**Introduction**

1. Gap Analysis < Produce a gap analysis document for the case study company :>

Anzac Airport is a small private airport located in Mytown, QLD, providing passenger and freight services to local clients and businesses. The airport must comply with all relevant Commonwealth and state regulations regarding airport operations. Anzac Airport's operations are divided across three main departments: Office Operations, Information Technology, and Ground Operations.

The current IT infrastructure is outdated, relying on peer-to-peer networks, which are causing inefficiencies and frequent desktop support issues. The systems in place do not adequately support the increasing demands of the business, and the CEO has identified that this legacy technology may be costing the company financially. The IT Manager has recognized the need to upgrade the network to a client-server architecture with full wireless integration to improve operational efficiency and support future growth.

This project aims to overhaul Anzac Airport's IT infrastructure to introduce state-of-the-art technology, ensuring it meets both business and technical requirements. The new system will offer improved reliability, security, scalability, and the ability to support email, file storage, and web services. The upgrade is critical to ensure the company's future growth, compliance with industry standards, and alignment with the CEO's vision for technological advancement.

|  |  |  |
| --- | --- | --- |
| Current State | Gap Analysis | Desired State |
| **Peer-to-peer network across departments** | The current network is inefficient, leading to slow performance and frequent desktop support issues. Peer-to-peer connections are unreliable for a growing business. | A client-server network is implemented, allowing centralized control, better performance, and easier maintenance. |
| **Wired LAN using 10/100 Ethernet in an ad-hoc topology** | Slow data transfer speeds, limited scalability, and outdated infrastructure. | Modern Ethernet standards (Gigabit or higher) with structured topology to improve speed, scalability, and reliability. |
| **Storage distributed across individual computers with inconsistent capacity management** | Storage is unstable, leading to data loss risks. Insufficient centralized storage for company data. | Centralized file storage system with redundancy and backup mechanisms, ensuring data integrity and reliability. |
| **Mixed operating systems on workstations (Windows 10 Home, Windows 10 Pro, Windows 8.1 Pro)** | Incompatibility issues across different operating systems, security risks with outdated versions. | Standardized operating system (e.g., Windows 11 Pro) across all workstations to enhance compatibility and security. |
| **No on-site email, web, or FTP services** | Reliance on external providers (e.g., Gmail), limiting control over data. No unified communication platform. | On-site email, web, and FTP services, with full control and integration into the company’s IT environment. |
| **Limited Wi-Fi access (IT staff only)** | Restricts operational flexibility, especially for mobile and on-the-go staff. | Full wireless integration across the entire facility, allowing seamless access for all staff. |
| **Dell OptiPlex desktops (2 to 6 years old, with varying RAM and storage capacity)** | Desktops have outdated hardware, causing performance issues. Some desktops are low on memory and storage, leading to further slowdowns. | New or upgraded desktops with modern hardware (e.g., 16GB RAM, 500GB SSD) to meet the performance demands of the business. |
| **No centralized server or domain controller** | No central management for authentication, user permissions, and resources. | Microsoft Active Directory Domain Services (AD DS) for centralized authentication and resource management, allowing single sign-on and easier user management. |
| **No redundancy in systems** | High risk of downtime and data loss in case of system failure. | Redundant systems with failover clustering to ensure high availability and quick recovery. |

**Network Design Option 1**

1. Server Installation Plan
2. Number of servers including specifications:

* **Total Servers:** 4
* **Server Specifications:**
  + **Processor:** Intel Xeon Gold 5412U Processor 24cores
  + **Memory:** 128GB DDR5 RAM
  + **Disk Capacity:** 1TB NVMe SSD, 2TB SSD (RAID 5 Configuration)
  + **Network:** Dual 10GbE NIC
  + **Redundant Components:** Power supply(UPS), network adapters (for failover)

