

**Planning the Infrastructure**

**Name**: Thong Thao

**Student ID**: 474587265

**Date**: 29/11/2023

**Contents**

[**Contents** 1](#_Toc152168437)

[PART 2 - Planning 2](#_Toc152168438)

[1. Client Requirements 2](#_Toc152168439)

[2. Deliverables 2](#_Toc152168440)

[3. Installation Notes 8](#_Toc152168441)

[4. Client Approval 13](#_Toc152168442)

[5. Reference 14](#_Toc152168443)

# PART 2 - Planning

## 1. Client Requirements

It is important for a network designer to understand the organisation and the client requirements before developing a network. For this first part of the document, you will detail:

1. A description of the structure and functions of the client’s organisation.

Albert & Allen Logistics (AA) is a private business that provides passenger transport and freight services for Australian-wide clients and businesses. The company has a head office with 510 employees, and also operates from a number of other locations around Australia.

|  |  |
| --- | --- |
| **Albert & Allen Logistics (AA)’s Structure** | **Albert & Allen Logistics (AA)’s Function** |
| Management | * Passenger transport * Freight Services |
| Administration |
| Call Centre |
| Logistics |
| IT |
| Maintenance |
| Other Department |

1. A description of the industry sector that the client’s organisation is part of.

Albert & Allen Logistics (AA) is a part of the transport and logistics. The transport and logistics industry are responsible for the movement of people and goods, and it is a vital part of the Australian economy.

## 2. Deliverables

1. List and provide a detailed explanation of expected compatibility issues and how they will be resolved.

There are three expected compatibility issues and solutions below:

* **Hardware Compatibility**: The Virtual Machines should be able to use the device’s resources, such as CPU, Memory, Disks.
* **Software Compatibility**: The Virtual Machines should be able to support different versions and updates of the components such as operating systems, and applications.
* **Network Compatibility**: the Virtual Machines should be able to handle network fluctuations, interruptions, and threats without compromising their functionality and quality. For example, bandwidth, latency, security, etc.

1. A list of hardware components (upgrades or additions), and why they are required.

There are some hardware components required to upgrades or additions.

* **Servers**: The existing servers need to upgrade and purchase new servers. For virtualisation, the servers should have high speed CPU, RAM, etc.
* **Storages**: The storage is the device that stores the data and programs. For virtualisation, the storage should have enough space, speed, and reliability to store the VM images and snapshots.
* **Networking**: The network is the device that connects the physical devices to other devices or to the internet. For virtual devices, the network should have enough bandwidth, latency, and security to handle the network traffic of the VMs.
* **UPS**: The UPS can be used to protect the servers and other network equipment from power outages.

1. A list of software components (virtualisation software, operating systems, etc.), and why they are required.

There are some software components virtualisation software, operating systems required for the project.

* **Hypervisors**: The hypervisor is a virtualisation software that creates and manages the VMs on the physical servers.
* **Operating Systems**: The operating systems are the software that run on the VMs and provide the basic function and interfaces for the applications. The OS should be compatible with the virtualisation software and the hardware.
* **Backup and Recovery Software**: The backup and recovery software is used to protect the VMs files and data.
* **Management Software**: The management software is used to manage the virtualised environment, including tools for monitoring, configuration and troubleshooting the VMs.

