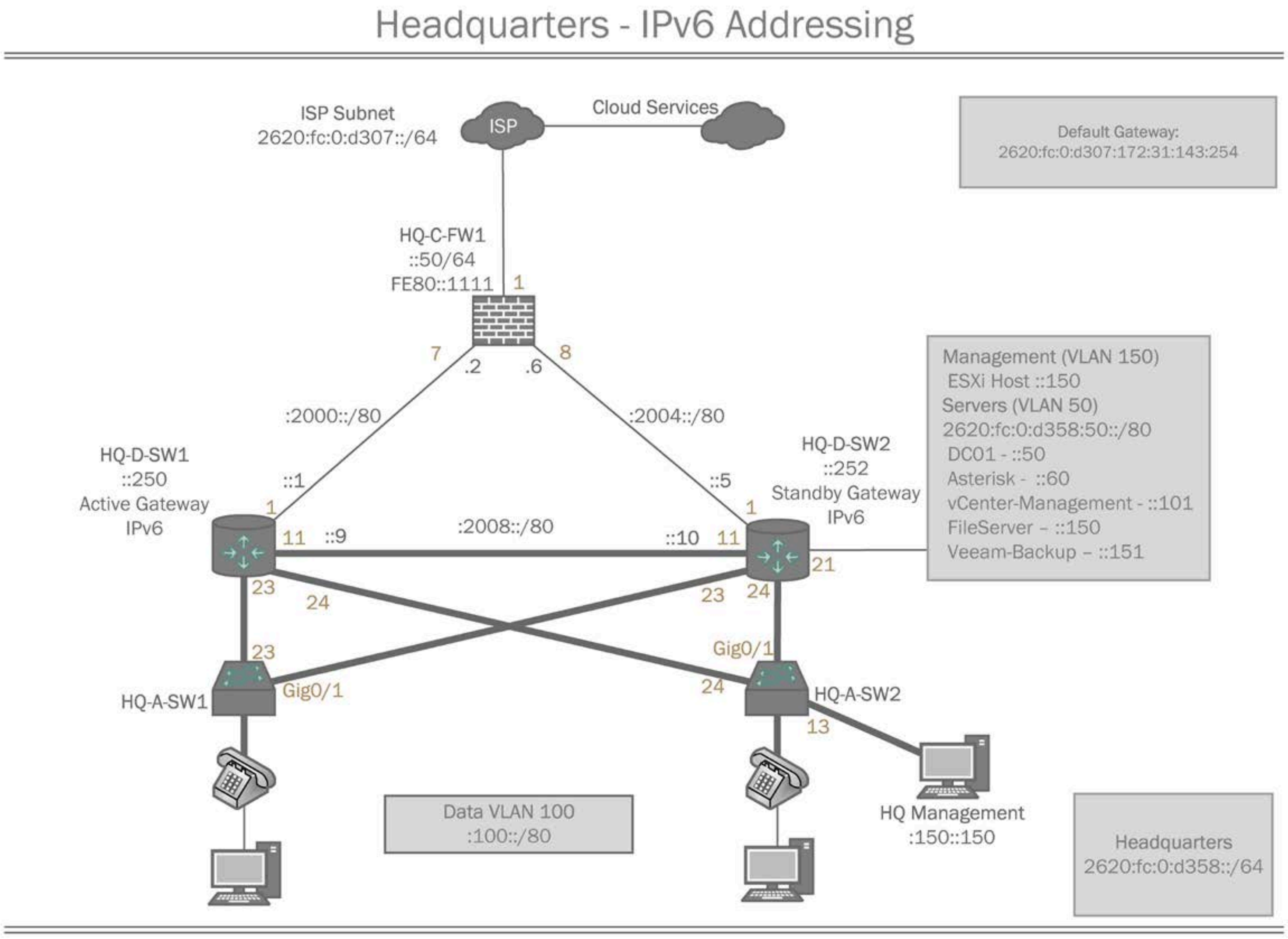
- Greenbone Security Assistant vulnerability scanner uncovered that the VoIP phones allow Telnet traffic and remote Telnet login with admin password, allowing remote admin access to the VoIP phones. In production we would change the default admin password.
- Grandstream Firmware update 1.0.1.97 disables the Telnet function by default, a more sane default.
- Could have used dot1x for authentication to Active Directory with the VoIP phones
- To deny wireless subnet access to the internal network ACLs had to be placed outgoing on HQ-D-SW2 on the downlinks, routed port to HQ-D-SW1 and links to the ESX/Server subnet. Standby negotiations cannot happen over the routed port between HQ-D-SW1 and HQ-D-SW2 so the traffic would have to go to the access layer and back up to the distribution layer if the distribution switches were to be standby neighbors. This would provide high-availability only in the event of an HQ-D-SW2 uplink failure because wireless relies on HQ-D-SW2 and the wireless controller. In this configuration ACLs would have to be placed on access ports on HQ-A-SW1 and HQ-A-SW2 on all operational ports. We chose to sacrifice high-availability for security and placed all of the ACLs on HQ-D-SW2 outgoing on ports that should not forward wireless traffic.
- QoS was not implemented, if quality of voice deteriorates we would have to implement QoS.
- ASA5505 does not support high-availability redundant gateways.
- OSPF does not support per-sub-interface costs for IPv4 or IPv6-specific load-balancing.
- Asterisk High severity remote-execution vulnerability that is not fixed by updates from the default Yum repositories or Asterisk module updates. It is a problem with the libsrtp.so.0 shared object not being found, although it is in /usr/lib64/. Asterisk-core-11.17.1-1_centos6.x86_64 depends on libsrtp.so.0, which is updated by the epel repository, which is correctly configured and enabled. The SONAME of the object was checked with objdump –p /usr/lib64/libsrtp.so.0 | grep SONAME, and it gives the proper result of libsrtp.so.0.

Appendix A: Network Diagrams

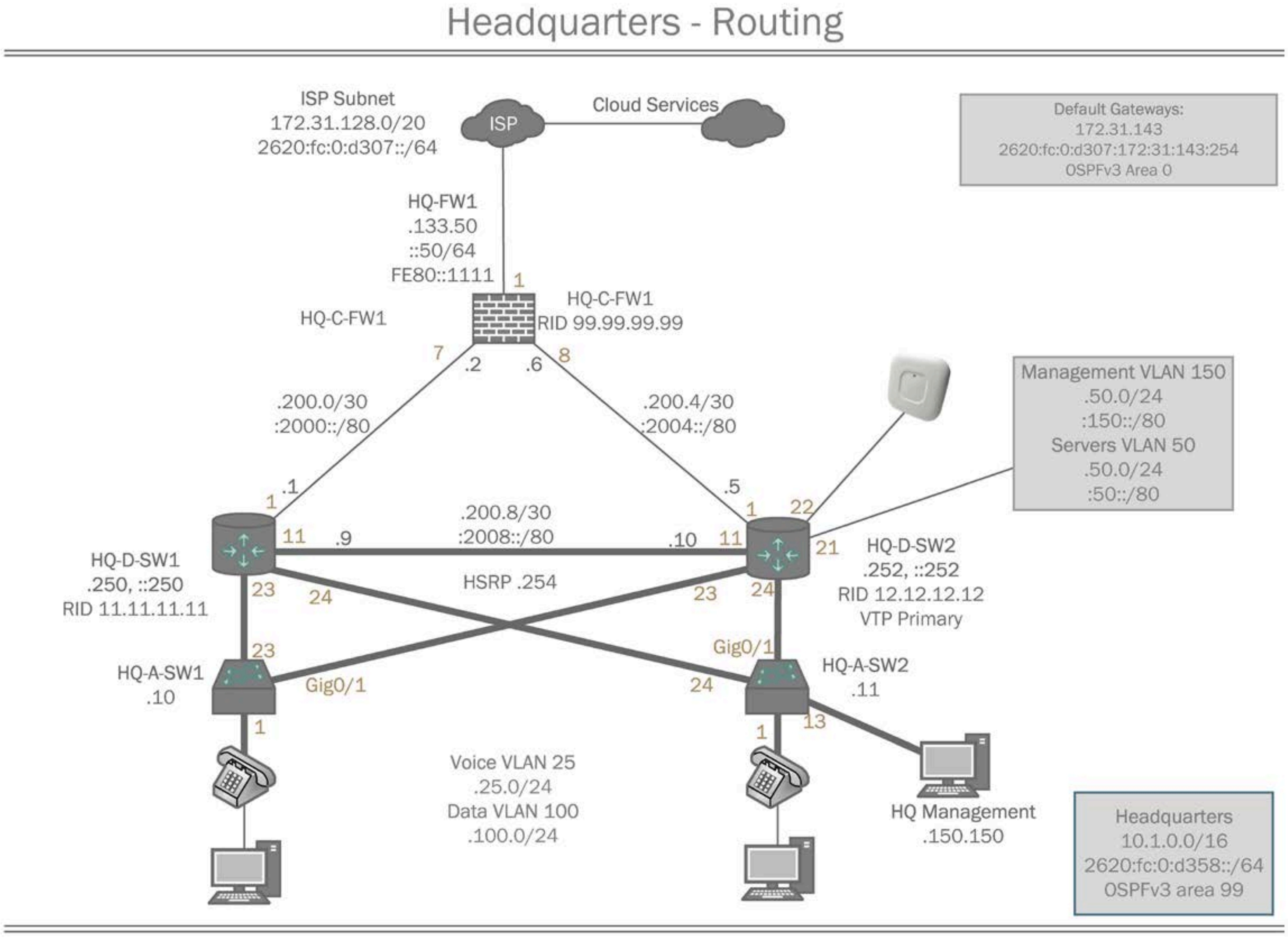
Headquarters - IPv4



Headquarters - IPv6



Headquarters – Routing



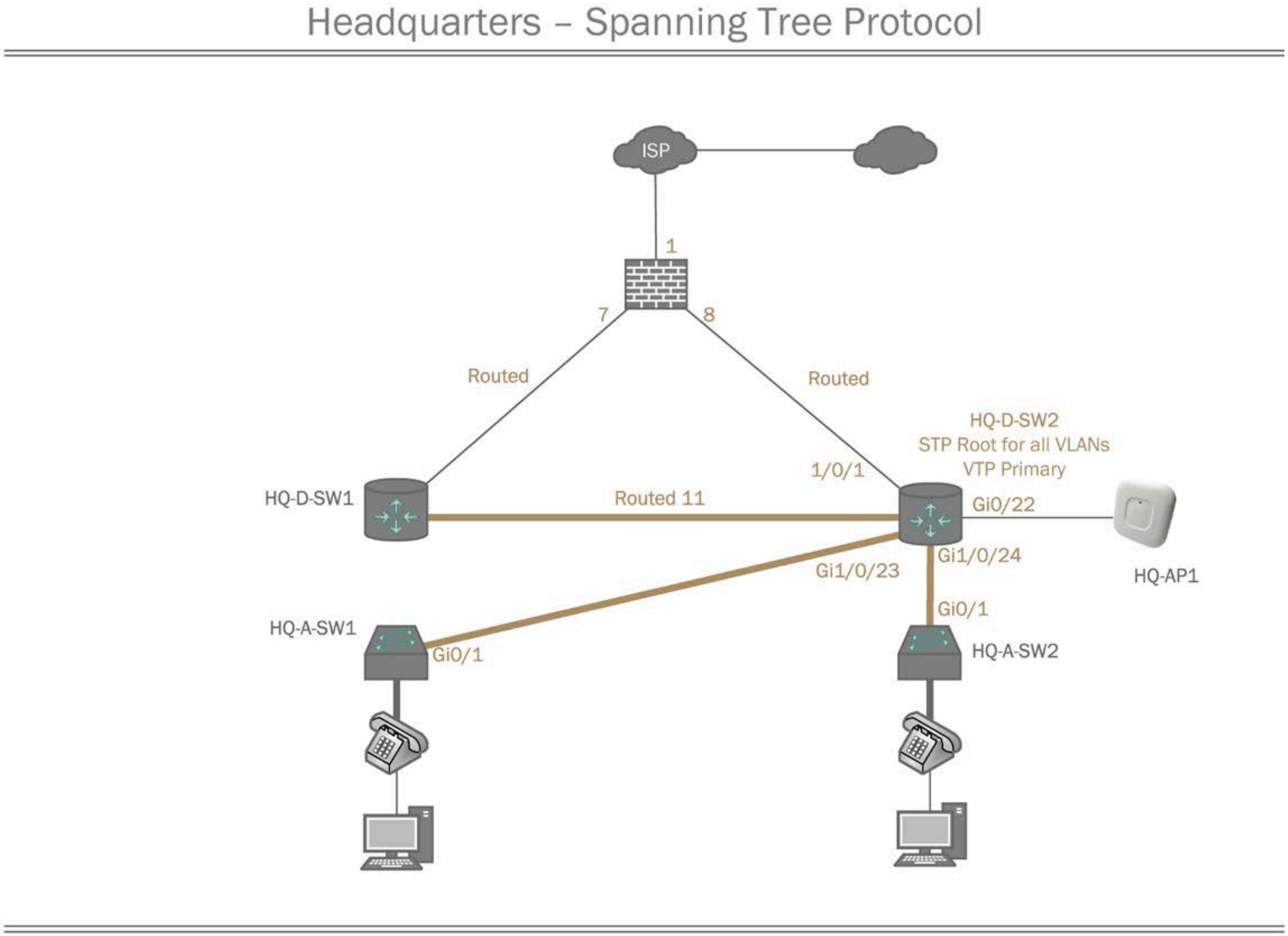
Headquarters - Routing

Default Gateways:
172.31.143
2620:fc:0:d307:172:31:143:254
OSPFv3 Area 0

Management VLAN 150
.50.0/24
:150::/80
Servers VLAN 50
.50.0/24
:50::/80

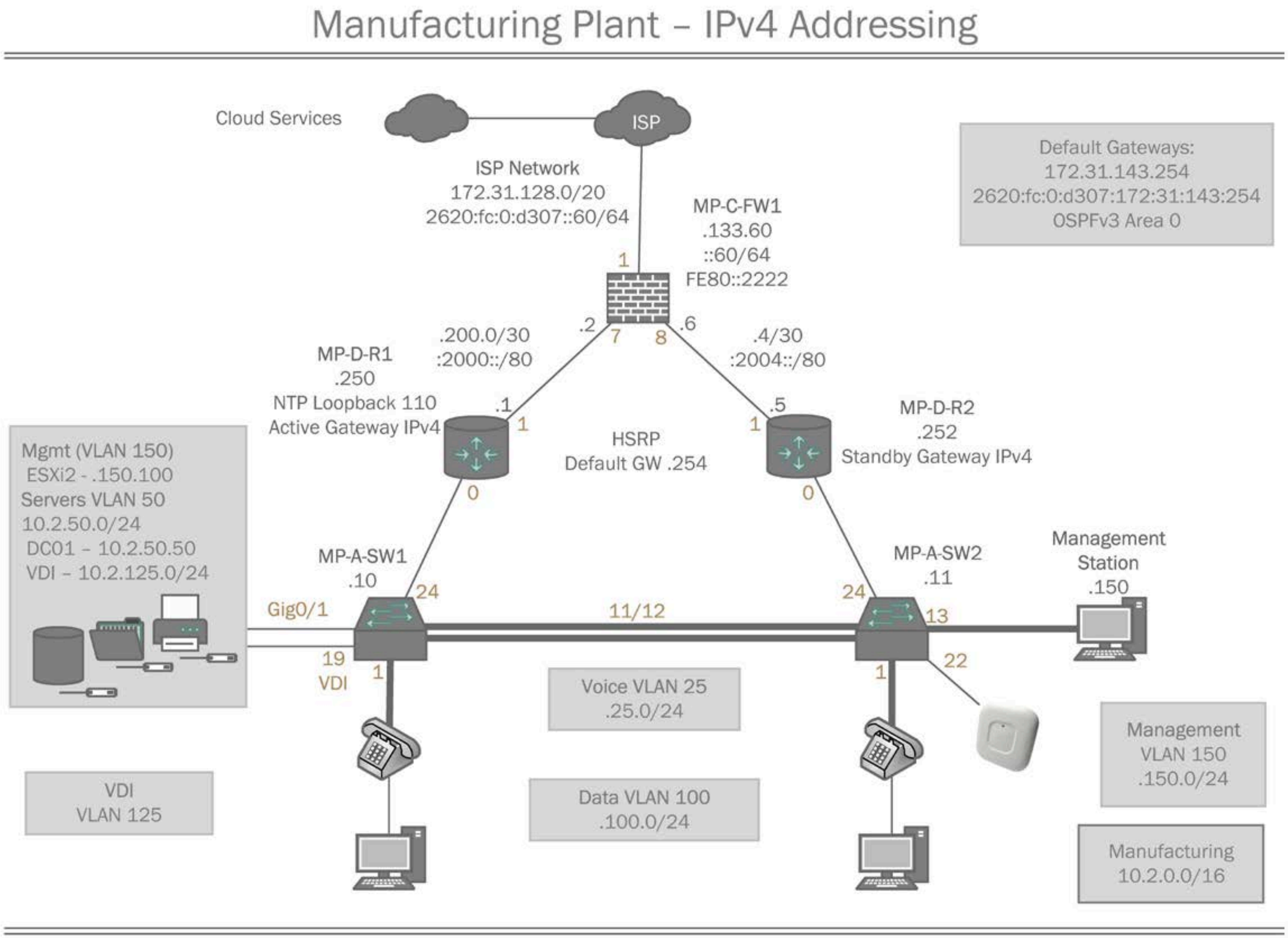
Headquarters
10.1.0.0/16
2620:fc:0:d358::/64
OSPFv3 area 99