1. Types of servers, OS and their Roles

|  |  |
| --- | --- |
| Server 1 | |
| Type of the server | Physical |
| OS | Windows Server 2022 Standard |
| Roles and applications installed | * Domain Controller (Primary) * DHCP Server * DNS Server (Primary) * File Server |
| Name | anzac-dc-01 |
| Server 2 | |
| Type of the server | Physical |
| OS | Windows Server 2022 Standard |
| Roles and applications installed | * File Server (Primary) * Backup for Active Directory * Backup for DNS * WSUS * Print Server |
| Name | anzac-fs-01 |
| Server 3 | |
| Type of the server | Physical |
| OS | * Windows Server 2022 Standard |
| Roles and applications installed | * + Exchange Server 2019 (Email Server)   + Office 365 Integration |
| Name | anzac-ex-01 |
| Server 1 | |
| Type of the server | Physical |
| OS | Fedora Server |
| Roles and applications installed | * + Proxy Server (Squid)   + NTP   + FTP   + Apache Web Server   + (Mail Server for assessment Purpose) |
| Name | anzac-lin-01 |

1. How would you install the Operating systems of servers and workstations?

The operating systems will be installed through an automated process using PXE (Preboot Execution Environment) and imaging software, such as **Windows Deployment Services (WDS)** for Windows-based servers.

1. What are the compatibility concerns of your server integration, what will be the solution? Potential compatibility issues could arise between **Windows** and **Fedora** server platforms, particularly in file sharing. To mitigate this, protocols such as **Samba** will be used to ensure smooth communication across platforms.
2. Network functionalities
3. **DHCP**

Anzac-dc-01 is DHCP server

IP Schema:

* Reserved for servers: 172.16.0.1 - 172.16.0.5
* Reserved for printers: 172.16.0.6 - 172.16.0.15
* DHCP pool for workstations: 172.16.0.16 onwards

1. **DNS**

* **Primary DNS Server:** anzac-dc-01 (Windows)
* **Backup DNS Server:** anzac-fs-01 (Windows)
* **Domain Name:** jamesanzac.com
* **No Sub-Domains** planned for the initial setup.

1. **Directory services including authentication (AD DS)**

* **OUs (Organizational Units):**
  + **Office OPs**
  + **IT**
  + **Ground OPs**
* **Groups:**
  + **grpAdminOffice**
  + **grpReception**
  + **grpHR**
  + **grpIT**
  + **grpWHS**
  + **grpExecutive**
  + **grpSecurity**
  + **grpBaggage**
  + **grpManagers Dual Group Holders**

**User Assignment:** Users will be allocated to groups based on their department or role. This will be determined via company consultation with continuous improvement.

1. **Update services**

* WSUS will be used to automate server and workstation updates. Updates will be scheduled weekly for workstations and monthly for servers.
* Fedora Server will be updated once a month manually outside normal working hours to ensure that any compatibility issues that could arise are sorted promptly.

1. **Network installation of operating systems**

As mentioned earlier, **PXE boot** with WDS will automate OS installation across workstations. Servers will be manually installed. Once connected network, servers will be manged by remote access to assign the services each will run.

1. **Email, FTP, and Web Services**

* **Email Software:** Exchange Server 2019 (Commercial)

(for assessment purposes Rocky mail has been used)

* **FTP Software:** Samba
* **Web Software:** Apache Web Server

1. **Print management**

Anzac-fs-01 will act as the print server. A shared network printer will be setup for each Organisational Unit which will be set via Group Policies as a default. All users will have access to network printers so printing in other OU areas can be done when required.

1. **Group Policies**

Group policies will be implemented for security purposes (e.g., restricting access to certain files or applications) and to deploy software across all workstations (e.g., Office 365 and antivirus software).

1. **Proxy Server**

The proxy server will be configured on the **Fedora Server** using **Squid Proxy** to monitor and filter internet traffic.

1. **NTP** <what software will be used to implement NTP. How are you going to synchronise the servers and workstations?>
2. Network security

**a) Server Integration and Authentication**

* **Authentication Model:** Windows-based, using **Active Directory** for centralized authentication. Multi-factor authentication (MFA) will be enabled for administrators.
* **Cross-Platform Authentication:** **Kerberos** will be used for authentication between Windows and Ubuntu platforms.
* **High Availability:** Redundancy will be achieved through replication between the primary domain controller and the backup on **anz-fs-02**.

**b) File Sharing**

* **File Store:** **Windows Server Distributed File System (DFS)** will be used for file sharing across departments, with permissions configured through **Active Directory**.
* **Cross-Platform Sharing:** **Samba** will be used to enable file sharing between the **Windows** and **Fedora** servers.

