2013

Equilibrium Consulting

Network Infrastructure Design Document for Chavhoj Canada Inc.'s Australia Infrastructure Expansion and Network Design and Installation Project

Prepared By: Justin Waelz, Serge Trunkin, Anton Shylo, Travis Vanos, and Chris Lageer

Date: October 21, 2013

TABLE OF CONTENTS

1. OVERVIEW

Equilibrium Consulting is proud to present to Chavhoj Canada Inc. our technical design documentation for the Australia Infrastructure Expansion and Network Design and Installation project.

Purpose of this Document:

This document is for use by Chavhoj Canada Inc., and is intended to provide an outline of the critical systems and services that Equilibrium Consulting has designed for your project. This includes data management, infrastructure security, remote access services, IT support systems, virtualization, daemon services, Active Directory, mobile communication, mail flow, patch management, videoconferencing, and the underlying LAN, wireless, firewall, WAN, and telephony infrastructures.

Use of this Document:

This document is broken down into the different major design areas for your project. The Table of Contents has hyperlinks enabled to allow you to navigate quickly to each section of the document.

- The major section headings are numbered, bolded, underlined, and in capital letters.
  - For example, **3. STORAGE MANAGEMENT AND FILE MANAGEMENT**

- The subsections underneath each major section, are numbered, bolded, and in sentence case.
  - For example, **3.1 Storage Area Network (SAN) Equipment Configuration**

- Within the subsections, further task breakdowns are bolded and in sentence case, and do not have any numerical identification.
  - For example, **Hard Drive Placement and Types:**

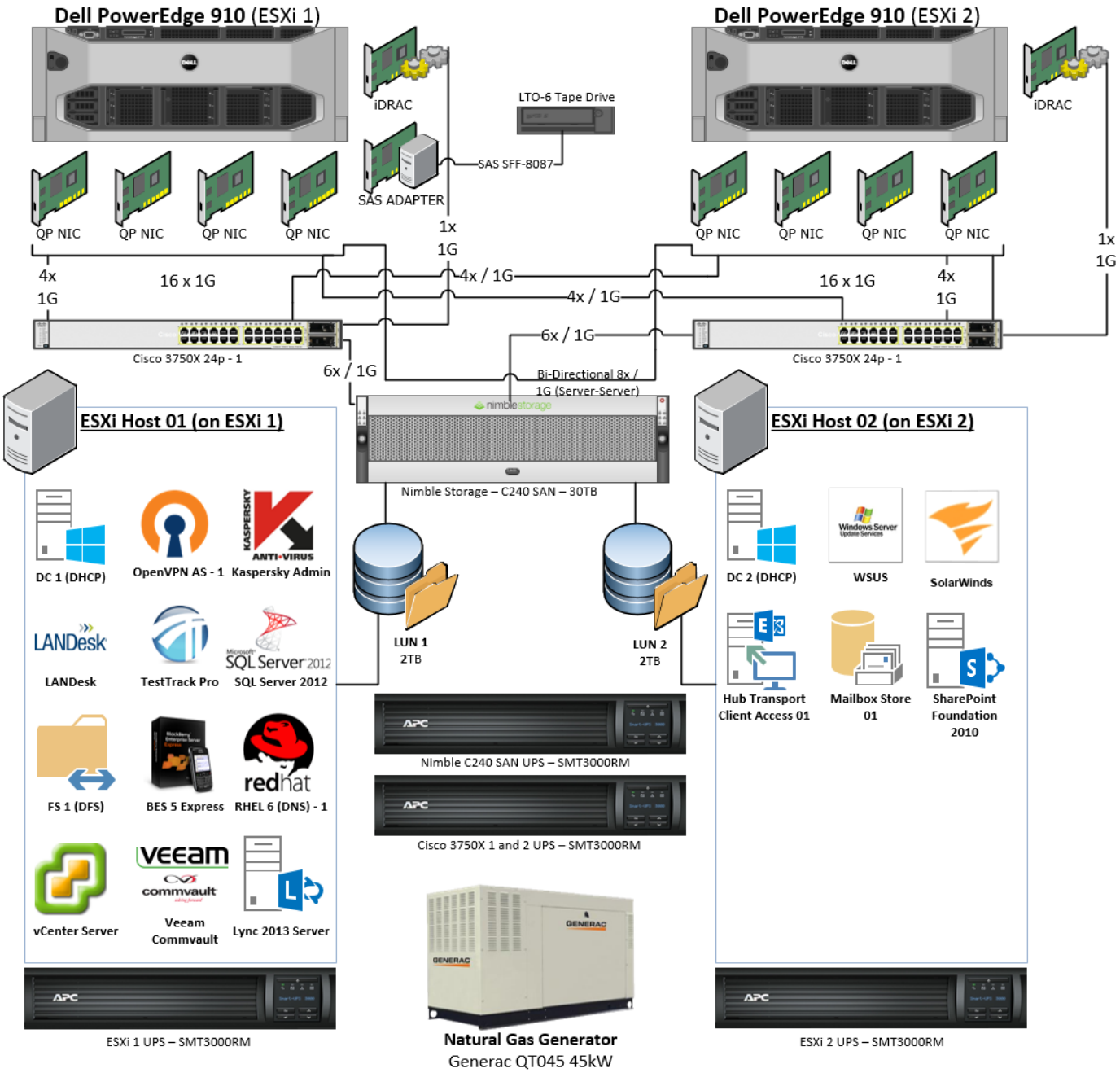
When possible, each section includes pictures of actual product functionality, or logical diagrams to explain how a technology will be implemented.

Where to Start:

Equilibrium Consulting encourages you to view Section 2 first, which will give you an in-depth understanding of our overall IT infrastructure solution, before diving into the technical designs for each component in our solution.

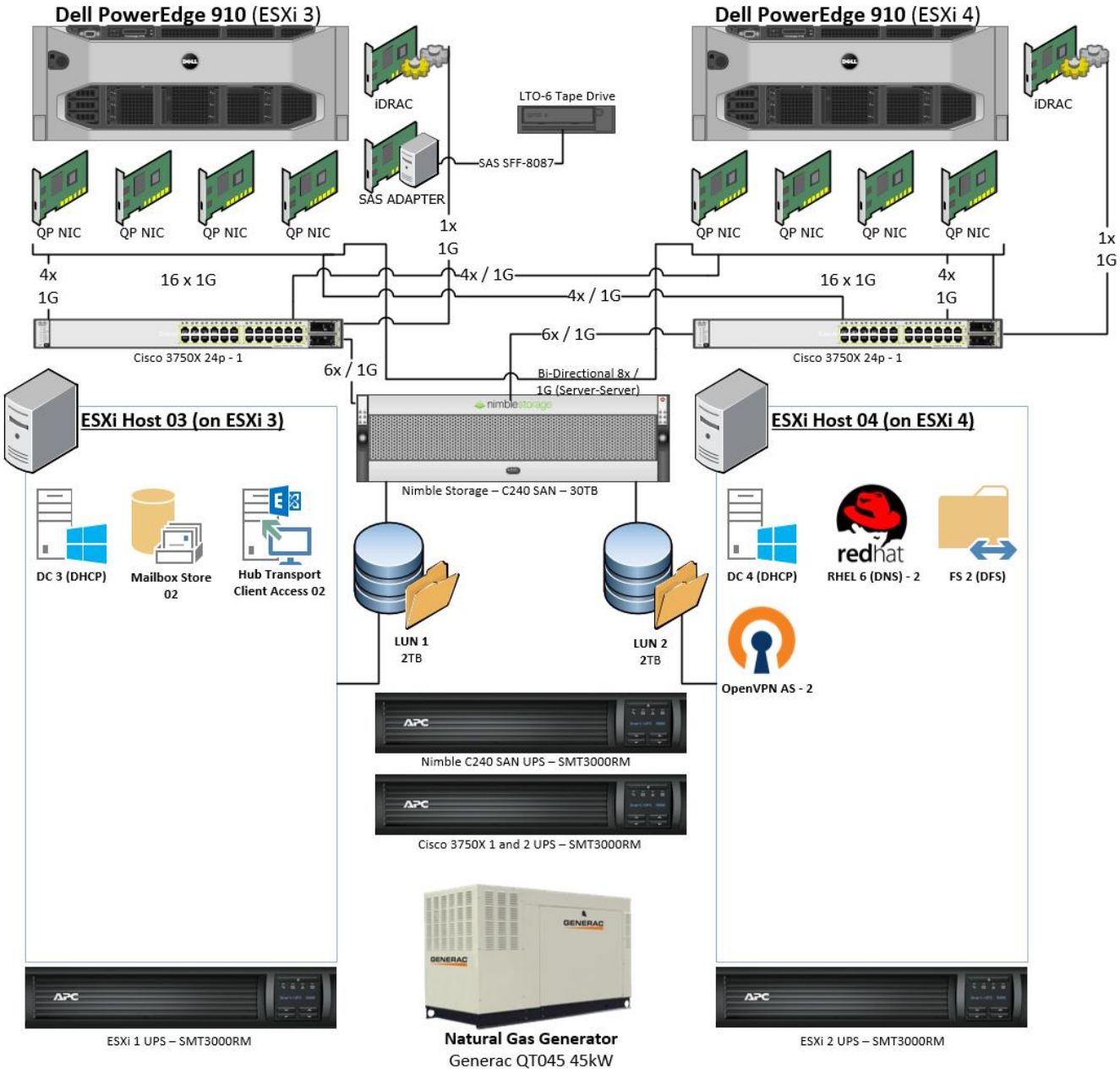
2. OVERALL DESIGN TOPOLOGIES

2.1 Data Center IT Infrastructure Topology – Sydney



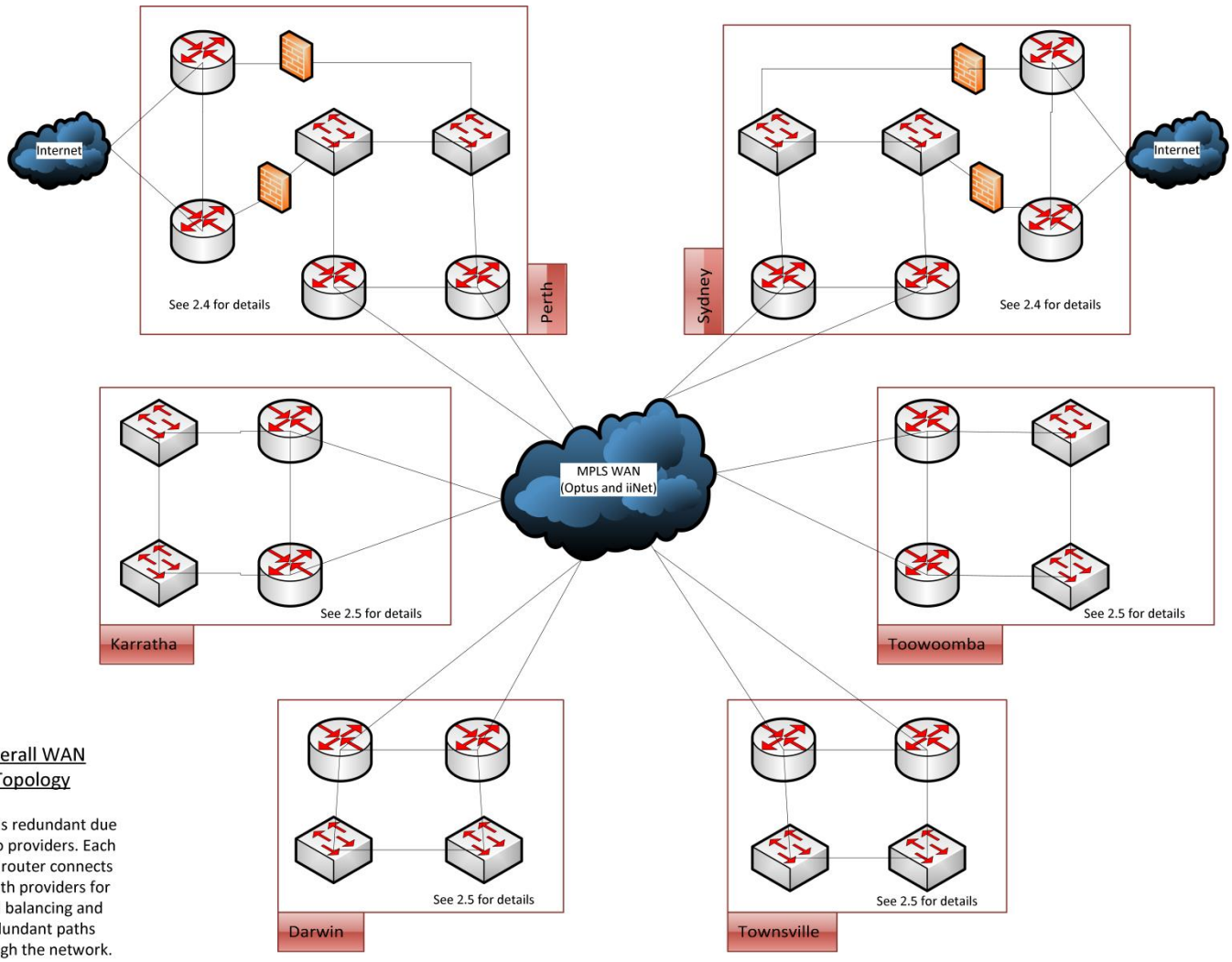
Content Expert: Entire Team (designed by Serge Trunkin)

2.2 Data Center IT Infrastructure Topology – Perth



Content Expert: Entire Team (designed by Serge Trunkin)

2.3 Overall WAN Topology



Overall WAN Topology

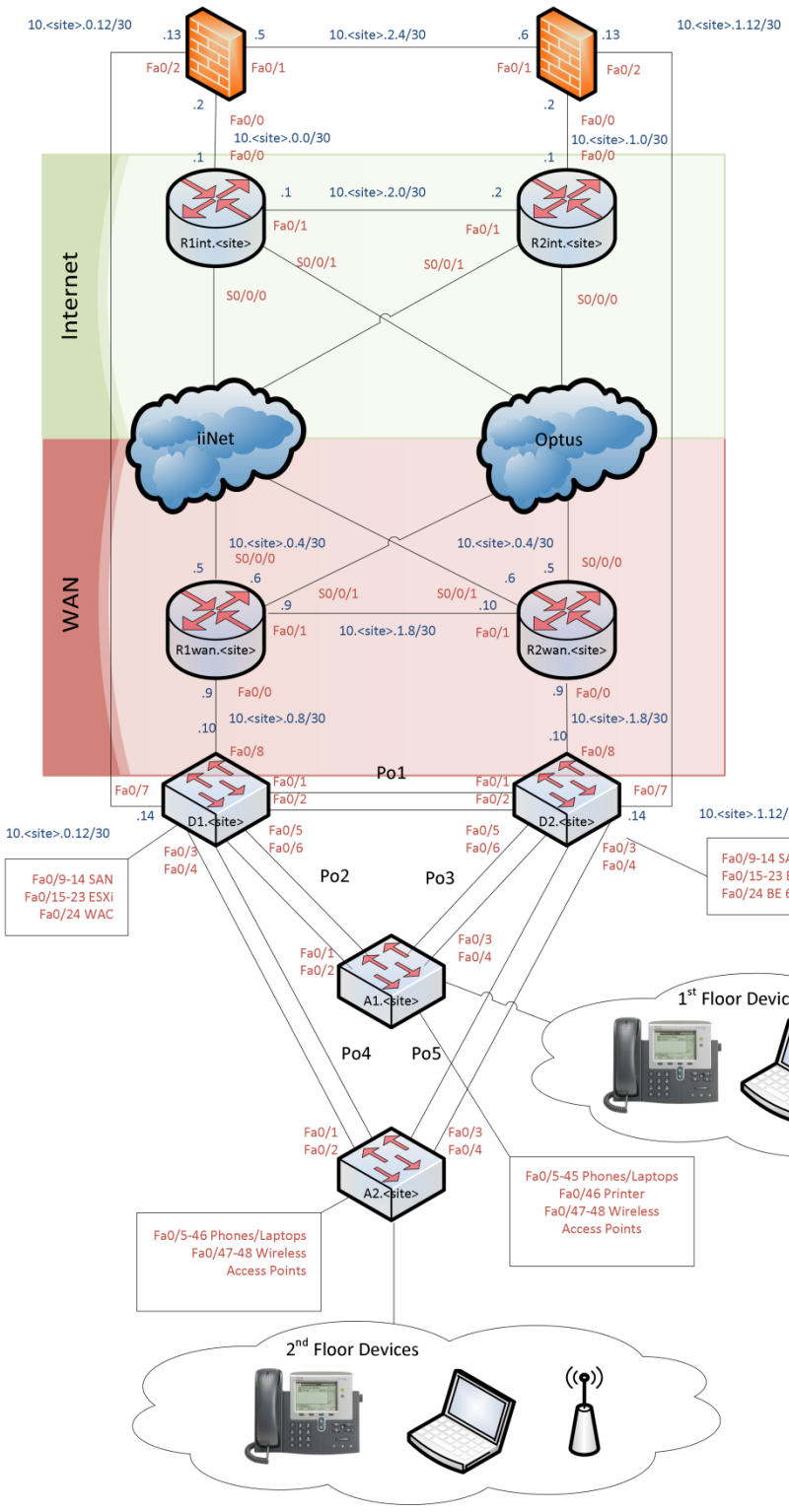
WAN is redundant due to two providers. Each WAN router connects to both providers for load balancing and redundant paths through the network.

Content Expert: Entire Team (designed by Chris Lageer)

2.4 Regional Office Networking Topology

Regional Office Networking Topology

This diagram shows the topology of the regional offices: Perth and Sydney. For ease of reading the Internet and WAN connections are coming from one cloud source, either Optus or iiNet. Connections to the Internet and WAN are not connected like this.



Addressing Scheme
10.<site>.<VLAN>.X

Site Codes

Sydney – 10
Toowoomba – 20
Townsville – 30
Perth – 40
Karratha – 50
Darwin – 60

VLANs

Mgmt – 5
Admin – 10
Office – 20
Sales – 30
Finance – 40
HR – 50
IT – 60
Servers – 70
Wifi – 80
Guest Wifi – 90
Admin Voice – 110
Office Voice – 120
Sales Voice – 130
Finance Voice – 140
HR Voice – 150
IT Voice – 160
Native – 200
Blackhole - 999

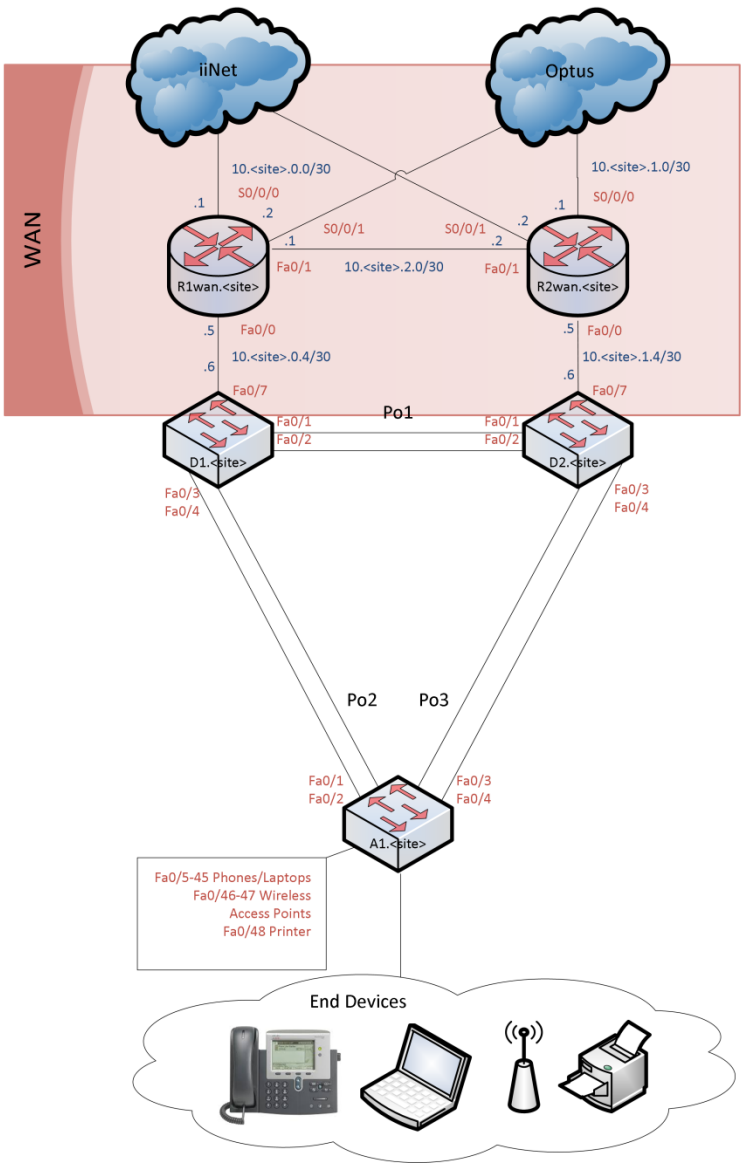
Point-to-Point (P2P) links use 10.<site>.0-2.X

Content Expert: Entire Team (designed by Chris Lageer)

2.5 Branch Office Networking Topology

Branch Office Networking Topology

This diagram shows the topology of the branch offices: Toowoomba, Townsville, Karratha and Darwin. All traffic flows out of the branch office through either the Optus or iiNet WAN connection. Internet traffic is sent to the closest regional office to be routed from there.