Headquarters - Spanning-Tree Protocol/STP



Headquarters – Spanning Tree Protocol

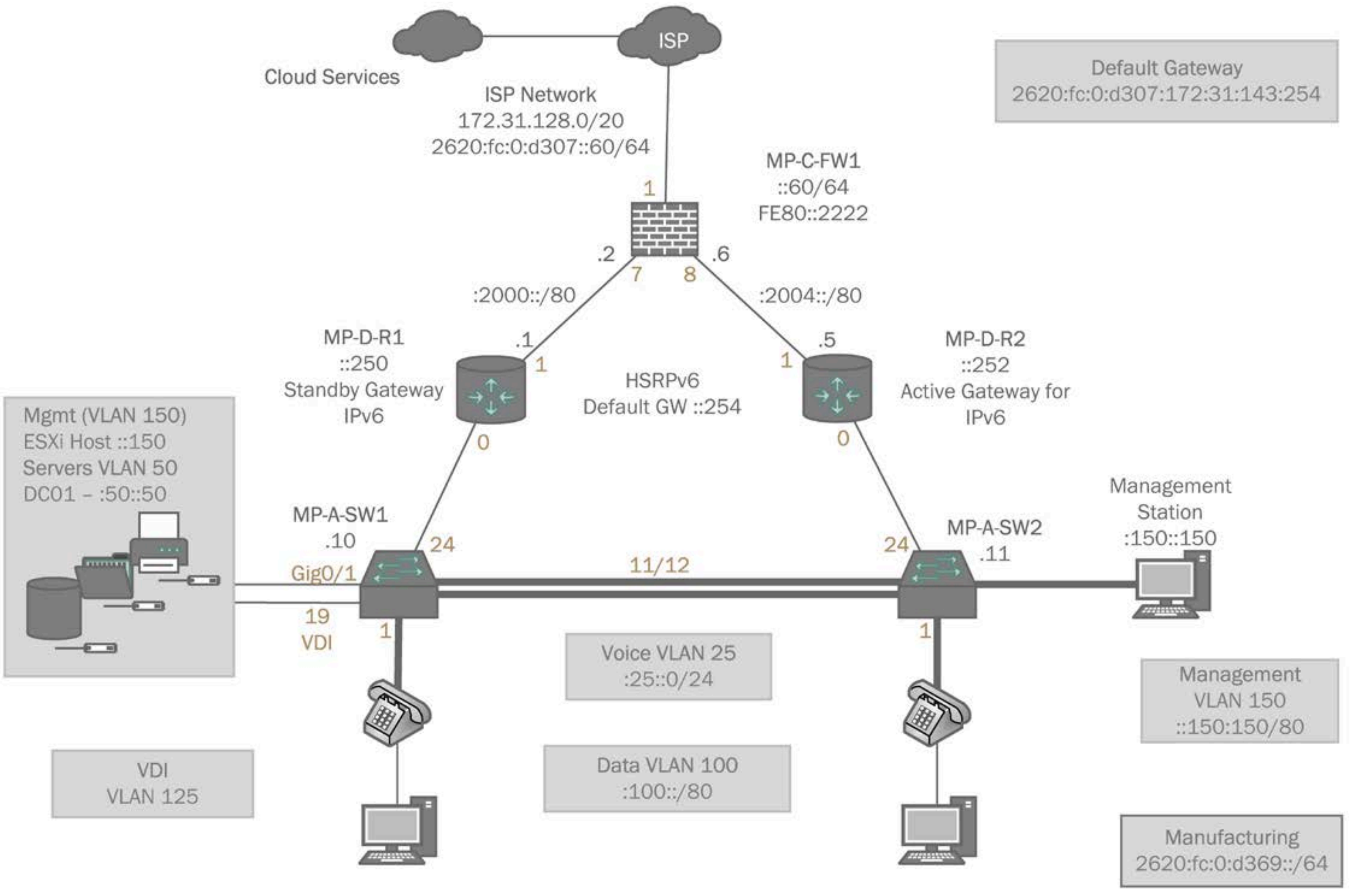
Manufacturing Plant - IPv4



Manufacturing Plant – IPv4 Addressing

Manufacturing Plant - IPv6

Manufacturing Plant – IPv6 Addressing



Cloud Services

ISP

ISP Network
172.31.128.0/20
2620:fc:0:d307::60/64

Default Gateway
2620:fc:0:d307:172:31:143:254

MP-C-FW1
::60/64
FE80::2222

:2000::/80

:2004::/80

MP-D-R1
::250
Standby Gateway
IPv6

HSRPv6
Default GW ::254

MP-D-R2
::252
Active Gateway for
IPv6

Mgmt (VLAN 150)
ESXi Host ::150
Servers VLAN 50
DC01 – :50::50

MP-A-SW1
.10

MP-A-SW2
.11

Management
Station
:150::150

Voice VLAN 25
:25::0/24

Management
VLAN 150
::150:150/80

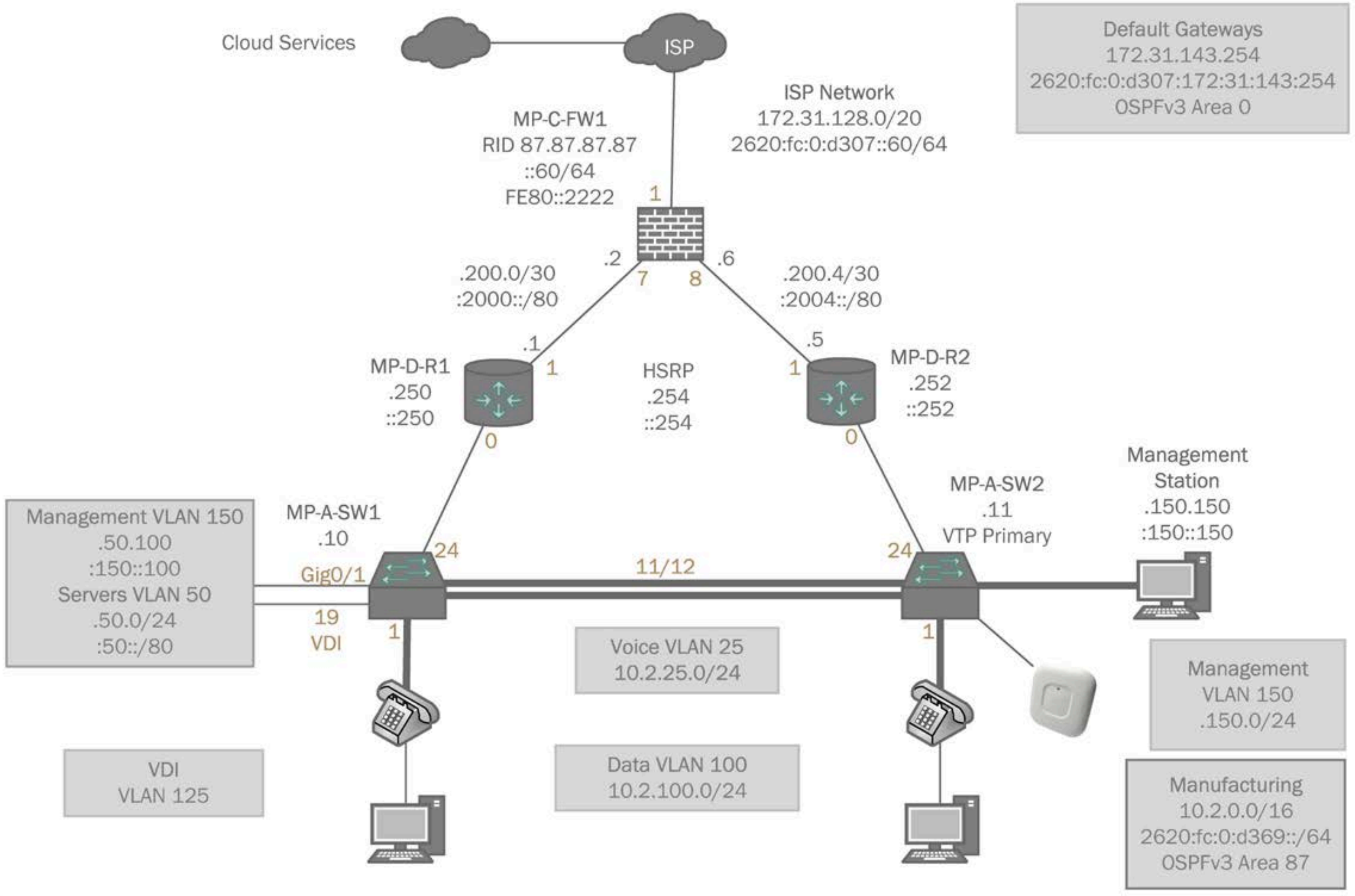
VDI
VLAN 125

Data VLAN 100
:100::/80

Manufacturing
2620:fc:0:d369::/64

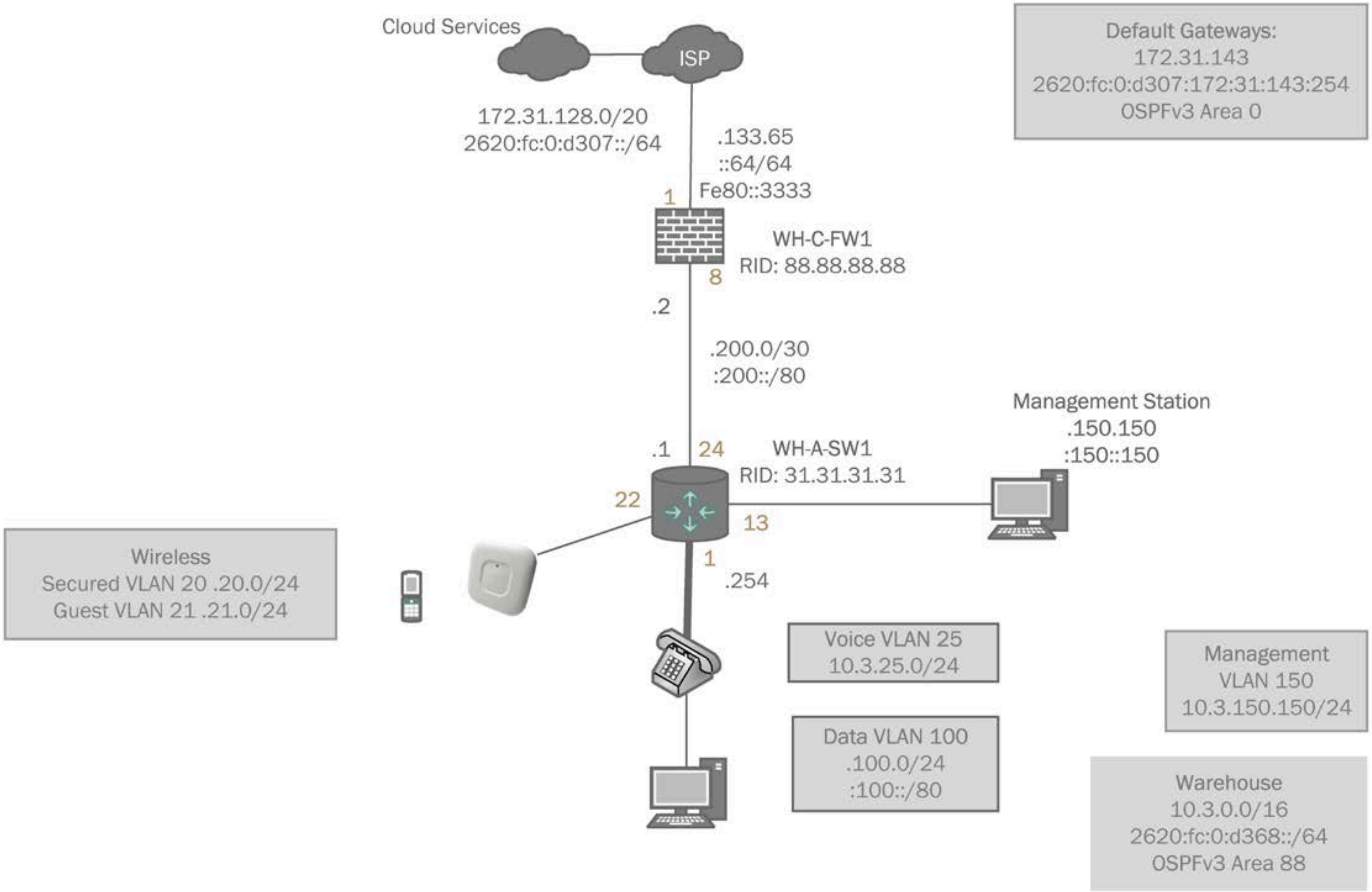
Manufacturing Plant - Routing

Manufacturing Plant – Routing



Warehouse – IPv4

Warehouse



Default Gateways:
172.31.143
2620:fc:0:d307:172:31:143:254
OSPFv3 Area 0

Wireless
Secured VLAN 20 .20.0/24
Guest VLAN 21 .21.0/24

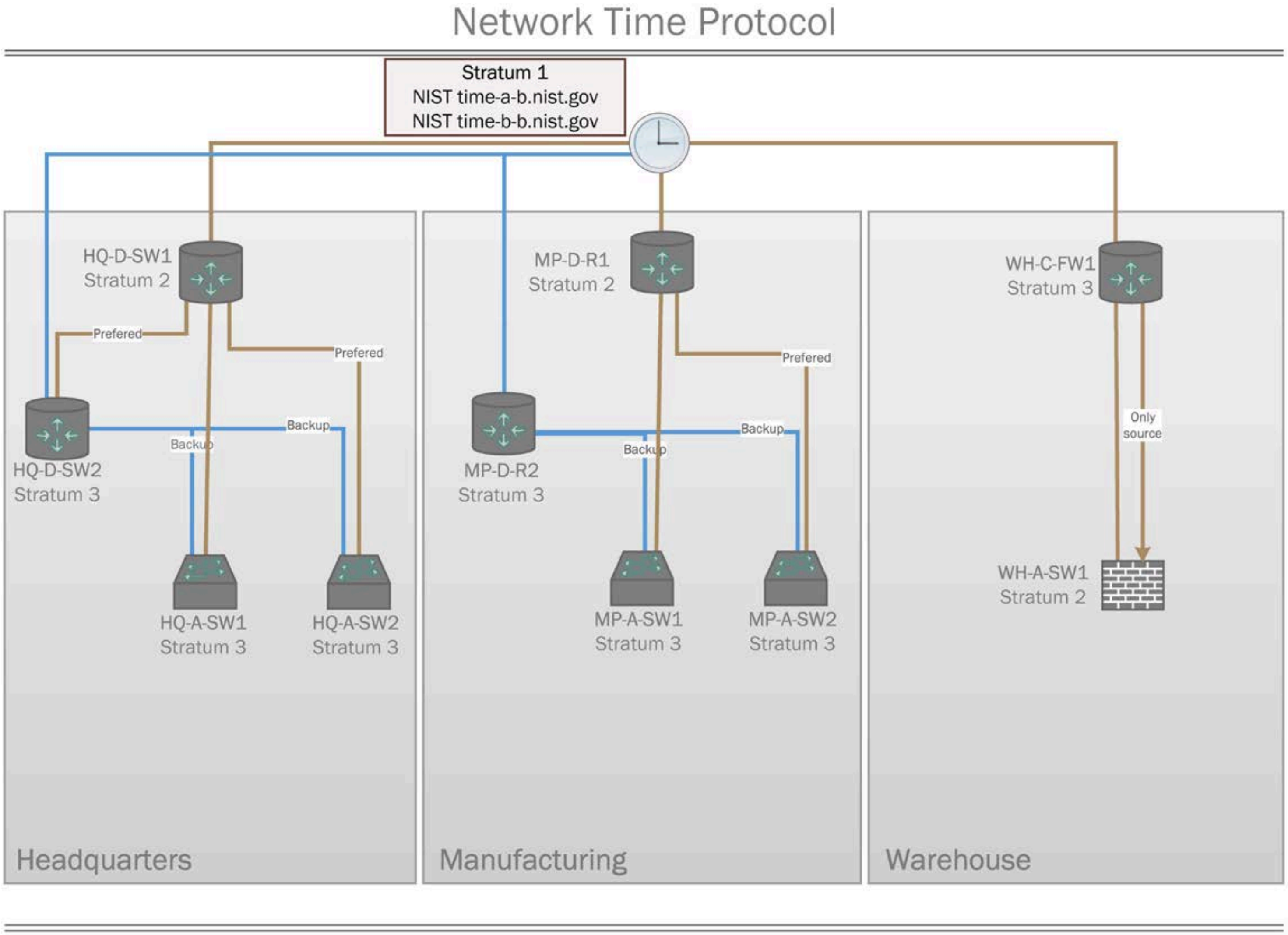
Voice VLAN 25
10.3.25.0/24

Data VLAN 100
.100.0/24
:100::/80

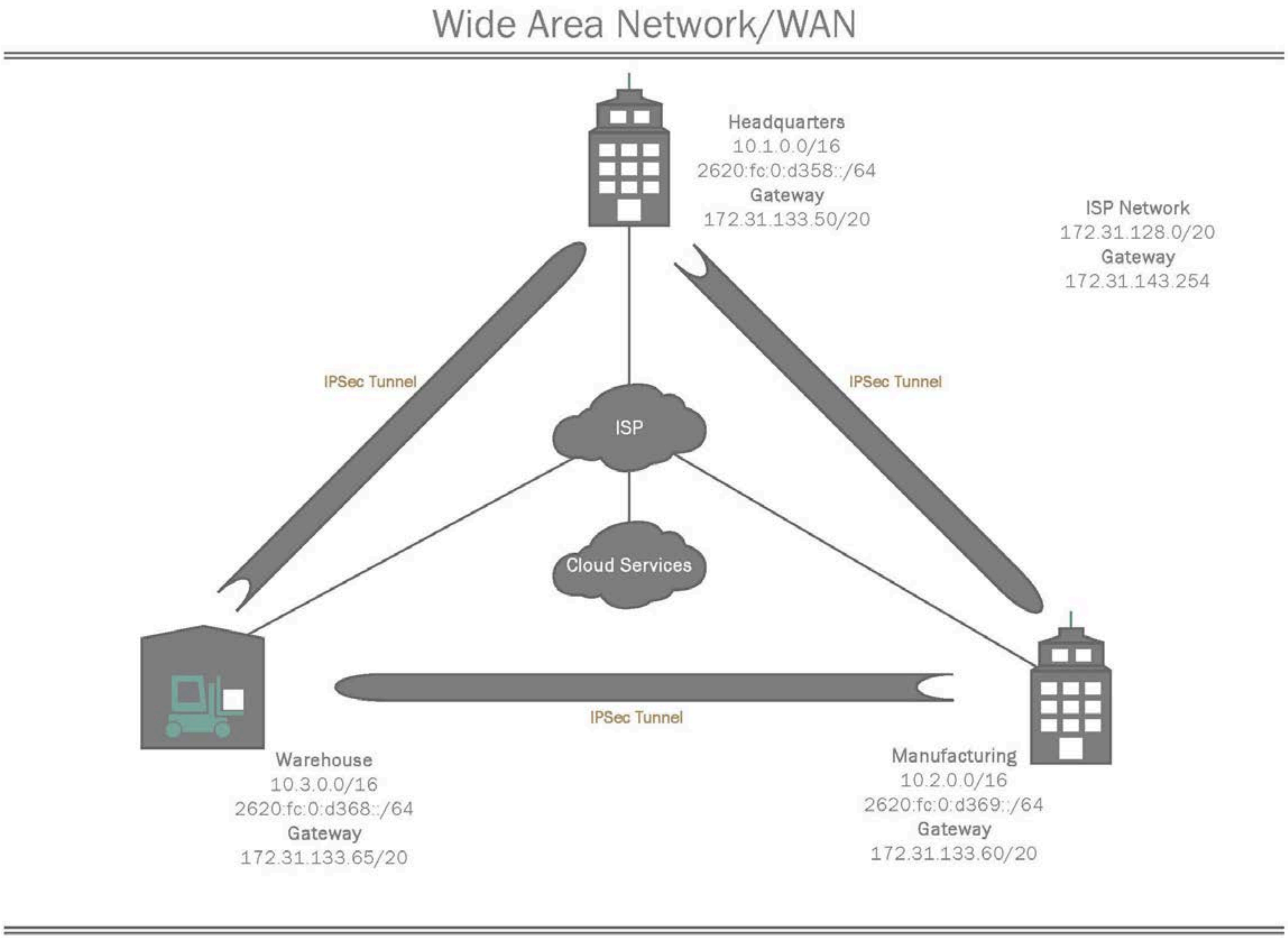
Management
VLAN 150
10.3.150.150/24

Warehouse
10.3.0.0/16
2620:fc:0:d368::/64
OSPFv3 Area 88

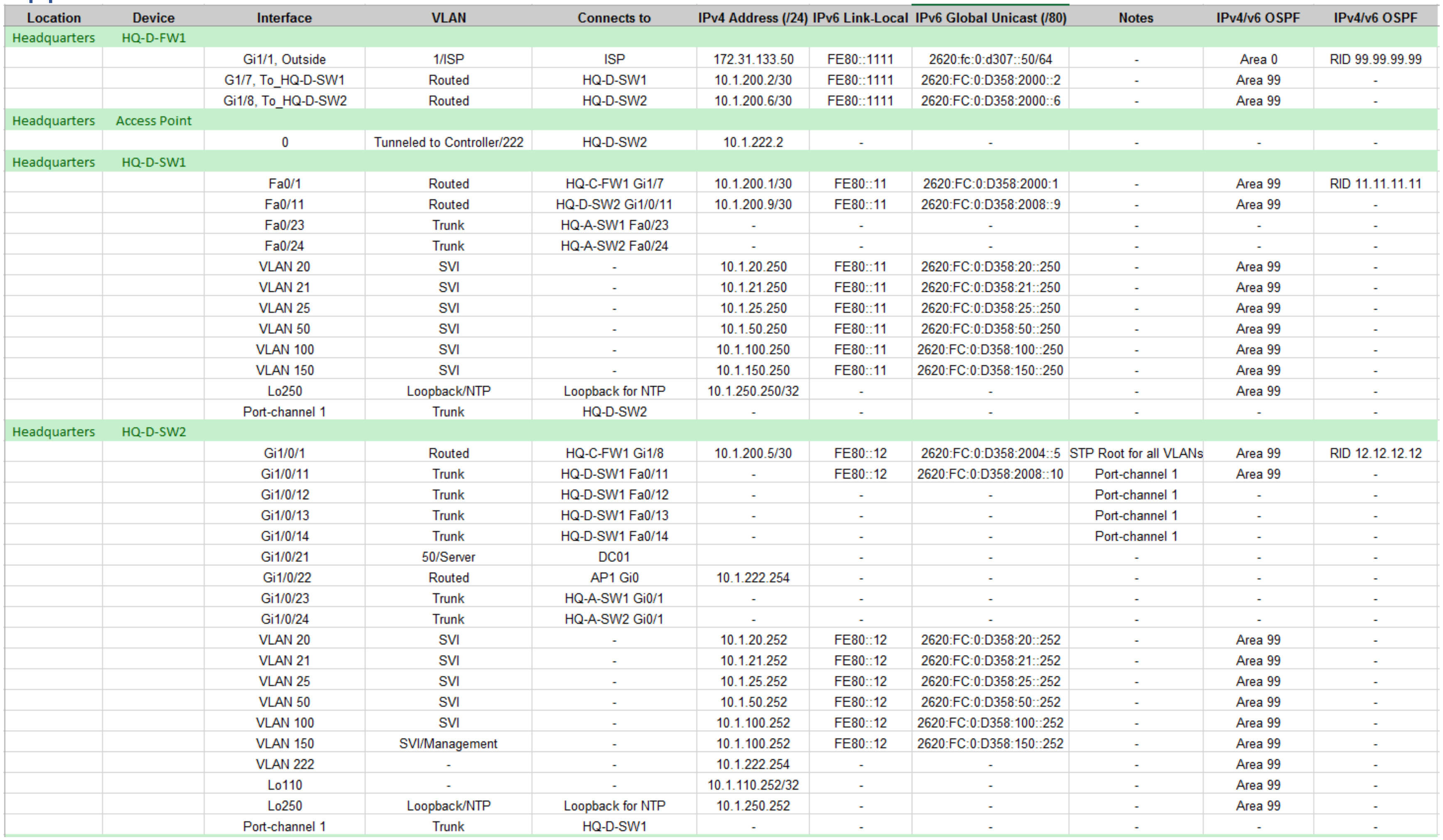
Network Time Protocol/NTP



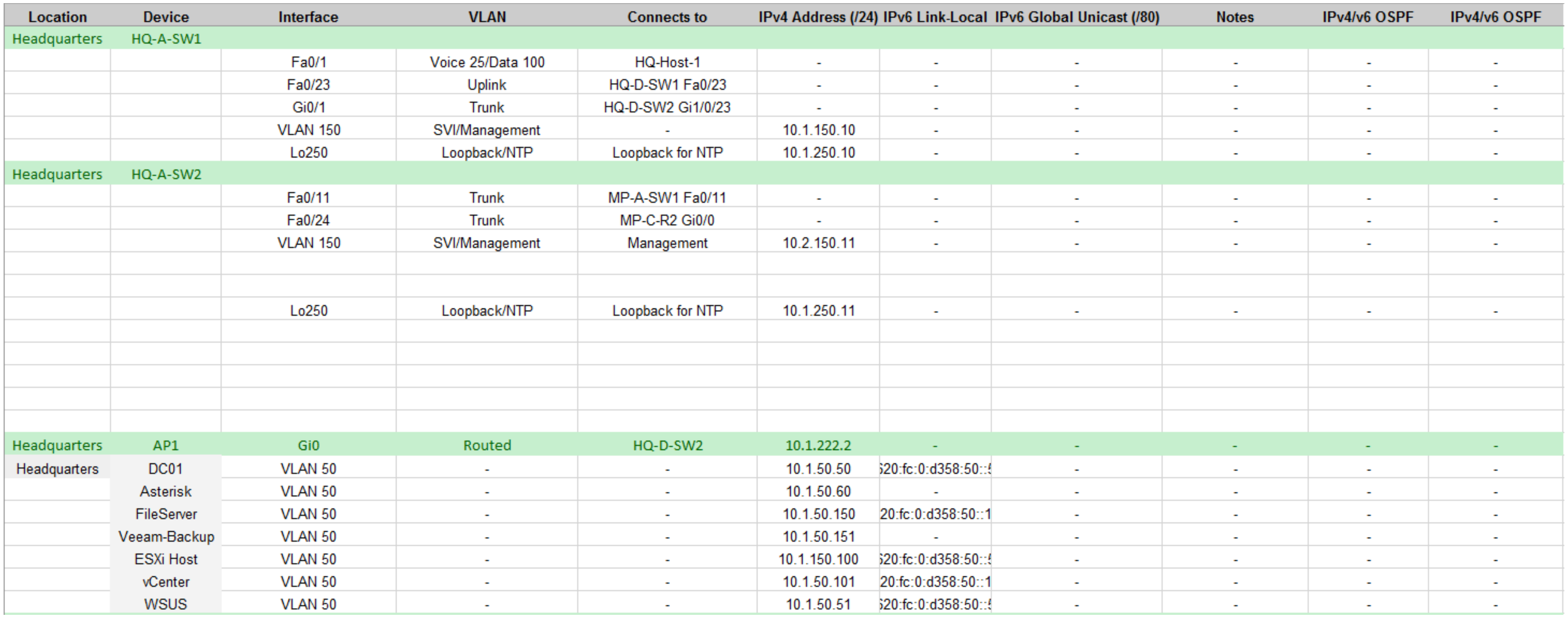
Wide-Area Network/WAN



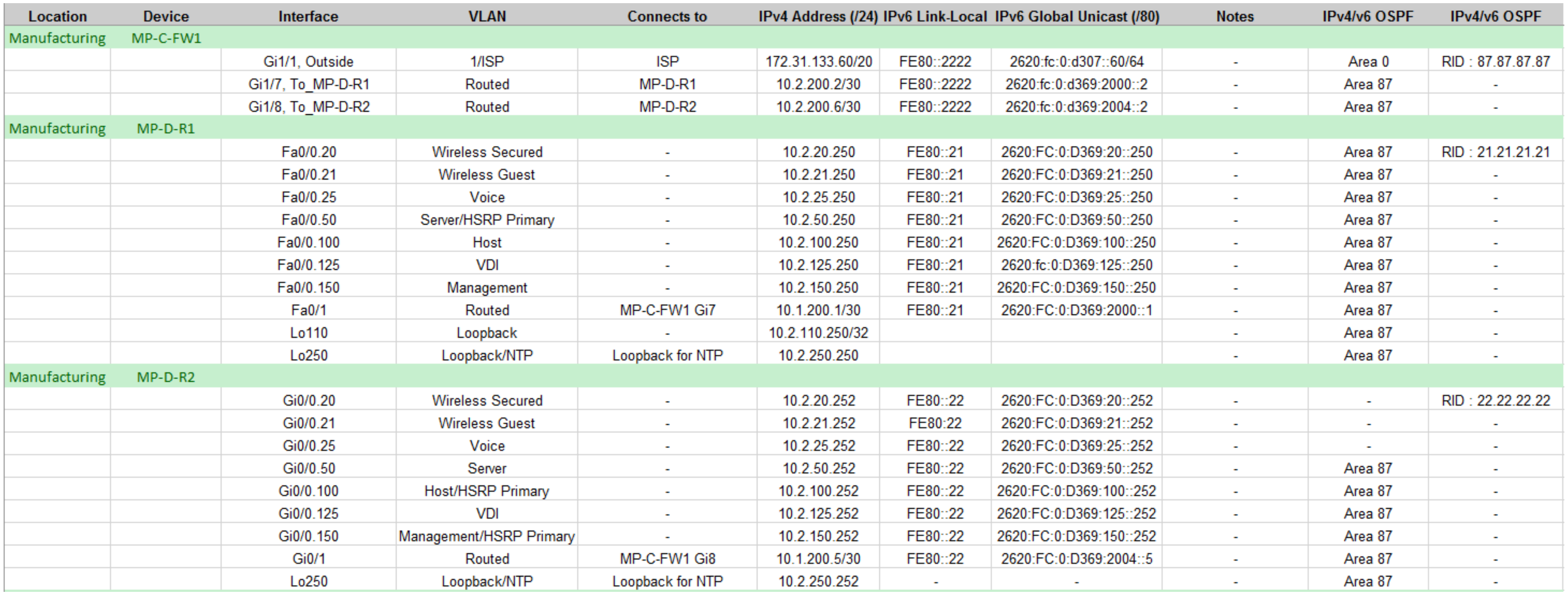
Appendix B: Cutsheet



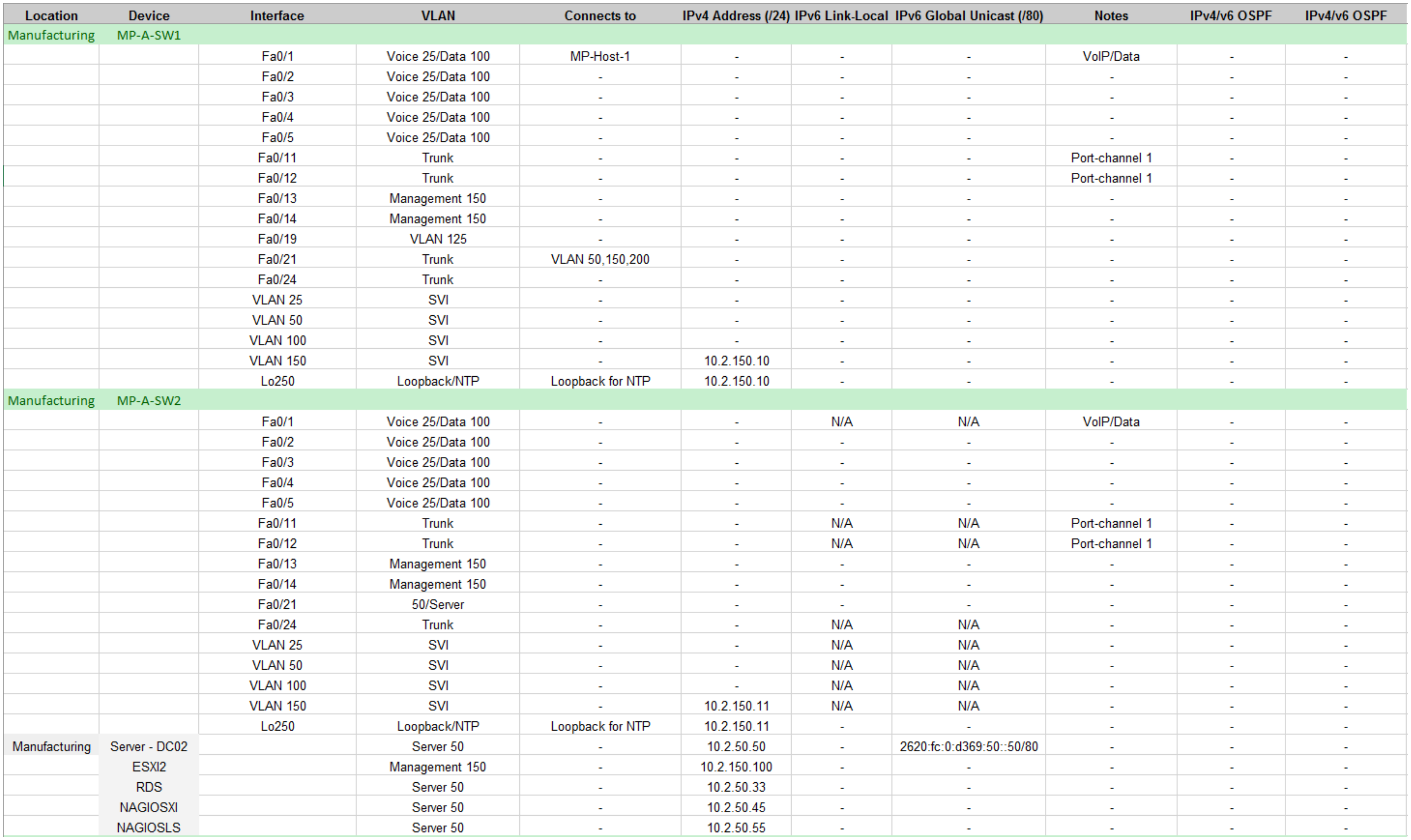
Location	Device	Interface	VLAN	Connects to	IPv4 Address (/24)	IPv6 Link-Local	IPv6 Global Unicast (/80)	Notes	IPv4/v6 OSPF	IPv4/v6 OSPF
Headquarters	HQ-D-FW1									
		Gi1/1, Outside	1/ISP	ISP	172.31.133.50	FE80::1111	2620:fc:0:d307::50/64	-	Area 0	RID 99.99.99.99
		G1/7, To_HQ-D-SW1	Routed	HQ-D-SW1	10.1.200.2/30	FE80::1111	2620:FC:0:D358:2000::2	-	Area 99	-
		Gi1/8, To_HQ-D-SW2	Routed	HQ-D-SW2	10.1.200.6/30	FE80::1111	2620:FC:0:D358:2000::6	-	Area 99	-
Headquarters	Access Point									
		0	Tunneled to Controller/222	HQ-D-SW2	10.1.222.2	-	-	-	-	-
Headquarters	HQ-D-SW1									
		Fa0/1	Routed	HQ-C-FW1 Gi1/7	10.1.200.1/30	FE80::11	2620:FC:0:D358:2000:1	-	Area 99	RID 11.11.11.11
		Fa0/11	Routed	HQ-D-SW2 Gi1/0/11	10.1.200.9/30	FE80::11	2620:FC:0:D358:2008::9	-	Area 99	-
		Fa0/23	Trunk	HQ-A-SW1 Fa0/23	-	-	-	-	-	-
		Fa0/24	Trunk	HQ-A-SW2 Fa0/24	-	-	-	-	-	-
		VLAN 20	SVI	-	10.1.20.250	FE80::11	2620:FC:0:D358:20::250	-	Area 99	-
		VLAN 21	SVI	-	10.1.21.250	FE80::11	2620:FC:0:D358:21::250	-	Area 99	-
		VLAN 25	SVI	-	10.1.25.250	FE80::11	2620:FC:0:D358:25::250	-	Area 99	-
		VLAN 50	SVI	-	10.1.50.250	FE80::11	2620:FC:0:D358:50::250	-	Area 99	-