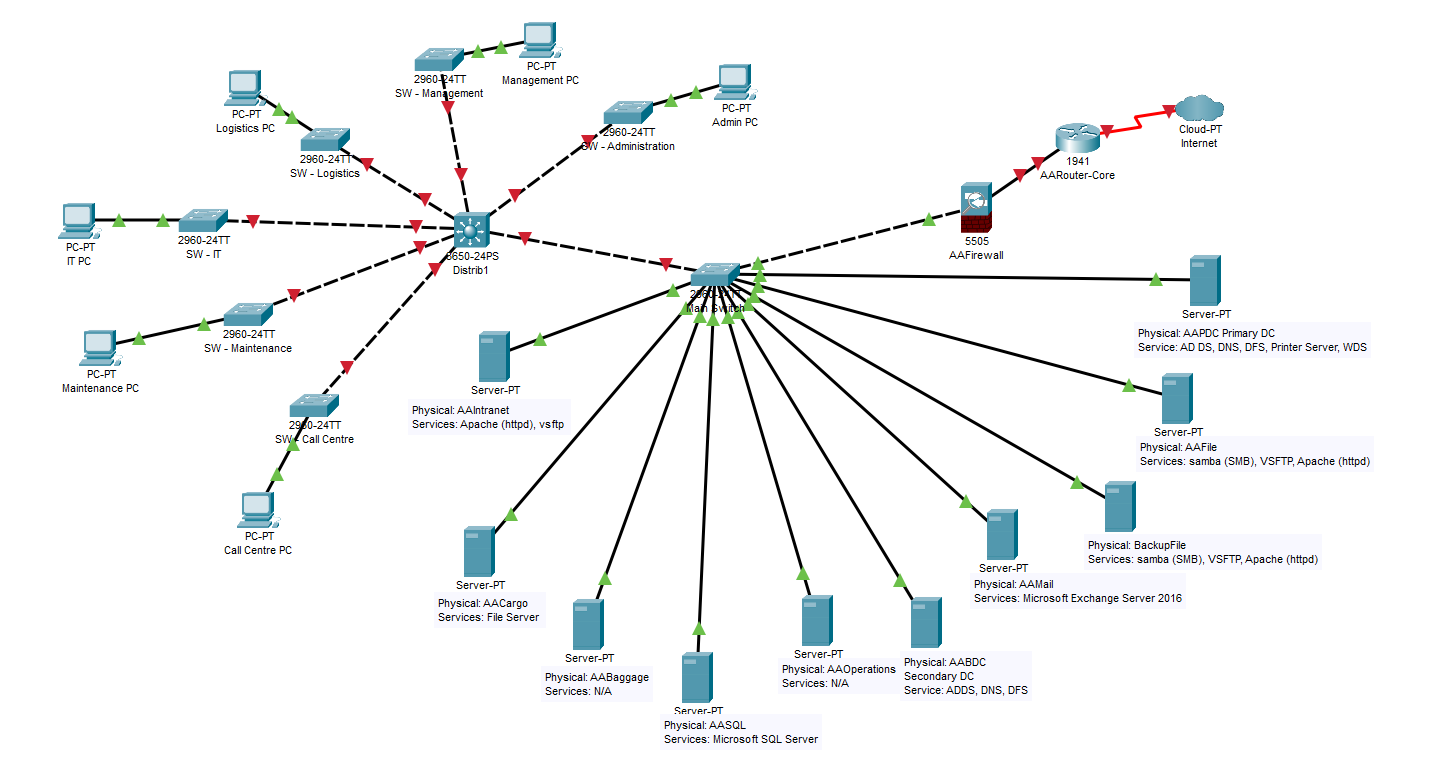
1. List and a detailed explanation of specific changes to the infrastructure (changed core network, installation, and configuration of hypervisors).

There are the specific changes to upgrade the infrastructure.

* Upgrading the Core Network Infrastructure to support the increased network traffic and provide redundancy.
* Installation and Configuration of Hypervisors on the new servers.
* Migrating data from physical servers to virtual servers.
* Configuring network storage devices for data storage and backup purposes.

1. Create two (2) logical topologies diagrams (before and after) showing where data is stored and how it is transferred across the network. The after topology should also show what is physical, what is virtual, which services will be running on VMs, and which services will be running on physical servers.