Addressing Scheme
10.<site>.<VLAN>.X

Site Codes

Sydney – 10
Toowoomba – 20
Townsville – 30
Perth – 40
Karratha – 50
Darwin – 60

VLANs

Mgmt – 5
Admin – 10
Office – 20
Sales – 30
Finance – 40
HR – 50
IT – 60
Servers – 70
Wifi – 80
Guest Wifi – 90
Admin Voice – 110
Office Voice – 120
Sales Voice – 130
Finance Voice – 140
HR Voice – 150
IT Voice – 160
Native – 200
Blackhole - 999

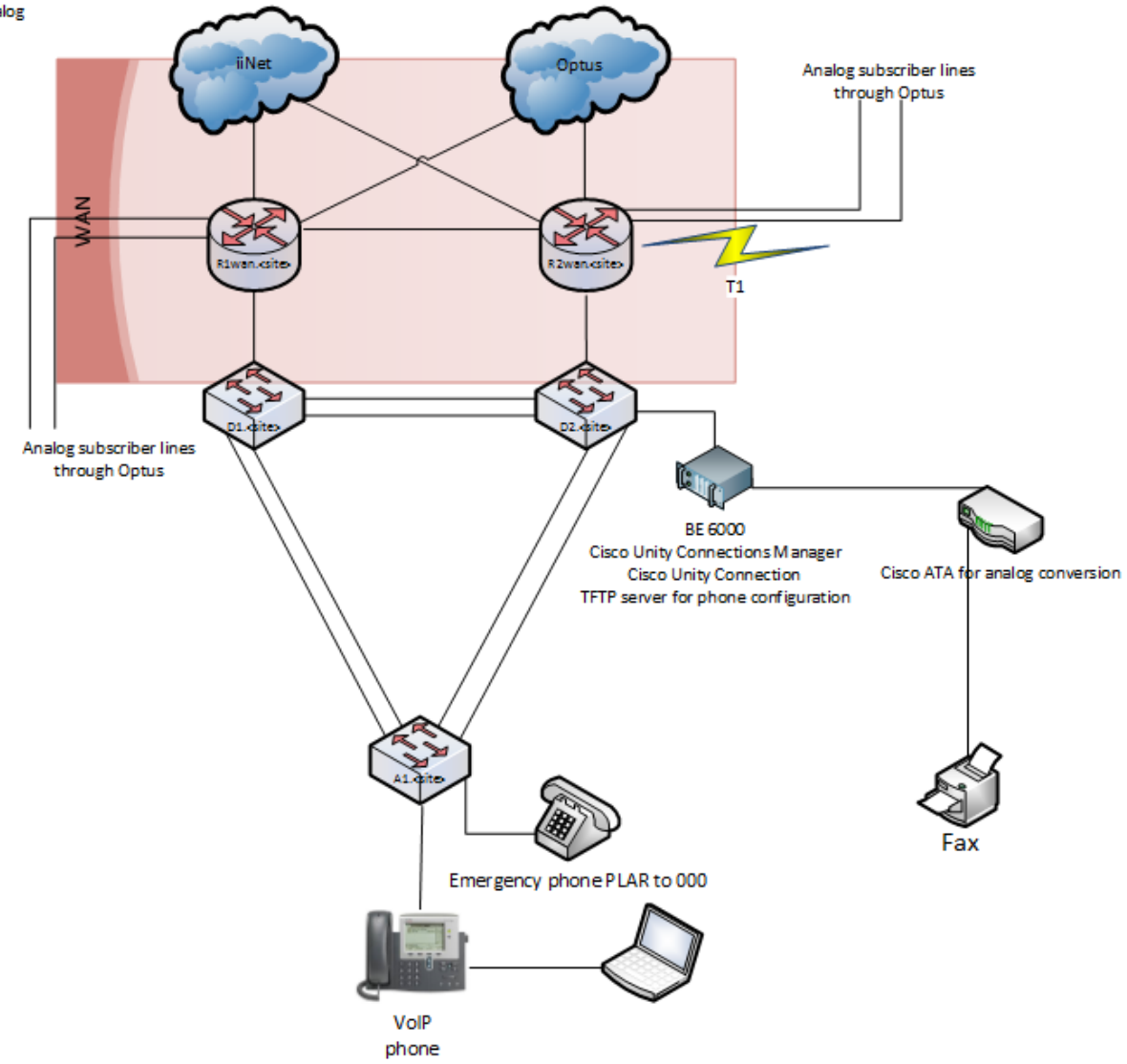
Point-to-Point (P2P) links use 10.<site>.0-2.X

Content Expert: Entire Team (designed by Chris Lageer)

2.6 Telephony Topology

Regional Office Telephony Topology

This diagram shows the telephony topology of the regional offices: Sydney and Perth. All phone calls flow in and out through the T1 line. The calls are routed to the BE 6000 server, which houses the Call Manager and Voicemail systems. Analog lines are present for emergency failover.



Content Expert: Entire Team (designed by Chris Lageer)

2.7 Network Diagram References

IP Addressing Scheme

10.<site>.<vlan>.x
Where x can be between 15-254

Site Subnets

Sydney – 10.10.x.x/16
Toowoomba – 10.20.x.x/16
Townsville – 10.30.x.x/16
Perth – 10.40.x.x/16
Karratha – 10.50.x.x/16
Darwin – 10.60.x.x/16

Telephony

Sydney: 1XXX
Toowoomba: 2XXX
Townsville: 3XXX
Perth: 4XXX
Karratha: 5XXX
Darwin: 6XXX

Spanning Tree Priorities

D1.<site> has been modified to have priority for:
- Office and Office Voice
- Admin and Admin Voice
- HR and HR Voice
- Guest Wifi

D2.<site> has been modified to have priority for:
- Sales and Sales Voice
- Finance and Finance Voice
- IT and IT Voice
- Wifi

VLANs

Name	VLAN	IP
P2P Links	n/a	10.<site>.0-2.x/30
Mgmt	5	10.<site>.5.x/24
Admin	10	10.<site>.10.x/24
Office	20	10.<site>.20.x/24
Sales	30	10.<site>.30.x/24
Finance	40	10.<site>.40.x/24
HR	50	10.<site>.50.x/24
IT	60	10.<site>.60.x/24
Servers	70	10.<site>.70.x/24
Wireless	80	10.<site>.80.x/24
Guest Wireless	90	10.<site>.90.x/24
Admin Voice	110	10.<site>.110.x/24
Office Voice	120	10.<site>.120.x/24
Sales Voice	130	10.<site>.130.x/24
Finance Voice	140	10.<site>.140.x/24
HR Voice	150	10.<site>.150.x/24
IT Voice	160	10.<site>.160.x/24
Native	200	n/a
Blackhole	999	n/a

Legend


Switch
D1/D2 – Cisco 3750X
A1 – Cisco 2960X


Router
Branch – Cisco 2911 ISR
Regional – Cisco 3945 ISR


Notebook
Lenovo ThinkPad X1 Carbon
Lenovo ThinkPad T430
Lenovo ThinkPad E531


Printer
- HP LaserJet M775z


Wireless Access Point
- Cisco Aironet 1242AG


Network Services
WAN – Optus/iiNet
Internet – Optus/iiNet


VoIP phones
- Cisco 7962G
- Cisco 7937G Conference pod

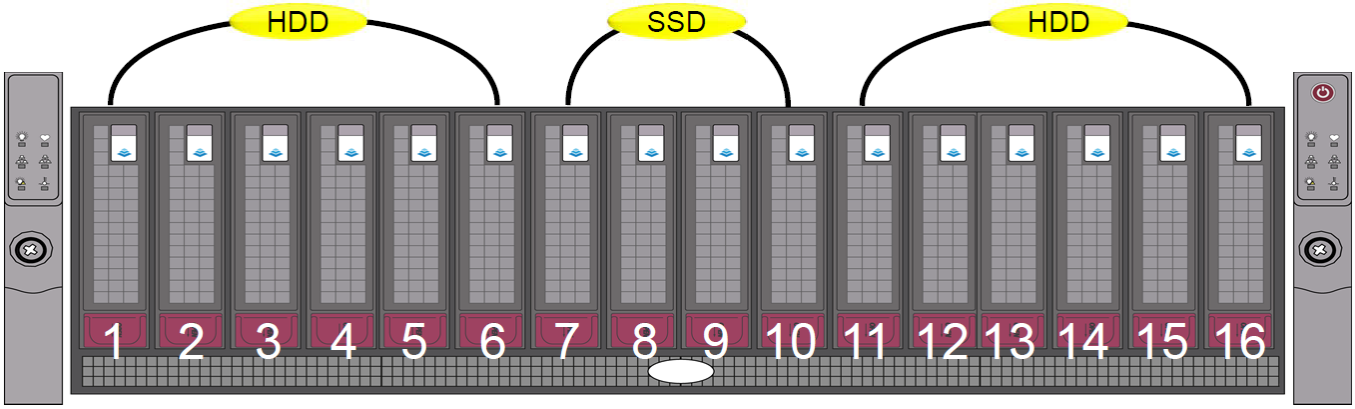

Firewall
- Cisco ASA 5525X

Content Expert: Entire Team (designed by Chris Lageer)

3. STORAGE MANAGEMENT AND FILE MANAGEMENT

3.1 Storage Area Network (SAN) Equipment Configuration

The primary storage equipment is two Nimble Storage CS240 Storage Area Network (SAN) devices. A SAN will be placed in each data center (the primary site at Sydney, and the failover site at Perth), and will be configured for volume replication to guarantee the availability of critical data should either site go down.



Hard Drive Placement and Types:

- Each Nimble CS240 SAN has 16 hard drives:
  - Slots 1-6 and 11-16 are populated with 2TB Western Digital Enterprise 7200 RPM SATA II hard drives
  - Slots 7-10 are populated with 160GB Intel 320 SATA II Solid State Drives (SSDs)

Hard Drive and Storage Configuration:

- For redundancy, the SAN is configured to operate in RAID 6 with a hot spare. This means that each SAN can withstand 2 hard drive failures. After the first hard drive failure, the hot spare will be put into use.

- Each SAN will have approximately 22TB of capacity, but with compression enabled on each iSCSI volume, and depending on the type of data stored on the volume, that number will grow.

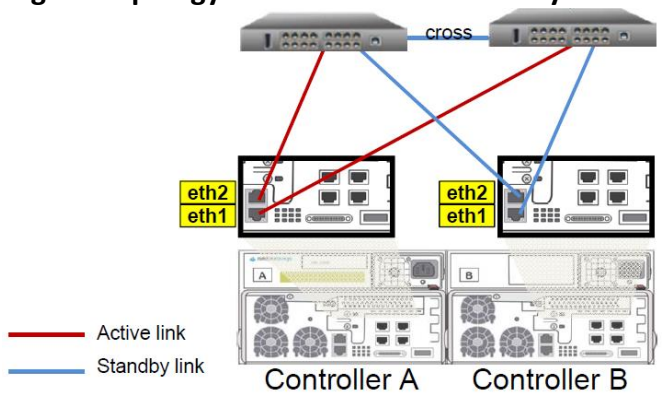
- As per the above image, each SAN utilizes compression algorithms to save on disk space. For example, for an ESXi datastore volume, the Volume Size might be 750GB, but with compression, only 740GB will be used on the SAN (i.e. you will have Space Savings on each iSCSI volume).

- For each application that needs to store data, a separate LUN (Logical Unit Number) will be provisioned on the SAN, and then connected to the device via iSCSI. For example, for SharePoint Foundation 2010's database, it will be hosted on a Microsoft SQL Server 2012 database, but that database will be stored on a dedicated iSCSI volume on the SAN. This allows for simplified backups and rapid data recovery via snapshots (snapshots are discussed in Section 3.3).

Power Supply Redundancy:

- Each SAN has redundant power supplies (for a total of 500 Watts), and will be connected to different UPS equipment in the data center.

Logical Topology for Network Connectivity:

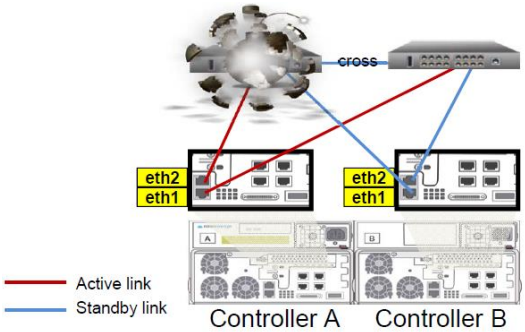


- Each SAN has two controllers for redundancy. At any one time, only one of the two controllers is active, and the other is in a standby mode.

- Each controller has 6 one-gigabit network ports (for a total of 12 one-gigabit network ports per SAN). The first two Ethernet ports on each controller (eth1 and eth2) are used for Management Interfaces. The remaining Ethernet ports (eth3-eth6 on each controller) are used for data.

- The SANs will be wired into the data center switching equipment (with Jumbo Ethernet frame support being enabled) utilizing mirrored sibling interfaces on the SAN controllers for the Management Interfaces, and a cross link between each switch. The cross link between the switches (configured as an EtherChannel bundle) allows for added redundancy should any of the gigabit ports fail on the SAN.

- Each mirrored sibling Management Interface (seen as eth1 on Controller A and Controller B above), is connected to the same switch. This allows for a switch to fail, while allowing for the controllers to failover seamlessly via eth2 (the other mirrored sibling Management Interface).



- To further clarify the network connectivity required for the SAN, consider the above example. The mirrored sibling ports were configured incorrectly, which means that the controllers cannot perform a proper failover (Controller B should have had eth1 going to the far right switch, and eth2 going to the far left switch). When the switch fails, if a controller were to fail too, such as Controller B, then the SAN would not be able to failover to Controller A (it relies on the mirrored sibling port on each controller, eth2 in this example, to be available).

Performance:

- Within a 3U form factor, due to SSD caching paired with Nimble Storage's Cache Accelerated Sequential Layout (CASL) algorithm, depending on the workload, each SAN will be able to perform approximately 16,000 - 40,000 Input/Output Operations Per Second (IOPS).

- For example, using the SQLIO Disk Subsystem Benchmark Tool, for 8K random writes, 18,000 IOPS is the average, and for 8K random reads, 40,000 IOPS is the average.

- For throughput, with 64K sequential write operations, the average performance is 260 MB/s, with 64K sequential read operations performing at an average of 800 MB/s.

- Therefore, the SAN will be able to fully utilize the underlying networking infrastructure.

Internet Small Computer System Interface (iSCSI) LUN Disk Quotas:

This section outlines the expected size of each iSCSI volume for the data generated by the critical applications in the IT Infrastructure. Extra space has been accounted for, in order to scale with your data growth. Each SAN will have identical volumes, for redundancy purposes. Any storage not specifically allocated for an application, will be stored in the ESXi datastore.

- Each ESXi server will have a 2TB datastore for virtual machines.
  - Each ESXi server will boot from a local RAID 1 volume.

- Microsoft SQL Server 2012 will require a 500GB volume for SharePoint data and logs, and a 500GB volume for LANDesk and TestTrack Pro data and logs (the Storage Profile for these volumes will be set to SQL, which means that the SAN will apply optimizations specific to SQL transactions).

- Each file server will have a 2TB volume for user data (such as their redirected Desktop and My Documents data) and corporate shared folders.

- All equipment will transmit their system logs to the centralized monitoring system, SolarWinds (see Section 18.1 for more information), which will then store the information on a 300GB volume.

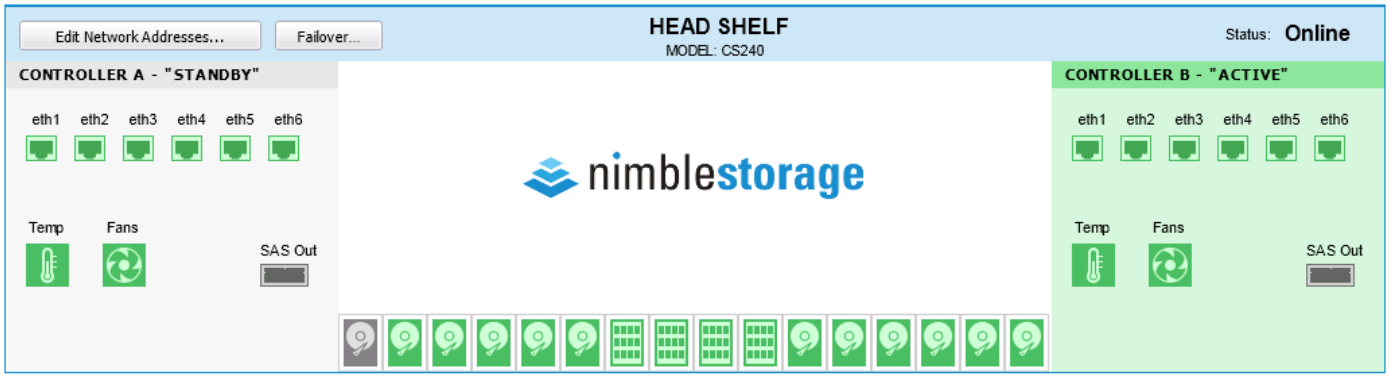
- A 2TB volume will be provisioned for Exchange mailbox databases.

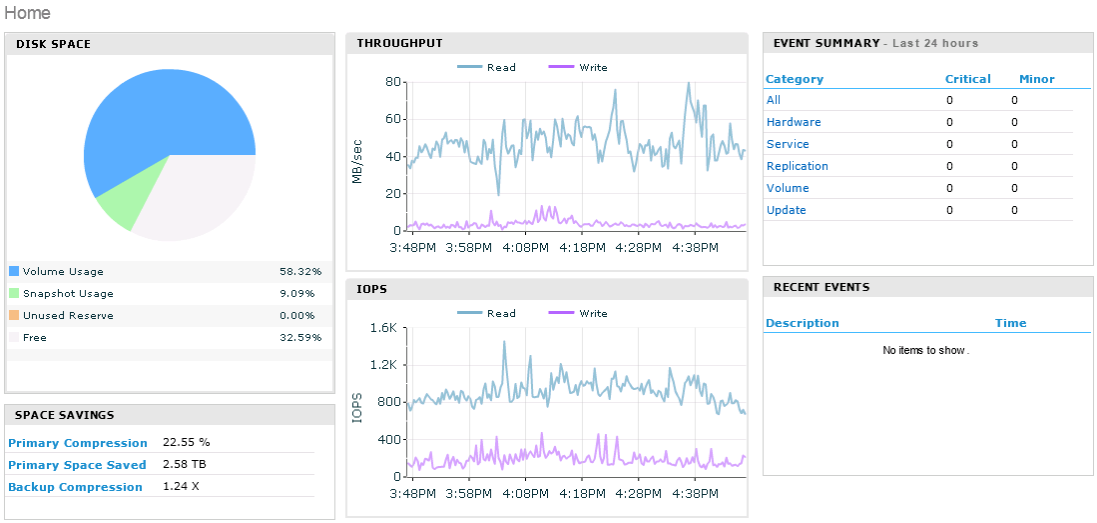
- For backups, a 4TB volume will be set aside for virtual machine data, and an additional 4TB volume will be set aside for data backups.

- All remaining storage space will be set aside for future growth.

SAN Monitoring:

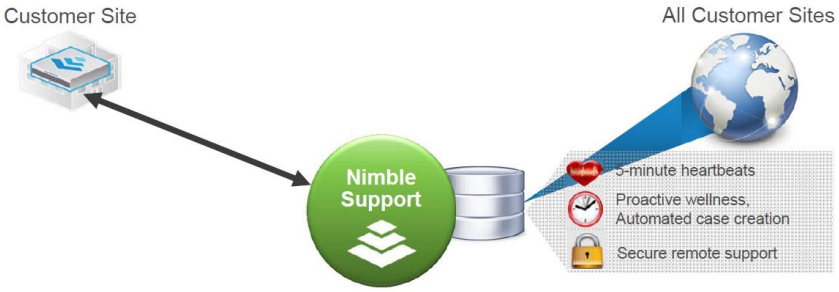
- Each Nimble Storage SAN has comprehensive monitoring, available via the secure (SSL webpage) management interface.





- By logging into the secure management interface, you will be able to centrally monitor the performance of the SAN, in addition to many of the critical physical components in the SAN (as seen above).

- If there is an equipment failure, then the System Administrator will be notified via email immediately. In addition, a ticket will be opened automatically with Nimble Storage Support, who will then contact you regarding the issue to provide technical support as needed.



- Moreover, "heartbeats" are sent on a 5-minute basis to Nimble Storage Support, to monitor the overall health of your SAN. Therefore, the firewall configuration will need to support the initiation of connections to the Internet from the SANs, over a secure connection.