		VLAN 100	SVI	-	10.1.100.250	FE80::11	2620:FC:0:D358:100::250	-	Area 99	-
		VLAN 150	SVI	-	10.1.150.250	FE80::11	2620:FC:0:D358:150::250	-	Area 99	-
		Lo250	Loopback/NTP	Loopback for NTP	10.1.250.250/32	-	-	-	Area 99	-
		Port-channel 1	Trunk	HQ-D-SW2	-	-	-	-	-	-
Headquarters	HQ-D-SW2									
		Gi1/0/1	Routed	HQ-C-FW1 Gi1/8	10.1.200.5/30	FE80::12	2620:FC:0:D358:2004::5	STP Root for all VLANs	Area 99	RID 12.12.12.12
		Gi1/0/11	Trunk	HQ-D-SW1 Fa0/11	-	FE80::12	2620:FC:0:D358:2008::10	Port-channel 1	Area 99	-
		Gi1/0/12	Trunk	HQ-D-SW1 Fa0/12	-	-	-	Port-channel 1	-	-
		Gi1/0/13	Trunk	HQ-D-SW1 Fa0/13	-	-	-	Port-channel 1	-	-
		Gi1/0/14	Trunk	HQ-D-SW1 Fa0/14	-	-	-	Port-channel 1	-	-
		Gi1/0/21	50/Server	DC01		-	-	-	-	-
		Gi1/0/22	Routed	AP1 Gi0	10.1.222.254	-	-	-	-	-
		Gi1/0/23	Trunk	HQ-A-SW1 Gi0/1	-	-	-	-	-	-
		Gi1/0/24	Trunk	HQ-A-SW2 Gi0/1	-	-	-	-	-	-
		VLAN 20	SVI	-	10.1.20.252	FE80::12	2620:FC:0:D358:20::252	-	Area 99	-
		VLAN 21	SVI	-	10.1.21.252	FE80::12	2620:FC:0:D358:21::252	-	Area 99	-
		VLAN 25	SVI	-	10.1.25.252	FE80::12	2620:FC:0:D358:25::252	-	Area 99	-
		VLAN 50	SVI	-	10.1.50.252	FE80::12	2620:FC:0:D358:50::252	-	Area 99	-
		VLAN 100	SVI	-	10.1.100.252	FE80::12	2620:FC:0:D358:100::252	-	Area 99	-
		VLAN 150	SVI/Management	-	10.1.100.252	FE80::12	2620:FC:0:D358:150::252	-	Area 99	-
		VLAN 222	-	-	10.1.222.254	-	-	-	Area 99	-
		Lo110	-	-	10.1.110.252/32	-	-	-	Area 99	-
		Lo250	Loopback/NTP	Loopback for NTP	10.1.250.252	-	-	-	Area 99	-
		Port-channel 1	Trunk	HQ-D-SW1	-	-	-	-	-	-



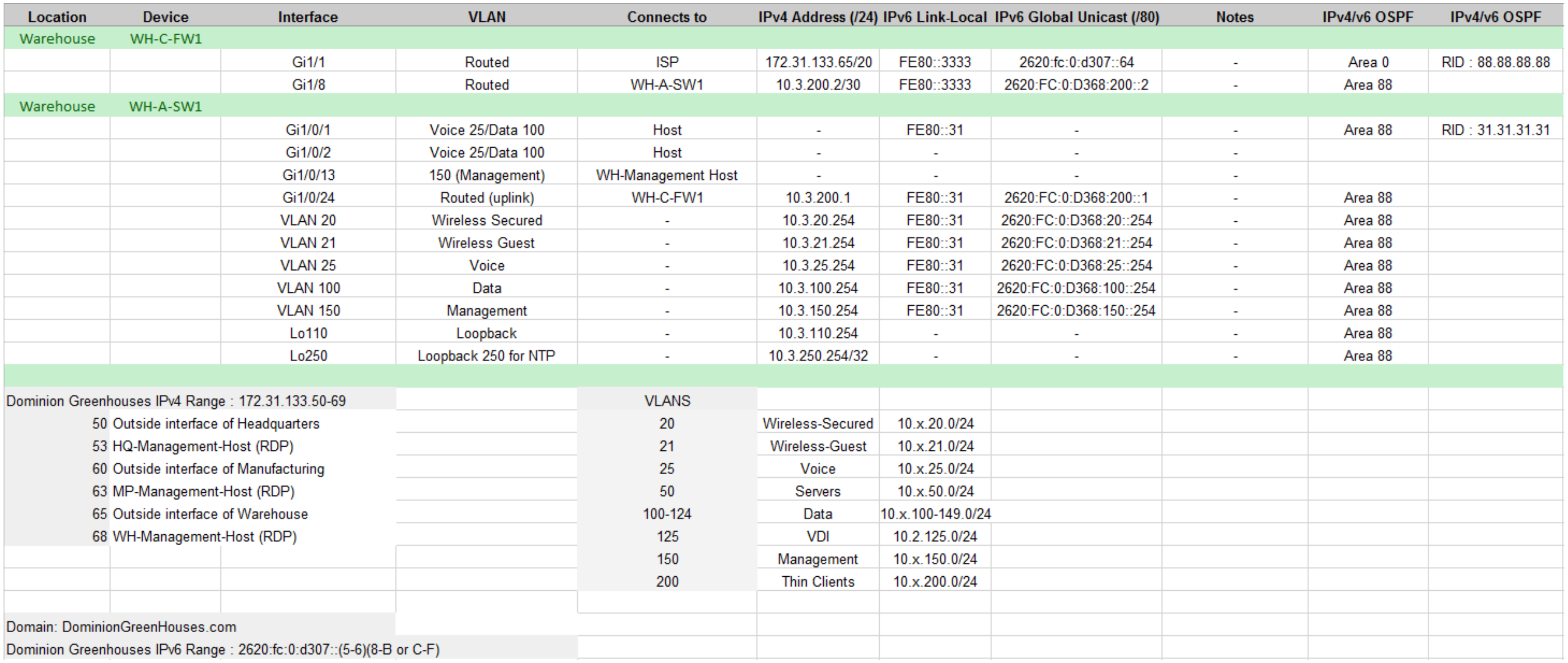
Location	Device	Interface	VLAN	Connects to	IPv4 Address (/24)	IPv6 Link-Local	IPv6 Global Unicast (/80)	Notes	IPv4/v6 OSPF	IPv4/v6 OSPF
Headquarters	HQ-A-SW1									
		Fa0/1	Voice 25/Data 100	HQ-Host-1	-	-	-	-	-	-
		Fa0/23	Uplink	HQ-D-SW1 Fa0/23	-	-	-	-	-	-
		Gi0/1	Trunk	HQ-D-SW2 Gi1/0/23	-	-	-	-	-	-
		VLAN 150	SVI/Management	-	10.1.150.10	-	-	-	-	-
		Lo250	Loopback/NTP	Loopback for NTP	10.1.250.10	-	-	-	-	-
Headquarters	HQ-A-SW2									
		Fa0/11	Trunk	MP-A-SW1 Fa0/11	-	-	-	-	-	-
		Fa0/24	Trunk	MP-C-R2 Gi0/0	-	-	-	-	-	-
		VLAN 150	SVI/Management	Management	10.2.150.11	-	-	-	-	-
		Lo250	Loopback/NTP	Loopback for NTP	10.1.250.11	-	-	-	-	-
Headquarters	AP1	Gi0	Routed	HQ-D-SW2	10.1.222.2	-	-	-	-	-
Headquarters	DC01	VLAN 50	-	-	10.1.50.50	520:fc:0:d358:50::5	-	-	-	-
	Asterisk	VLAN 50	-	-	10.1.50.60	-	-	-	-	-
	FileServer	VLAN 50	-	-	10.1.50.150	20:fc:0:d358:50::1	-	-	-	-
	Veeam-Backup	VLAN 50	-	-	10.1.50.151	-	-	-	-	-
	ESXi Host	VLAN 50	-	-	10.1.150.100	520:fc:0:d358:50::5	-	-	-	-
	vCenter	VLAN 50	-	-	10.1.50.101	20:fc:0:d358:50::1	-	-	-	-
	WSUS	VLAN 50	-	-	10.1.50.51	520:fc:0:d358:50::5	-	-	-	-