**Before Logical Topology**

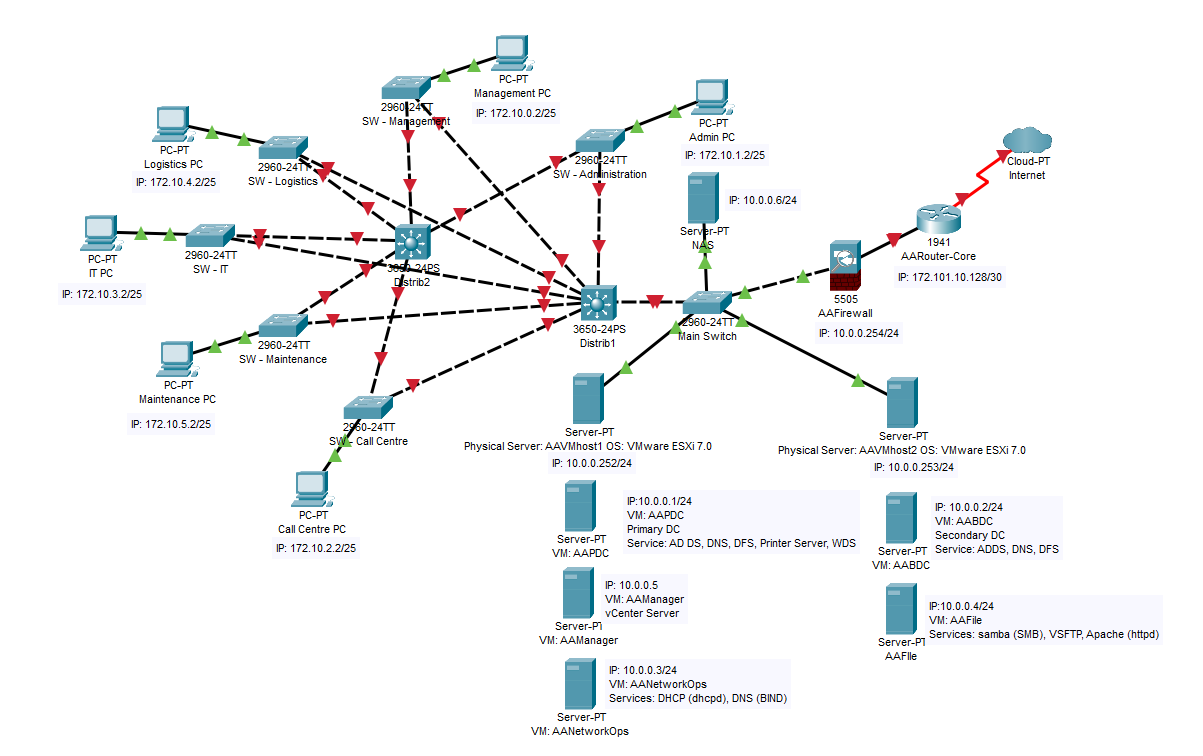


Based on the logical topology above the data is stored on the physical servers (Linux) and transferred across the network using standard Ethernet protocols.

The physical server including:

* Primary domain controller (AAPCD)
* Backup domain controller (AABCD)
* File server (AAFile)
* Backup File Server (BackupFile)
* Mail Server (AAMail)
* Monitoring Server (AAOperations)
* Database Server (AASQL)
* Application Server (AABaggage)
* Application and file server (AACargo)
* Intranet web application (AAIntranet)

**After Logical Topology**



The after logical topology is shown above. It consists of two hypervisors, AAVMhost1 and AAVMhost2. The hypervisors host a variety of virtual machines, including:

AAVMhost1:

* Primary domain controller (VM)
* Linux network operations server (VM)
* vCenter - AAManager (VM)

AAVMhost2:

* Backup domain controller (VM)
* File server (VM)

NAS:

* Network Attached Storage (TrueNas)

The data is stored on the virtual servers (Linux) and transferred across the network. The Linux network operations server stores the DHCP and DNS databases.

1. TCP/IP addressing scheme that is appropriate for your network design this will include both virtualised and physical components.

|  |  |
| --- | --- |
| Physical TCP/IP Address Scheme | |
| IP address | 172.10.0.0 |
| Subnet mask | 255.255.252.0 |
| Default gateway (WAN) | 10.0.0.254 |
| Virtualisation TCP/IP Address Scheme | |
| IP address | 10.0.0.0 |
| Subnet mask | 255.255.255.0 |
| Default gateway (WAN) | 10.0.0.254 |