3.2 File Management (Shared Folders, User Profiles, DFS, and SharePoint Foundation 2010)

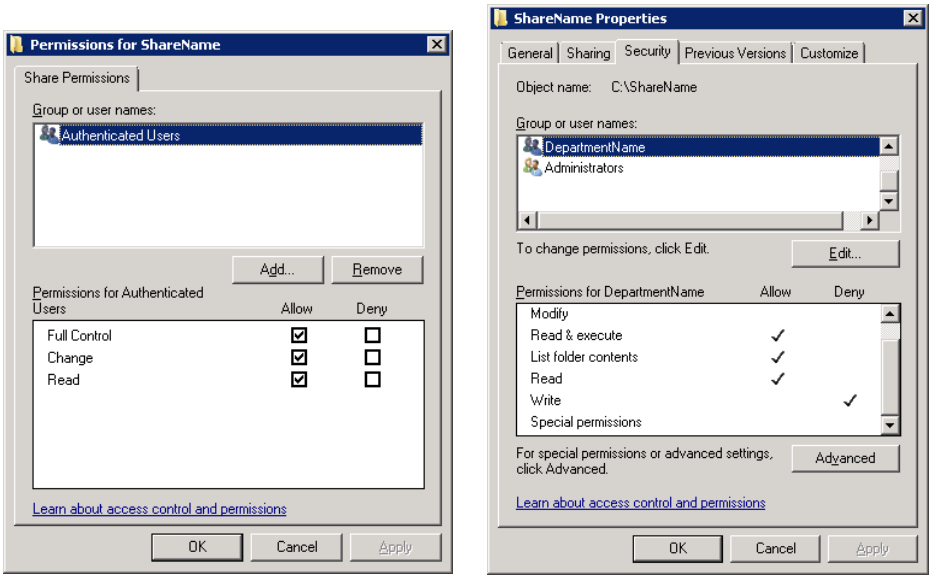
Shared Folder Management:

- For sharing files that do not require strict version control, basic file shares will be used with Active Directory security groups controlling access to them.

- Each department will have their own department level shared folder, which restricts access to only those in that department (and corporate executives).

- A corporate share will also be provided, to simplify the sharing of large documents company-wide.

- For any shared folders that contain confidential information, for added security, they will be created with a dollar sign at the end of the share name (this will hide it from the list of available shares unless you know the exact name of the shared folder).



- As seen above on the left, the Share Permissions will be set to Authenticated Users with Full Control, and then the Security (NTFS) Permissions (on the right) will be set based on department groups, in order to control access to the shared folders.

- Thus, the folder shares utilize NTFS Permissions with Active Directory security groups for access control.

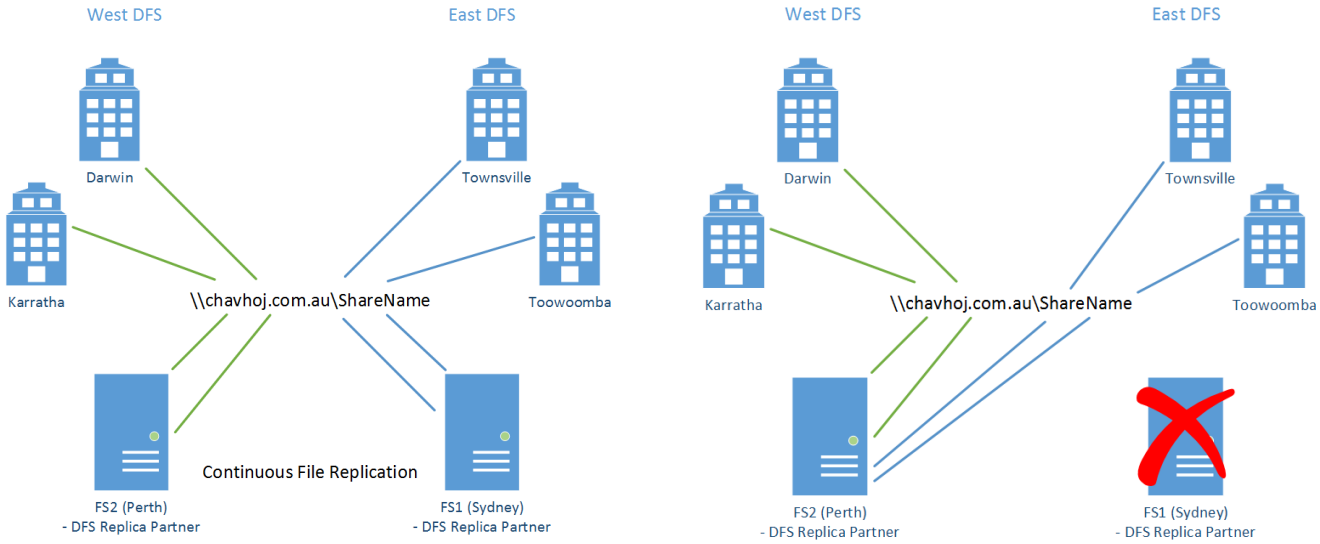
User Profile Storage:

- Employee Active Directory accounts will utilize specific folder redirection (such as their Desktop and My Documents) to a Distributed File System (DFS) share, which means that if an employee's laptop is damaged, all of their files will be safely stored in our high availability data center, and you will only need to pay to replace or repair the damaged laptop.

- Offline Folder Synchronization will be enabled on each employee's account, so that even while disconnected from the network, they will have access to their files (which will synchronize back to the data center centralized storage once they are back in the office or when they are on OpenVPN).

Distributed File System (DFS) Topology:

- The Shared Folders for Chavhoj Canada Inc. will be hosted on two member servers, File Server 1 (FS1) and File Server 2 (FS2). FS1 will reside in the Sydney data center, and FS2 will reside in the Perth data center.



- In order to guarantee resiliency, Doman-based DFS will be implemented. This means that instead of having file shares hosted on a single server at a single site, the shares will be distributed and replicated between data centers. As seen in the above on the left, when accessing shares, each site will contact the closest data center.

- In the event of a failure at one of the data centers, such as Sydney as seen above on the right, then when users try to access the shares, DFS will transparently direct them to the operational file server, which in this example is File Server 2 at Perth.

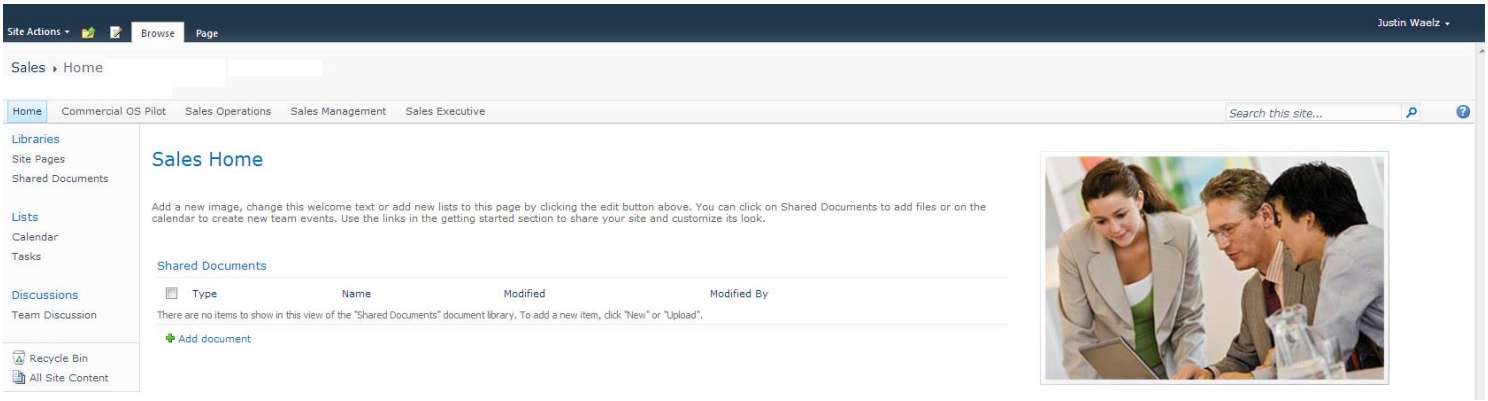
SharePoint Foundation 2010:

- For centralized document management with versioning, SharePoint Foundation 2010 sites will be used. Each department will have a dedicated SharePoint site that they only have access to, in addition to a corporate SharePoint site that the entire company can access.

- SharePoint Foundation 2010 will require at least 8GB of RAM and 4 virtual CPUs, with a SQL server backend with at least 12GB of RAM and 4 virtual CPUs. Internet Information Services (IIS) will be used to host the SharePoint sites, and that is a free software installation on the SharePoint Foundation 2010 server.

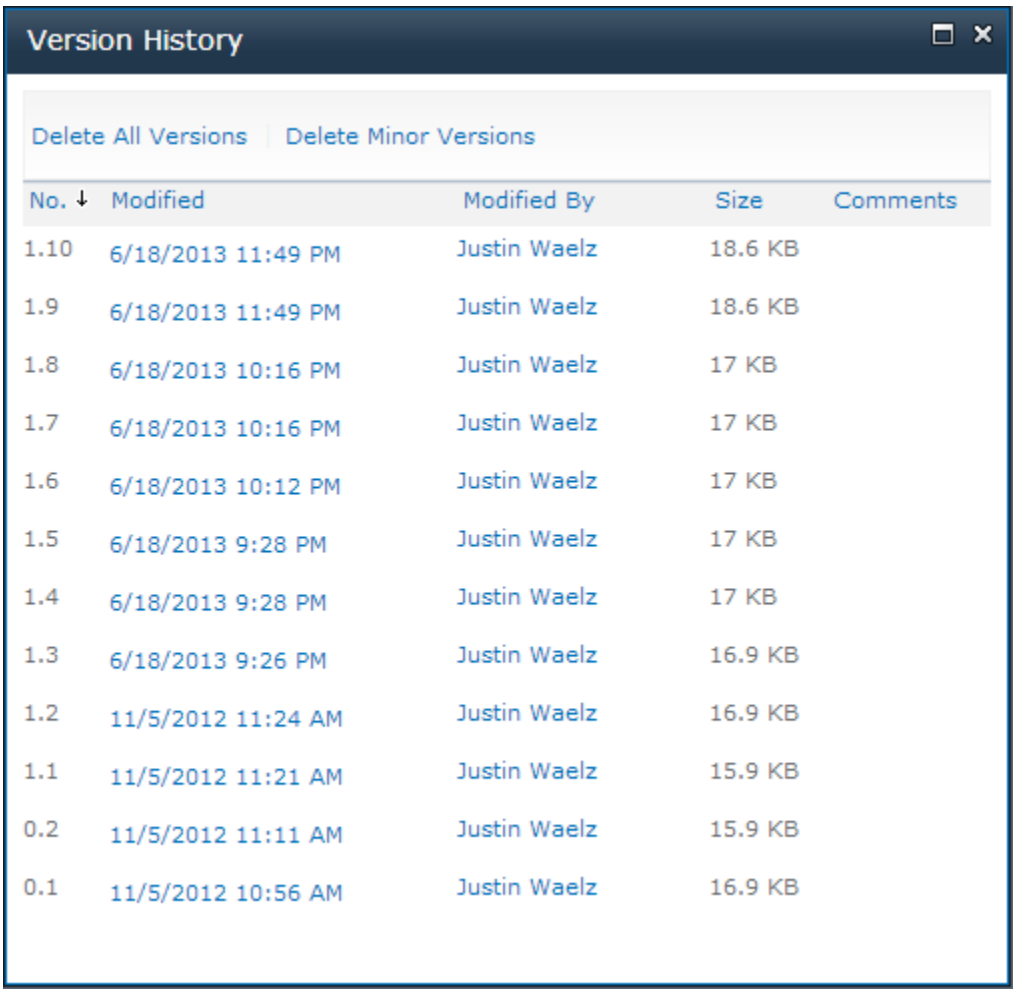
- Active Directory security groups will be used to control access to the SharePoint sites. Employees that should be allowed to upload and modify documents will be assigned the Contribute permission in SharePoint. Administrators (IT Help Desk and Executives) that have full control over the site will be assigned the Full Control permission in SharePoint. Finally, employees that should not be able to edit content in SharePoint, will be assigned the Read permission.

- All sites will be accessed over SSL (HTTPS) for added security.

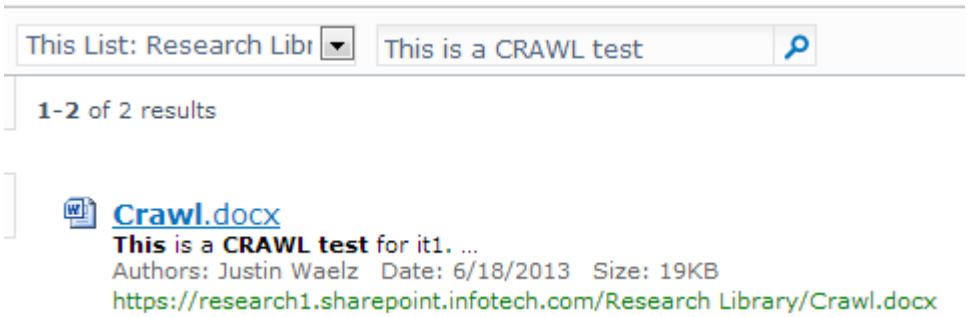


- For each department, they can have sub-sites under their main site (accessible at, for example, https://sales.sharepoint.chavhoj.com.au), for each individual project or logical grouping of files. For example, in the above image, Sales Operations would be a sub-site, and would be accessible via https://sales.sharepoint.chavhoj.com.au/salesops).
  - In order to allow for access to the SharePoint sites when not on the internal network, a public IP address can be setup for the SharePoint Foundation 2010 server, which will then require a Wildcard SSL Certificate of *.sharepoint.chavhoj.com.au.

- To simplify the management of SharePoint, users will be able to retrieve their deleted files from the site's Recycle Bin for 90 days. If the user deletes their file from the Recycle Bin, then the System Administrator can retrieve it from the secondary recycle bin (also within a 90-day period), or from a backup.



- Versioning (as seen above) and file Check Outs before editing will be enabled, to control revisions in each Document Library. Even with document versioning enabled for major and minor revisions, the database file for each site will stay under 50GB.



- As seen above, each site will have indexed content search enabled, which will allow users to quickly search for files. This will utilize Microsoft Search Server 2010 Express (installed on the SharePoint Foundation 2010 server), which will crawl through the content, allowing you to search within files for your search query.

3.3 Backup (Snapshots, CommVault, and Veeam), Archival (Tapes), and Encryption Strategy

Backup Strategy Overview – Snapshots:

- For critical storage volumes (i.e. the Exchange mailbox databases, file shares, and the SharePoint database), data snapshots will be configured that enable rapid file recovery. Each SAN snapshot includes the data changed since the last snapshot, and thus, the snapshot files are very small and easily compressed.
  - Daily Snapshots – Occur on Monday, Tuesday, Wednesday, Thursday, and Friday at 11:30 PM
    - Kept for 30 Days
  - Hourly Snapshots – Occur on Monday, Tuesday, Wednesday, Thursday, and Friday, hourly starting at 8:00 AM until 5:00 PM
    - Kept for 30 business hours
- By using snapshots, Chavhoj Canada Inc.'s IT department will be able to quickly recover files from the most commonly restored areas of email and user files.

Backup Strategy Overview – CommVault:

All applications that have data, will have CommVault backup agents installed, which will backup the folders containing user and configuration date, as per the schedule outlined in this section.

- The target for backup data is a storage volume on each SAN. This means that during a backup, data is first transferred to the SAN in Sydney, and then it is transferred to the SAN in Perth, in order to have two copies of all backup data.
- Weekly Full Backups occur every Saturday at staggered times between 8:00 PM and 3:00 AM, in order to avoid saturating the networking infrastructure.
- Incremental Backups occur every Monday, Tuesday, Wednesday, Thursday, Friday, and Sunday, at staggered times between 10:00 PM and 4:00 AM. Incremental backups were chosen for their speed and small size (as opposed to Differential Backups), meaning they can be quickly transferred to the failover data center (Perth) without utilizing extensive network resources.
- SQL Logs are backed up hourly, in addition to the above weekly and incremental schedules.
- During data backups, CommVault will perform data deduplication, which will greatly reduce the size of each backup set (and as a result, will require at least 32GB of RAM, and 6 virtual CPUs).

Backup Strategy Overview – Veeam:

Virtual machines are backed up for the purpose of operating system recovery, and not file recovery. CommVault handles file backups, and thus, Veeam backups are only concerned with preserving the virtual machines should one become corrupted or otherwise inoperable.

- Veeam backups of all virtual machine operating system drives occur weekly on Friday at 10:00 PM, and are kept for 2 weeks, purely for disaster recovery purposes. CommVault backs all critical data up separately, and in the event of a failure and recovery, a Veeam backup would be utilized, and then the required iSCSI volumes would be attached to the virtual machine, and service would be restored.

Archival Strategy Overview – Tapes:
In order to meet your retention policy of 5 years, tape backups will be utilized. Each LTO-6 tape can hold 2.5TB of raw data, or 6.25TB of compressed data.

For data with retention periods of less than 5 months, backups will be kept on the redundant, high availability SAN storage devices:
- Weekly Full Backups will have a retention period of 60 days.
- Incremental Backups will have a retention period of 14 days.
- Veeam backups will have a retention period of 2 weeks.

For data with retention periods of 5 months or more, backups will be kept on tapes, stored in the failover data center:
- Monthly Full Backups will be kept for a retention period of 5 years.

- After the retention periods have been met, CommVault and Veeam will automatically age out the data, allowing it to be deleted.

Encryption Strategy Overview:
- Employee laptops with sensitive information (such as financial information), will have TrueCrypt volumes configured, in order to guarantee data confidentiality in the event of theft.

- For data backups that contain sensitive information, CommVault will encrypt them during the backup process.

4. SERVER INFRASTRUCTURE SECURITY

4.1 Physical Infrastructure Security

As per your request, we will work with your contractors to ensure that the following physical security devices are implemented.
- Biometric access to all areas that house IT equipment, and swipe cards controlling general building access
- The installation of video surveillance equipment, in order to catch any individuals that attempt to steal or damage corporate equipment
- The installation of HVAC (Heating, Ventilation, and Air Conditioning) systems in all areas with IT equipment
- The installation of an Inert Gas Fire Suppression System (IGFSS) in each regional office's data center, in order to protect against fires
- To protect the smaller branch office IT closets, we recommend placing DuPont FE-36 fire extinguishers nearby
- In addition, the racks we have selected include locking doors to prevent tampering (see Section 9.2)

Therefore, by securing access to the IT systems, and protecting them from the environment, the overall IT Infrastructure will be physically secure.

4.2 Administrative Permissions and Management Consoles

Administrative Permission Control:

In order to reduce the potential of malware and accidental system changes from affecting our critical servers in production, only the System Administrator will be able to directly login to the severs via Remote Desktop with a highly privileged account, to be used only during emergencies.

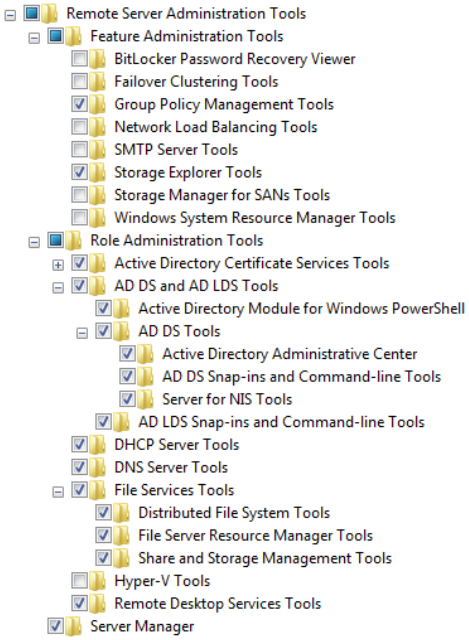
- The Principle of Least Privilege will be applied to all accounts in the IT department. This means that no accounts will be a member of the Administrators, Domain Admins, Enterprise Admins, and Schema Admins highly privileged groups.
  - Security groups for daily IT tasks (such as joining a computer to a domain) will provide the required level of access for the IT help desk team.

- The Administrator account for the entire domain will be restricted to only being used during the initial setup of the domain, and for emergency disaster recovery scenarios. A complex password for the Administrator account will be set, the account will be renamed to a fictitious employee's name, the account's description will be cleared, we will deny its ability to login to any computers over the network, and finally, the account will be disabled.

- For additional security, a decoy "Administrator" account, which has no privileges on your network, will be created. System monitoring will be configured to alert IT management to any changes to either the original Administrator account, or the decoy one.

Management Consoles:

To further prevent IT staff from directly managing critical servers via Remote Desktop, remote management tools will be deployed.



- Remote Server Administration Tools will be deployed onto each IT laptop, and then specific management features (such as those above on the left for the System Administrator), depending on their job role, will be enabled on their laptops. This will allow for the management of services, such as Active Directory Users and Computers and Group Policies (as seen above on the right), without connecting with Remote Desktop to a Domain Controller.

4.3 Antivirus (Kaspersky) and Spam Filtering (Postini)

Antivirus Software:

To secure the servers and employee laptops from viruses and other malicious intrusion, Kaspersky Endpoint Security 10 antivirus software will be installed. Kaspersky antivirus uses an administration server for centralized management, which allows you to install the software remotely onto any system connected to the domain.

- The Kaspersky Administration Kit server is the heart of the antivirus system, and will be configured to ensure that once a device joins the domain, that antivirus software will be installed automatically. As seen above, the Administration Kit will allow for computers to be grouped together (via Managed computers), so that each department, depending on their workload, can be scanned and patched at different times without affecting device performance.

- For example, full system scans will be configured to run daily starting at 6:00 PM to 7:00 PM, in order to avoid affecting the performance of end user devices and servers during business hours.