Location	Device	Interface	VLAN	Connects to	IPv4 Address (/24)	IPv6 Link-Local	IPv6 Global Unicast (/80)	Notes	IPv4/v6 OSPF	IPv4/v6 OSPF
Manufacturing	MP-C-FW1									
		Gi1/1, Outside	1/ISP	ISP	172.31.133.60/20	FE80::2222	2620:fc:0:d307::60/64	-	Area 0	RID : 87.87.87.87
		Gi1/7, To_MP-D-R1	Routed	MP-D-R1	10.2.200.2/30	FE80::2222	2620:fc:0:d369:2000::2	-	Area 87	-
		Gi1/8, To_MP-D-R2	Routed	MP-D-R2	10.2.200.6/30	FE80::2222	2620:fc:0:d369:2004::2	-	Area 87	-
Manufacturing	MP-D-R1									
		Fa0/0.20	Wireless Secured	-	10.2.20.250	FE80::21	2620:FC:0:D369:20::250	-	Area 87	RID : 21.21.21.21
		Fa0/0.21	Wireless Guest	-	10.2.21.250	FE80::21	2620:FC:0:D369:21::250	-	Area 87	-
		Fa0/0.25	Voice	-	10.2.25.250	FE80::21	2620:FC:0:D369:25::250	-	Area 87	-
		Fa0/0.50	Server/HSRP Primary	-	10.2.50.250	FE80::21	2620:FC:0:D369:50::250	-	Area 87	-
		Fa0/0.100	Host	-	10.2.100.250	FE80::21	2620:FC:0:D369:100::250	-	Area 87	-
		Fa0/0.125	VDI	-	10.2.125.250	FE80::21	2620:fc:0:D369:125::250	-	Area 87	-
		Fa0/0.150	Management	-	10.2.150.250	FE80::21	2620:FC:0:D369:150::250	-	Area 87	-
		Fa0/1	Routed	MP-C-FW1 Gi7	10.1.200.1/30	FE80::21	2620:FC:0:D369:2000::1	-	Area 87	-
		Lo110	Loopback	-	10.2.110.250/32			-	Area 87	-
		Lo250	Loopback/NTP	Loopback for NTP	10.2.250.250			-	Area 87	-
Manufacturing	MP-D-R2									
		Gi0/0.20	Wireless Secured	-	10.2.20.252	FE80::22	2620:FC:0:D369:20::252	-	-	RID : 22.22.22.22
		Gi0/0.21	Wireless Guest	-	10.2.21.252	FE80:22	2620:FC:0:D369:21::252	-	-	-
		Gi0/0.25	Voice	-	10.2.25.252	FE80::22	2620:FC:0:D369:25::252	-	-	-
		Gi0/0.50	Server	-	10.2.50.252	FE80::22	2620:FC:0:D369:50::252	-	Area 87	-
		Gi0/0.100	Host/HSRP Primary	-	10.2.100.252	FE80::22	2620:FC:0:D369:100::252	-	Area 87	-
		Gi0/0.125	VDI	-	10.2.125.252	FE80::22	2620:FC:0:D369:125::252	-	Area 87	-
		Gi0/0.150	Management/HSRP Primary	-	10.2.150.252	FE80::22	2620:FC:0:D369:150::252	-	Area 87	-
		Gi0/1	Routed	MP-C-FW1 Gi8	10.1.200.5/30	FE80::22	2620:FC:0:D369:2004::5	-	Area 87	-
		Lo250	Loopback/NTP	Loopback for NTP	10.2.250.252	-	-	-	Area 87	-



Location	Device	Interface	VLAN	Connects to	IPv4 Address (/24)	IPv6 Link-Local	IPv6 Global Unicast (/80)	Notes	IPv4/v6 OSPF	IPv4/v6 OSPF
Manufacturing	MP-A-SW1									
		Fa0/1	Voice 25/Data 100	MP-Host-1	-	-	-	VoIP/Data	-	-
		Fa0/2	Voice 25/Data 100	-	-	-	-	-	-	-
		Fa0/3	Voice 25/Data 100	-	-	-	-	-	-	-
		Fa0/4	Voice 25/Data 100	-	-	-	-	-	-	-
		Fa0/5	Voice 25/Data 100	-	-	-	-	-	-	-
		Fa0/11	Trunk	-	-	-	-	Port-channel 1	-	-
		Fa0/12	Trunk	-	-	-	-	Port-channel 1	-	-
		Fa0/13	Management 150	-	-	-	-	-	-	-
		Fa0/14	Management 150	-	-	-	-	-	-	-
		Fa0/19	VLAN 125	-	-	-	-	-	-	-
		Fa0/21	Trunk	VLAN 50,150,200	-	-	-	-	-	-
		Fa0/24	Trunk	-	-	-	-	-	-	-
		VLAN 25	SVI	-	-	-	-	-	-	-
		VLAN 50	SVI	-	-	-	-	-	-	-
		VLAN 100	SVI	-	-	-	-	-	-	-
		VLAN 150	SVI	-	10.2.150.10	-	-	-	-	-
		Lo250	Loopback/NTP	Loopback for NTP	10.2.150.10	-	-	-	-	-
Manufacturing	MP-A-SW2									
		Fa0/1	Voice 25/Data 100	-	-	N/A	N/A	VoIP/Data	-	-
		Fa0/2	Voice 25/Data 100	-	-	-	-	-	-	-
		Fa0/3	Voice 25/Data 100	-	-	-	-	-	-	-
		Fa0/4	Voice 25/Data 100	-	-	-	-	-	-	-
		Fa0/5	Voice 25/Data 100	-	-	-	-	-	-	-
		Fa0/11	Trunk	-	-	N/A	N/A	Port-channel 1	-	-
		Fa0/12	Trunk	-	-	N/A	N/A	Port-channel 1	-	-
		Fa0/13	Management 150	-	-	-	-	-	-	-
		Fa0/14	Management 150	-	-	-	-	-	-	-
		Fa0/21	50/Server	-	-	-	-	-	-	-
		Fa0/24	Trunk	-	-	N/A	N/A	-	-	-
		VLAN 25	SVI	-	-	N/A	N/A	-	-	-
		VLAN 50	SVI	-	-	N/A	N/A	-	-	-
		VLAN 100	SVI	-	-	N/A	N/A	-	-	-
		VLAN 150	SVI	-	10.2.150.11	N/A	N/A	-	-	-
		Lo250	Loopback/NTP	Loopback for NTP	10.2.150.11	-	-	-	-	-
Manufacturing	Server - DC02		Server 50	-	10.2.50.50	-	2620:fc:0:d369:50::50/80	-	-	-
	ESXI2		Management 150	-	10.2.150.100	-	-	-	-	-
	RDS		Server 50	-	10.2.50.33	-	-	-	-	-
	NAGIOSXI		Server 50	-	10.2.50.45	-	-	-	-	-
	NAGIOSLS		Server 50	-	10.2.50.55	-	-	-	-	-



Location	Device	Interface	VLAN	Connects to	IPv4 Address (/24)	IPv6 Link-Local	IPv6 Global Unicast (/80)	Notes	IPv4/v6 OSPF	IPv4/v6 OSPF
Warehouse	WH-C-FW1									
		Gi1/1	Routed	ISP	172.31.133.65/20	FE80::3333	2620:fc:0:d307::64	-	Area 0	RID : 88.88.88.88
		Gi1/8	Routed	WH-A-SW1	10.3.200.2/30	FE80::3333	2620:FC:0:D368:200::2	-	Area 88	
Warehouse	WH-A-SW1									
		Gi1/0/1	Voice 25/Data 100	Host	-	FE80::31	-	-	Area 88	RID : 31.31.31.31
		Gi1/0/2	Voice 25/Data 100	Host	-	-	-	-		
		Gi1/0/13	150 (Management)	WH-Management Host	-	-	-	-		
		Gi1/0/24	Routed (uplink)	WH-C-FW1	10.3.200.1	FE80::31	2620:FC:0:D368:200::1	-	Area 88	
		VLAN 20	Wireless Secured	-	10.3.20.254	FE80::31	2620:FC:0:D368:20::254	-	Area 88	
		VLAN 21	Wireless Guest	-	10.3.21.254	FE80::31	2620:FC:0:D368:21::254	-	Area 88	
		VLAN 25	Voice	-	10.3.25.254	FE80::31	2620:FC:0:D368:25::254	-	Area 88	
		VLAN 100	Data	-	10.3.100.254	FE80::31	2620:FC:0:D368:100::254	-	Area 88	
		VLAN 150	Management	-	10.3.150.254	FE80::31	2620:FC:0:D368:150::254	-	Area 88	
		Lo110	Loopback	-	10.3.110.254	-	-	-	Area 88	
		Lo250	Loopback 250 for NTP	-	10.3.250.254/32	-	-	-	Area 88	
Dominion Greenhouses IPv4 Range : 172.31.133.50-69				VLANS						
50	Outside interface of Headquarters			20	Wireless-Secured	10.x.20.0/24				
53	HQ-Management-Host (RDP)			21	Wireless-Guest	10.x.21.0/24				
60	Outside interface of Manufacturing			25	Voice	10.x.25.0/24				
63	MP-Management-Host (RDP)			50	Servers	10.x.50.0/24				
65	Outside interface of Warehouse			100-124	Data	10.x.100-149.0/24				
68	WH-Management-Host (RDP)			125	VDI	10.2.125.0/24				
				150	Management	10.x.150.0/24				
				200	Thin Clients	10.x.200.0/24				
Domain: DominionGreenHouses.com										
Dominion Greenhouses IPv6 Range : 2620:fc:0:d307::(5-6)(8-B or C-F)										

Appendix C: Quantitative Risk Analysis

Table C.I: Mitigated Results for Residual Risk

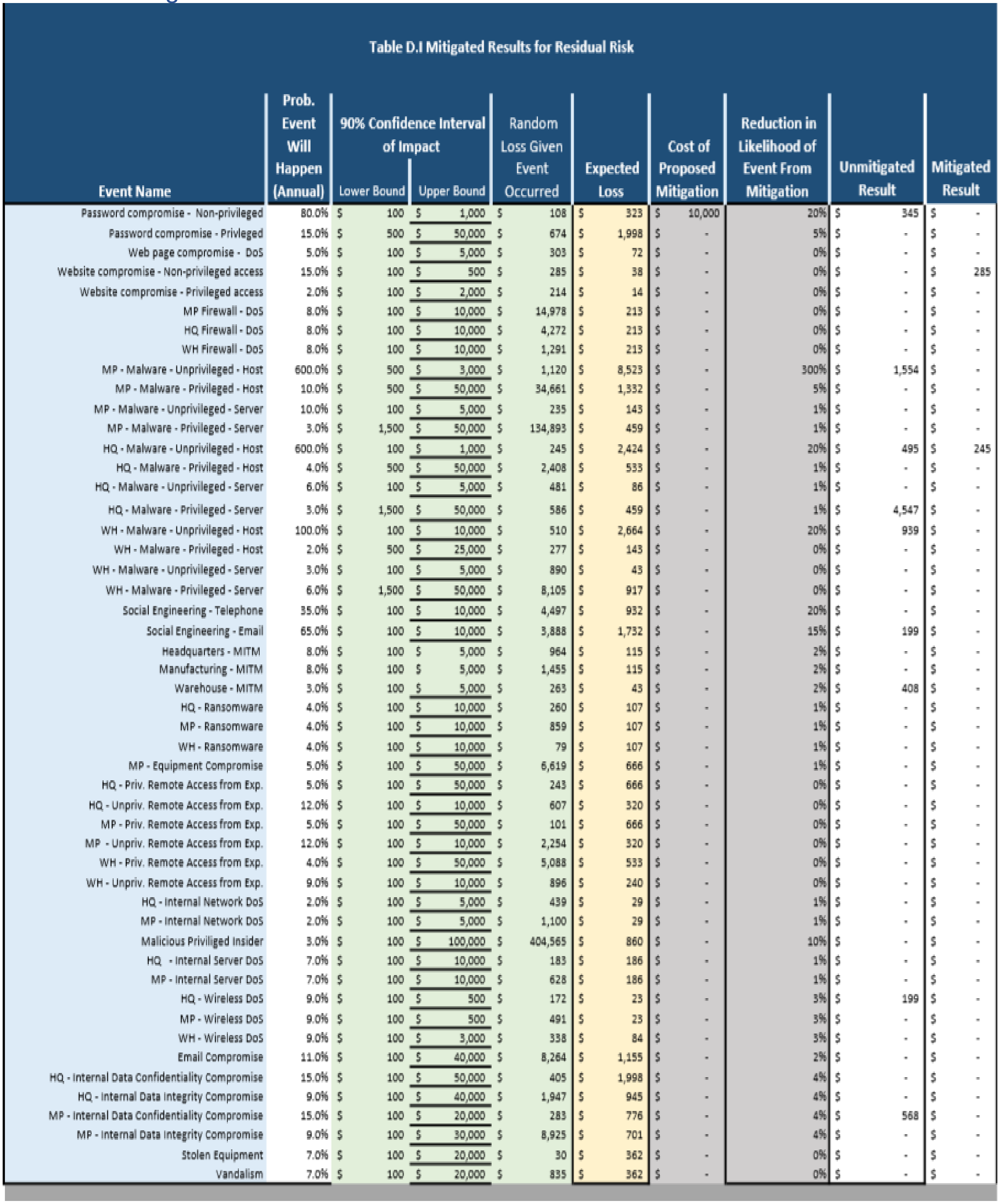


Table D.I Mitigated Results for Residual Risk

Event Name	Prob. Event Will Happen (Annual)	90% Confidence Interval of Impact		Random Loss Given Event Occurred	Expected Loss	Cost of Proposed Mitigation	Reduction in Likelihood of Event From Mitigation	Unmitigated Result	Mitigated Result
		Lower Bound	Upper Bound						
Password compromise - Non-privileged	80.0%	$ 100	$ 1,000	$ 108	$ 323	$ 10,000	20%	$ 345	$ -
Password compromise - Privleged	15.0%	$ 500	$ 50,000	$ 674	$ 1,998	$ -	5%	$ -	$ -
Web page compromise - DoS	5.0%	$ 100	$ 5,000	$ 303	$ 72	$ -	0%	$ -	$ -
Website compromise - Non-privileged access	15.0%	$ 100	$ 500	$ 285	$ 38	$ -	0%	$ -	$ 285
Website compromise - Privileged access	2.0%	$ 100	$ 2,000	$ 214	$ 14	$ -	0%	$ -	$ -
MP Firewall - DoS	8.0%	$ 100	$ 10,000	$ 14,978	$ 213	$ -	0%	$ -	$ -
HQ Firewall - DoS	8.0%	$ 100	$ 10,000	$ 4,272	$ 213	$ -	0%	$ -	$ -
WH Firewall - DoS	8.0%	$ 100	$ 10,000	$ 1,291	$ 213	$ -	0%	$ -	$ -
MP - Malware - Unprivileged - Host	600.0%	$ 500	$ 3,000	$ 1,120	$ 8,523	$ -	300%	$ 1,554	$ -
MP - Malware - Privileged - Host	10.0%	$ 500	$ 50,000	$ 34,661	$ 1,332	$ -	5%	$ -	$ -
MP - Malware - Unprivileged - Server	10.0%	$ 100	$ 5,000	$ 235	$ 143	$ -	1%	$ -	$ -
MP - Malware - Privileged - Server	3.0%	$ 1,500	$ 50,000	$ 134,893	$ 459	$ -	1%	$ -	$ -
HQ - Malware - Unprivileged - Host	600.0%	$ 100	$ 1,000	$ 245	$ 2,424	$ -	20%	$ 495	$ 245
HQ - Malware - Privileged - Host	4.0%	$ 500	$ 50,000	$ 2,408	$ 533	$ -	1%	$ -	$ -
HQ - Malware - Unprivileged - Server	6.0%	$ 100	$ 5,000	$ 481	$ 86	$ -	1%	$ -	$ -
HQ - Malware - Privileged - Server	3.0%	$ 1,500	$ 50,000	$ 586	$ 459	$ -	1%	$ 4,547	$ -
WH - Malware - Unprivileged - Host	100.0%	$ 100	$ 10,000	$ 510	$ 2,664	$ -	20%	$ 939	$ -
WH - Malware - Privileged - Host	2.0%	$ 500	$ 25,000	$ 277	$ 143	$ -	0%	$ -	$ -
WH - Malware - Unprivileged - Server	3.0%	$ 100	$ 5,000	$ 890	$ 43	$ -	0%	$ -	$ -
WH - Malware - Privileged - Server	6.0%	$ 1,500	$ 50,000	$ 8,105	$ 917	$ -	0%	$ -	$ -
Social Engineering - Telephone	35.0%	$ 100	$ 10,000	$ 4,497	$ 932	$ -	20%	$ -	$ -
Social Engineering - Email	65.0%	$ 100	$ 10,000	$ 3,888	$ 1,732	$ -	15%	$ 199	$ -
Headquarters - MITM	8.0%	$ 100	$ 5,000	$ 964	$ 115	$ -	2%	$ -	$ -
Manufacturing - MITM	8.0%	$ 100	$ 5,000	$ 1,455	$ 115	$ -	2%	$ -	$ -
Warehouse - MITM	3.0%	$ 100	$ 5,000	$ 263	$ 43	$ -	2%	$ 408	$ -
HQ - Ransomware	4.0%	$ 100	$ 10,000	$ 260	$ 107	$ -	1%	$ -	$ -
MP - Ransomware	4.0%	$ 100	$ 10,000	$ 859	$ 107	$ -	1%	$ -	$ -
WH - Ransomware	4.0%	$ 100	$ 10,000	$ 79	$ 107	$ -	1%	$ -	$ -
MP - Equipment Compromise	5.0%	$ 100	$ 50,000	$ 6,619	$ 666	$ -	1%	$ -	$ -
HQ - Priv. Remote Access from Exp.	5.0%	$ 100	$ 50,000	$ 243	$ 666	$ -	0%	$ -	$ -
HQ - Unpriv. Remote Access from Exp.	12.0%	$ 100	$ 10,000	$ 607	$ 320	$ -	0%	$ -	$ -
MP - Priv. Remote Access from Exp.	5.0%	$ 100	$ 50,000	$ 101	$ 666	$ -	0%	$ -	$ -
MP - Unpriv. Remote Access from Exp.	12.0%	$ 100	$ 10,000	$ 2,254	$ 320	$ -	0%	$ -	$ -
WH - Priv. Remote Access from Exp.	4.0%	$ 100	$ 50,000	$ 5,088	$ 533	$ -	0%	$ -	$ -
WH - Unpriv. Remote Access from Exp.	9.0%	$ 100	$ 10,000	$ 896	$ 240	$ -	0%	$ -	$ -
HQ - Internal Network DoS	2.0%	$ 100	$ 5,000	$ 439	$ 29	$ -	1%	$ -	$ -
MP - Internal Network DoS	2.0%	$ 100	$ 5,000	$ 1,100	$ 29	$ -	1%	$ -	$ -
Malicious Priviliged Insider	3.0%	$ 100	$ 100,000	$ 404,565	$ 860	$ -	10%	$ -	$ -
HQ - Internal Server DoS	7.0%	$ 100	$ 10,000	$ 183	$ 186	$ -	1%	$ -	$ -
MP - Internal Server DoS	7.0%	$ 100	$ 10,000	$ 628	$ 186	$ -	1%	$ -	$ -
HQ - Wireless DoS	9.0%	$ 100	$ 500	$ 172	$ 23	$ -	3%	$ 199	$ -
MP - Wireless DoS	9.0%	$ 100	$ 500	$ 491	$ 23	$ -	3%	$ -	$ -
WH - Wireless DoS	9.0%	$ 100	$ 3,000	$ 338	$ 84	$ -	3%	$ -	$ -
Email Compromise	11.0%	$ 100	$ 40,000	$ 8,264	$ 1,155	$ -	2%	$ -	$ -
HQ - Internal Data Confidentiality Compromise	15.0%	$ 100	$ 50,000	$ 405	$ 1,998	$ -	4%	$ -	$ -
HQ - Internal Data Integrity Compromise	9.0%	$ 100	$ 40,000	$ 1,947	$ 945	$ -	4%	$ -	$ -
MP - Internal Data Confidentiality Compromise	15.0%	$ 100	$ 20,000	$ 283	$ 776	$ -	4%	$ 568	$ -
MP - Internal Data Integrity Compromise	9.0%	$ 100	$ 30,000	$ 8,925	$ 701	$ -	4%	$ -	$ -
Stolen Equipment	7.0%	$ 100	$ 20,000	$ 30	$ 362	$ -	0%	$ -	$ -
Vandalism	7.0%	$ 100	$ 20,000	$ 835	$ 362	$ -	0%	$ -	$ -