The company currently has 510 employees at the central office (including the ten IT staff). Therefore, I consider that there are over 510 devices. I will use subnet mask “supernet” of /22, it has totally 1024 IP address, useable 1022 IP and divide subnet from original to 6 department and for another department as the table below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Department** | **Subnet Mask** | **Network Address** | **Usable Addresses** | **Broadcast Address** |
| **Management** | 255.255.255.0 | 172.10.0.0 | 172.10.0.1 - 172.10.0.254 | 172.10.0.255 |
| **Administration** | 255.255.255.0 | 172.10.1.0 | 172.10.1.1 - 172.10.1.254 | 172.10.1.255 |
| **Call Centre** | 255.255.255.0 | 172.10.2.0 | 172.10.2.1 - 172.10.2.254 | 172.10.2.255 |
| **IT** | 255.255.255.0 | 172.10.3.0 | 172.10.3.1 - 172.10.3.254 | 172.10.3.255 |
| **Logistics** | 255.255.255.0 | 172.10.4.0 | 172.10.4.1 - 172.10.4.254 | 172.10.4.255 |
| **Maintenance** | 255.255.255.0 | 172.10.5.0 | 172.10.5.1 - 172.10.5.254 | 172.10.5.255 |
| ***Other Department*** | *255.255.255.0* | *172.10.6.0 - 172.10.255.0* | *172.10.6.1 - 172.10.255.254* | *172.10.6.255 -*  *172.10.255.255* |

1. Formal procedures for the following:
2. backup and recovery.

* Regularly scheduled backups of virtual machine images and data.
* Testing of backup integrity and restoration processes to verify data recoverability.
* Offsite storage of backup data to protect against physical damage or loss at the primary site.
* Documentation of backup procedures, including the schedule, retention policy, and responsible personnel.

1. management tasks:

* Regular monitoring of performance metrics, such as CPU usage, memory utilisation, and network traffic.
* Patch management and software updates to maintain security and stability.
* User access management, including user account creation, modification, and removal.
* Documentation of management procedures, including roles and responsibilities.

1. UPS configuration:

* Installation and configuration of UPS devices to provide backup power during power outages or fluctuations.
* Regular testing of UPS systems to ensure proper functioning and battery capacity.
* Documentation of UPS configuration, including load capacity, runtime, and maintenance procedures.

1. Describe how the storage infrastructure will be configured and managed as per industry standards.

The storage infrastructure in the virtualised environment will be configured and managed according to industry standards. This includes implementing best practices for physical security, Authentication and authorisation, isolation storage, data protection, restoration assurance and encryption.

**Physical security**: The storage devices and components should be protected from unauthorized access, theft, damage, or tampering. This may include locking the cabinets, restricting access to the data centre, using surveillance cameras, and implementing alarms and sensors.

**Authentication and authorisation**: The storage infrastructure should enforce strong authentication mechanisms for users and administrators who access the storage resources, such as passwords, tokens, certificates, or biometrics. The access rights and privileges should be granted based on the principle of least privilege and role-based access control. The access policies should be regularly reviewed and updated to reflect the current needs and roles of the users and administrators.

**Data protection**: The storage infrastructure will incorporate data protection mechanisms such as RAID (Redundant Array of Independent Disks) for fault tolerance and data redundancy. Regular backups of virtual machine images and data will be performed to ensure data integrity and facilitate disaster recovery.

**Isolation Storage**: The storage infrastructure should isolate the data of different users, applications, or tenants from each other to prevent unauthorized access, leakage, or interference. It may include using encryption, zoning, masking, or other techniques to create logical partitions or boundaries within the physical storage devices and components.

**Restoration assurance**: The storage infrastructure should verify that the data restored from backup, replication, snapshot, or other methods is consistent and accurate with the original data. This may include using checksums, hashes, signatures, or other methods to validate the integrity of the data before and after restoration.

**Encryption**: The storage infrastructure should encrypt the data at rest and in transit to protect it from unauthorized access, modification, or disclosure. The encryption keys should be securely generated, stored, managed, and rotated according to best practices. The encryption algorithms and protocols should be strong and up to date with the current standards.

## 3. Installation Notes

For the last part of this document, you will detail the sequence of tasks required to complete setting up the Virtualised environment and respond to feedback from the client, the information must include:

1. Step-by-step installation procedure for:
2. Installing the hypervisor platform

* Ensure that the physical server meets the hardware requirements for the hypervisor platform.
* Download the hypervisor software from the vendor's website.
* Create a bootable installation media, such as a USB drive or DVD, with the hypervisor software.
* Insert the installation media into the server and boot from it.
* Follow the on-screen instructions to install the hypervisor software.
* Configure the necessary network settings and other options during the installation process.
* Once the installation is complete, restart the server and verify that the hypervisor is running.