- Any device that is connected to the domain without antivirus installed, will be placed into the Unassigned computers group, as seen above, and will automatically be scheduled for immediate antivirus installation.

- Antivirus definition updates are scheduled to be installed daily between 3:00 AM and 5:00 AM on test computers, and then the following evening at 8:00 PM to 10:00 PM for all other systems. This will allow for the IT staff to prevent the deployment of any updates that cause problems during testing.

- Special antivirus policies (such as firewall management and scanning exclusions) will be configured for each type of server, because certain file antivirus operations can negatively affect system performance (such as scanning every file on SharePoint Foundation 2010 in real-time).

Spam Filtering (Postini):

In order to stop malicious content from entering Chavhoj Canada Inc.'s network via email, Postini spam filtering will be configured. This means that prior to the delivery of email messages to your on-site Exchange environment, Postini's anti-spam and malware detection scanners will have scanned the emails and quarantined anything suspicious.

Quarantine Summary 10/11/2013

To Justin Waelz

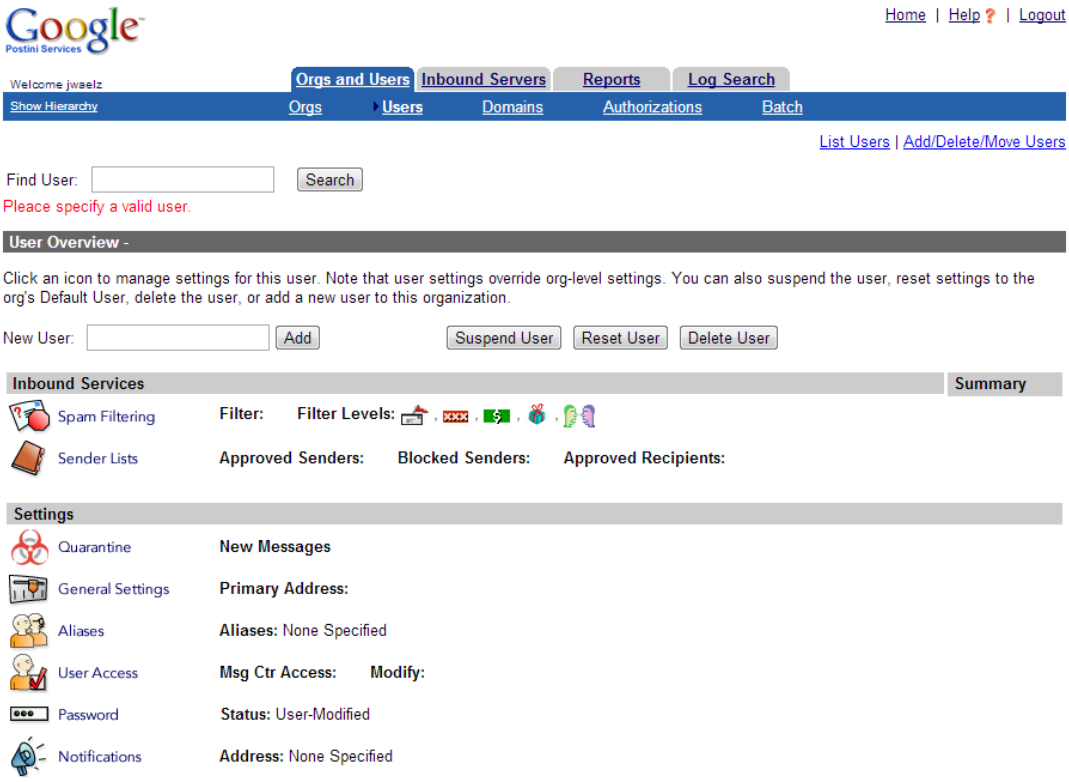
These messages were quarantined before they reached your inbox as potential spam and virus-infected messages. If there is something here that should have delivered to you, please contact your friendly neighbourhood Helpdesk

Junk Messages 1 Message

From	Subject	Date
team@email.evernote.com	Introducing the Evernote Market	10/11/2013 4:59 am

- As seen above, every day at 3:00 PM, a list of emails that were quarantined by Postini's services, will be emailed to your employees.

- In order to release an email from the spam filter, the end user will be required to submit a ticket to your IT staff. Self-service spam releases (i.e. the ability for end users to release their own spam messages) will be disabled, in order to prevent the accidental release of dangerous emails.



Google Postini Services

Home | Help | Logout

Welcome jwaelz

Orgs and Users | Inbound Servers | Reports | Log Search

Show Hierarchy | Orgs | Users | Domains | Authorizations | Batch

List Users | Add/Delete/Move Users

Find User: Search

Please specify a valid user.

User Overview -

Click an icon to manage settings for this user. Note that user settings override org-level settings. You can also suspend the user, reset settings to the org's Default User, delete the user, or add a new user to this organization.

New User: Add Suspend User Reset User Delete User

Inbound Services | Summary

Spam Filtering — Filter: Filter Levels:

Sender Lists — Approved Senders: Blocked Senders: Approved Recipients:

Settings

Quarantine — New Messages

General Settings — Primary Address:

Aliases — Aliases: None Specified

User Access — Msg Ctr Access: Modify:

Password — Status: User-Modified

Notifications — Address: None Specified

- As seen above, your IT staff will have access to the central control panel for Postini's services for Chavhoj Canada Inc., which will allow them to add users to your subscription, release quarantined messages, and setup approved safe domains that will bypass spam filtering.

5. LOCAL DEVICE AND REMOTE ACCESS SECURITY

5.1 Laptop Setup and Physical Security

Laptop Setup:

To suit your needs of a mobile workforce, we selected three different laptops models. Each laptop will be imaged to have a clean installation of Windows 7 Professional (fully patched), antivirus, OpenVPN client software, Microsoft Office 2013, Flash, Java, Google Chrome, Adobe Reader, Printers, LANDesk client software, and any other applications that your employees use on a regular basis.

- On the far left, is the Lenovo ThinkPad X1 Carbon, which is for Executive employees, and it offers high performance in a lightweight package (i5 2.70GHz CPU, 4GB of RAM, 120GB SSD).

- In the middle, is the Lenovo ThinkPad T430, which is for Management employees, and it offers high performance in a slightly heavier package (i5 2.60GHz CPU, 4GB of RAM, 500GB 7200 RPM hard drive).

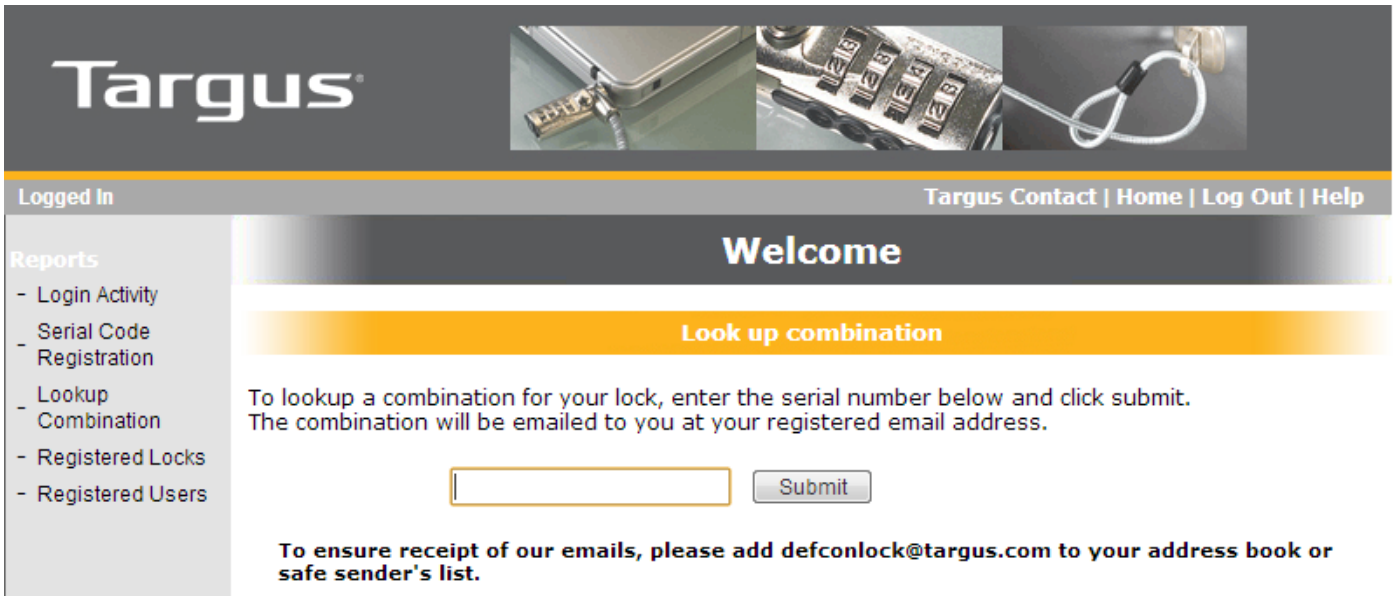
- On the far left, is the Lenovo ThinkPad E531, which is for all other employees, and it offers medium performance in a slightly bulkier package (i3 2.50GHz CPU, 4GB of RAM, 320GB 7200 RPM hard drive).

- All laptop models selected have a fingerprint reader, which will be setup for the employee when IT delivers their laptop to them. Biometric access is part of our overall server infrastructure security plan, and thus why it is important for it to be used by all employees (as opposed to their potentially weak passwords).

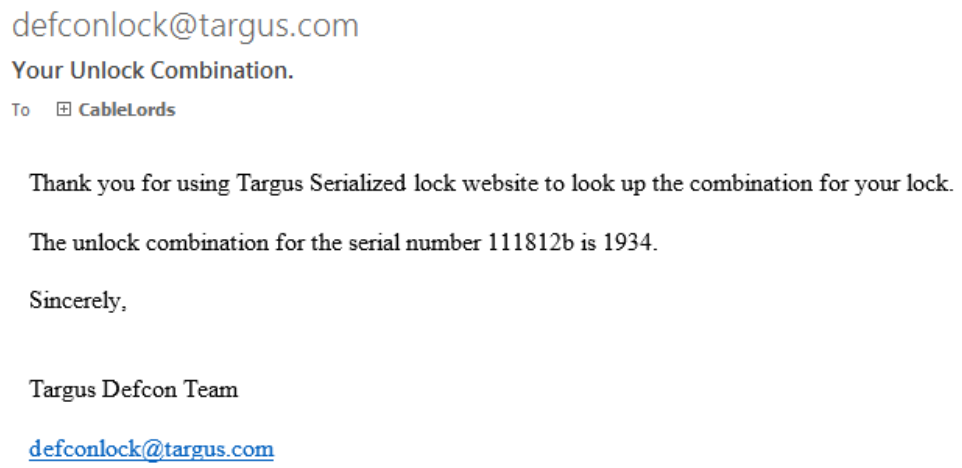
Physical Security:

All laptops users will be assigned a Targus DEFCON serialized laptop lock (which uses the Kensington Security Slot on each laptop), in order to lock their laptop to their desk, in order to prevent theft.

- Seen above, each laptop lock has a 4-digit combination (the portion in red). The code to unlock the laptop lock is stored in a secure database, managed by Targus.



- As seen above, your IT staff will be granted access to Targus' website for retrieving laptop lock combinations. In addition, Postini spam filtering will be set to allow all emails from defconlock@targus.com through the spam filter.



- As seen above, the requested laptop lock combination will be emailed to your IT staff within 30 seconds of inputting the serial number into Targus' website.

5.2 Secure Remote Access (OpenVPN)

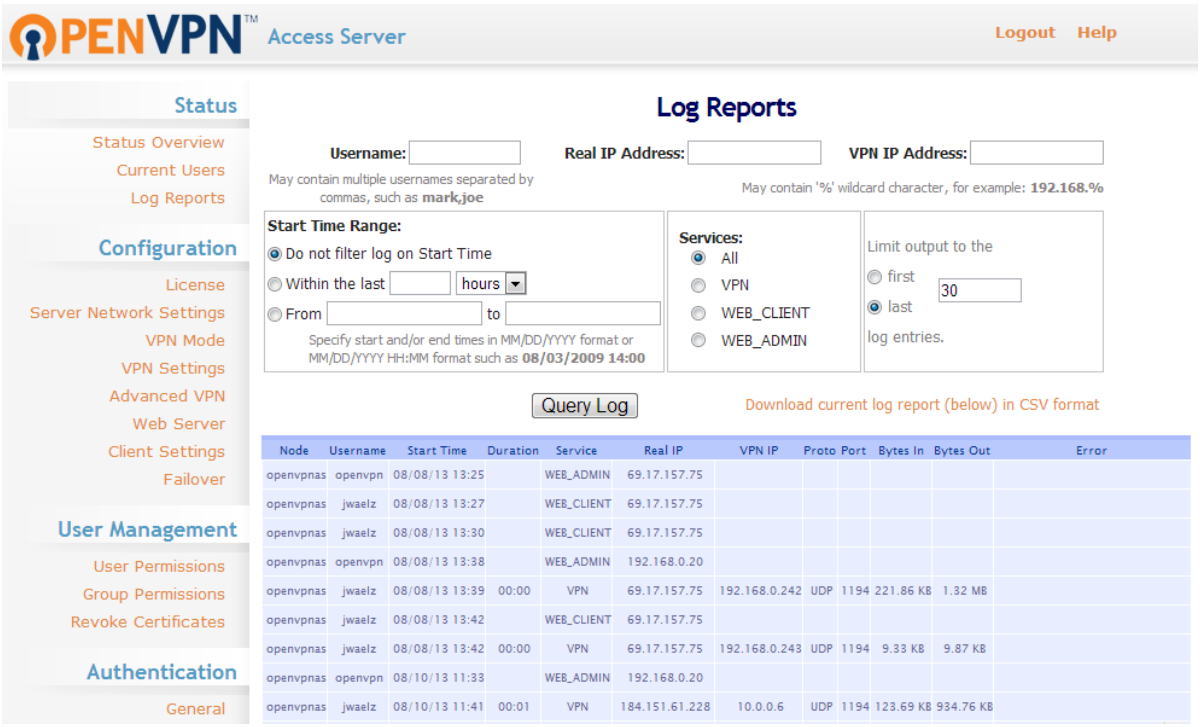
OpenVPN Access Server:

In order to allow for secure remote access to your internal resources, two OpenVPN Access Servers will be deployed in an ESXi environment. By having two servers acting in a failover cluster, you will be able to withstand the loss of an Access Server in either the Sydney or the Perth data center, without affecting external client connectivity.

- SSLv3 and TLSv1 with RC4 ciphers will be enabled, which will protect the VPN solution from the BEAST (Browser Exploit Against SSL/TLS) vulnerability, and thus improve the overall security of the VPN service.

- Authentication (username and password) to OpenVPN will use LDAP, with the username based on the sAMAccountName attribute (i.e. the username for Justin Waelz would be jwaelz) in Active Directory.

- A dedicated VLAN and IP addressing will be used for employees on OpenVPN, which will be limited regarding which networks they have access to (for example, they will not be able to access the network that the backup servers are on).



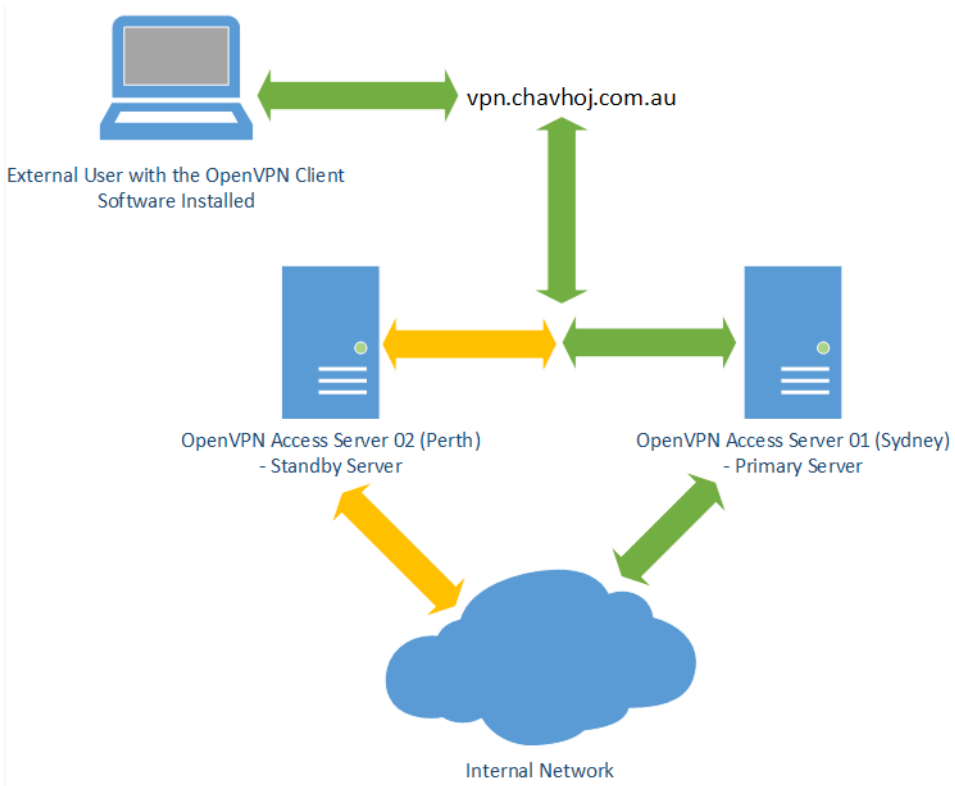
- As seen above, advanced logging will be enabled, so that access attempts from any regions where employees are not known to be, can be flagged for review, and blocked at the firewall if necessary.

- To prevent saturating the VPN service with stale connections, each session will timeout after 24 hours.

- Performance on the VPN will be limited by the external employee's Internet connection, and the average data transferred during a VPN session is under 1GB, depending on usage habits. For example, if a user is using a remote desktop session over the VPN, then less than 300MB of data will be transmitted during an 8-hour session.

OpenVPN Client Software:
Each employee laptop will require OpenVPN software to be installed. The OpenVPN software is used to connect to the Public IP address of the OpenVPN server, which will then handle the creation of a secure tunnel.

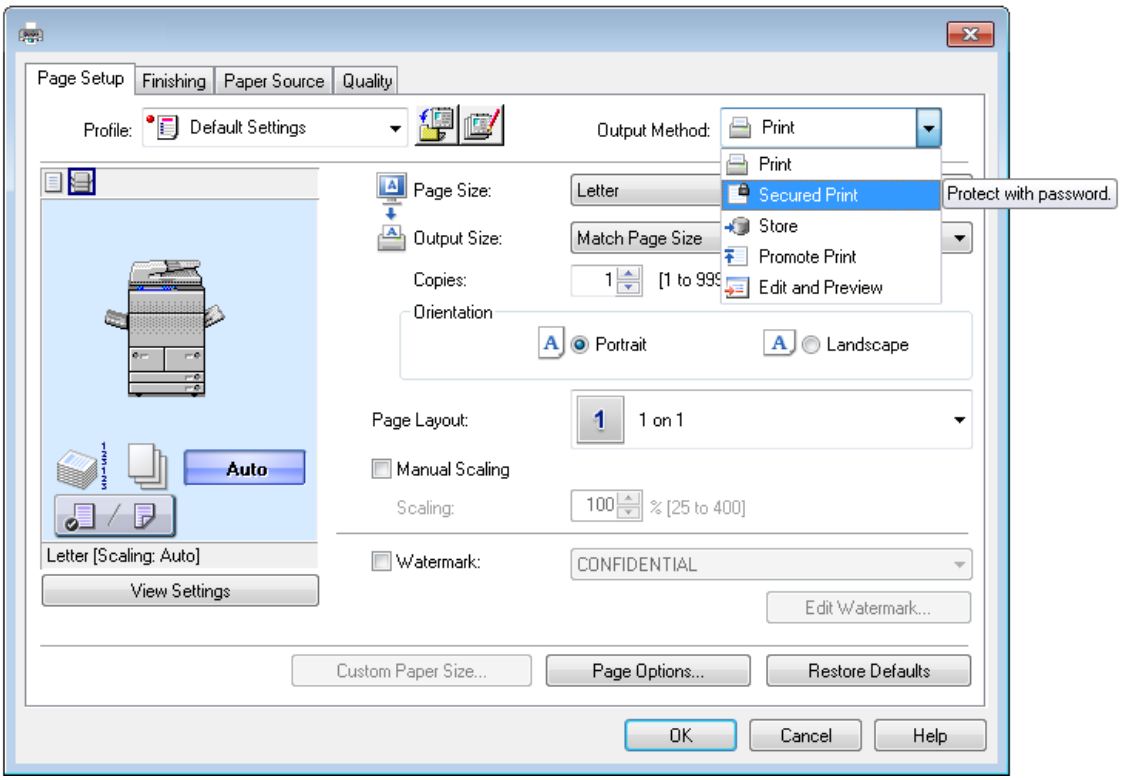
- As seen above, your external employees will launch the OpenVPN client software, and then put in the server name of vpn.chavhoj.com.au, which will resolve to the Public IP address of the OpenVPN Access Server cluster. After pressing Connect, a secure tunnel to your internal network will be established.