Table C.II/DIII Residual and Inherent Risk

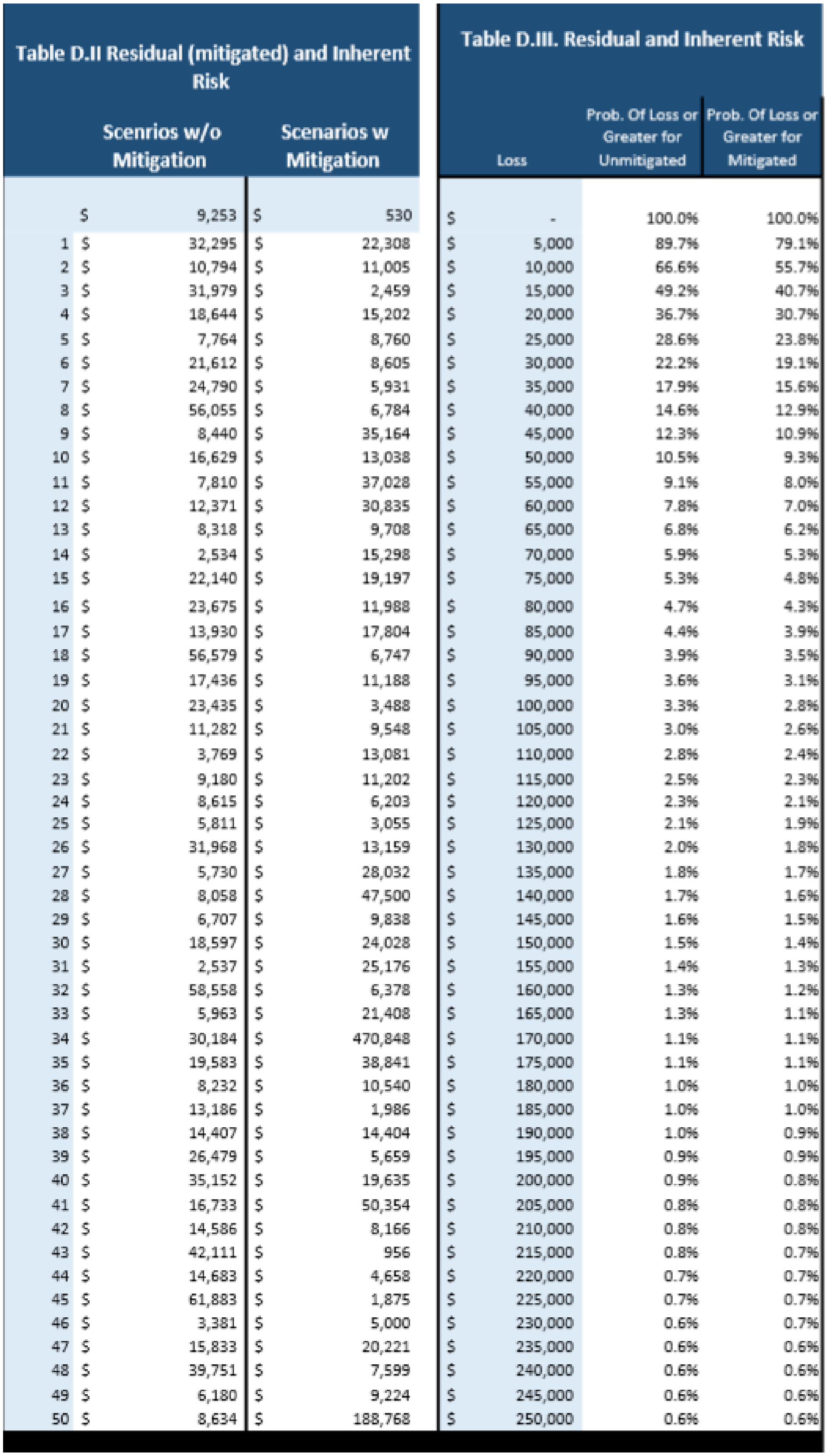


	Table D.II Residual (mitigated) and Inherent Risk		Table D.III. Residual and Inherent Risk		
	Scenrios w/o Mitigation	Scenarios w Mitigation	Loss	Prob. Of Loss or Greater for Unmitigated	Prob. Of Loss or Greater for Mitigated
	$ 9,253	$ 530	$ -	100.0%	100.0%
1	$ 32,295	$ 22,308	$ 5,000	89.7%	79.1%
2	$ 10,794	$ 11,005	$ 10,000	66.6%	55.7%
3	$ 31,979	$ 2,459	$ 15,000	49.2%	40.7%
4	$ 18,644	$ 15,202	$ 20,000	36.7%	30.7%
5	$ 7,764	$ 8,760	$ 25,000	28.6%	23.8%
6	$ 21,612	$ 8,605	$ 30,000	22.2%	19.1%
7	$ 24,790	$ 5,931	$ 35,000	17.9%	15.6%
8	$ 56,055	$ 6,784	$ 40,000	14.6%	12.9%
9	$ 8,440	$ 35,164	$ 45,000	12.3%	10.9%
10	$ 16,629	$ 13,038	$ 50,000	10.5%	9.3%
11	$ 7,810	$ 37,028	$ 55,000	9.1%	8.0%
12	$ 12,371	$ 30,835	$ 60,000	7.8%	7.0%
13	$ 8,318	$ 9,708	$ 65,000	6.8%	6.2%
14	$ 2,534	$ 15,298	$ 70,000	5.9%	5.3%
15	$ 22,140	$ 19,197	$ 75,000	5.3%	4.8%
16	$ 23,675	$ 11,988	$ 80,000	4.7%	4.3%
17	$ 13,930	$ 17,804	$ 85,000	4.4%	3.9%
18	$ 56,579	$ 6,747	$ 90,000	3.9%	3.5%
19	$ 17,436	$ 11,188	$ 95,000	3.6%	3.1%
20	$ 23,435	$ 3,488	$ 100,000	3.3%	2.8%
21	$ 11,282	$ 9,548	$ 105,000	3.0%	2.6%
22	$ 3,769	$ 13,081	$ 110,000	2.8%	2.4%
23	$ 9,180	$ 11,202	$ 115,000	2.5%	2.3%
24	$ 8,615	$ 6,203	$ 120,000	2.3%	2.1%
25	$ 5,811	$ 3,055	$ 125,000	2.1%	1.9%
26	$ 31,968	$ 13,159	$ 130,000	2.0%	1.8%
27	$ 5,730	$ 28,032	$ 135,000	1.8%	1.7%
28	$ 8,058	$ 47,500	$ 140,000	1.7%	1.6%
29	$ 6,707	$ 9,838	$ 145,000	1.6%	1.5%
30	$ 18,597	$ 24,028	$ 150,000	1.5%	1.4%
31	$ 2,537	$ 25,176	$ 155,000	1.4%	1.3%
32	$ 58,558	$ 6,378	$ 160,000	1.3%	1.2%
33	$ 5,963	$ 21,408	$ 165,000	1.3%	1.1%
34	$ 30,184	$ 470,848	$ 170,000	1.1%	1.1%
35	$ 19,583	$ 38,841	$ 175,000	1.1%	1.1%
36	$ 8,232	$ 10,540	$ 180,000	1.0%	1.0%
37	$ 13,186	$ 1,986	$ 185,000	1.0%	1.0%
38	$ 14,407	$ 14,404	$ 190,000	1.0%	0.9%
39	$ 26,479	$ 5,659	$ 195,000	0.9%	0.9%
40	$ 35,152	$ 19,635	$ 200,000	0.9%	0.8%
41	$ 16,733	$ 50,354	$ 205,000	0.8%	0.8%
42	$ 14,586	$ 8,166	$ 210,000	0.8%	0.8%
43	$ 42,111	$ 956	$ 215,000	0.8%	0.7%
44	$ 14,683	$ 4,658	$ 220,000	0.7%	0.7%
45	$ 61,883	$ 1,875	$ 225,000	0.7%	0.7%
46	$ 3,381	$ 5,000	$ 230,000	0.6%	0.7%
47	$ 15,833	$ 20,221	$ 235,000	0.6%	0.6%
48	$ 39,751	$ 7,599	$ 240,000	0.6%	0.6%
49	$ 6,180	$ 9,224	$ 245,000	0.6%	0.6%
50	$ 8,634	$ 188,768	$ 250,000	0.6%	0.6%

Figure C.I: Inherent Risk, Residual Risk and Risk Tolerance

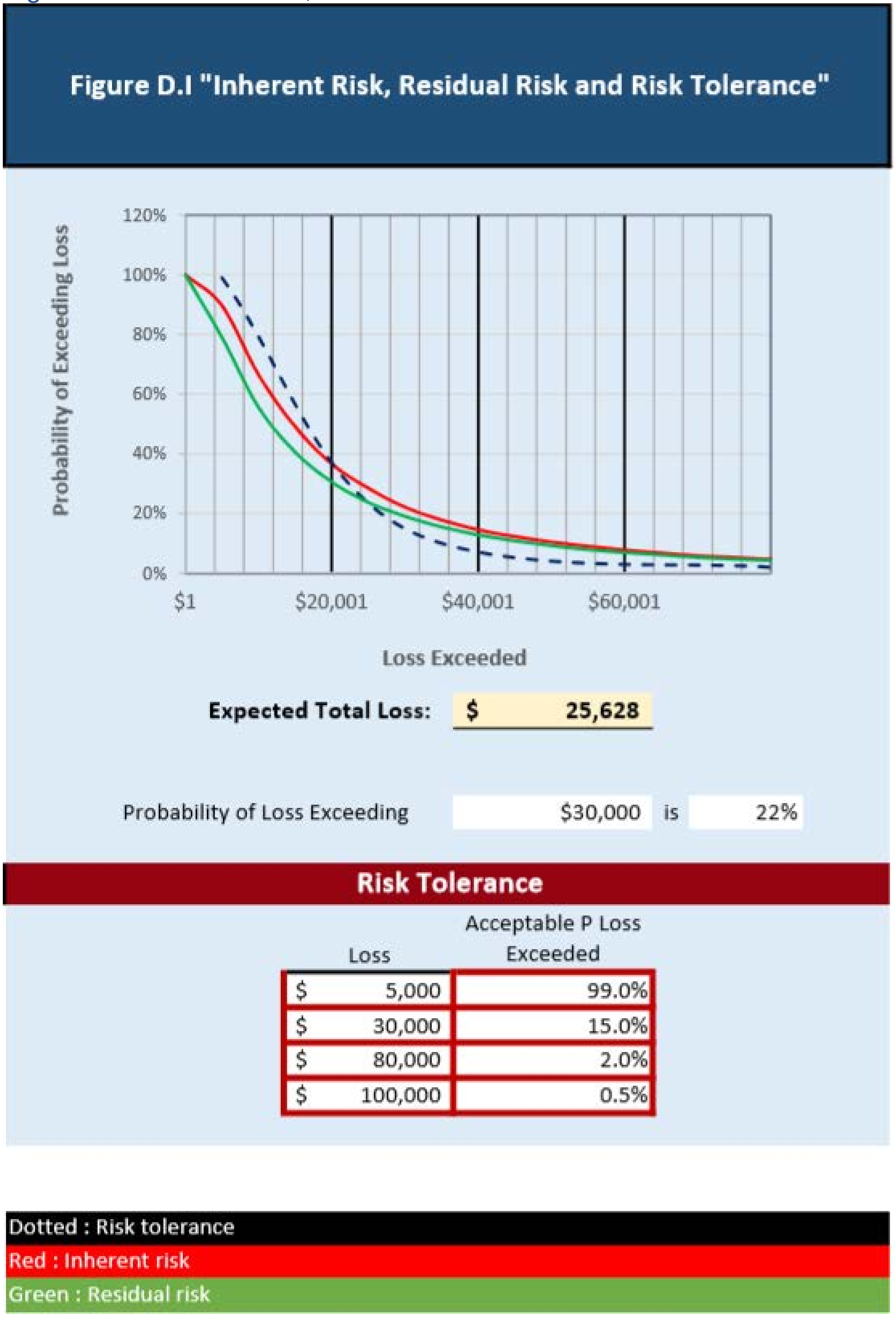


Figure D.I "Inherent Risk, Residual Risk and Risk Tolerance"

Expected Total Loss: **$ 25,628**

Probability of Loss Exceeding $30,000 is 22%

Risk Tolerance

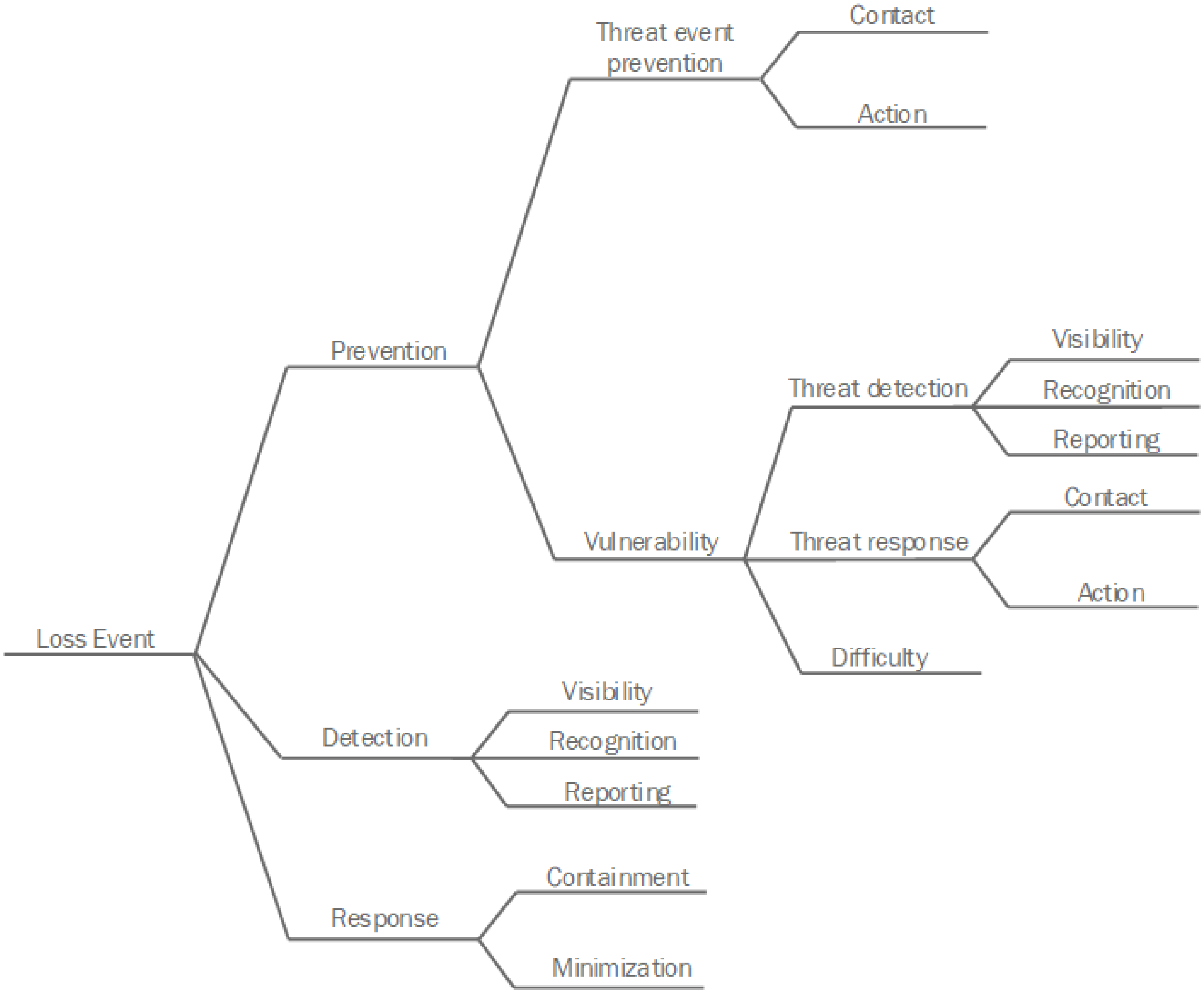
Loss	Acceptable P Loss Exceeded
$ 5,000	99.0%
$ 30,000	15.0%
$ 80,000	2.0%
$ 100,000	0.5%

Dotted : Risk tolerance

Red : Inherent risk

Green : Residual risk

Figure C.II Defense in-depth Analysis



Measuring and Managing Information Risk. pg. 252.

Appendix D: Support Documentation and Resources

Visit the NetEng Tech Solutions Website and Github page for freely available scripts and resources including the script to add users to Active Directory from a csv file, a script to check files for non-ASCII characters and a Python script that uses the Netmiko library to send bulk secure configuration and monitoring commands to network devices: **https://github.com/netengtechsolutions**

D.I Python Bulk Network Configuration Script

A Python script that uses the netmiko library to send bulk backup, show or configuration commands to network devices.
SSH access to each device is required from the station that is running the script.
Structures for network devices are hard-coded from Line 34-117.