1. Installing one of the Microsoft Windows Server virtual machines

* Launch the hypervisor management interface.
* Create a new virtual machine, specifying the desired configuration (e.g., CPU, memory, storage).
* Attach the Windows Server installation media (e.g., ISO file) to the virtual machine.
* Start the virtual machine and follow the on-screen instructions to install Windows Server.
* Configure the necessary settings during the installation process, such as network configuration and administrator password.
* Once the installation is complete, install any necessary updates and configure additional services as required.

1. Installing one of the Linux Server virtual machines

* Launch the hypervisor management interface.
* Create a new virtual machine, specifying the desired configuration (e.g., CPU, memory, storage).
* Attach the Linux Server installation media (e.g., ISO file) to the virtual machine.
* Start the virtual machine and follow the on-screen instructions to install Linux Server.
* Configure the necessary settings during the installation process, such as network configuration and root password.
* Once the installation is complete, install any necessary updates and configure additional services as required.

1. Reasonable timeframe for the conversion, this will need to be shown in a Gant chart.

A Gantt chart can be created to visualise the timeline and tasks involved in the conversion process. The chart should include tasks such as hardware preparation, hypervisor installation, virtual machine creation, data migration, testing, and final deployment. The duration of each task should be estimated based on the project scope and resources available.

*(Excel File: ICTNWK557\_ICTNWK559\_AT1\_Part2\_GranttChart\_Thong)*

1. Details of a TCP/IP sub-netting plan for the virtualised and management networks, that will include the following tables:

|  |  |  |  |
| --- | --- | --- | --- |
| Host | IP address | Subnet mask | Default gateway |
| AAVMhost1 | 10.0.0.253 | 255.255.255.0 | 10.0.0.254 |
| Virtual machines | | | |
| Host | IP address | Subnet mask | Default gateway |
| AAPDC | 10.0.0.1 | 255.255.255.0 | 10.0.0.254 |
| AANetworkOps | 10.0.0.3 | 255.255.255.0 | 10.0.0.254 |

|  |  |  |  |
| --- | --- | --- | --- |
| Host | IP address | Subnet mask | Default gateway |
| AAVMhost2 | 10.0.0.252 | 255.255.255.0 | 10.0.0.254 |
| Virtual machines | | | |
| Host | IP address | Subnet mask | Default gateway |
| AABDC | 10.0.0.2 | 255.255.255.0 | 10.0.0.254 |
| AAFile/EmailServer | 10.0.0.4 | 255.255.255.0 | 10.0.0.254 |

|  |  |
| --- | --- |
| AAManager/VCS | |
| IP address | 10.0.0.5 |
| Subnet mask | 255.255.255.0 |
| Default gateway (WAN) | 10.0.0.254 |

|  |  |
| --- | --- |
| AAFirewall | |
| IP address (LAN) | 10.0.0.254 |
| Subnet mask | 255.255.255.0 |
| IP address (WAN) | 172.101.10.128 |
| Subnet mask | 255.255.255.252 |
| Default gateway (WAN) | 172.101.10.1 |

|  |  |
| --- | --- |
| VMWebClient (Optional) | |
| IP address | DHCP |
| Subnet mask | 255.255.255.0 |
| Default gateway (WAN) | 10.0.0.254 |

Note, the above tables are to be included in your document.

1. List and explain the available tools and software that you will use to manage the hypervisor and virtual servers. Your explanation should explain how they are to be configured, and when you will use them.

**Hypervisor Management Tools:**

* VMware vCenter Server: A centralized management console for VMware vSphere environments. vCenter Server provides a single pane of glass view for managing all of your ESXi hosts and virtual machines.
* VMware vSphere Client: A graphical management console for individual ESXi hosts and virtual machines. vSphere Client allows you to perform tasks such as creating, configuring, and managing virtual machines.