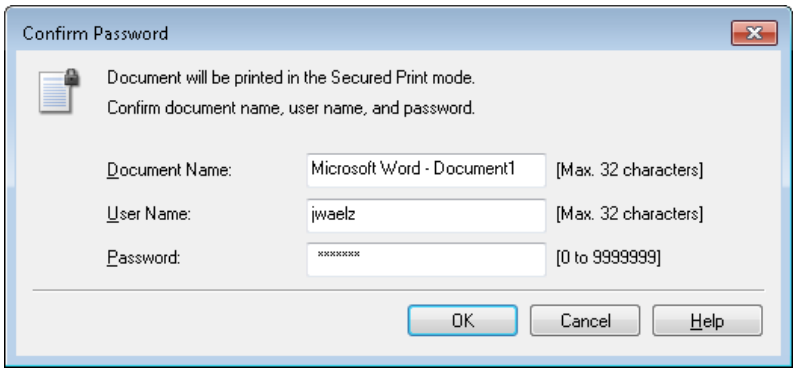
- The above logical diagram shows an OpenVPN client connecting to vpn.chavhoj.com.au, and then having a secure tunnel created through the Primary OpenVPN Access Server (the green path) to the internal network. The failover standby server (the orange path) is waiting for a failure at the primary site before it begins to service VPN access requests.

5.3 Printer Security

Our technical solution includes a printer at each office, and because the printers will be shared amongst the employees in the office, we will implement Secure Print services.



- As seen in the above image, when an employee goes to print a file, they will have the option to perform a Secure Print.



- After inputting a filename, their Active Directory account name, and a onetime use password, the employee can then send the file to the printer. Once he or she walks to the printer, they put in their Secure Printer password, and then the file is printed.

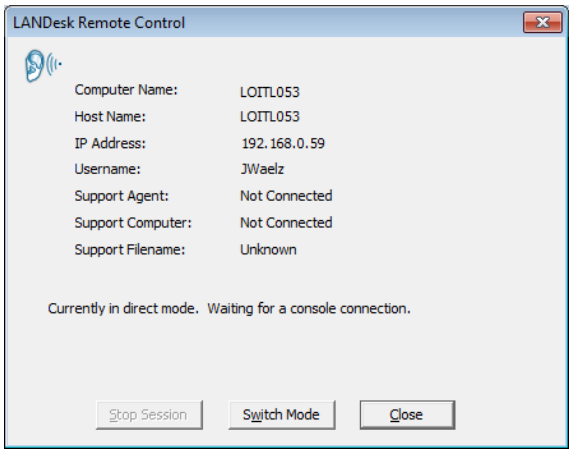
- By utilizing the Secure Print functionality of the HP LaserJet Enterprise MFP M775z printers, it will cut down on paper waste (as print jobs timeout after an hour of not being printed, as opposed to being printed right away and never being picked up).

6. IT SUPPORT SYSTEMS

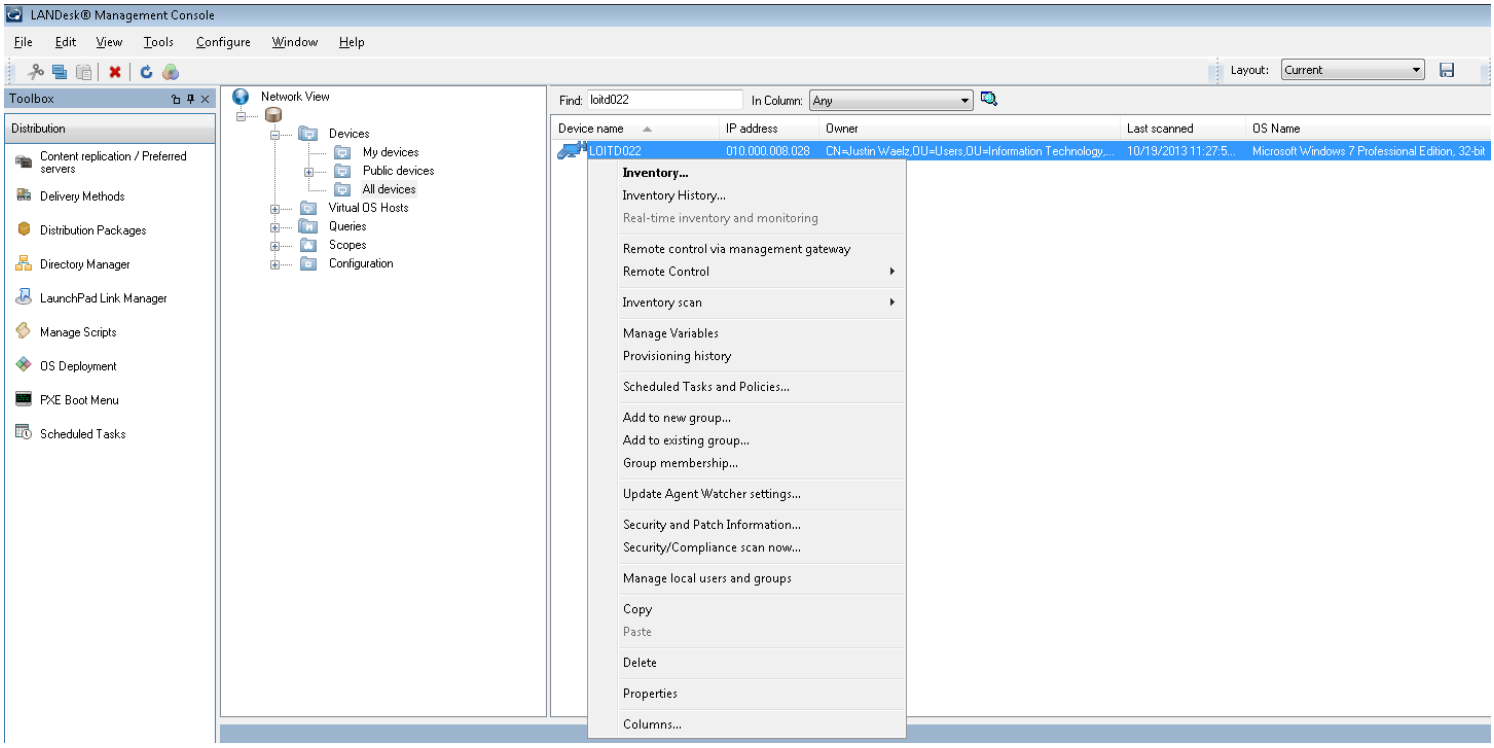
In order to efficiently manage the Windows devices on your network and respond to user support requests, our solution utilizes LANDesk and TestTrack Pro. The Windows Server 2012 virtual machine hosting these applications will require at least 8GB of RAM, and 4 virtual CPUs. In addition, a SQL backend database will be required for these services.

6.1 Computer Management (LANDesk)

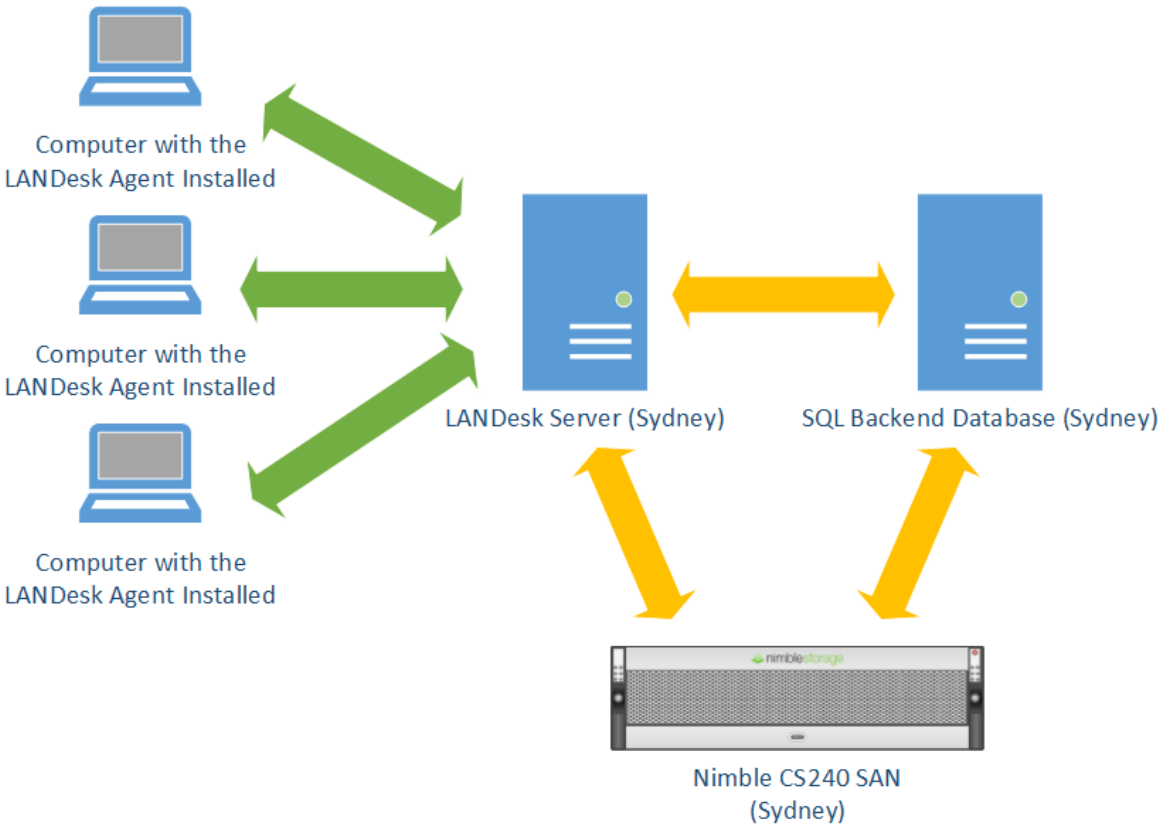
To allow IT staff to remotely manage employee workstations, deploy packages, and create an inventory of all equipment attached to the domain, LANDesk Management Suite 9.5 Suit will be deployed.



- As shown above, a lightweight application for LANDesk must be installed on all employee workstations before it can be managed via the LANDesk Management Console.



- Your IT staff will be granted access to the LANDesk Management Console, as shown above, which will allow them to remotely manage computers, deploy applications, and view inventory information.



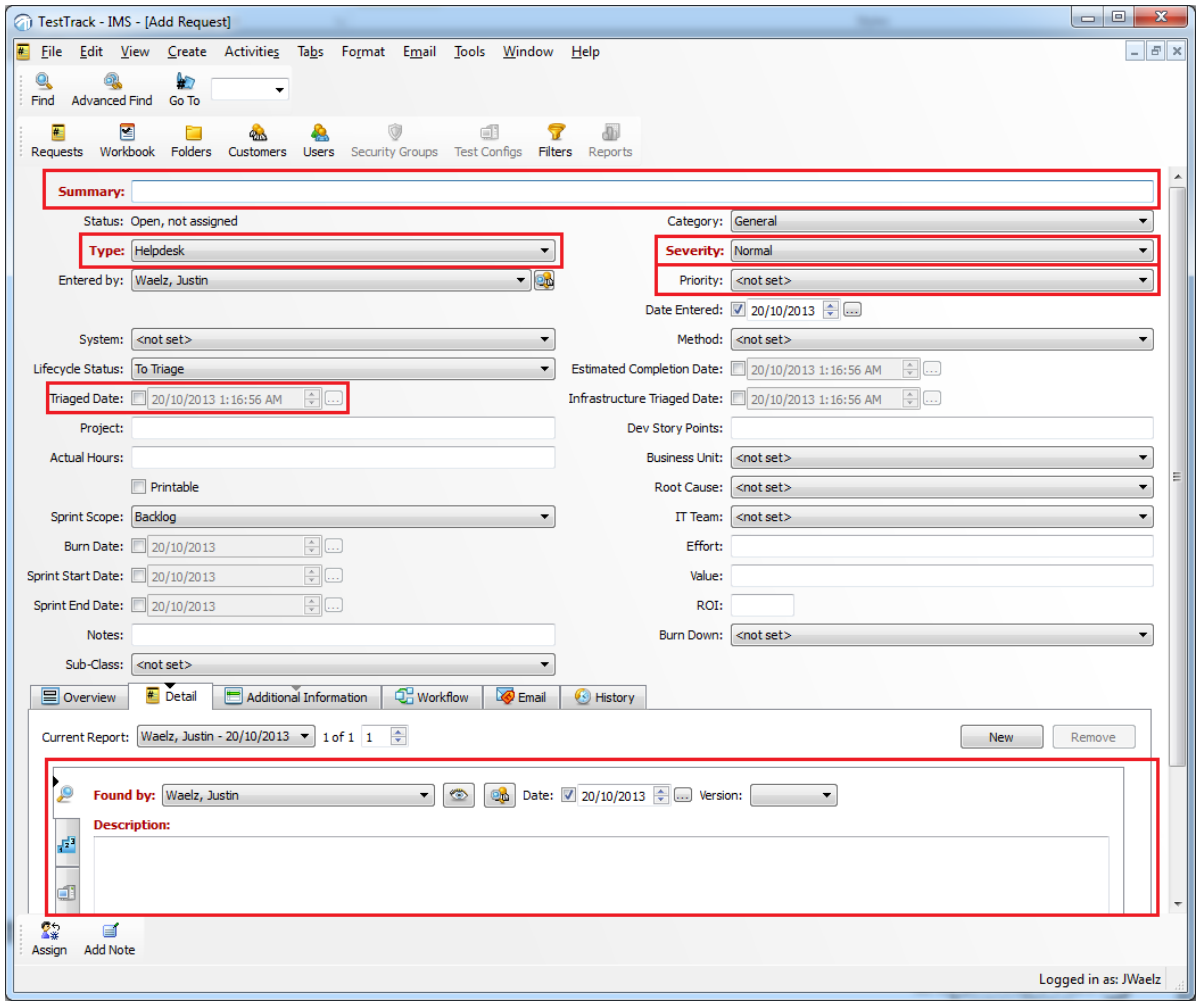
- Shown above is the logical layout of the devices required for LANDesk to function. The green arrows indicate client-server communications. All LANDesk "nodes" (employee laptops) talk to the LANDesk Server, which in turn has configuration data stored in a backend SQL database. Both the LANDesk Server and the backend SQL database have iSCSI volumes that are stored on the Nimble Storage SAN.

6.2 User Support Request Management (TestTrack Pro)

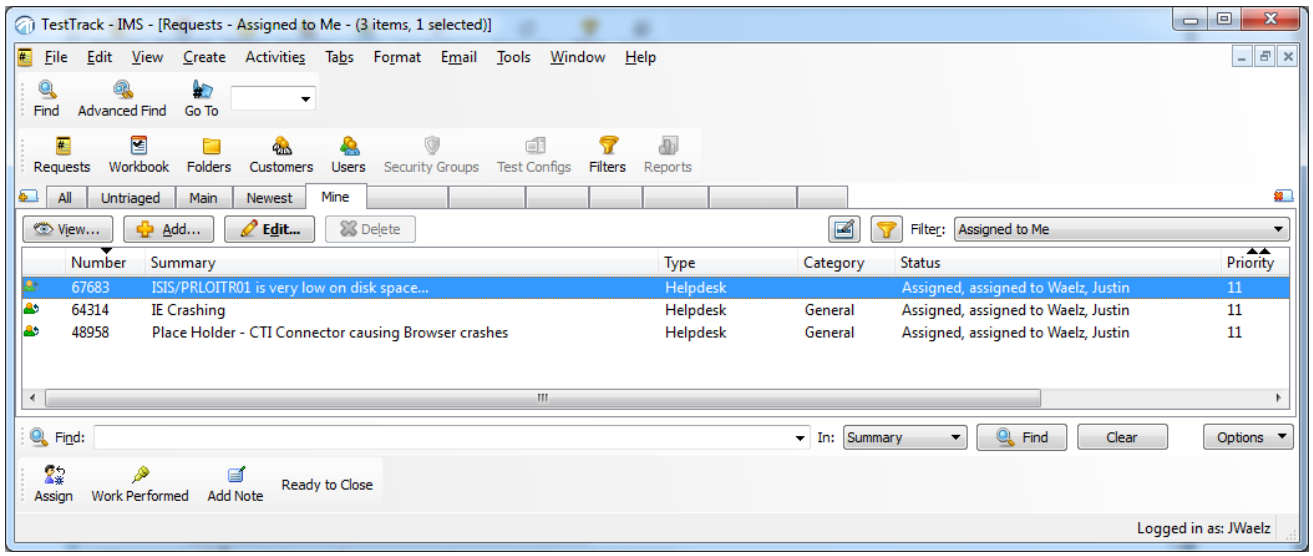
To be able to efficiently respond to end user support requests, a ticketing system will be deployed. TestTrack Pro allows for categorization, prioritization, and task workflow management of support requests, in order to ensure that requests are triaged, worked on, and completed, within a timely manner.

- TestTrack Pro requires a backend SQL database to store configuration and ticketing data.

- To allow for automated replies to be sent from TestTrack Pro to users, Exchange mail connectors will need to be setup to permit the delivery of mail from the IP address of the TestTrack Pro server. Thus, when a ticket is submitted, everyone in help desk will receive an email alert, and when a ticket is closed, the user that opened the ticket will be informed of the solution.



- As seen above in red, there are key fields that will be added to TestTrack Pro during the configuration of the application.



- Once the IT help desk employees are configured with a license, they will be able to begin working on tickets assigned to them by the Help Desk Manager, as shown above. The estimated ticket load per day to begin with is 150 tickets, and that will eventually be reduced to approximately 50 tickets per day.

7. VIRTUALIZATION

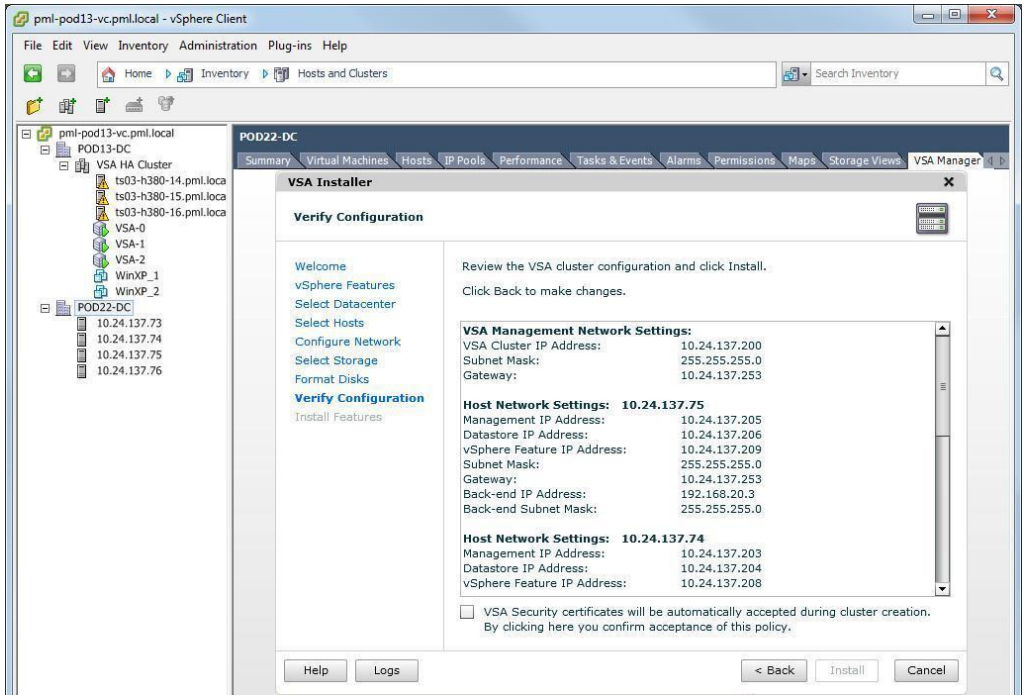
This section will describe the overall resiliency, flexibility, scalability, and management features that our virtualization solution provides. Chavhoj Canada Inc. will be using vCenter Server with Operations Management to ensure that administrators have end-to-end visibility of the virtual infrastructure, as well as comprehensive management tools.

7.1 Virtual Infrastructure Management

vCenter Server will provide centralized management of your virtual infrastructure. This will ensure that administrators can streamline security and availability, simplify day-to-day tasks, and reduce the complexity of managing the virtual infrastructure. vCenter server will be fully integrated with Microsoft Active Directory, in order to granularly control and limit access to authorized users only.

By providing a single console that is globally accessible for the IT staff, all configurations are performed in one place, and in addition, vCenter Server provides access to tools such as:

- **vMotion** – vMotion allows for the manual migration of virtual machines, as well as load balancing
- **High Availability** – High Availability automatically load balances critical systems to ensure availability
- **Fault Tolerance** – Fault Tolerance ensures the continuous operation of systems even in the case of server failure



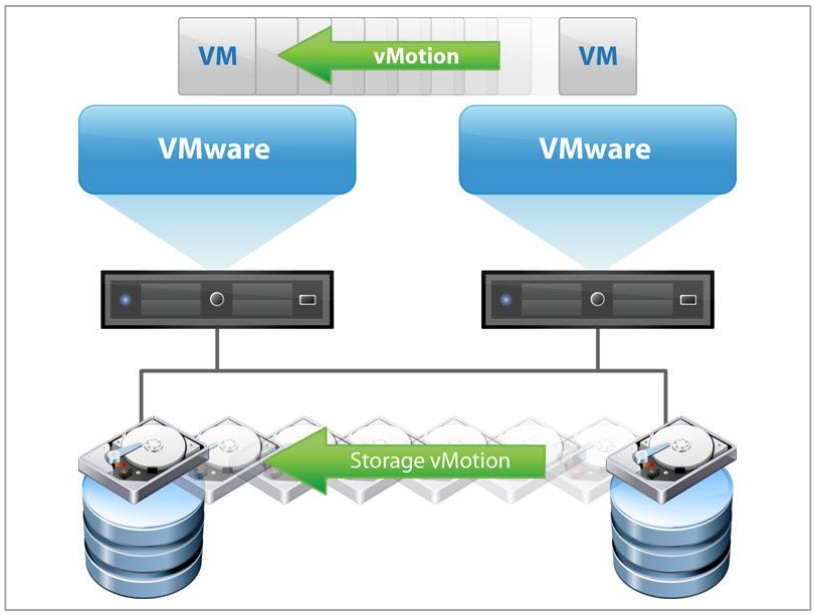
As seen above, the vCenter console provides an overview of all configurations that have been applied to a specific data center (and all nodes in it). This is a great tool for troubleshooting configurations.