bulknetwork.py

```
"""
    Title:      bulknetwork.py
    Desc:        Send bulk network commands to devices with netmiko
    Date:       March 2, 2019
    Version:    1.3
    Python Ver: 3.6.8
    Writer:         Darren Sylvain

"""

import sys
import getopt
from netmiko import ConnectHandler
from datetime import datetime
from getpass import getpass
import random

# netmiko : multi-vendor library to simplify Paramiko SSH connections to network devices :
https://github.com/ktbyers/netmiko
# datetime : used to determine and print out how long a function takes to run
# getpass : allows the script to ask for the password when it runs rather than hardcoding it here
#   request the password from user
# random is used to generate a value to tack onto the end of the save name when saved to
flash, because
#   the script chokes if a file with same name already exists
password = getpass()

# create a dictionary representing each device
# supported device_types can be found on the github page
# global_delay_factor tells Netmiko to wait longer than default (default ~100seconds) for the
command to complete
#   global_delay_factor=2 doubles the value of ALL delays. (delay_factor=2 would have doubled
only delays after send_command
#   which would likely work as well but I'm not in a hurry)
# Device Naming convention <Location>_<(C)ore|(D)istribution|(A)ccess>_<Device><Device#>
# TODO: use sqlite for device dictionaries so this can be removed from the script
HQ_A_SW1 = {
	'device_type': 'cisco_ios',
	'ip': '10.1.150.10',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}
HQ_A_SW2 = {
	'device_type': 'cisco_ios',
	'ip': '10.1.150.11',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}
HQ_D_SW1 = {
	'device_type': 'cisco_ios',
	'ip': '10.1.250.250',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}
HQ_D_SW2 = {
	'device_type': 'cisco_ios',
	'ip': '10.1.250.252',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}
HQ_C_FW1 = {
	'device_type': 'cisco_asa',
	'ip': '10.1.200.6',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}
MP_A_SW1 = {
	'device_type': 'cisco_ios',
	'ip': '10.2.150.10',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}
MP_A_SW2 = {
	'device_type': 'cisco_ios',
	'ip': '10.2.150.11',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}
MP_D_R1 = {
	'device_type': 'cisco_ios',
	'ip': '10.2.250.250',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}
MP_D_R2 = {
	'device_type': 'cisco_ios',
	'ip': '10.2.250.252',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}
MP_C_FW1 = {
	'device_type': 'cisco_asa',
	'ip': '172.31.133.60',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}
WH_A_SW1 = {
	'device_type': 'cisco_ios',
	'ip': '10.3.250.254',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}
WH_C_FW1 = {
	'device_type': 'cisco_asa',
	'ip': '172.31.133.65',
	'username': 'trogdor',
	'password': password,
	'global_delay_factor': 2,
}

#Temporary bunch of lists and strings. The strings are used to print information about which device is being connected to by Netmiko
HQ_network_devices = [HQ_A_SW1, HQ_A_SW2, HQ_D_SW1, HQ_D_SW2]
HQ_network_devices_strings = ['HQ_A_SW1', 'HQ_A_SW2', 'HQ_D_SW1', 'HQ_D_SW2']
MP_network_devices = [MP_A_SW1, MP_A_SW2, MP_D_R1, MP_D_R2]
MP_network_devices_strings = ['MP_A_SW1', 'MP_A_SW2', 'MP_D_R1', 'MP_D_R2']
WH_network_devices = [WH_A_SW1]
WH_network_devices_strings = ['WH_A_SW1']
all_network_devices = [HQ_A_SW1, HQ_A_SW2, HQ_D_SW1, HQ_D_SW2, MP_A_SW1, MP_A_SW2, MP_D_R1, MP_D_R2, WH_A_SW1]
all_network_devices_strings = ['HQ_A_SW1', 'HQ_A_SW2', 'HQ_D_SW1', 'HQ_D_SW2', 'MP_A_SW1', 'MP_A_SW2', 'MP_D_R1', 'MP_D_R2', 'WH_A_SW1']
all_firewalls = [HQ_C_FW1, MP_C_FW1, WH_C_FW1]
all_firewalls_strings = ['HQ_C_FW1', 'MP_C_FW1', 'WH_C_FW1']
```

```
HQ_firewalls = [HQ_C_FW1]
HQ_firewalls_strings = ['HQ_C_FW1']
MP_firewalls = [MP_C_FW1]
MP_firewalls_strings = ['MP_C_FW1']
WH_firewalls = [WH_C_FW1]
WH_firewalls_strings = ['WH_C_FW1']

#Pretty much all functions use total_time = end_time - start_time just to time the function call
#The ssh connections are handled by ConnectHandler, devices require ssh access

def configure(devices, devices_strings, cmd):
    #Send a single configuration command to the device
    #This could be modified to accept multiple commands but cmd would have to be passed as a
list
    #   of strings, and then the 'config_commands = [cmd]' command can be omitted.
    start_time = datetime.now()
    i = 0
    for each_device in devices:
        net_connect = ConnectHandler(**each_device)
        print (f'Connecting to {devices_strings[i]} and sending \'{cmd}\'')
        config_commands = [cmd]
        output = net_connect.send_config_set(config_commands)
        print(f"\n\n========Device {devices_strings[i]}-{each_device['device_type']} ========")
        i = i + 1
        print(output)
        print("++++++++ End ++++++++")
    end_time = datetime.now()
    total_time = end_time - start_time
    print(f'configure duration : {total_time}')

def show(devices, devices_strings, cmd):
    start_time = datetime.now()
    i = 0
    for each_device in devices:
        net_connect = ConnectHandler(**each_device)
        print (f'Connecting to {devices_strings[i]} and sending \'{cmd}\'')
        output = net_connect.send_command(cmd)
        #print header
        print(f"\n\n========Device {devices_strings[i]}-{each_device['device_type']} ========")
        i = i + 1
        print(output)
        print("++++++++ End ++++++++")
    end_time = datetime.now()
    total_time = end_time - start_time
    print(f'configure duration : {total_time}')

def backup_firewalls_flash(firewalls, firewalls_strings):
    start_time = datetime.now()
    randvalue = random.randint(1,100000)
    i = 0
    for each_firewall in firewalls:
        net_connect = ConnectHandler(**each_firewall)
        print (f"\nConnecting to {firewalls_strings[i]} and sending backup to flash command")
        cmd = f'copy run disk0:/backup_config_{start_time.month}_{start_time.day}_{randvalue}'
        output = net_connect.send_command(
                cmd,
                expect_string=r'Source filename'
                )
        output += net_connect.send_command('\n', expect_string=r'Destination filename')
        output += net_connect.send_command('\n', expect_string=r'#')
        print(f"\n\n========Device {firewalls_strings[i]}-{each_firewall['device_type']} ========")
        i = i + 1
        print(output)
        print("++++++++ End ++++++++")
    end_time = datetime.now()
    total_time = end_time - start_time
    print(f'backup_firewalls_flash duration : {total_time}')

def backup_network_devices_flash(network_devices, network_devices_strings):
    start_time = datetime.now()
    randvalue = random.randint(1,100000)
    i = 0
    for each_device in network_devices:
        net_connect = ConnectHandler(**each_device)
        print (f"\nConnecting to {network_devices_strings[i]} and sending backup to flash
command")
        cmd = f'copy run flash:/backup_config_{start_time.month}_{start_time.day}_{randvalue}'
        output = net_connect.send_command(
                cmd,
                expect_string=r'Destination filename'
                )
        output += net_connect.send_command('\n', expect_string=r'#')
        print(f"\n\n========Device {network_devices_strings[i]}-{each_device['device_type']}
========")
        i = i + 1
        print(output)
        print("++++++++ End ++++++++")
    end_time = datetime.now()
    total_time = end_time - start_time
    print(f'backup_network_devices_flash duration : {total_time}')

def backup_firewalls_tftp(firewalls, firewalls_strings, tftp_server):
    start_time = datetime.now()
    randvalue = random.randint(1,100000)
    i = 0
    for each_firewall in firewalls:
        net_connect = ConnectHandler(**each_firewall)
        print (f"\nConnecting to {firewalls_strings[i]} and sending backup to tftp command")
        cmd = f'copy running-config tftp:'
        dest_filename =
f'{firewalls_strings[i]}_{start_time.month}_{start_time.day}_{start_time.year}_{randvalue}'
        print (f'Attempting to save config as {dest_filename}')
        output = net_connect.send_command(cmd, expect_string=r'Source filename')
        output += net_connect.send_command('', expect_string=r'Address or name of remote
host')
        output += net_connect.send_command(f'{tftp_server}', expect_string=r'Destination
filename')
        output += net_connect.send_command(f'{dest_filename}', expect_string=r'#')
        print(f"\n\n========Device {firewalls_strings[i]}-{each_firewall['device_type']} ========")
        i = i + 1
        print(output)
        print("++++++++ End ++++++++")
    end_time = datetime.now()
    total_time = end_time - start_time
    print(f'backup_firewalls_tftp duration : {total_time}')

def backup_network_devices_tftp(network_devices, network_devices_strings, tftp_server):
    start_time = datetime.now()
    randvalue = random.randint(1,100000)
    i = 0
    for each_device in network_devices:
        net_connect = ConnectHandler(**each_device)
        print (f"\nConnecting to {network_devices_strings[i]} and sending backup to tftp command")
        cmd = f'copy running-config tftp:'
        dest_filename =
f'{network_devices_strings[i]}_{start_time.month}_{start_time.day}_{start_time.year}_{randvalue}
'
        print (f'Attempting to save config as {dest_filename}')
        output = net_connect.send_command(
                cmd,
                expect_string=r'Address or name of remote host'
                )
        output += net_connect.send_command(f'{tftp_server}', expect_string=r'Destination
filename')
        output += net_connect.send_command(f'{dest_filename}', expect_string=r'#')
        print(f"\n\n========Device {network_devices_strings[i]}-{each_device['device_type']}
========")
        i = i + 1
        print(output)
        print("++++++++ End ++++++++")
    end_time = datetime.now()
    total_time = end_time - start_time
    print(f'backup_network_devices_tftp duration : {total_time}')

def get_command():  #Gets the command to send from the user
    confirm = ''
    while "y" not in confirm:
        cmd = input("Enter command to send to device : ")
        confirm = input(f"Confirm command to send [y|n], X to cancel : {cmd} : ")
        if "y" in confirm:
            print ('Confirmed')
            return(cmd)
        elif "X" in confirm:
            print ('Cancelling')
            return (31)


def device_choice():    #Allows user to select from a predefined set of lists of network devices
    choice = ''
    firewall = ''
    while choice not in [1,2,3,4,5,6,7,8]:
        choice = input(f'''
        Enter a number for which devices should receive backup/configuration
        1) All HQ Network Devices : HQ_A_SW1, HQ_A_SW2, HQ_D_SW1, HQ_D_SW2
        2) All MP Network Devices : MP_A_SW1, MP_A_SW1, MP_D_R1, MP_D_R2
        3) All WH Network Devices : WH_A_SW1
        4) All Network Devices : HQ_A_SW1, HQ_A_SW2, HQ_D_SW1, HQ_D_SW2,
MP_A_SW1, MP_A_SW2, MP_D_R1, MP_D_R2, WH_A_SW1
        5) All Firewalls : HQ_C_FW1, MP_C_FW1, WH_C_FW1
        6) HQ Firewalls : HQ_C_FW1
        7) MP Firewalls : MP_C_FW1
        8) WH Firewalls : WH_C_FW1
        Choice (1-8) : ''')
        choice = int(choice)

        #Firewalls and routers/switches should be kept in separate lists and firewalls should be a
choice
              # that is >= 5 here. Connecting to asa firewalls and switches/routers requires a different
              # function so it's necessary to differentiate between the two
        if choice == 1:
            devices = HQ_network_devices
            device_string = HQ_network_devices_strings
        elif choice == 2:
            devices = MP_network_devices
            device_string = MP_network_devices_strings
        elif choice == 3:
            devices = WH_network_devices
            device_string = WH_network_devices_strings
        elif choice == 4:
            devices = all_network_devices
            device_string = all_network_devices_strings
        elif choice == 5:
            devices = all_firewalls
            device_string = all_firewalls_strings
        elif choice == 6:
            devices = HQ_firewalls
            device_string = HQ_firewalls_strings
        elif choice == 7:
            choice = MP_firewalls
            device_string = MP_firewalls_strings
        elif choice == 8:
            devices = WH_firewalls
            device_string = WH_firewalls_strings
    if choice >= 5:
      firewall = True
   return (devices, device_string, firewall)

def backup_or_send():   #Allows user to select yes or no to if they want to perform a backup
   backup = input('Perform backup [y] or enter custom command [n] : ')
   if 'y' in backup:
      return True
   else:
      return False

def get_backup_type():  #Allows user to enter backup types from a set of options
   choice = ''
   flash = False
   tftp = False
   while choice not in [1,2,3]:
      choice = input(f'''
         What type of backup?
         1) flash
         2) tftp
         3) both
         Choice (1-3) : ''')
      choice = int(choice)

      if choice == 1:
         flash = True
      elif choice == 2:
         tftp = True
      elif choice == 3:
         flash = True
         tftp = True
   return (flash,tftp)

def main():
   backup = backup_or_send()   #Check if user wants to back up devices or send a
configuration or read command
   (devices, device_string, firewall) = device_choice()    #Allows user to select targeted devices

   if backup:
      (flash,tftp) = get_backup_type()    #get_backup_type returns booleans for flash and tftp
      if flash:
         if firewall:    #firewalls had to be separated out because they use disk0:/ instead of
flash0:/ and the prompts are different
            backup_firewalls_flash(devices, device_string)
         else:
            backup_network_devices_flash(devices, device_string)
      if tftp:
         tftp_server = input("Enter IP address of tftp server : ")
         if firewall:
            backup_firewalls_tftp(devices, device_string, tftp_server)
         else:
            backup_network_devices_tftp(devices, device_string, tftp_server)
```

```
        sys.exit(42)

    if not backup:  #if not a backup assume the user wants to send a configuration or read
command
        command = get_command() #allow user to enter command
        if isinstance(command, str):    #make sure user entered a valid string and an error wasn't
returned
            if command.startswith('show'):
                show(devices, device_string, command)
            else:
                configure(devices, device_string, command)
        else:
            sys.exit(31)

if __name__ == "__main__":
    main()
```

E.II Demo of bulknet.py Script

```
C:\Users\trogdor\Desktop\bulknetwork-master>bulknet.py
Password:
Perform backup [y] or enter custom command [n] : n

        Enter a number for which devices should receive backup/configuration
        1) All HQ Network Devices : HQ_A_SW1, HQ_A_SW2, HQ_D_SW1, HQ_D_SW2
        2) All MP Network Devices : MP_A_SW1, MP_A_SW1, MP_D_R1, MP_D_R2
        3) All WH Network Devices : WH_A_SW1
        4) All Network Devices : HQ_A_SW1, HQ_A_SW2, HQ_D_SW1, HQ_D_SW2,
MP_A_SW1, MP_A_SW2, MP_D_R1, MP_D_R2, WH_A_SW1
        5) All Firewalls : HQ_C_FW1, MP_C_FW1, WH_C_FW1
        6) HQ Firewalls : HQ_C_FW1
        7) MP Firewalls : MP_C_FW1
        8) WH Firewalls : WH_C_FW1
        Choice (1-8) : 4
Enter command to send to device : show run | include service password-encryption
Confirm command to send [y|n], X to cancel : show run | include service password-encryption :
y
Confirmed
Connecting to HQ_A_SW1 and sending 'show run | include service password-encryption'


========Device HQ_A_SW1-cisco_ios ========
service password-encryption
++++++++ End ++++++++

Connecting to HQ_A_SW2 and sending 'show run | include service password-encryption'
========Device HQ_A_SW2-cisco_ios ========
service password-encryption
++++++++ End ++++++++

Connecting to HQ_D_SW1 and sending 'show run | include service password-encryption'
========Device HQ_D_SW1-cisco_ios ========
service password-encryption
++++++++ End ++++++++

Connecting to HQ_D_SW2 and sending 'show run | include service password-encryption'
========Device HQ_D_SW2-cisco_ios ========
service password-encryption
++++++++ End ++++++++

Connecting to MP_A_SW1 and sending 'show run | include service password-encryption'
========Device MP_A_SW1-cisco_ios ========
service password-encryption
++++++++ End ++++++++

Connecting to MP_A_SW2 and sending 'show run | include service password-encryption'
========Device MP_A_SW2-cisco_ios ========
service password-encryption
```

```
+++++++++ End +++++++++

Connecting to MP_D_R1 and sending 'show run | include service password-encryption'
========Device MP_D_R1-cisco_ios ========
service password-encryption
+++++++++ End +++++++++

Connecting to MP_D_R2 and sending 'show run | include service password-encryption'
========Device MP_D_R2-cisco_ios ========
service password-encryption
+++++++++ End +++++++++

Connecting to WH_A_SW1 and sending 'show run | include service password-encryption'
========Device WH_A_SW1-cisco_ios ========
service password-encryption
+++++++++ End +++++++++
configure duration : 0:01:37.798064
```

E.III Find Non-Ascii Characters

ImportUserstoAD_2.1.ps1 does not like non-ascii characters. This script will find lines with non-ascii characters and print them out with a line number so they can be manually changed before running ImportUserstoAD_v2_1.ps1

findnonascii.py

```
#  Darren Sylvain
#  March 31, 2019
#  Search a .csv file for non-ascii characters
# This requires python3.7 because the isascii() function is new to 3.7

import sys

CRED = '\033[91m'
CEND = '\033[0m'

def usage():
    print(CRED + "Usage : python3.7 findnonascii.py <file>" + CEND)

#############Script start#############


def main():
    if len(sys.argv) < 2:
        usage()
        quit()

    FILE = sys.argv[1]
    print("File is " + FILE)

    try:
        fd = open(FILE, 'r')
    except:
        fd = None
        print("Error opening file")

    linenumber = 0

    for line in fd:
        linenumber = linenumber + 1
        if not line.isascii():
            print(f"Line {linenumber} : {line}")
    fd.close()

if __name__ == "__main__":
    main()
```

E.IV Import Users to Active Directory

A Powershell script to add users to Active Directory while creating the necessary groups and OUs. Creation of Groups and OUs requires user confirmation. Creation of users does not require confirmation. This script checks if the user, group or OU exist before creating any of them and continues if they do, or, offers to create them if they don't. An existing group or OU elicits no message but a message will be printed for an existing User. Existing Users will not be modified in any way.
A few variables are hardcoded, such as domain, user container/path, and credentials (line 8 and lines 163-169).
Use a CSV file with the headings used in 'NETE2980 - Employee Names.csv' where Group1 is the Organizational Unit, Group2 is a primary group and Group3 is an optional secondary group. Additional AD user information can be entered at line 97, like mail addresses etc.. For example, right now it will put all the new users in Company "Dominion Greenhouses". The format of the login name can be modified at lines 92-94. Currently 91 truncates the SamAccountName to 20 chars and removes any spaces in first or last name and joins firstname+lastname to create the User Principal Name.
The provided file is in .xlsx format so one option is to convert it using Excel. CSV files should be checked for non-ascii characters prior to running ImportUserstoAD, one option is to use findnonascii.py.

importUserstoAD_v2_1.ps1

```
#  Darren Sylvain
#  March 23, 2019
#  Starts a remote session to the domain controller and adds users to the domain based on the
contents of a  .csv file

param($FILE)

#Start up the remote session the domain controller
$RPS = New-PSSession -ComputerName WIN-M135PP2325P.dominiongreenhouses.com -
Credential dominiongreenho\administrator
Enter-PSSession $RPS

try {
   $WarningPreference = "SilentlyContinue"                    #Stops errors if modules were already
imported
   Import-PSSession -Session $RPS -Module ActiveDirectory
} catch {}

$WarningPreference = "Inquire"


function Usage {
   Write-Host "Enter a csv file to create users from" -ForegroundColor Red
   Write-Host "`n`Usage: ImportADUsers.ps1 <full\path\to\csvfile>" -ForegroundColor Green
   Exit-PSSession
```

```
    Exit
}

#This function checks if something exists in AD. Returns True or False
#eg. check if OU exists w/ IDENTITY="OU=HQ,DC=dominiongreenhouses,DC=com"
# Check if GROUP exists / IDENTITY="CN=Finance,DC=dominiongreenhouses,DC=com"
function CheckExists ($IDENTITY) {
        if([adsi]::Exists("LDAP://$IDENTITY")) {
            return $True
        } else {
            Write-Host "$IDENTITY does not exist" -ForegroundColor Yellow
            return $False
        }
}

#Creates an Organizational Unit within the Parent Path. Returns True on Success and False on
Failure.
#New-ADOrganizationalUnit returns an empty string even when it completes successfully, so
there's no point checking the return value
function CreateOU ($OU, $PARENT) {
    try {
        New-ADOrganizationalUnit -name $OU -path $PARENT -
ProtectedFromAccidentalDeletion $True -Confirm
        Write-Host "Created $OU in $PARENT" -ForegroundColor Green
        return $True
    } catch {
        Write-Host "Unable to create $OU in $PARENT" -ForegroundColor Red
        Exit-PSSession
        exit
    }
}


#PARENT is hardcoded "DC=dominiongreenhouses,DC=com"
#This function attempts to create the ADGroup and returns the result of the attempt
#New-ADGroup returns nothing even when it completes successfuly so there's no point
checking the return value
function CreateGroup($GROUP, $USER_PATH) {
    try {
        New-ADGroup -Name $GROUP -SamAccountName $GROUP -GroupCategory Security -
GroupScope Global -DisplayName $GROUP -Path $USER_PATH -Description "Created by
ImportUsers.ps1 script"
        Write-Host "$GROUP group created in $USER_PATH" -ForegroundColor Green
        return $True
    } catch {
        $RESULT = $False
        Write-Host "Error creating $GROUP group in $USER_PATH" -ForegroundColor Red
        Exit-PSSession
        exit
    }
}
```

```
#Checks if a useraccount exists by checking the Name variable. Returns True or False and
complains.
function CheckUserExists($FIRST,$LAST) {
    $NAME = "$LAST $FIRST"
    try {
        $RESULT = Get-ADUser -Filter "name -like '$NAME'"
        if ($RESULT) {
            Return $True
        } else {
            Return $False
        }
    }catch {
        Write-Host "Error searching for user $NAME" -ForegroundColor Red
        Return $False
    }
}

#Creates a user with the given parameters. Returns True on success and False on defeat.
#New-ADUser returns nothing on success so the return is not checked
#TESTED
function
CreateUser($FIRSTNAME,$LASTNAME,$PASSWORD,$GROUP,$USER_PATH,$MANAGEM
ENT) {
    try {
        $SAM = "$FIRSTNAME$LASTNAME"
        if ( $SAM.Length -gt 20) { $SAM = $SAM.Substring(0,20) }    #Truncate names to 20 chars
for legacy support. Could have bumped this up because we don't need legacy support.
        $FIRST_TEMP = $FIRSTNAME -replace '\s',''                  #Get rid of whitespace in names
to create the User Principal login name (UPN)
        $LAST_TEMP = $LASTNAME -replace '\s',''
        $UPN = "$FIRST_TEMP$LAST_TEMP"

        #More options could be added here to the New-ADUser command if more detail is
required, eg. email address.
        $DEVNULL = New-ADUser  -Name "$LASTNAME $FIRSTNAME" -UserPrincipalName
$UPN -SamAccountName $SAM -GivenName "$FIRSTNAME $LASTNAME" -Surname
$LASTNAME -DisplayName $SAM -Department $OU -Company "Dominion Greenhouses" -
AccountPassword (ConvertTo-SecureString $PASSWORD -AsPlainText -Force) -
ChangePasswordAtLogon $true -Path "$USER_PATH" -Enabled $true
        $Message = 'User Firstname:{0}, LastName:{1}, PATH:{2}, GROUP:{3}, Management: {4}
created' -f $FIRSTNAME,$LASTNAME,$USER_PATH,$GROUP,$MANAGEMENT
        Write-Host $Message -ForegroundColor Green
        Add-ADGroupMember $GROUP -Members $SAM
        #If the Management flag is true add the user to the Management group
        if ( $MANAGEMENT ) {
            $DEVNULL = Add-ADGroupMember "Management" -Members $SAM
        }
        return $True
    } catch {
        $Message = 'Error creating User Firstname:{0}, LastName:{1}, PATH:{2}, GROUP:{3},
Management: {4}' -f $FIRSTNAME,$LASTNAME,$USER_PATH,$GROUP,$MANAGEMENT
        Write-Host $Message -ForegroundColor Red
        Exit-PSSession
        exit
    }
}

#Checks if the given file is readable, yells otherwise.
function CheckReadable($FILE) {
    #check if file exists, otherwise print Usage and exit
    if ( Test-Path $FILE ) {
        try {
            [System.IO.File]::OpenRead($FILE).Close()
            Return $true
        } catch {
            Write-Host "$FILE is not readable" -ForegroundColor Red
            Return $false
        }
    } else {    #Test-Path $FILE has failed
        Write-Host "File doesn't exist" -ForegroundColor Red
        Return $false
    }
}



######################Script start############################


#If no file is passed on the command line print Usage and exit
if (!$FILE) { Usage }

$READABLE = CheckReadable($FILE)
if ( -not ($READABLE) ) {
    usage
    Write-Host "Exiting" -ForegroundColor Red
}

$CSVFILE = Import-Csv $FILE
ForEach ( $LINE in $CSVFile ) {
    $FIRSTNAME = $LINE."First Name"     #Read user first name from column labeled 'First
Name'
    $LASTNAME = $LINE."Last Name"       #Read user last name from column labeled 'Last
Name'
    $PASSWORD = $LINE.Password        #Read user password from column labeled 'Password'
    $OU = $LINE.Group1               #Read user Organizational Unit from column labeled 'OU'
    $MAINGROUP = $LINE.Group2          #Read user Main Group from column labeled 'Group2'
    $SPECIALGROUP = $LINE.Group3      #Read user Special Group from column labeled
'Group3'
```

```
  #TRIM all the strings that have been read from the CSV
  $FIRSTNAME = $FIRSTNAME.Trim()
  $LASTNAME = $LASTNAME.Trim()
  $PASSWORD = $PASSWORD.Trim()
  $OU = $OU.Trim()
  $MAINGROUP = $MAINGROUP.Trim()
  $SPECIALGROUP = $SPECIALGROUP.Trim()

  $PARENT='DC=dominiongreenhouses,DC=com'
  $OU_IDENTITY = "OU=$OU,$PARENT"     #The OU_IDENTITY is the full path of the OU
  $USER_PATH = "CN=Users,$PARENT"    #The user group path is created in the PARENT
path in Users
  $MAINGROUP_IDENTITY = "CN=$MAINGROUP,$USER_PATH"
  $SPECIALGROUP_IDENTITY = "CN=$SPECIALGROUP,$USER_PATH"
  $GIVENNAME = "$FIRSTNAME $LASTNAME"
  $USER_IDENTITY = "CN=$GIVENNAME,$USER_PATH"


  #CheckOUExists takes the full path of an OU and returns True or False
  #Eg. OU_IDENTITY="OU=HQ,DC=dominiongreenhouses,DC=com"
  $OU_EXISTS = CheckExists "$OU_IDENTITY"
  if( -not ($OU_EXISTS) ) {                              #If the OU does not exist, prompt to
see if the the OU should be created
    $SHOULD_CREATE_OU = Read-host -Prompt "Create $OU_IDENTITY? [y|n]"
    if($SHOULD_CREATE_OU -eq "y") {                           #If 'y' create the OU, any
other entry stops the script
      try {
        CreateOU "$OU" "$PARENT"                              #eg. CreateOU "HQ"
"DC=dominiongreenhouses,DC=com"
      } catch {
        Write-Host "Error creating OU $OU in Parent $PARENT. Exiting."
        Exit-PSSession                                  #Exit the session before exiting the
script
        exit
      }
    } else {
        Write-Host "Exiting. Cannot create users in undefined AD Organizational Units"
        Exit-PSSession                                  #Exit the session before exiting the
script
        exit
    }
  }

  #Check if the current Group exists. CheckExists takes the GROUP name and the PATH to
the group in the form of $PATH='CN=USERS,DC=dominiongreenhouses,DC=com'.
  $GROUP_EXISTS = CheckExists "$MAINGROUP_IDENTITY"                    #CheckExists
"CN=Finance,CN=Users,DC=dominiongreenhouses,DC=com"

  if ( -not ($GROUP_EXISTS) ) {                              #If the GROUP does not exist,
should it be created?
```

```
        $SHOULD_CREATE_GROUP = Read-Host -Prompt "Group $MAINGROUP for
$FIRSTNAME $LASTNAME does not exist. Create group $MAINGROUP_IDENTITY ? [y|n]"
        if ($SHOULD_CREATE_GROUP -eq "y") {
            try {
                $DEVNULL = CreateGroup "$MAINGROUP" "$USER_PATH"
#CreateGroup "Finance" "CN=Users,DC=dominiongreenhouses,DC=com"
            } catch {
                Write-Host "Error creating $MAINGROUP in $USER_PATH"
                Exit-PSSession
                exit
            }
        } else {
            Write-Host "Exiting. Cannot create users in undefined Groups"
            Exit-PSSession
            exit
        }
    }
#Check if the SPECIALGROUP column from the file has something special, like 'Summer
Student' or 'Manager"
#SPECIALGROUP comes from the 'Group3' column of the file and is optional
    if ( -not ([string]::IsNullOrEmpty($SPECIALGROUP)) ) {
        $GROUP_EXISTS = CheckExists "$SPECIALGROUP_IDENTITY"
        if ( -not ($GROUP_EXISTS) ) {
            try {
                $SHOULD_CREATE_GROUP = Read-Host -Prompt "Special Group
'$SPECIALGROUP' for $FIRSTNAME $LASTNAME does not exist. Create Special Group
'$SPECIALGROUP' in $SPECIALGROUP_IDENTITY ? [y|n]"
                if ($SHOULD_CREATE_GROUP -eq "y") {
                    $GROUP_CREATED = CreateGroup "$SPECIALGROUP" "$USER_PATH"
#CreateGroup "Management" "CN=Users,DC=dominiongreenhouses,DC=com"
                } else {
                    Write-Host "Exiting. Cannot create users in undefined Groups"
                    Exit-PSSession
                    exit
                }
            } catch {
                Write-Host "Error creating group $SPECIALGROUP_IDENTITY. Exiting"
                Exit-PSSession
                exit
            }
        }
    }

    $USER_EXISTS = CheckUserExists "$FIRSTNAME" "$LASTNAME"

    if ($USER_EXISTS) {
        Write-Host "User $GIVENNAME already exists. Skipping User" -ForegroundColor Cyan
    } else {
        $USER_PATH = "OU=$OU,$PARENT"
        if ( $SPECIALGROUP -eq "Management" ) {
            #CreateUser "Agent" "Smith" "P@ssw0rd" "HQ"
"CN=Users,DC=dominiongreenhouses,DC=com"
            $RESULT = CreateUser "$FIRSTNAME" "$LASTNAME" "$PASSWORD"
"$MAINGROUP" "$USER_PATH" $true
        } else {
            $RESULT = CreateUser "$FIRSTNAME" "$LASTNAME" "$PASSWORD"
"$MAINGROUP" "$USER_PATH" $false
        }
    }
}


Write-Host "Exiting" -ForegroundColor Green
Exit-PSSession
```