**c) Data Migration and Backup**

* **Data Migration Strategy:** Data from the old systems will be migrated using **robocopy** for Windows systems and **rsync** for Linux systems.
* **Backup Plan:** **Veeam** will provide daily incremental backups and weekly full backups. The data will be stored both locally and in a secure cloud location.

**d) Firewalls and Virus Protection**

* **Firewall:** **Cisco Meraki MX105** will serve as the primary firewall for network security, offering VPN, intrusion prevention, and content filtering.
* **Virus Protection:** **Avast Business** will be deployed to all workstations and servers to protect against malware and viruses.

1. Network prototype topology

**Network Design Option 2**

1. Server Installation Plan
2. Number of servers including specifications: <Describe how many servers and their specifications Processor, memory, Disk capacity, Network etc... and redundant components if configured >
3. Types of servers, OS and their Roles <Describe what type of servers (Physical, virtual, cloud etc.), what OS is going to be installed on each server and how you allocate severs for each of the network services and applications. Replicate the following tables for number of servers in your design.

|  |  |
| --- | --- |
| Server 1 | |
| Type of the server |  |
| OS |  |
| Roles and applications installed |  |
| Name |  |

1. How would you install the Operating systems of servers and workstations <Explain if this is a manual process or an automated process>
2. What are the compatibility concerns of your server integration, what will be the solution? <Compatibility issues that need to be identified between different server platforms and server technology used>
3. Network functionalities

<For each service below: describe what server is going to be used, what server is going to be used as a backup, the server roles that you are going to install and configure in Anzac network. Describe in detail what are the functionalities of each server role is. Refer to the guidelines given alongside the service>

1. DHCP <describe IP schema you are going to use and in scope and out of scope plan>
2. DNS <explain what name is going to be used for the domain, whether you are going to create sub domains>
3. Directory services including authentication (AD DS) <explain what OUs are going to be created and what resources are going to be included in each OU. what groups are going to be created and how users are allocated to each group>
4. Update services <explain how you plan to update servers (with different Oss) and workstations, how you automate the process, how frequently you plan to update machines>
5. Network installation of operating systems <explain how you are going to install operating systems on servers and workstations, how you plan to automate the process for some/all of the machines>
6. Email, FTP and WEB services <Explain what email/FTP/WEB software going to be used (Commercial or Open source) and name the software>
7. Print management <explain how you plan to deploy the printers to users>
8. Group Policies <explain what purposes you are going to use the group policies e.g. security purposes, deploying applications, services etc.>
9. Proxy Server <what software will be used to implement Proxy>
10. NTP <what software will be used to implement NTP. How are you going to synchronise the servers and workstations>
11. Network security

<Identify and describe at least four security technologies you are going to implement for Anzac Airport to secure the network infrastructure>

1. Server integration and authentication
2. Authentication <Explain the authentication model suggested in your network design. Is it a Windows based? What policies are used, What measures taken to protect Administrator account >
3. Authentication between different server platforms <Explain How you use the above model to authenticate users between different server platforms (OS) and what protocols are going to be used in your server integration that meets the organisation’s network requirements? >
4. High availability < Explain how redundancy and replication can be applied to the authentication model>
5. File sharing
6. File sharing including file sharing between different file systems <Explain what type of storage going to be used as shared file store. Describe your file sharing strategy and how file sharing can be done between different operating systems, for Anzac Airport including file permissions, consider the integrated server environment when you plan>

1. Folder structure <Produce a diagram that shows the partitions that need to be created, and the file and folder systems that are needed>
2. Data migration and back up
3. Data Migration Strategy <Explain how you are going to migrate data in existing network to the new shared file sore. Identify data migration and data backup and recovery requirements before new network installation>
4. Data backup plan < Explain the backup plan of the new network. (how often you back up the data and what type of backup) Consider continuous confidentiality, integrity, and availability of Anzac Airport’s >
5. Fire walls and Virus protection
6. Identify Firewall options for network security
7. How do you implement virus protection?
8. Network prototype topology

<Draw a prototype of your suggested network using an industry accepted schematic designing tool>