7.2 Fault Tolerance and Load Balancing

A number of features have been implemented for providing a fault tolerant and high-performance virtual infrastructure. In this section, motion, high-availability, and fault tolerance will be covered, as well as the Distributed Resource Scheduler (DRS) and Site Recovery Manager (SRM).

vMotion:

- vMotion is a critical tool that will allow administrators to move and relocate virtual machines to other vSphere hosts, as well as to different geographical sites.
  - This process is very useful in case system upgrades are required. In this case, the system administrator can gracefully migrate a virtual machine to a different physical server, while achieving zero downtime in the process



The image above shows vMotion in progress.

High Availability and Fault Tolerance:

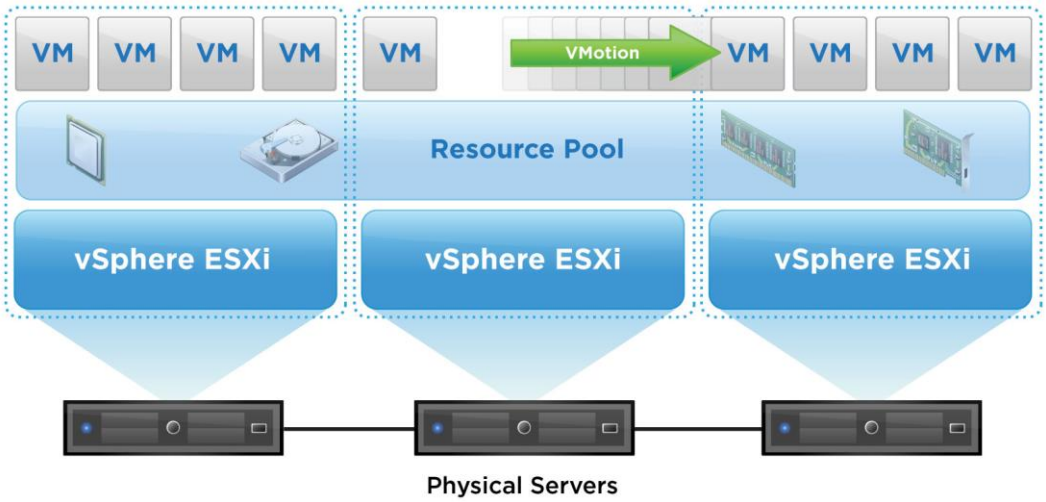
The vCenter High Availability feature provides automated and manual failover and failback. This will ensure that the availability of critical services exists at not only the server level, but also at the application level.

Chavhoj Canada Inc.'s virtual infrastructure has been configured with a high level of resilience. In addition to the High Availability features described above, Fault Tolerance has also been implemented. Fault Tolerance features allow for a virtual server to fail at one site, and then have it be brought back up at another site.

Distributed Resource Scheduler (DRS):
Distributed Resource Scheduler (DRS) is a powerful tool, which automatically optimizes virtual machine performance.

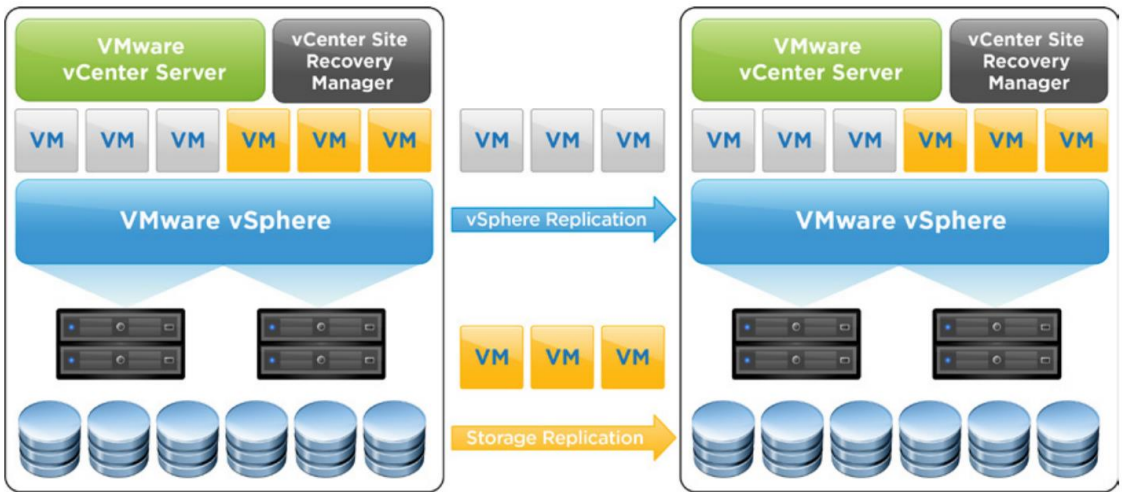
By leveraging resource availability on other nodes in the virtual infrastructure, DRS is able to analyze resource availability and schedule accordingly, which ensures that systems are not overprovisioned, thus making resources more available.

DRS looks at the overall load of the individual vCenter node, as well as the resource utilization of other nodes. It is able to determine if free resources are available, and if so, it schedules the hardware resources accordingly.



The above image is a diagram showing the ability of virtual machines to switch resource pools based on availability of resources (i.e. load balancing).

Site Recovery Manager (SRM):
Site Recovery Manager (SRM) is an essential tool to provide complete reliability, by ensuring seamless transitions of a whole site's virtual infrastructure.



The above image shows SRM in action, migrating a site as well as its storage to a different site.

7.3 Virtual Infrastructure Practical Load Balancing

This section will provide an overview of the virtualized servers, as well as the practical applications for the failover and load balancing features.

- The overall virtual infrastructure topology can be seen in Section 2.1 and in Section 2.2.

Virtual Infrastructure Overview:

Below is an overview of the virtual machines that will be running on virtual infrastructure. In addition, resource utilizations have been calculated (as seen to the right of each ESXi server), taking into account vendor specific recommendations plus 10%. The resources are based on CPU and RAM.

Sydney (Primary Site)

ESXi 1

- Domain Controller 01 (DHCP 01)
- OpenVPN Access Server 01
- Kaspersky Administration Server
- LANDesk and TestTrack Pro
- Microsoft SQL Server 2012
- File Server 1 (FS1)
- BlackBerry Enterprise Server (BES) 5.0.4 Express
- DNS 01 (Red Hat Enterprise Linux 6)
- vCenter
- Veeam and CommVault
- Lync Server 2013

ESXi 2

- SharePoint Foundation 2010
- Windows Server Update Services (WSUS)
- Exchange
  - Hub Transport and Client Access Server 01
  - Mailbox Database 01
- Domain Controller 02
- SolarWinds System Monitor

Perth (Secondary/Failover Site)

ESXi 3

- Exchange
  - Hub Transport and Client Access Server 02
  - Mailbox Database 02
- Domain Controller 03 (DHCP 02)

ESXi 4

- Domain Controller 04
- DNS 02 (Red Hat Enterprise Linux 6)
- File Server 02 (FS2)
- OpenVPN Access Server 02

As you can see by the committed resources for each ESXi host, the Perth site has been setup in such a way, where the load factor is significantly less than the Sydney site. This enables us to achieve a high level of fault tolerance as well as on-demand resource scheduling, by automatically moving a virtual machine from one site to another.

Flexible Resources:

As mentioned, the virtual infrastructure for Chavhoj Canada Inc. has been designed to offer maximum scalability and performance.

These "flexible" resources (the orange section of the resource charts) are just that, they are flexible. vCenter will automatically allocate them as "burst resources" to virtual machines that are in need of them.

- For example, if the Microsoft SQL Server 2012 virtual machine requires more resources than that which are committed to it, the virtual machine will utilize the flexible resources in the resource pool.

Complete Site Redundancy:
As an additional precaution, in addition to vCenter failover features, we have ensured that there is complete site redundancy at the architectural level for the virtualization system.

The precautions in place are as follows:
Primary Site Independency – The primary site, Sydney, is completely independent. In the event Perth, the secondary site, completely fails, no data will be lost, and all critical systems and infrastructure will continue to function as usual, as Perth is mainly used for load balancing.

Primary Site Failure – In the event that the Sydney site fails, safeguards are in place to ensure that Chavhoj Canada Inc.'s systems continue to function. Perth has a complete real-time shadow copy of the Sydney site's virtual machines. With the help of SRM, we are able to instantly failover from Sydney to Perth.

The virtual machine site copies are as follows:

Sydney	**Perth**
ESXi 1	ESXi 4 has a copy of ESXi 1
ESXi 2	ESXi 3 has a copy of ESXi 2

Practical Inta-Site and Inter-Site Load Balancing:
This section will focus on the practical application of load balancing within Chavhoj Canada Inc.'s virtual environment with vMotion and DRS.

As mentioned above, the proper resource allocation and scheduling has allowed for flexibility in load balancing. The two main technologies that will be used by Chavhoj Canada Inc.'s IT staff are vMotion (live virtual machine migration) and DRS.

vMotion allows for a live virtual machine, or a whole node, to be moved, with zero downtime, even to a different geographical site. This is crucial for two reasons:
1. This will allow for a node being serviced because of a hardware upgrade or failure to move to another node in real-time, without suffering an outage.
2. Balancing server loads by manually moving systems that are overloaded to another server with more free resources, allows for optimal virtual machine performance. However, this is the least likely usage of vMotion, as we have implemented DRS to automatically schedule resources in real-time.

As stated above, Distributed Resource Scheduling is crucial for Chavhoj Canada Inc. to ensure the high availability of the virtual infrastructure. This will ensure that, if, for example, the Microsoft SQL Server 2012 virtual machine on ESXi Node 1 requires more CPU resources, it will be able to analyze the cluster for resources.
- Since ESXi Node 2 is closest, it will see if there are resources available on it, and if so, it will utilize those resources. This provides maximum availability by ensuring that systems are not overscheduled.

8. DAEMON SERVICES

8.1 Domain Name System (DNS)

The DNS solution that we are implementing in Chavhoj Canada Inc.'s environment, is based on Berkeley Internet Name Daemon (BIND) 9.

- BIND 9 is a high-performance, secure, and reliable DNS server that will be installed on a UNIX-like operating system, Red Hat Enterprise Linux 6.
- Once configured, BIND 9 will offer unparalleled performance, rock solid security, and very light resource usage for your DNS services.
- BIND 9 offers full compatibility with all Windows services that are being deployed as part of our IT solution.

The following sections will focus mainly on the load balancing and security features that will be implemented for Chavhoj Canada Inc.'s DNS server.

DNS Deployment:

Our DNS solution will employ a Master-Slave topology for DNS. There will be 2 DNS servers, one at each site (1 at Sydney and 1 at Perth).

- Sydney DNS Server – Master
  - Clients at Sydney, Toowoomba, and Townsville will use the Sydney DNS server as their primary DNS server, and Perth for their secondary DNS server.

- Perth DNS Server – Slave
  - Clients at Perth, Karratha, and Darwin will use the Perth DNS server as their primary DNS server, and Sydney for their secondary DNS server.

This type of deployment will ensure fast and reliable name resolution based on the client's geographical location.

DNS Redundancy:

The DNS server infrastructure contains both a primary and secondary DNS server. In case of a server failure, the other DNS server has a copy of Chavhoj Canada Inc.'s DNS zones.

- In addition, changes are propagated in real-time due to the *allow-notify* directive, which informs the other DNS server of zone changes, so that zone transfers (updates) may occur.

DNS Security – BIND 9:

We have implemented a number of security features to protect Chavhoj Canada Inc. against DNS-based malicious intrusions. The following section explains the security configurations that we will use, which are specific to BIND 9.

Domain Name System Security Extensions (DNSSEC) – DNSSEC is a feature that cryptographically signs the zone transfers and zone files with asynchronous (public-private key) encryption. This ensures that zone transfers (updates) are not tampered with. Using this security feature helps to prevent against spoofed DNS server updates, which hackers may use in order to derail clients from accessing resources.

Transaction Signature (TSIG) – TSIG is another security feature, which requires the DNS servers to verify each other, not only at the "IP-Address only" level, but at the private/public keys level as well. Once our DNS servers are authenticated with each other, they will not receive updates from potentially malicious sources.

DNS Security – Red Hat Enterprise Linux 6:
In addition to hardening (securing) the BIND 9 DNS service, special care has been taken to secure the operating system as well, on which the DNS service is running on. Some crucial configuration steps are as follows:
Security-Enhanced Linux (SELinux) – SELinux ensures that processes are extremely restricted and locked down, making sure that processes are only able to access resources which they have been specifically allowed.

Jails – The DNS service will be been running in an isolated environment, known as a Jail, with no access to tools that it does not need. For example, this means that if a hacker does gain access to the system, they will be unable to do anything.

8.2 Dynamic Host Configuration Protocol (DHCP)

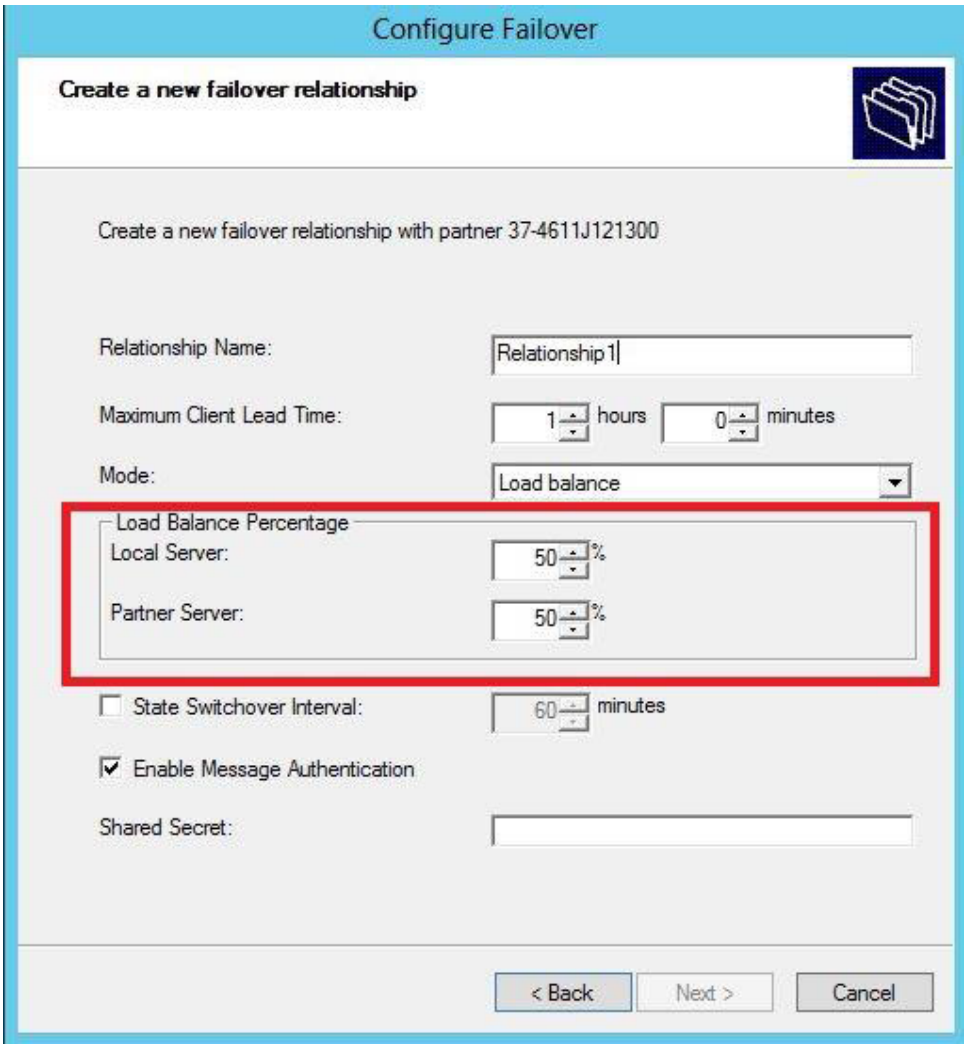
DHCP will be installed as a server role on a hardened virtual instance of Microsoft Windows Server 2012. This will ensure complete integration with Windows clients.

Redundancy and Load Balancing:
A number of features have been implemented to ensure DHCP redundancy and load balancing, which will guarantee optimal performance. Outlined below are the DHCP techniques we will implement for Chavhoj Canada Inc.

Multiple DHCP Servers – Each regional office is equipped with a DHCP server for redundancy.

Failover Cluster – This option places the Sydney DHCP server in a cluster with the redundant Perth DHCP server, and the Perth DHCP server will assume the load if the primary DHCP server fails at Sydney, and vice versa.

Load Sharing Failover – Additionally, the Microsoft Windows Server 2012 operating system has allowed us the ability to use the new Load Sharing Failover mode. In this mode, the two DHCP servers simultaneously serve IP addresses and options to clients on a given subnet. The client requests are load balanced and shared between the two DHCP servers. If a failure does occur, the remaining server takes the entire load.



The above image is a sample configuration showing the setup page for Load Sharing Failover. Note the "Shard Secret", which can be set to ensure that only authorized servers can load balance.

DHCP for the Telephony Infrastructure:

Each VoIP phone will receive its IP address configuration from the DHCP server, and will include option 150.

- Option 150 is the IP address of the Trivial File Transfer Protocol (TFTP) server, which will be the BE6000 to which the phone is near. This will allow the phone to pick up any changes automatically on startup, and the server can push out changes and restarts to the phone as needed.

DHCP Scopes:

The network for DHCP that Chavhoj Canada Inc. will be using is 10.0.0.0 /8 (10.<Site>.<VLAN>.15-254).

Below is the scope chart for the sites, as well as the specialized VLANs.

10.	SITE	VLAN	.15 – 254
10.	10 – Sydney	**5** – Management	.15 – 254
	20 – Toowoomba	**10** – Admin	
	30 – Townsville	**20** – Office	
	40 – Perth	**30** – Sales	
	50 – Karratha	**40** - Finance	
	60 – Darwin	**50** – HR	
		60 – IT	
		70 – Servers	
		80 – Wi-Fi	
		90 – Guest Wi-Fi	
		110 – Admin Voice	
		120 – Office Voice	
		130 – Sales Voice	
		140 – Finance Voice	
		150 – HR Voice	
		160 – IT Voice	
		200 – Native	
		999 – Black hole	

For example, the DHCP pool for Sales in Perth would be 10.40.30.15-254. The DHCP pool for IT Voice in Sydney would be 10.10.160.15-254. Addresses not listed for the network ranges are reserved for static addressing.

8.3 Printer Infrastructure

For Chavhoj Canada Inc., we have selected the HP LaserJet Enterprise MFP M775z colour printer with network connectivity.

Printer Location:

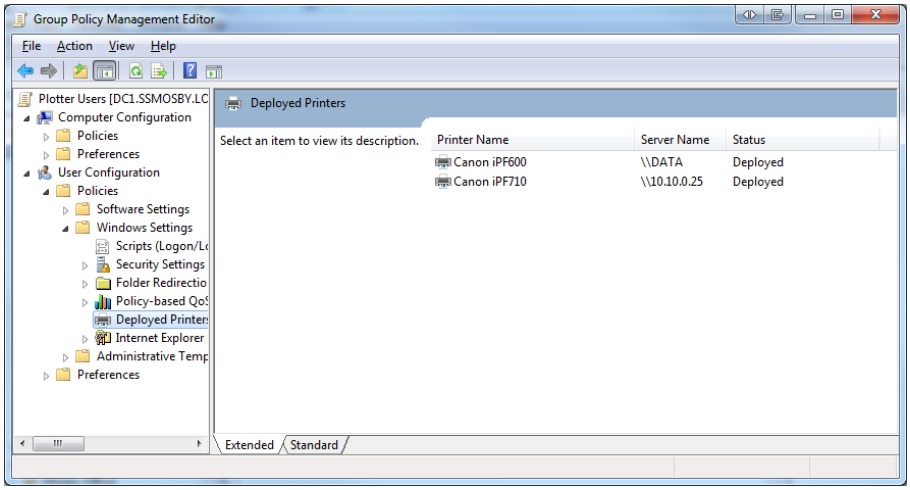
In order to accommodate proper business functions, one printer will be placed at each site in a shared location.

Printer Management:

- The printers will be deployed to users via Group Policy (the printer deployed will depend on the location of the user, as defined by their Security Group memberships).