Pinger Script

The *pinger.py* script below was used to ensure that redundant and highly-available routing was functioning properly for all VLAN gateways. In all cases no ICMP packets were dropped.

pinger.py

```
#  Darren Sylvain
#  March 23, 2019
#  Script to ping a list of IP addresses continuously

$HQ_Gateways = "10.1.20.254","10.1.21.254","10.1.25.254","10.1.50.254","10.1.150.254"
$MP_Gateways =
"10.2.20.254","10.2.21.254","10.2.25.254","10.2.50.254","10.2.125.254","10.2.150.254"
$HQ_Gateways_IPv6 =
"2620:fc:0:d358:50::50","2620:fc:0:d358:100::1","2620:fc:0:d358:150::150"
$MP_Gateways_IPv6 =
"2620:fc:0:d369:50::50","2620:fc:0:d369:100::1","2620:fc:0:d369:150::150"

while ($true) {
    foreach ($IP in $MP_Gateways) {
        if (test-connection $IP -count 1 -Quiet)
            { Write-Host -ForegroundColor Green "Ping success on $IP" }
            else { Write-Host -ForegroundColor Red "Ping Failed on $IP" }
        Start-Sleep -Milliseconds 100
    }
}
```

Appendix E: Scan Results

E.I Discovery Scan External

The range owned by Dominion Manufacturing is 172.31.133.50-69. Careful not to scan outside of the network.

172.31.133.50/31 is range 172.31.133.50-51
172.31.133.52/30 is range 172.31.133.52-55
172.31.133.56/29 is range 172.31.133.56-63
172.31.133.64/30 is range 172.31.133.64-67
172.31.133.68/31 is range 172.31.133.68-69

```
Nmap scan report for 172.31.133.50 (Headquarters – HQ-C-FW1)
Host is up (0.00s latency).
Not shown: 98 filtered ports

PORT    STATE SERVICE
22/tcp  open  ssh
443/tcp open  https
```

```
Nmap scan report for HQManagement.DominionGreenHouses.com (172.31.133.53)
Host is up (0.00s latency).
Not shown: 96 filtered ports

PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
```

```
Nmap scan report for 172.31.133.60 (Manufacturing – MP-C-FW1)
Host is up (0.00s latency).
Not shown: 98 filtered ports

PORT    STATE SERVICE
22/tcp  open  ssh
443/tcp open  https
```

```
Nmap scan report for MPManagement.DominionGreenHouses.com (172.31.133.63)
Host is up (0.00s latency).
Not shown: 96 filtered ports

PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
```

```
Nmap scan report for 172.31.133.65 (Warehouse - WH-C-FW1)
Host is up (0.00s latency).
Not shown: 98 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
443/tcp open  https
```

```
Nmap scan report for WHManagement.DominionGreenHouses.com (172.31.133.68)
Host is up (0.0020s latency).
Not shown: 95 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
```

E.II Discovery Scan Internal Headquarters

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-06 21:02 EDT
Nmap scan report for 10.1.20.250 (Secured Wireless VLAN HQ-D-SW1)
Host is up (0.0079s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.20.252 (Secured Wireless VLAN HQ-D-SW2)
Host is up (0.0045s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.20.254 (Secured Wireless HSRP Virtual IP/Default Gateway)
Host is up (0.0051s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

```
Nmap scan report for 10.1.21.250 (Guest Wireless VLAN HQ-D-SW1)
Host is up (0.0027s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.21.252 (Guest Wireless VLAN HQ-D-SW2)
Host is up (0.0043s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.21.254 (Guest Wireless VLAN HSPR Virtual IP/Default Gateway)
Host is up (0.0051s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.25.1 (VoIP Phone)
Host is up (0.0053s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http

Nmap scan report for 10.1.25.250 (VoIP VLAN HQ-D-SW1)
Host is up (0.0088s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.25.252
Host is up (0.0042s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.25.254 (VoIP VLAN HSRP Virtual IP/Default Gateway)
Host is up (0.0055s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for DC01.DominionGreenHouses.com (10.1.50.50) (DC01)
```

```
Host is up (0.00070s latency).
Not shown: 91 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5666/tcp open  nrpe

Nmap scan report for WSUS.DominionGreenHouses.com 10.1.50.51 (WSUS Server)
Host is up (0.00078s latency).
Not shown: 95 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 10.1.50.60 (Asterisk Server)
Host is up (0.00075s latency).
Not shown: 95 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
3306/tcp open  mysql
5666/tcp open  nrpe

Nmap scan report for 10.1.50.100 (ESX1)
Host is up (0.0011s latency).
Not shown: 95 filtered ports
PORT     STATE  SERVICE
22/tcp   closed ssh
80/tcp   open   http
427/tcp  open   svrloc
443/tcp  open   https
8000/tcp open   http-alt

Nmap scan report for 10.1.50.101 (vSphere Management Server)
Host is up (0.00072s latency).
Not shown: 91 closed ports
PORT     STATE SERVICE
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
```

```
389/tcp  open  ldap
443/tcp  open  https
445/tcp  open  microsoft-ds
514/tcp  open  shell
3389/tcp open  ms-wbt-server

Nmap scan report for FS01.DominionGreenHouses.com (10.1.50.150) (FileServer)
Host is up (0.00075s latency).
Not shown: 96 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for Veeam.DominionGreenHouses.com (10.1.50.151) (Veeam Server)
Host is up (0.00073s latency).
Not shown: 94 closed ports
PORT     STATE SERVICE
111/tcp  open  rpcbind
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
3389/tcp open  ms-wbt-server

Nmap scan report for 10.1.50.250 (Servers VLAN HQ-D-SW1)
Host is up (0.0028s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.50.252 (Servers VLAN HQ-D-SW2)
Host is up (0.0052s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.50.254 (Servers VLAN HSPR Virtual IP/Default Gateway)
Host is up (0.0049s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.100.1 (Host on Data VLAN 100)
Host is up (0.0013s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE
```

```
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 10.1.100.250 (Data VLAN 100 HQ-D-SW1)
Host is up (0.0073s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.100.252 (Data VLAN 100 HQ-D-SW2)
Host is up (0.0045s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.100.254 (Data VLAN 100 HSPR Virtual IP/Default Gateway)
Host is up (0.0050s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.150.10 (Management VLAN HQ-A-SW1)
Host is up (0.0083s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 00:22:56:6D:F6:C1 (Cisco Systems)

Nmap scan report for 10.1.150.11 (Management VLAN HQ-A-SW2)
Host is up (0.0100s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 00:22:56:3D:F0:41 (Cisco Systems)

Nmap scan report for 10.1.150.150 (Management VLAN 150 Management Host)
Host is up (0.00099s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:89:3A:A5 (VMware)
```

```
Nmap scan report for 10.1.150.250 (Management VLAN 150 HQ-D-SW1)
Host is up (0.011s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: D0:57:4C:16:95:48 (Cisco Systems)

Nmap scan report for 10.1.150.252 (Management VLAN 150 HQ-D-SW2)
Host is up (0.0079s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 6C:B2:AE:F4:72:7D (Unknown)

Nmap scan report for 10.1.150.254 (Management VLAN 150 HSPR Virtual IP/Default Gateway)
Host is up (0.0090s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 00:00:0C:9F:F0:96 (Cisco Systems)

Nmap scan report for 10.1.200.1 (HQ-D-SW1 uplink)
Host is up (0.0024s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.200.3 (broadcast on 200.0/30 ??? Seems to be a false return for
10.1.200.2 on HQ-C-FW1)
Host is up (0.00098s latency).
All 100 scanned ports on 10.1.200.3 are filtered

Nmap scan report for 10.1.200.5 (Uplink on HQ-D-SW2)
Host is up (0.0024s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.200.6 (Downlink on HQ-C-FW1)
Host is up (0.0010s latency).
Not shown: 99 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.1.200.9 (HQ-D-SW1 on routed port to HQ-D-SW2)
```

```
Host is up (0.015s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.200.10 (HQ-D-SW2 on routed port to HQ-D-SW1)
Host is up (0.0027s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.222.2 (AP1)
Host is up (0.0088s latency).
All 100 scanned ports on 10.1.222.2 are closed

Nmap scan report for 10.1.222.254 (AP Gateway VLAN 222 HSPR Virtual IP/Default Gateway)
Host is up (0.0025s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.250.250 (NTP Loopback HQ-D-SW1)
Host is up (0.0028s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.1.250.252 (NTP Loopback HQ-D-SW2)
Host is up (0.0025s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 65536 IP addresses (42 hosts up) scanned in 5174.14 seconds
```

E.III Discover Scan Internal Manufacturing

```
Nmap scan report for 10.2.20.250 (Secured Wireless VLAN MP-D-R1)
Host is up (0.012s latency).
All 100 scanned ports on 10.2.20.250 are closed

Nmap scan report for 10.2.20.252 (Secured Wireless VLAN MP-D-R2)
Host is up (0.0037s latency).
All 100 scanned ports on 10.2.20.252 are closed
```

```
Nmap scan report for 10.2.20.254 (Secured Wireless HSRP Virtual IP/Default Gateway)
Host is up (0.012s latency).
All 100 scanned ports on 10.2.20.254 are closed

Nmap scan report for 10.2.21.250 (Guest Wireless VLAN MP-D-R1)
Host is up (0.013s latency).
All 100 scanned ports on 10.2.21.250 are closed

Nmap scan report for 10.2.21.252 (Guest Wireless VLAN MP-D-R2)
Host is up (0.0034s latency).
All 100 scanned ports on 10.2.21.252 are closed

Nmap scan report for 10.2.21.254 (Guest Wireless HSRP Virtual IP/Default Gateway)
Host is up (0.013s latency).
All 100 scanned ports on 10.2.21.254 are closed

Nmap scan report for 10.2.25.250 (VoIP VLAN MP-D-R1)
Host is up (0.0080s latency).
Not shown: 97 closed ports
PORT     STATE    SERVICE
139/tcp  filtered netbios-ssn
1025/tcp filtered NFS-or-IIS
5900/tcp filtered vnc

Nmap scan report for 10.2.25.252 (VoIP VLAN MP-D-R2)
Host is up (0.0016s latency).
All 100 scanned ports on 10.2.25.252 are closed

Nmap scan report for 10.2.25.254 (VoIP HSRP Virtual IP/Default Gateway)
Host is up (0.012s latency).
All 100 scanned ports on 10.2.25.254 are closed

Nmap scan report for 10.2.50.33 (RDS)
Host is up (0.00099s latency).
Not shown: 94 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 10.2.50.45 (NagiosXI)
Host is up (0.0017s latency).
Not shown: 97 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
```

```
Nmap scan report for 10.2.50.50 (DC02)
Host is up (0.00079s latency).
Not shown: 93 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 10.2.50.55 NagiosLS)
Host is up (0.0021s latency).
Not shown: 97 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https

Nmap scan report for 10.2.50.100 (ESXI2)
Host is up (0.0013s latency).
Not shown: 95 filtered ports
PORT     STATE  SERVICE
22/tcp   closed ssh
80/tcp   open   http
427/tcp  open   svrloc
443/tcp  open   https
8000/tcp open   http-alt

Nmap scan report for 10.2.50.250 (Management VLAN HQ-D-SW1)
Host is up (0.0087s latency).
Not shown: 97 closed ports
PORT     STATE    SERVICE
139/tcp  filtered netbios-ssn
1025/tcp filtered NFS-or-IIS
5900/tcp filtered vnc

Nmap scan report for 10.2.50.252 (Management VLAN HQ-D-SW2)
Host is up (0.0015s latency).
All 100 scanned ports on 10.2.50.252 are closed

Nmap scan report for 10.2.50.254 (Management HSRP Virtual IP/Default Gateway)
Host is up (0.013s latency).
All 100 scanned ports on 10.2.50.254 are closed

Nmap scan report for 10.2.100.250 (Hosts Data VLAN 100 VLAN HQ-D-SW1)
Host is up (0.011s latency).
Not shown: 97 closed ports
PORT     STATE    SERVICE
80/tcp   filtered http
```

```
1720/tcp filtered h323q931
5900/tcp filtered vnc

Nmap scan report for 10.2.100.252 (Hosts Data VLAN 100 VLAN HQ-D-SW2)
Host is up (0.0019s latency).
All 100 scanned ports on 10.2.100.252 are closed

Nmap scan report for 10.2.100.254 (Hosts Data VLAN 100 HSRP Virtual IP/Default Gateway)
Host is up (0.013s latency).
All 100 scanned ports on 10.2.100.254 are closed

Nmap scan report for 10.2.110.250 (VLAN 110 Loopback for NTP HQ-D-SW1)
Host is up (0.011s latency).
Not shown: 98 closed ports
PORT     STATE    SERVICE
1720/tcp filtered h323q931
5900/tcp filtered vnc

Nmap scan report for 10.2.125.1 (MP VDI Host)
Host is up (0.0013s latency).
Not shown: 94 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 10.2.125.12 (MP VDI Host)
Host is up (0.0031s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 10.2.125.250 (VDI VLAN 125 HQ-D-SW1)
Host is up (0.012s latency).
All 100 scanned ports on 10.2.125.250 are closed

Nmap scan report for 10.2.125.252 (VDI VLAN 125 HQ-D-SW2)
Host is up (0.0022s latency).
All 100 scanned ports on 10.2.125.252 are closed

Nmap scan report for 10.2.125.254 (VDI VLAN 125 HSRP Virtual IP/Default Gateway)
Host is up (0.015s latency).
All 100 scanned ports on 10.2.125.254 are closed

Nmap scan report for 10.2.150.10 (Management VLAN HQ-A-SW1)
```

```
Host is up (0.011s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 00:21:1B:AC:BA:C2 (Cisco Systems)

Nmap scan report for 10.2.150.11 (Management VLAN HQ-A-SW2)
Host is up (0.014s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 00:21:1B:50:62:41 (Cisco Systems)

Nmap scan report for 10.2.150.150 (Management Host)
Host is up (0.0016s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:F9:F3:4B (VMware)

Nmap scan report for 10.2.150.250 (Management VLAN 150 HQ-D-SW1)
Host is up (0.011s latency).
All 100 scanned ports on 10.2.150.250 are closed
MAC Address: 00:1F:CA:05:42:68 (Cisco Systems)

Nmap scan report for 10.2.150.252 (Management VLAN 150 HQ-D-SW2)
Host is up (0.0019s latency).
All 100 scanned ports on 10.2.150.252 are closed
MAC Address: 7C:AD:74:9E:EE:50 (Cisco Systems)

Nmap scan report for 10.2.150.254 (Management VLAN 150 HSRP Virtual IP/Default Gateway)
Host is up (0.0021s latency).
All 100 scanned ports on 10.2.150.254 are closed
MAC Address: 00:00:0C:9F:F0:96 (Cisco Systems)
```

E.IV Discovery Scan Internal Warehouse

```
Nmap scan report for 10.3.25.4 (VoIP Phone)
Host is up (0.015s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http

Nmap scan report for 10.3.25.5 (VoIP Phone)
```

```
Host is up (0.020s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http

Nmap scan report for 10.3.25.254 (VoIP VLAN 25 Default Gateway)
Host is up (0.0061s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.3.100.254 (Hosts Data VLAN 100 Default Gateway)
Host is up (0.0057s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.3.110.252 (NTP VLAN 110 Loopback WH-A-SW1)
Host is up (0.0057s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.3.150.254 (Management VLAN 150 Default Gateway)
Host is up (0.0074s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 70:69:5A:37:49:7D (Unknown)
```

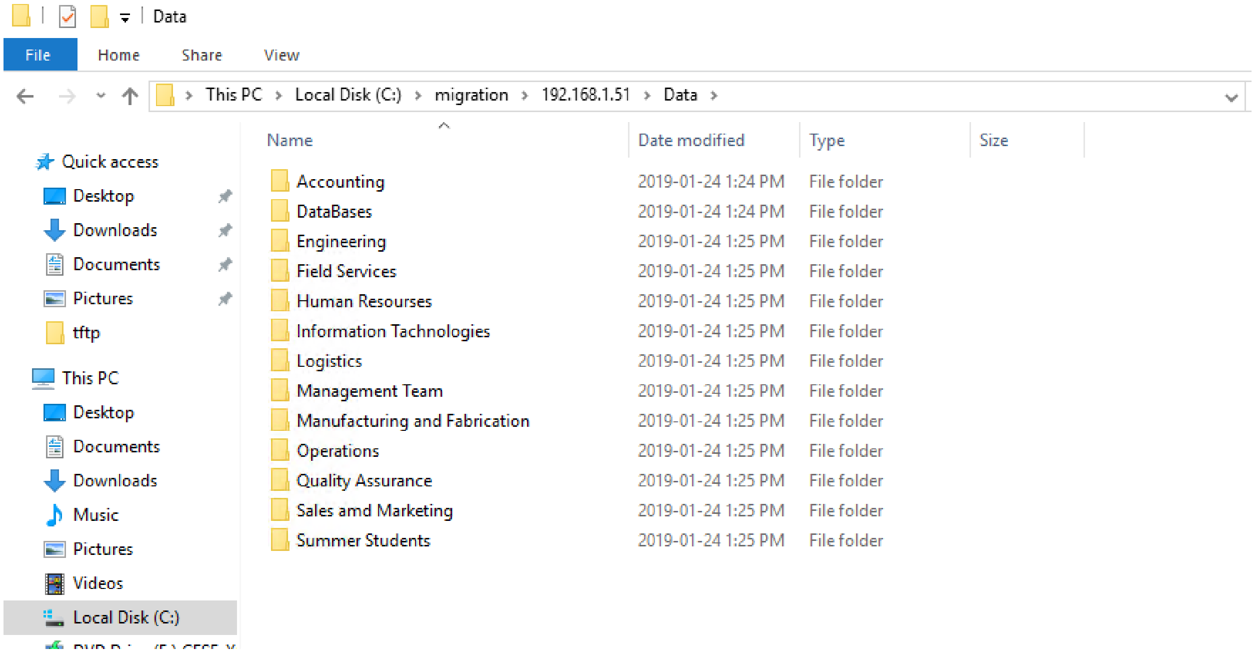
Appendix F: AD & RDP

F.I Active Directory Migration

1. Promote the new server as a DC.
2. Verify the replication of Active Directory, DNS and other related DC content.
3. Transfer FSMO roles:
   a. Active Directory Users and Computers> Operations Master > Change RID, PDC, and Infrastructure.
   b. Active Directory Domains and Trusts > Operations Master > Change Domain Naming Operations Master.
   c. To transfer the schema master: run “regsvr32 schmmgmt.dll” command line. > Add “Active Directory Schema” snap-in in mmc. > Right click and select Operations Master > Change Current Schema Master.
4. Verify FSMO roles holder using “netdom query” command.
5. Raising forest and domain functional level will be done after migration File Server.

