Northumberland College

worldskillsuk
excellence at work

# Network Systems Administrator

# Pre-Competition Activity

## Introduction

This practice paper is based on a work place scenario in which you, as Network Manager, are tasked with the job of building a prototype client/server network. Your work is split into the following sections:

## TASK 1

Computer and Network Setup
Domain Setup
User Account and Group Setup
Security Configuration
Network Administration

## TASK 2

Shared Resources
Security configuration
Network Administration

## What you should have:

- This script.
- Blank paper
- Pens/Pencils
- Oracle Virtual Box Manager complete with the following virtual machines:
    - Windows Server
    - Windows Client
- Evidence File

During this exercise you will be asked to record data and capture screenshots in your Evidence File. Save your Evidence File as **NSA Evidence <your name>** on the desktop of the base system.

## TASK 1

## Raytec Industries

You have been given the post of Network Manager at an electronics manufacturer, Raytec Industries. As part of your role you have been asked to set up a prototype network consisting of a server and a client computer. The server will be running the Windows Server 2008 R2 operating system and the client computer will be running the Windows 7 operating system.

The default username is administrator and the default password is Pa$$w0rd

## Server Setup

- The server will need to be setup with the following settings:

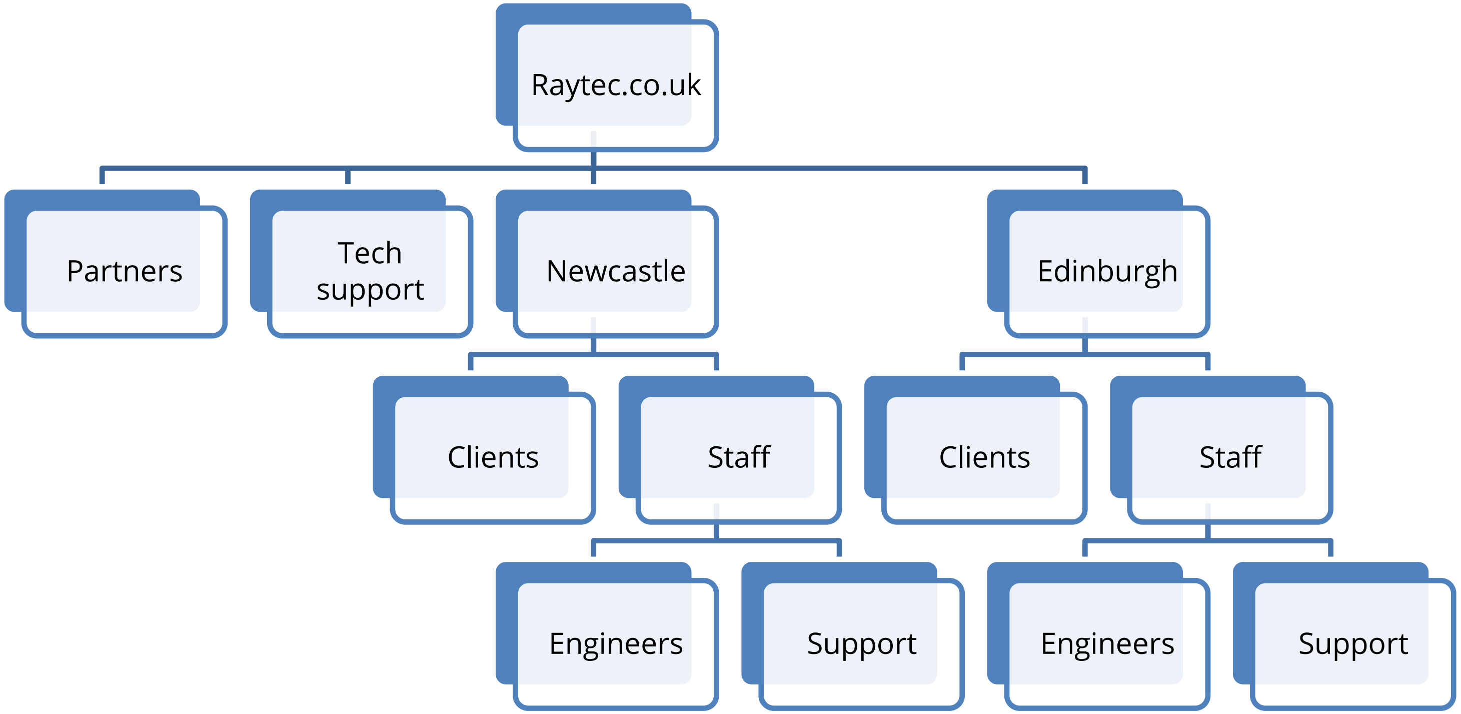
| | |
|---|---|
| **Role** | Server |
| **Name** | ServerXX<br>where XX is your station no. |
| **IPv4 address** | 172.16.5.10 /24 |