- The print services are enabled by installing drivers onto the Domain Controllers. Users will be unable to connect to the printers directly, which ensures that only the print servers can manage the print jobs.

- In addition to being able to control access to the printers, this will simplify the driver install process, because the Domain Controllers will contain all the required device drivers in a centralized location.



The image above shows a printer published in Active Directory through Group Policy.

- The printer model selected has a number of management capabilities in order to streamline management. HP, the manufacturer, has a number of MIBs (Management Information Bases, which integrate into our SolarWinds centralized system management solution), which can alert administrators of system failures, toner levels, and paper levels.

- In addition to this, the printer has chargeback support, meaning that departments can be individually billed for print jobs if required, which will ensure users are more environmentally conscious when printing.

9. DATA CENTER INFRASTRUCTURE AND MANAGEMENT

We have taken every effort to ensure that Chavhoj Canada Inc.'s data centers are state of the art. In order to ensure operation even in blackouts and brownouts, we have implemented a two-tier solution.

9.1 Power Infrastructure and Equipment Locations

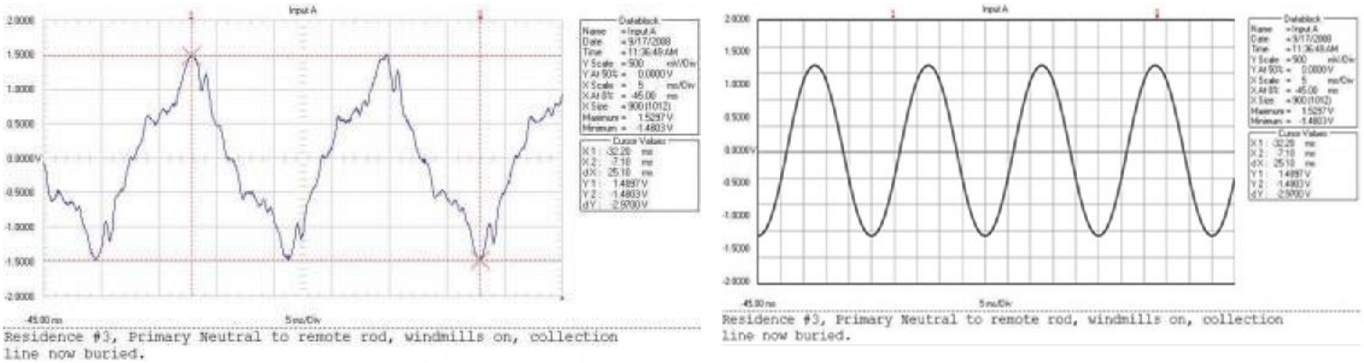
Power Infrastructure – Uninterruptable Power Supplies (UPSs):

In the case of UPS Power Supplies, we have selected the APC 3000 series, which offer reliable power in any condition.

- Unlike some other UPS equipment, the APC 3000 series uses the AC line power as the primary power source, which prevents unnecessary wear on the battery, prolonging the life of the unit.

- In addition to this, the power is constantly filtered. This ensures that there is no unneeded load and irregular conditions on the hardware power supplies (that are connected to the UPS).

- In case of a brownout condition, the automatic voltage regulation circuitry is activated to correct the problem. The battery and inverter circuitry supplies the backup power in case of a blackout.



The above image is a comparison of dirty versus filtered electricity. The filtered electricity is smoothed out by the APC UPS, and this provides clean power to the hardware and prolongs life.

Power Infrastructure – Natural Gas Generator:

The second line of electrical defense is the Generac QT045 45kW Natural gas generator, which is installed at each data center.

- This generator has been chosen because of the fuel type, natural gas.

- Unlike traditional diesel-powered generators, natural gas-type generators do not require fuel to be added continuously from an external source.

- As long as the generator is connected directly to a source of natural gas, it is able to function indefinitely.

- Furthermore, the generator model was selected due to real-world testing and performance data gathered in comparison to other leading generators. Moreover, this generator has AC filtering, providing reliable and clean power to all of the dependent devices.

9.2 Data Center Rack Security

To ensure that only authorized personnel have access to racks, we have integrated the APC NetBotz rack locks. These rack locks will secure the racks and prevent unauthorized access while adding logging, time restrictions, on-demand access to third parties, and environmental sensors for temperate and humidity.

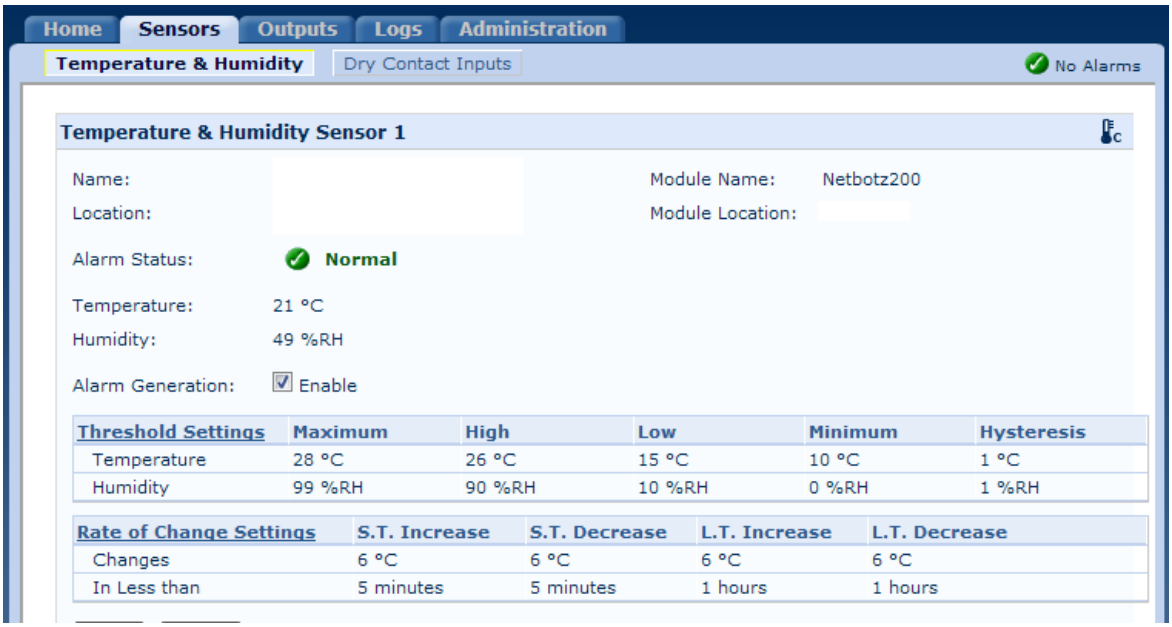
- Configurable alerts allow for a proactive approach in determining failing data center climate controls, which will help to prolong the life of the data center equipment.

The APC NetBotz will utilize two-factor authentication:

- Keys
- Smartcards with Radio-Frequency Identification (RFID) chips

In order to further secure and lock-down the system, the APC NetBotz are networked and support integration into Active Directory via LDAP. This allows you to grant access to only certain users or groups, as well as keep a log of all access attempts.

APC NetBotz will be installed at every regional office rack in Sydney and Perth, as well as in all branch office wiring closets.



The above image shows some of the monitoring features available with APC NetBotz.

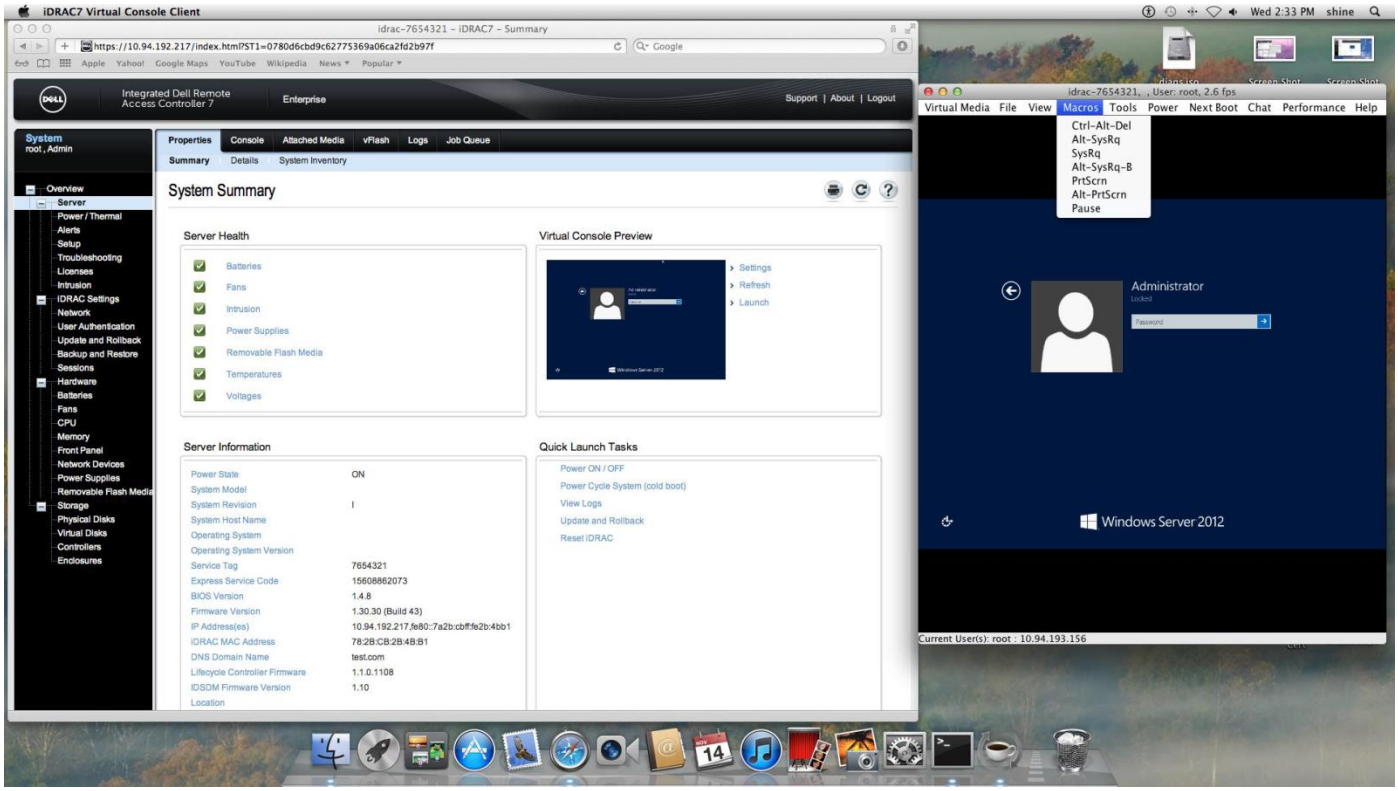
Content Expert: Serge Trunkin

9.3 Remote Server Management

If remote configuration of the server hardware is required, two means of management will be installed at the regional offices.

- Dell iDRAC
  - The iDRAC is the primary remote access tool, which allows you to configure the servers from outside of the data center, as well as perform management tasks on various configurations, such as controlling the networking hardware that is built-in into the server.

  - In addition to this, it grants us access to the Virtual Console and Virtual Media, which allows us to install/upgrade the operating system, or to just simply control the unit as if there was a keyboard and monitor attached. The iDRACs will be fully integrated into the Active Directory infrastructure, in order to control user access.



The above image is a screenshot of the iDRAC interface running on a PowerEdge R910 server, managing a Microsoft Windows Server 2012 operating system.

- IOGear IP KVM GCN1000
  - If, in the unlikely event, the iDRAC fails, the fallback method is to use the IOGear IP KVM, which will allow for a physical Keyboard, Video display, and Mouse-like experience from any authorized Internet-connected device.

10. ACTIVE DIRECTORY ARCHITECTURE

10.1 Microsoft Windows Server 2012

The underlying operating system for all Microsoft services will be Microsoft Windows Server 2012.

Microsoft Windows Server 2012's minimum requirements are as follows:
CPU – 1.4GHz 64-bit processor
RAM – 512MB
Storage – 32GB

As per best practices, the above minimum requirements will be met or exceeded in order to ensure optimal performance.

10.2 Domain Controllers

We will be installing 4 Domain Controllers using Microsoft Windows Server 2012.

- There will be 2 Domain Controllers at each regional office running in the ESXi infrastructure.
- The Flexible Single Master Operation (FSMO) roles will be split between the Domain Controllers in Sydney.
- All Domain Controllers are Global Catalog servers, and will replicate objects between each other.

10.3 Organizational Units

- After creating a new forest for the chavhoj.com.au domain, we will create an Organizational Unit hierarchical structure separating Australia into West and East.
- For West and East, the folder structure will be broken down further by city.
- Within each city, there will be a folder for each department, and in every department, there will be a folder for Users and Groups, and Computer objects.
- Security Groups will also be created based on the departments, in order to easily manage access to resources.

10.4 Group Policies

Group Policies that focus on security will be configured depending on an employee's security group memberships. For example, Executive employees might be able to have limited local administrative permissions to install software on their assigned laptop, while regular employees will not be able to run any installers.

- The group policies created will align with Microsoft's best practices and industry standards.

10.5 Active Directory Sites

The IP address ranges for West and East will be used to control which Domain Controller a client will use to authenticate to the domain.

- For example, if an employee in the West site IP address range is trying to login, then their account will be authenticated by a Domain Controller in the Perth data center.

Sites are also used to facilitate the replication of domain information between the data centers on a schedule.

11. MOBILE COMMUNICATIONS

11.1 Mobile Device Policy

Mobile Device Policies will be applied to employee phones (via either ActiveSync or BES) to ensure that they comply with our overall security plan for Chavhoj Canada Inc.'s mobile data.

- Mobile Policies will be applied depending on the department that the employee is in.
- The policies applied to the mobile devices will not limit the basic functionality of the device, but rather, they will focus on securing the data contained on the mobile device (for example, a device password and device encryption will be enforced).

11.2 BlackBerry Enterprise Server (BES) 5.0.4 Express

BlackBerry Enterprise Server (BES) 5.0.4 Express will be used to control older BlackBerry devices, while modern BlackBerry devices will be connected to ActiveSync. BES requires a backend Microsoft SQL Server 2012 database, which is available in Sydney's virtualized infrastructure.

BlackBerry Enterprise Server (BES) 5.0.4 Express' minimum requirements are as follows:
CPU – 1.4GHz 64-bit processor
RAM – 2GB
Storage – 32GB

As per best practices, the above minimum requirements will be met or exceeded in order to ensure optimal performance.

BES Policies will be applied to older BlackBerry devices, with a focus on usability and data security.

12. MAIL SERVERS

12.1 Microsoft Exchange 2010

Microsoft Exchange 2010 has been selected to handle email services for Chavhoj Canada Inc.

Microsoft Exchange 2010's minimum requirements are as follows:
CPU – 2.1GHz Dual Core 64-bit processor
RAM for the Hub Transport and Client Access Server Roles Combined) – 4GB

RAM for the Mailbox Role – 4GB plus an average of 15MB per mailbox

- Chavhoj Canada Inc. has 135 employees, and with 20% growth (162 employees total), an additional 2.5GB of memory will be required.
  - To allow for optimal performance, 8GB of RAM will be used for the mailbox role servers

Storage (for the Exchange to be installed) – 30GB (the mailboxes are stored on iSCSI volumes)

As per best practices, the above minimum requirements will be met or exceeded in order to ensure optimal performance.

12.2 Exchange Roles

Each regional office will have 2 Exchange virtual machines, split into the following configuration.

- Hub Transport and Client Access Role
  - Postini spam filtering will be configured to forward safe email messages to the Exchange mail infrastructure
- Mailbox Role
  - The two mailbox servers will be configured in a Database Availability Group (DAG), so that if Sydney goes down, for example, the mailbox server in Perth will be able to begin servicing requests

By separating the Exchange 2010 roles, our solution will be resilient and efficient due to load balancing.

12.3 Database Availability Group (DAG)

For high availability, the database mailbox roles are configured in a Database Availability Group (DAG). Each mailbox database is stored on a SAN volume, and is protected with regular backups. If an entire mailbox server goes down, the DAG partner will begin servicing all email requests. The mailbox databases are kept synchronized via DAG, to make sure that failover is possible at any time.

13. PATCH MANAGEMENT

13.1 Windows Server Update Services (WSUS)

Windows Server Update Services (WSUS) will be deployed in order to create centralized patch management.

WSUS' minimum requirements are as follows:
CPU – 1.4GHz 64-bit processor
RAM – 1GB
Storage – 15GB

As per best practices, the above minimum requirements will be met or exceeded in order to ensure optimal performance.

WSUS will be installed on a Microsoft Windows Server 2012 virtual machine in Sydney. WSUS is not a critical service, and can withstand a few hours of downtime (and thus why a single server will be used for WSUS).

- Sydney's WSUS server will obtain Microsoft updates directly from Microsoft's upstream servers.
- Windows Updates will be stored locally to save on network bandwidth during patch deployments.
- Patches will be deployed to a group of test workstations first, and then approved for installation after business hours for each department.
    - The patching cycle will begin the week after Patch Tuesday (the second Tuesday of each month), to give the IT staff time to test the patches before deploying, yet while not being too far behind on Microsoft patches.

14. VIDEOCONFERENCING AND INSTANT MESSAGING

14.1 Microsoft Lync Server 2013

Microsoft Lync Server 2013 is an optional component for your IT infrastructure, which will provide videoconferencing and instant messaging services for your employees. Microsoft Lync Server 2013 will be installed on a separate virtual machine on Microsoft Windows Server 2012 in the Sydney data center.

- Since you have chosen to utilize Microsoft Lync Server 2013, we have included information about it in this section.

Microsoft Lync Server 2013's minimum requirements are as follows:
CPU – 1.4 GHz 64-bit processor
RAM –1GB
Storage – 15GB

As per best practices, the above minimum requirements will be met or exceeded in order to ensure optimal performance.

15. LOCAL ACCESS AND DISTRIBUTION INFRASTRUCTURE

The Local Area Network (LAN) can be broken down into two separate configurations, being the branch offices and the regional offices. See Section 2.4 for a topology of the regional offices of Sydney and Perth, and Section 2.5 for the branch offices of Toowoomba, Townsville, Karratha, and Darwin, in addition to the IP addressing scheme and Virtual LAN (VLAN) assignments. All regular ports on the two switch models used are gigabit, and the network cabling throughout all buildings is CAT6, in order to support this speed and any future performance increases. One of our ISPs, Optus, will install the required network cabling, including cubical drops and wiring to the network rooms.

Regional Offices – Each regional office has two Cisco 3750X 24-port switches for the Distribution Layer, and two Cisco 2960X 48-port switches for the Access Layer (one for each floor of the building, see Section 2.4 for more details).

Branch Offices – Each branch office has two Cisco 3750X 24-port switches for the Distribution Layer, and one Cisco 2960X 48-port switch for the Access Layer (see Section 2.5 for more details).

All switches on the LAN will be setup to allow configuration and maintenance remotely through Secure Shell (SSH), and locally through the console port. This will allow an IT technician to troubleshoot problems efficiently, while keeping the devices secure.

Technical Overview:

The LAN has been designed to be fully redundant, with backup paths throughout, so that any one failed network link will not stop data from flowing across the network. At the same time, precautions have been taken to prevent switching loops and to speed up network convergence. In order to provide a fast, secure, and reliable design, the following features have been added:

Virtual LANs (VLANs) – To separate logical data types, multiple VLANs have been created. This will help to control traffic by setting up specific VLAN priorities and Quality of Service (QoS). A list of the VLANs created can be seen in Section 2.7. VLAN information will be shared between devices by two VLAN Trunking Protocol (VTP) servers (the Cisco 3750X Distribution Layer switches at each regional office). All Cisco 2960X Access Layer switches will be in client mode. Spanning tree priorities will be modified to help balance the traffic between Distribution Layer switches, and can be seen in Section 2.7.

Enhanced Interior Gateway Routing Protocol (EIGRP) – For fast convergence and network learning, EIGRP will be used on all routing devices. All EIGRP packets will be encrypted.

Hot Standby Router Protocol (HSRP) – By using HSRP on the routers, one virtual gateway can be advertised by the DHCP servers. This way, if a router goes down, the standby router will take over the job of the virtual gateway, and traffic will continue to flow without the need to change the default gateway on end devices. All HSRP updates will be encrypted.

Rapid Per-VLAN Spanning Tree+ (Rapid PVST+) – For rapid network convergence, as well as modified priorities to balance VLANs across the Distribution layer switches, Rapid PVST+ will be used. PortFast will also be enabled on all end device interfaces on the Access Layer switches.

EtherChannel – All connections between the Distribution and Access Layer will be over paired aggregated links, or EtherChannels. This includes the connection between the two Distribution Layer switches. EtherChannel helps to provide a scalable increase in bandwidth, as well as quasi-load balancing.

VLAN Blackhole – For security reasons, all unused ports will be assigned to a VLAN Blackhole, as described in the VLAN table in Section 2.7. Any device connected to such a port will be on a VLAN that is not allowed anywhere on the network. This only applies to the ports with nothing connected to them on the switches. We understand the mobile desires of your company, and as such, MAC filtering is not being implemented.

Bridge Protocol Data Unit (BPDU) Guard – For security reasons, BPDU guard will be enabled on all PortFast enabled ports, except where our Cisco Lightweight Access Points are connected. If a device is detected on a guarded port that sends out BPDUs, such as a switch, then the port will be shutdown and stay down for 10 minutes after the offending device is disconnected. This is to help protect against rogue network devices being connected to the Chavhoj Canada Inc.'s network.