F.II File Server Migration

1. Create new Windows 2016 servers and add it to the domain.
2. Download and install Microsoft File Server Migration Toolkit on the new server.
3. Share the “Data” folder on the network in the old server.
4. Run Migration Tool Select network, point to network share and select path to copy files. Verify copied files, and migration report



Name	Date modified	Type	Size
Accounting	2019-01-24 1:24 PM	File folder	
DataBases	2019-01-24 1:24 PM	File folder	
Engineering	2019-01-24 1:25 PM	File folder	
Field Services	2019-01-24 1:25 PM	File folder	
Human Resourses	2019-01-24 1:25 PM	File folder	
Information Technologies	2019-01-24 1:25 PM	File folder	
Logistics	2019-01-24 1:25 PM	File folder	
Management Team	2019-01-24 1:25 PM	File folder	
Manufacturing and Fabrication	2019-01-24 1:25 PM	File folder	
Operations	2019-01-24 1:25 PM	File folder	
Quality Assurance	2019-01-24 1:25 PM	File folder	
Sales amd Marketing	2019-01-24 1:25 PM	File folder	
Summer Students	2019-01-24 1:25 PM	File folder	

F.III Thin Clients - RDS

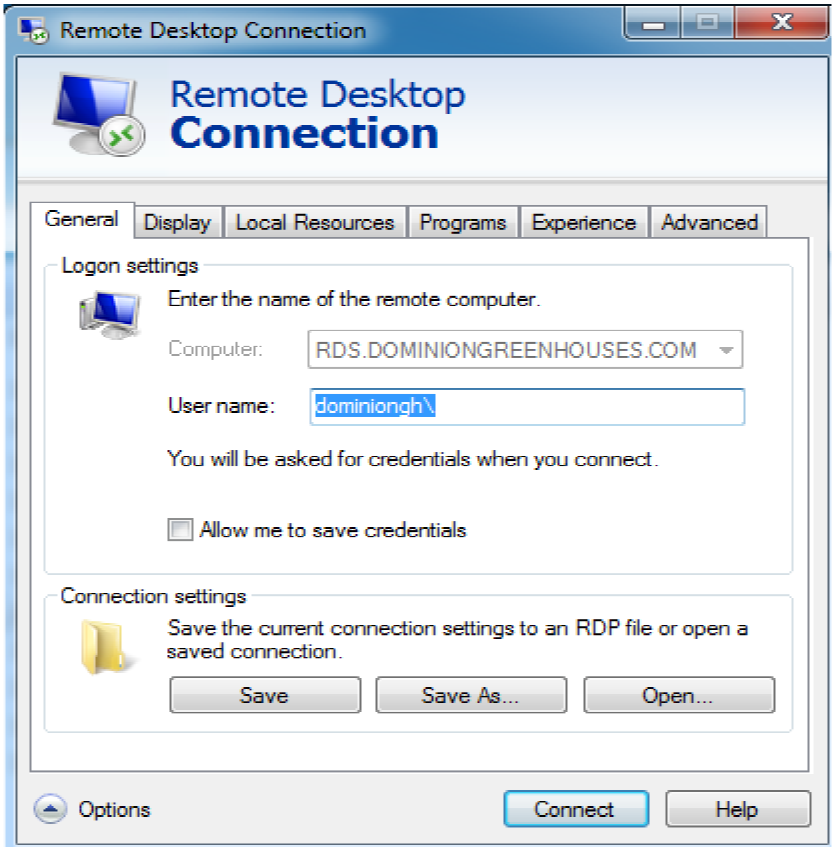
Server-side:

1. Create a new Windows Server 2016 and add it to the domain.
2. Run “Add Roles and Features Wizard” and select “Remote Desktop Services Installation” as the installation type.
3. Then, select “Virtual machine-based desktop deployment” since we are deploying VDIs.
4. Select “RDS (local server) as the RD Connection Broker, RD Web Access, and RD Session Host.
5. This installation will also install Hyper –V for virtualizing our VDIs. Point to Hyper – V on the left pane and create a Windows 10 template. Then, sysprep and shutdown the template VM.
6. Click to Remote Desktop Services on the left pane, and create a new Collection.
7. Select “Personal virtual desktop connection” as the collection type, since we are deploying persistent VDIs.
8. Select the Virtual Desktop Template we created in Step 5.
9. In the User Assignment section, check the “Add the user account to the local Administrators group on the virtual desktop” option.
10. In the next two sections provide “Unattended installation settings” such as time section, Active Directory domain name, OU, and User groups.
11. Specify the number of virtual desktops and the path to store them. Then finish the wizard.

Client-side:

1. Deploy a Windows 10 PC and connect to a Manufacturing Plant switch port with VLAN 125 (VDI VLAN) access.
2. Delete all local users on the computer.

3. Create and save an RDP file for our RD gateway.



Enter the name of the remote computer.

Computer: RDS.DOMINIONGREENHOUSES.COM

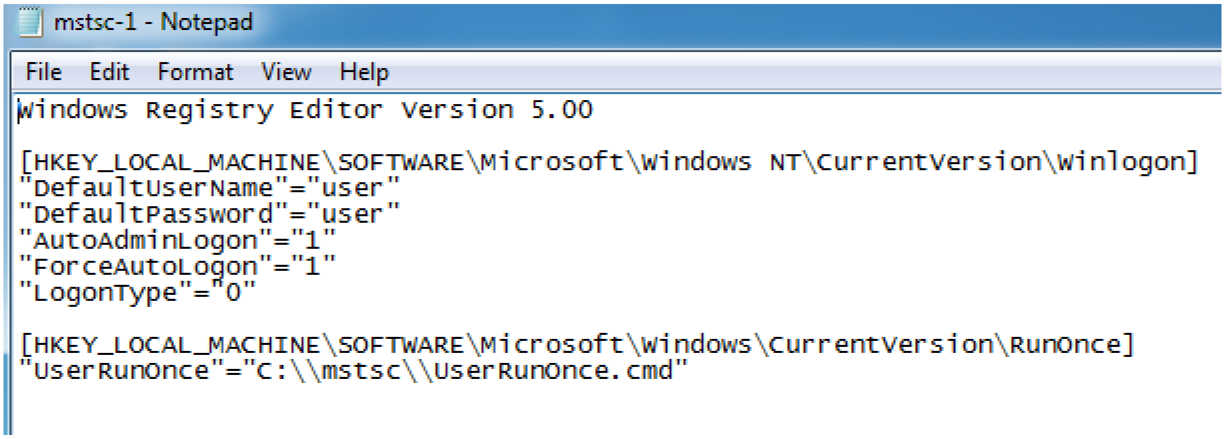
User name: dominiongh\

You will be asked for credentials when you connect.

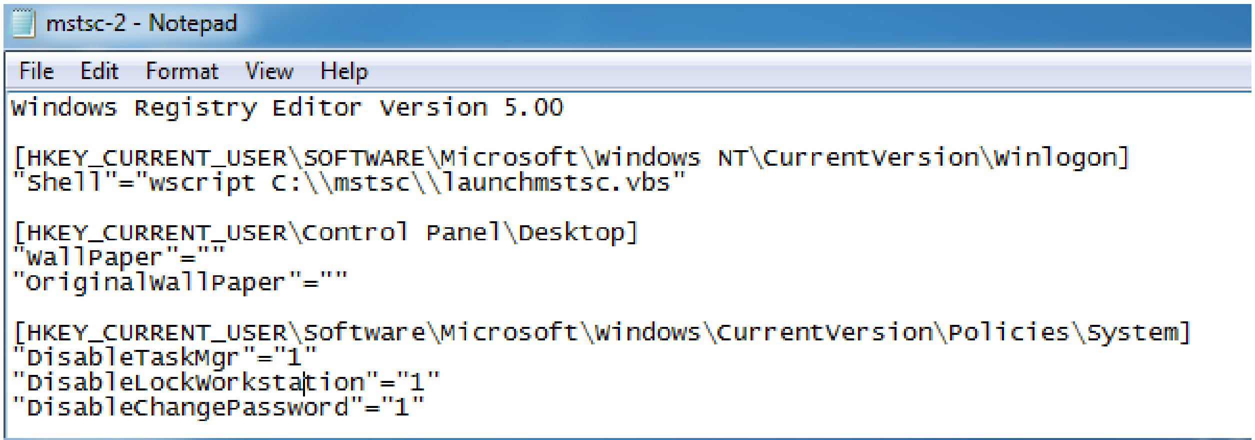
□ Allow me to save credentials

Save the current connection settings to an RDP file or open a saved connection.

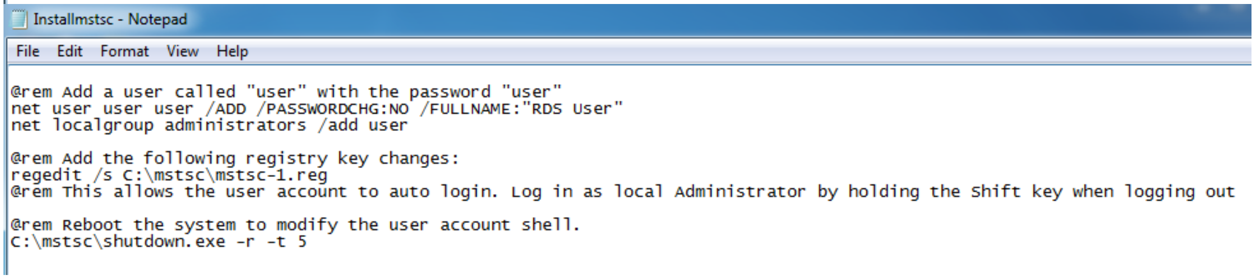
4. Scripts and Registration Entries used for Windows 10 PC to RDP to our RD Gateway and not show any local login info.



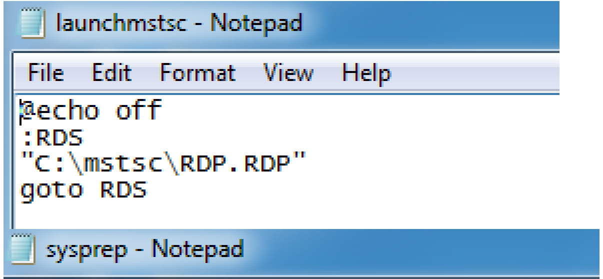
```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"DefaultUserName"="user"
"DefaultPassword"="user"
"AutoAdminLogon"="1"
"ForceAutoLogon"="1"
"LogonType"="0"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce]
"UserRunOnce"="C:\\mstsc\\UserRunOnce.cmd"
```



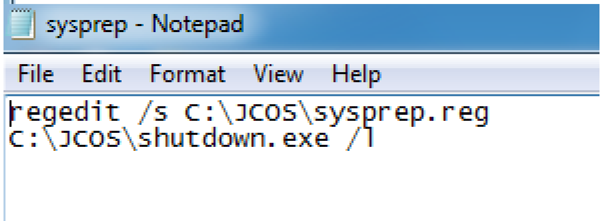
```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"Shell"="wscript C:\\mstsc\\launchmstsc.vbs"

[HKEY_CURRENT_USER\Control Panel\Desktop]
"WallPaper"=""
"OriginalWallPaper"=""

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableTaskMgr"="1"
"DisableLockWorkstation"="1"
"DisableChangePassword"="1"
```



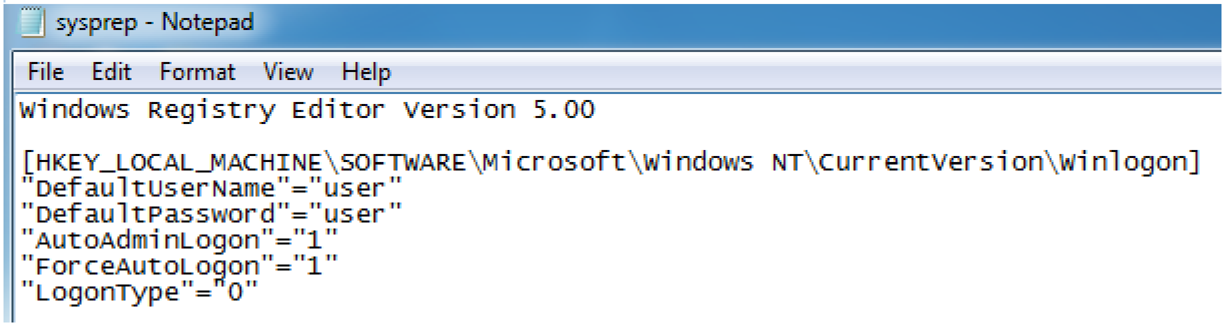
```
@rem Add a user called "user" with the password "user"
net user user user /ADD /PASSWORDCHG:NO /FULLNAME:"RDS User"
net localgroup administrators /add user

@rem Add the following registry key changes:
regedit /s C:\mstsc\mstsc-1.reg
@rem This allows the user account to auto login. Log in as local Administrator by holding the Shift key when logging out

@rem Reboot the system to modify the user account shell.
C:\mstsc\shutdown.exe -r -t 5
```



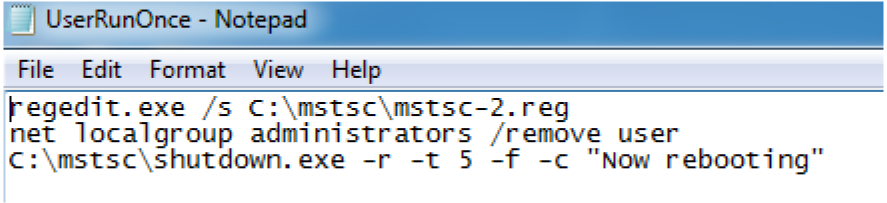
```
@echo off
:RDS
"C:\mstsc\RDP.RDP"
goto RDS
```



```
regedit /s C:\JCOS\sysprep.reg
C:\JCOS\shutdown.exe /l
```

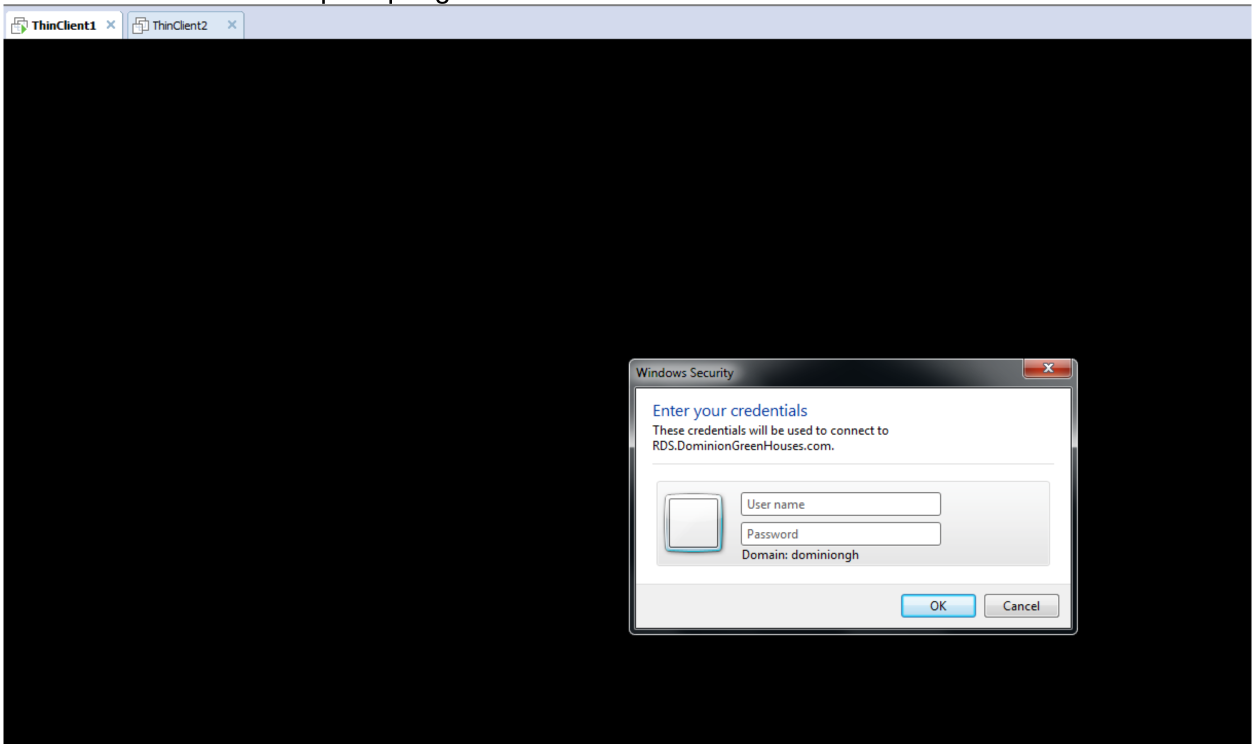


```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"DefaultUserName"="user"
"DefaultPassword"="user"
"AutoAdminLogon"="1"
"ForceAutoLogon"="1"
"LogonType"="0"
```



```
regedit.exe /s C:\mstsc\mstsc-2.reg
net localgroup administrators /remove user
C:\mstsc\shutdown.exe -r -t 5 -f -c "Now rebooting"
```

5. All scripts and RDP file we created “RDP.rdp” are placed in the “C:/MSTC: folder in the Windows 10 PC
6. Run the InstallMSTC.cmd as administrator for once. This will restart the computer.
7. Windows will now log in without any local login screen and RDP to the RD Gateway which will be prompting to enter credentials



Enter your credentials

These credentials will be used to connect to RDS.DominionGreenHouses.com.

Domain: dominiongh

8. To log in locally to make changes, press and hold Shift key.

References

Freund, J., & Jones, J. (2015). Measuring and managing information risk a FAIR approach. Amsterdam: Elsevier, Butterworth-Heinemann.

Hubbard, D. W., & Seiersen, R. (2016). How to measure anything in cybersecurity risk. Hoboken, NJ: Wiley.

Hubbard, D. W. (2014). How to measure anything: Finding the value of intangibles in business. Hoboken, NJ: John Wiley & Sons.

Google | G Suite Service Level Agreement | Online 11/4/19 | Available: https://gsuite.google.com/terms/sla.html

https://www.iperiusbackup.net/en/benefits-virtualization-administrator-would-get-from-using-vmware-esxi/

https://searchservervirtualization.techtarget.com/tip/Understanding-VMware-ESXi-features

https://searchvirtualdesktop.techtarget.com/definition/Remote-Desktop-Services-RDS

https://www.veeam.com/vmware-esx-backup.html