- Default IPV6 Settings should be accepted.
- Set up the ServerXX as a domain controller with a domain name of Raytec.co.uk. Set the Directory Services restore Password to Pa$$w0rd.
- Set up a DHCP server, this server must have the IPV4 addresses 172.16.5.1 – 172.16.5.15 excluded from scope use.
- MAC address 78-E7-D1-C3-C3-E0 must have the IPV4 address 172.16.5.18 reserved for its specific use.
- The DHCP server should issue the following IPV4 DNS server address and the default gateway address for the network.
    - DNS = 172.16.5.10

- Default Gateway = 172.16.5.10

## Domain Structure

- Within the domain create the following OU structure:



## User Account and Group Setup

Create the following users in the appropriate OUs. Use an appropriate naming convention for usernames.

| Name | Job Role | OU | Permanent / Temporary |
|---|---|---|---|
| Your name | Network Manager | Tech support | Permanent (hopefully!) |
| Frank Smith | IT technician | Tech support | Permanent |
| Francis Smith | IT technician | Tech support | Permanent |
| Jane Dunn | Partner | Partner | Permanent |
| Francis Jones | Partner | Partner | Permanent |
| Paul Rennie | Admin support | Newcastle/Support | Temporary |
| Jenny Smith | Engineer | Newcastle/Engineers | Permanent |
| Ray Snell | Admin support | Newcastle/Support | Permanent |
| Nicholas Young | Engineer | Newcastle/Engineers | Temporary |
| Service1 | Service account | Tech support | Permanent |

- All users should have an initial password of **R@ytec15**
- The Network Manager account should be added to the administrators group
- Users should **NOT** be forced to change their password when they logon.
- All users except the Network Manager and the Service account are only allowed to logon Monday –Friday and 8am – 6pm.
- All temporary staff contracts will end on 7th Aug this year. Ensure the user accounts of all temporary staff will expire on this date.

**Note:** the IT technicians should **NOT** be made administrators.

- The password of the Service Account must be set to not expire.

Record the username for each user you have created in your **Evidence file**.

Create the following groups at the root of the Raytec.co.uk domain and add the required user accounts:

| **Group Name** | **Membership** |
|---|---|
| Management | • Network manager<br>• All partners |
| Support staff | • All admin support staff |
| Technical support | • Network manager<br>• All IT technicians |
| Staff | • All staff accounts |
| Projects | • All partners<br>• Engineers |

**Note:** You may add more groups to aid administration if you wish.

Record the membership list for each group in your **Evidence file**.

## Security configuration

Plan and implement the following security rules for the organisation:

a. All passwords except the Service account must be changed every 28 days.
b. You cannot use any of the previous 10 passwords.
c. Accounts will be locked after 3 bad password attempts and should be unlocked after 15 minutes.
d. Only administrators, IT technicians and the Network Manager are allowed to log on to the Domain Controller.

Indicate how many of these security settings have been configured with their name and location in the **Evidence file**.