**Tools and Software:**

* Monitoring tools can be used to monitor the performance and health of the hypervisors and virtual machines. *Example: Zabbix, Nagios*
* Backup and recovery tools can be used to backup and restore the hypervisors and virtual machines. *Example: Veeam Backup and Replication, VMware vSphere Data Protection.*

1. Description of how you will integrate the virtual computers into the existing network design.

* Determine the network requirements of the virtual computers, includes the IP address range, subnet mask, gateway address, and DNS server addresses.
* Configure the virtual network switch. I will configure the virtual network switch to use the IP address range and subnet mask that you determined in step 1.
* Connect the virtual computers to the virtual network switch by editing the virtual machine's network settings.
* Configure the routing on the physical network. I will add a route to the virtual network subnet on the physical router or firewall. This will allow traffic to flow between the virtual computers and the physical network.

1. A paragraph discussing the best High-Availability (HA) options for this virtual environment.

VMware vSphere High Availability delivers the availability required by most applications running in virtual machines, independent of the operating system and applications running in it. High Availability provides uniform, cost-effective failover protection against hardware and operating system outages within your virtualised IT environment.

1. A paragraph discussing the traditional apps vs. virtual machine backup software (third party tools).

**Traditional backup applications** are designed to back up physical servers and workstations. They work by copying individual files and folders from the source system to the backup destination. This approach can be effective for backing up simple systems, but it can become inefficient and time-consuming for backing up complex systems with multiple applications and large datasets.

**Virtual machine backup software** is designed specifically to back up virtual machines. It works by creating snapshots of the VM's state, which includes all its files, applications, and data. Snapshots can be created quickly and efficiently, and they can be restored to the VM to recover from data loss or corruption.

1. Detail of how the virtual servers will be tested. Testing should include.
2. Connectivity: This involves verifying that the virtual servers can communicate with other network resources, such as physical servers, network switches, and other virtual machines. Connectivity testing can be performed by pinging IP addresses, accessing shared files or services, and testing network connectivity between different virtual machines.
3. Availability: Availability testing aims to ensure that the virtual servers are accessible and operational when needed. This can involve simulating different failure scenarios, such as shutting down a physical server or disconnecting a network switch, to determine if the virtual servers can failover to another host and continue operating without interruption. Availability testing should also include testing the responsiveness of critical services running on the virtual servers.
4. Performance: Performance testing evaluates the performance of the virtual servers under different workloads and conditions. This can involve generating simulated traffic or load on the virtual servers to measure their response time, throughput, and resource utilisation. Performance testing should also include stress testing to determine the maximum capacity and scalability of the virtual servers.

Your solution should take into consideration the following priorities:

* A maximum 70% server utilisation of resources to allow high availability of memory, data, and processing power.
* Redundant server infrastructure, for example, server power supplies, UPS, primary domain controller and secondary domain controller and redundant VM hosts
* Redundant network infrastructure, including additional switches and routers, network links and protocols to ensure redundancy such as LACP and STP
* Future storage requirements including VM backups/snapshots/testing.
* Support for increased network traffic such as switches to accommodate high availability and the traffic from four physical + 12 virtual servers.
* The ability to migrate data from physical servers to virtual servers when needed.

## 4. Client Approval

**To:** Thong Thao (Network technician)

**From:** Shawn Long (IT manager at AA Logistics)

**Subject:** Review and approval for server virtualisation plan

I have reviewed the planning document and I would like to approve all the steps undertaken for this project. I would like to thank Thong for putting forward his plan to update our physical server infrastructure and that we look forward to the installation and configuration of the planned solution.

Signed: *Shawn Long* Date:30/11/2023

## 5. Reference

*Chandramouli, R & Pinhas, D 2020, ‘Security Guidelines for Storage Infrastructure’, NIST Special Publication 800-209.*

‌ *(VMware)*

*King, J. (2013). Did you know vCenter Server can manage multiple hypervisors? [online] https://blogs.vmware.com/vsphere/2013/04/did-you-know-vcenter-server-can-manage-multiple-hypervisors.html. Available at: www.vmware.com [Accessed 16 Nov. 2023].*

*‌Liquid Web. (2022). Best Practices for a VMware High Availability (HA) Cluster. [online] Available at: https://www.liquidweb.com/blog/vmware-ha-cluster-best-practices/ [Accessed 20 Nov. 2023].*

*Best Virtual Machine Backup Tools & Software. (2020). Server Watch. [online] 9 Sep. Available at: https://www.serverwatch.com/backup/virtual-machine-backup-tools/ [Accessed 15 Oct. 2020].*

‌

‌

‌