Power over Ethernet (PoE) – PoE will be enabled on all Access Layer ports connected to a Voice over Internet Protocol (VoIP) phone, so that the VoIP phones will receive power.

Addressing Scheme – The IP addressing scheme for all offices will follow the same scheme 10.<Site>.<VLAN>.15-254, where <Site> refers to the site numbers, and <VLAN> refers to the VLAN numbers in Section 2.7. The reason the final octet starts at 15, is to allow for a range of static addresses at the beginning of each subnet. These static addresses will likely only be used for servers.

Passwords and Encryption – Update packets will be encrypted to ensure that no one intruding into the network can learn its layout. Passwords will also be used for the console port, Secure Shell (SSH), and enable account. These passwords will also be encrypted using the *service password-encryption* command.

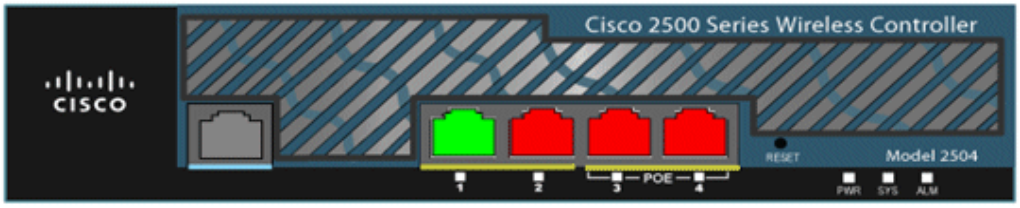
16. LOCAL WIRELESS ARCHITECTURE AND AUTHENTICATION

16.1 Cisco Wireless LAN Controllers (WLCs)

Cisco Wireless LAN Controllers (WLCs) allow for centralized, simplified wireless configuration. With redundancy at both regional offices, the wireless management system will always be accessible and available for administration operations. The Cisco WLCs will allow the configuration of wireless policies and security settings.

Hardware Specifications:

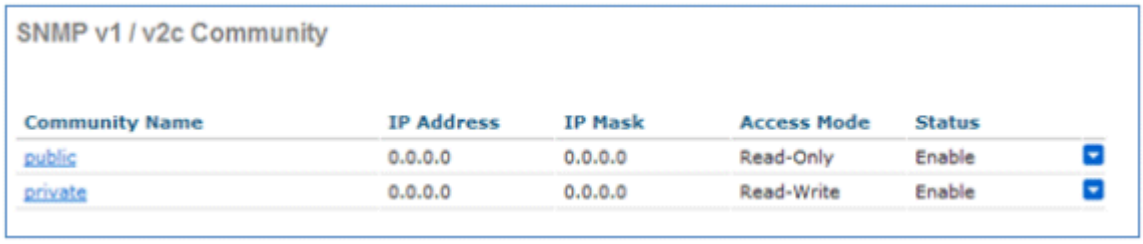
- Data Ports – 4 x 1Gbps Ethernet ports
- Console Port – 1x RJ45
- Power Supply – 1x external 48 volt power supply



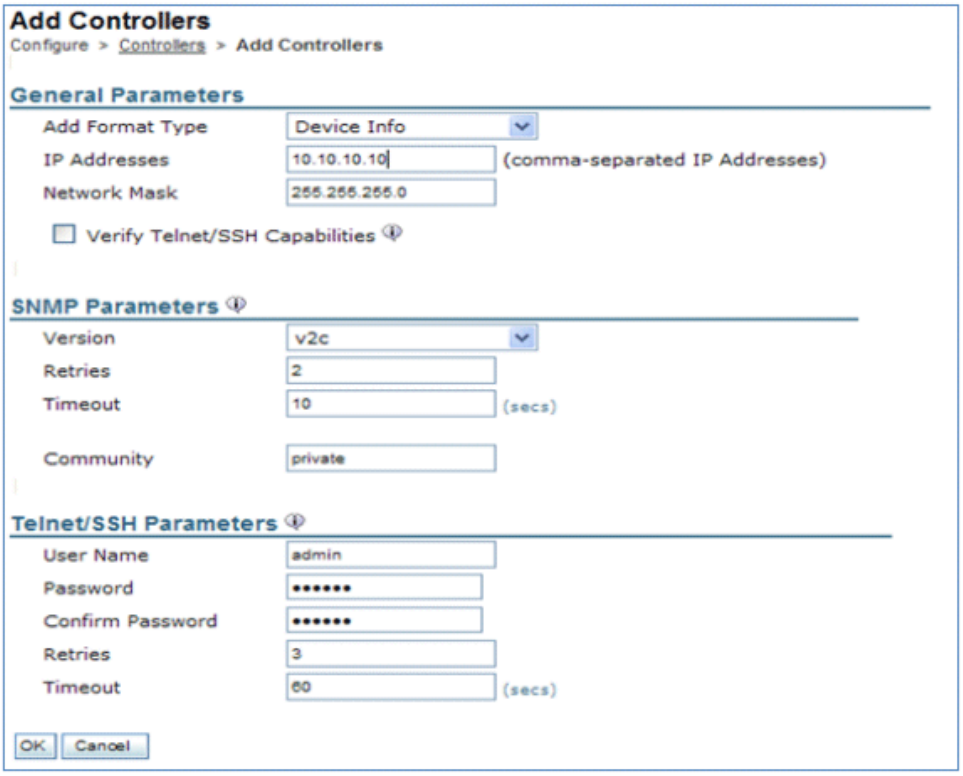
The image above shows the port placement on a Cisco 2500 WLC.

16.2 Cisco Wireless Control System (WCS)

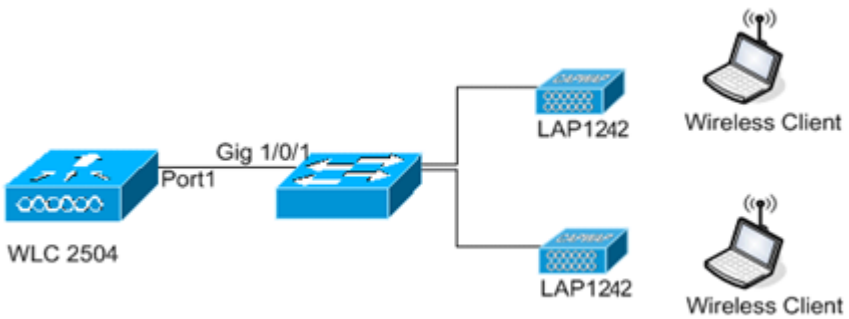
The Cisco Wireless Control System (WCS) is the management software used to manage the Cisco 2500 series WLC in order to provide advanced management features. Simple Network Management Protocol version 2 (SNMPv2) will be locked down on the Cisco 2500 WLC, in order to prevent security risks.



The correct, secure configuration for SNMPv2 on the Cisco 2500 WLC, is shown above.



In the above image, the Cisco WLC has been added successfully, and is now ready to be provisioned by the Cisco WCS.



The diagram above shows the logical placement of the Cisco WLC.

Content Expert: Travis Vanos

16.3 Cisco Lightweight Access Points

Cisco Lightweight Access Points are used at both branch and regional offices for local wireless access.

- Two access points are used at each branch office, and two access points are used on each floor at the regional offices.

Hardware Features:

- Radio Mode – Dual-radio operation mode (2.4Ghz and 5GHz)
- Console Port – 1x RJ45
- UL 2043 compliance
- Anti-theft features

17. SECURE CORPORATE CLIENT INTERNET ACCESS

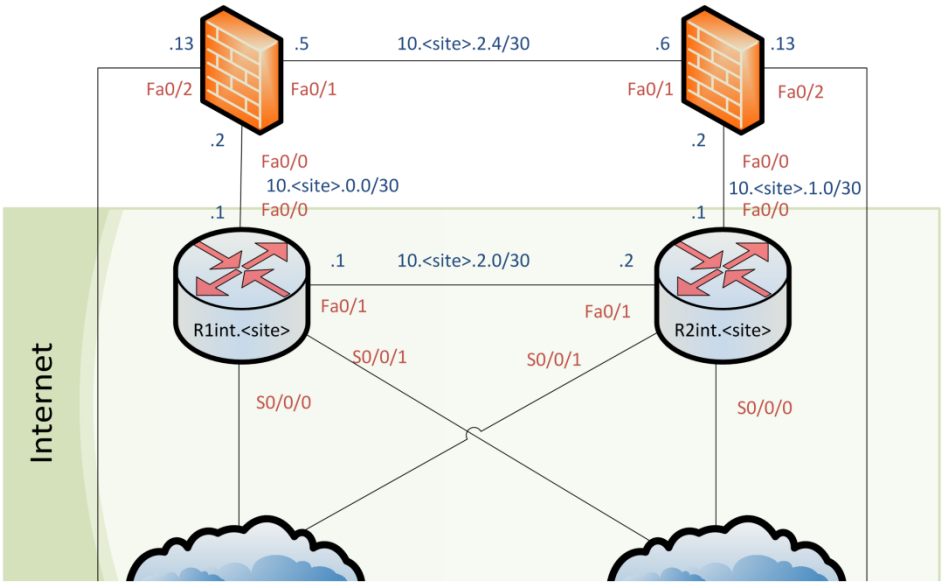
17.1 Cisco ASA 5525-X Firewalls

Four Cisco ASA 5525X firewalls will be placed in an active/passive configuration at the regional offices. Thus, at any one time, there will be two active firewalls, one at each data center.

- All traffic from each office leaves through either of the two active firewalls.

- Access Control Lists (ACLs) have been configured and Integrated with Active Directory for seamless access management.

- Web authentication with the Cisco Adaptive Security Device Manager (ASDM) utilizes Remote Authentication Dial In User Service (RADIUS).
  - This allows for central access management, and reduces the potential risk of web-based attacks on any firewall or unauthorized configuration changes.



The logical topology above shows the placement of the firewalls for a data center.

Content Expert: Travis Vanos

Hardware Specifications:

- 2Gbps stateful inspection throughput
- Able to support 20,000 connections per second, and 500,000 concurrent sessions
- Supports up to 200 VLANs
- 12GB of RAM
- 8GB of Flash Memory
- 120GB SSD
- 8 Gigabit Ethernet Ports
- Redundant power supply

By utilizing Cisco ASA 5525X firewalls with Active Directory integration, puts Chavhoj Canada Inc. in compliance of 7 of the 12 requirements for Payment Card Industry Data Security Standard (PCI DSS).

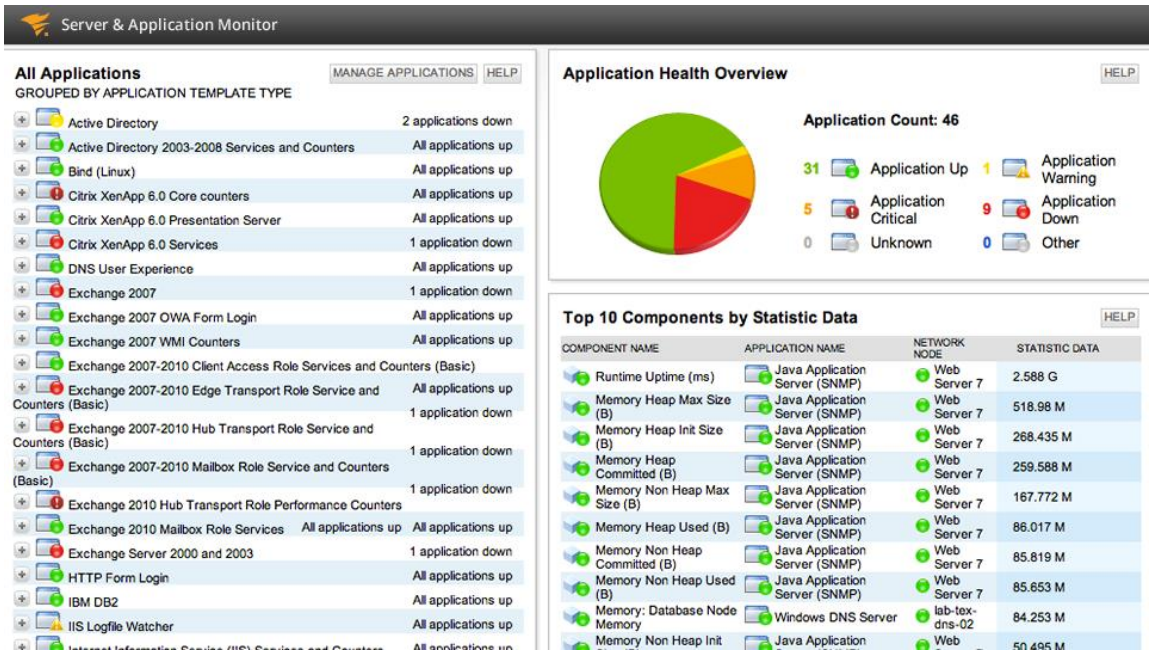
18. CENTRALIZED SYSTEM MONITORING

18.1 SolarWinds

SolarWinds has been chosen to fulfill a myriad of network management, monitoring, and discovery tools for the IT infrastructure. SolarWinds will be hosted on a virtual machine in the Sydney data center, on Microsoft Windows Server 2012.

Key Features:

- Scheduled Configuration Backups
- Policy Management
- Role-Based Access Control
- Multivendor Support
- Configuration Change History
- Web-Based Configuration Viewing, Tracking, and Reporting

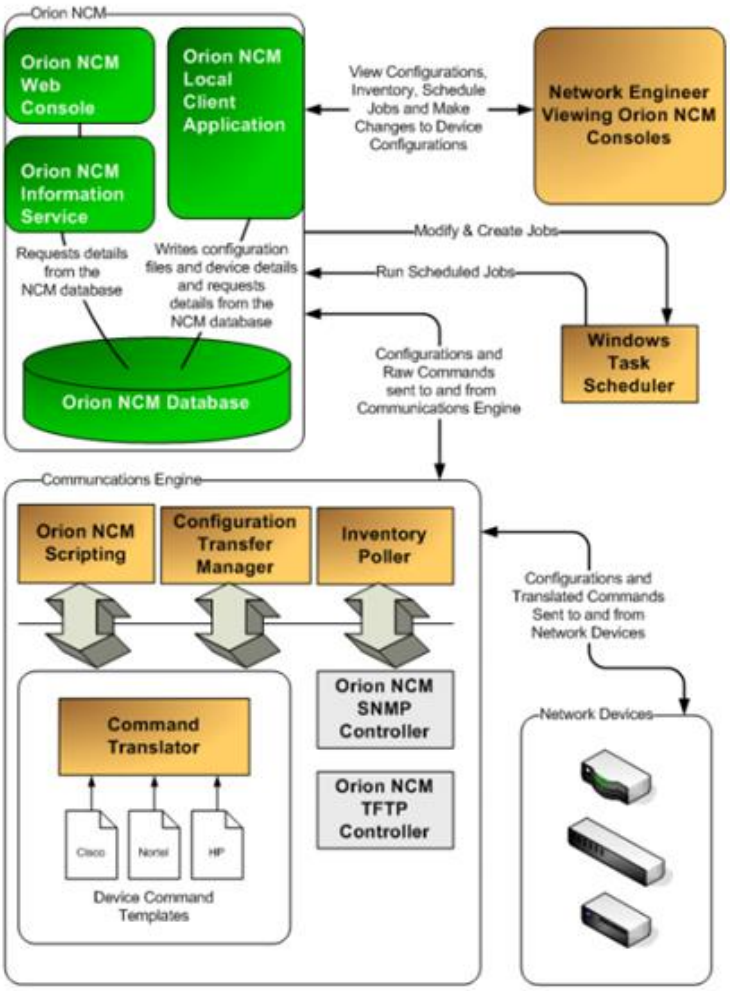


The above image is an example of the system monitoring page for critical servers and applications.

Content Expert: Travis Vanos

SolarWinds Network Configuration Manager (NCM):

The SolarWinds Network Configuration Manager (NCM) integrates with the Windows Task Scheduler to perform key tasks, such as nightly backups of configurations and node inventory scans. All configuration changes and user activity are stored in the SolarWinds NCM database.



The diagram above explains the role of the SolarWinds NCM.

19. CORPORATE WAN INFRASTRUCTURE, SECURITY, AND MANAGEMENT

The Wide Area Network (WAN) can be broken down into two separate topologies, being the branch offices and the regional offices

- See Section 2.3 for an overview of the WAN topology

Regional Offices – Each regional office has four Cisco 3945 ISR, two for WAN connectivity, and two for Internet connectivity (see Section 2.4 for more details).

Branch Offices – Each branch office has two Cisco 2911 ISR for WAN connectivity (see Section 2.5 for more details). There is no direct internet access at each branch office; instead, all traffic is forwarded to the default gateway of the nearby regional office.

Technical Overview:

The WAN network is being provided and maintained by our Internet Service Providers (ISPs), Optus and iiNet.

- There are two different WAN networks for redundancy in case one ISP goes down, in addition to providing load balancing.

- The ISP WAN links connected to Chavhoj Canada Inc.'s network in a partial-mesh topology.

- The network links are transparent to us since, the ISPs are using Multiprotocol Label Switching (MPLS), and the edge routers for the MPLS WAN cloud are on the provider's network.
  - This means that Chavhoj Canada Inc.'s network design is easy to integrate into the WAN cloud, since we can use our own private IP addressing and the MPLS edge router will label it and forward it at fast Layer 2 switching speeds across the provider's network to its destination.
  - The terminal edge router on the ISP's network will then remove the label, so that the unaltered packet can be routed from there.

- MPLS supports Quality of Service (QoS) for our required telephony performance.

- At each regional office, Optus and iiNet also have fiber lines terminating at a box outside of the building. The termination point connects to Chavhoj Canada Inc.'s network through a series of RJ45 cables to the Cisco 3945 ISRs. From here, they enter the network through a firewall.

- Since the Internet connection is only available through the regional offices of Sydney and Perth, the System Administrator and his or her team can better monitor and control the amount and type of traffic that enters or leaves the network. Moreover, the IT staff can create baselines and watch for bottlenecks or areas of high traffic, and plan for future expansion accordingly.

20. CORPORATE TELEPHONY DESIGN AND DEPLOYMENT

The equipment for the telephony structure consists of two main areas, being network equipment and end devices. Every Voice over Internet Protocol (VoIP) phone includes a switch port, allowing a computer and a VoIP phone to share the same network drop and port on a switch. This helps reduce the amount of equipment needed.

Network Equipment:

- Network equipment includes two Cisco Business Edition 6000 servers, with one located at each regional office, as well as the network modules for the routers at all office locations. Other than that, the VoIP part of the telephony network makes use of the existing LAN and WAN architecture.

- A T1 line will be setup at each regional office, providing 23 channels for incoming and outgoing voice calls. Analog lines will also be setup, with two for each branch office, and four for each regional office. These lines are for emergency failover in case of a network or T1 failure. An overview of the telephony network can be seen in Section 2.6.

End Devices:

- End devices include a Cisco 7962G Unified IP phone for each worker/cubical, Cisco 7937G Unified IP conference phones for each conference/boardroom, and a few analog phones (provided free of charge through our analog phone line subscription with Optus).

Technical Overview:

T1 Lines – Each T1 line has 23 voice channels and a 24th for data (such as Caller ID). The T1 lines connect to a WAN Cisco 3945 ISR at each regional office through a Cisco High-Density Digital Voice Network Module.

Analog Lines – Analog lines will come into each regional office through two Cisco IP Communications Voice Network Modules on each Cisco 3945 ISR, which allows for two analog connections each. Branch offices use only one module on one of their Cisco 2911 ISR. These connections will be used for emergency failover. One emergency phone will be located in each office reception area with a direct connection to Australian emergency services (000 in Australia, not the North American 911). When the receiver is picked up, it will automatically dial 000. This will be achieved through Private Line Automatic Ringdown (PLAR).

Fax Service – Fax calls will be received over the T1 lines, converted to a VoIP packet by the BE6000, and then converted back into an analog signal by a Cisco ATA before entering the printer/fax station through a standard RJ11 phone cable. This prevents the need of having a dedicated analog line for fax services.

VoIP Phones – VoIP phones are used for enhanced productivity, including inter-site 4-digit dialing and voicemail. Additional phone features will be setup, including call parking, paging, Music on Hold (MOH), and hunt groups. Each Cisco 7962G phone also has room for up to four lines for future expansion.

Phone Setup – Each VoIP phone will receive its IP configuration from a DHCP server, and will include option 150. Option 150 is the IP address of the Trivial File Transfer Protocol (TFTP) server, which will be the BE6000 to which the phone is near. This will allow the phone to pick up any changes automatically on startup, and the server can push out changes and restarts to the phone as needed.

Compression – All VoIP packets will be compressed using the G.729 codec, in order to help reduce the size of the bandwidth required from 64kbps to 8kbps.

Quality of Service (QoS) – QoS will be adjusted to give the highest priority to VoIP packets, in order to ensure that calls are not lost, and that their quality stays high.

Numbering Scheme – Each site will use a different 4-digit extension in order to logically separate them from each other.

- Sydney – 1XXX
- Toowoomba – 2XXX
- Townsville – 3XXX
- Perth – 4XXX
- Karratha – 5XXX
- Darwin – 6XXX