## Network Administration Tasks

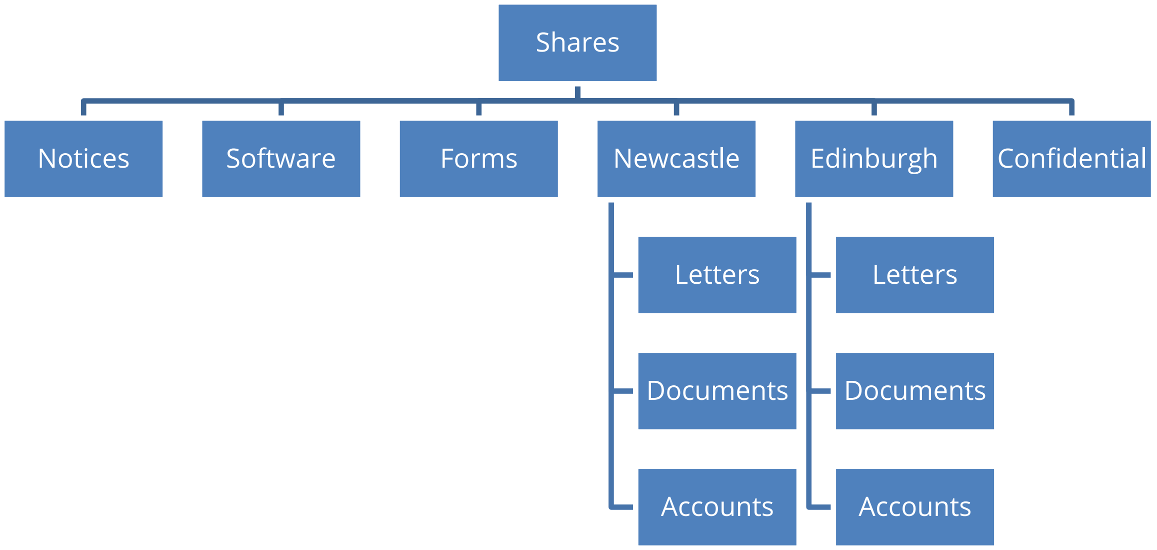
- One of the applications to be run on the server requires a large amount of memory. Modify the virtual memory settings on the server to provide a minimum of 2.5 times the amount of physical RAM. To make the computer run more efficiently, all virtual memory should be placed on a different drive to the operating system.

Record with screenshots the two network Administration tasks, above, in the **Evidence file.**

# TASK 2

## Shared Resources

Create the following folder structure on the C: drive of the server:



Share the folders with the following settings:

All folders should retain System and Administrative permissions

| **Folder path** | **Share name** | **NTFS Permissions** |
|---|---|---|
| Shares\notices | Group_Notices | Full control: Management<br>Modify: Support staff<br>Read: Authenticated users |
| Shares\Software | Software_Share | Full control: Technical Support<br>Read and execute: Authenticated Users |
| Shares\Confidential | Confidential | Full control:Management |

- All the above folders should be shared with share permissions set to Full control for Authenticated Users.

Record the NTFS Permissions configured for each shared folder in the **Evidence file**.

Add a shared printer to the server with the following settings:

| | |
|---|---|
| **Printer name** | Office printer |
| **Port type** | TCP/IP |
| **IP Address** | 172.16.5.15 |
| **Printer type** | HP LaserJet 4250 printer |
| **Print server settings** | Custom settings |
| **Print server protocol** | LPR |
| **Queue name** | Lp1 |
| **Permissions** | Print: Staff<br>Manage Documents: Support Staff<br>Manage Printer: Technical support |

**Note:**

- **The printer does not need to be physically installed**
- **Do not use the query printer option to detect the printer driver.**
- **There may be a long pause when detecting the printer, this is normal.**
- **Do not print a test page!**

## Group Policy

Create the following group policy objects:

| GPO Name | GPO Description |
|---|---|
| Folder Redirection | Use folder redirection to redirect the Documents and AppData folders to a shared folder on the server.  Each user should have their own folder. |
| Start Menu | Remove the Games link and Run command from the Start menu. |

Note: All the files required to implement the policies are on the disk provided

- The Folder Redirection policy should be applied to all users
- The Start Menu policy should be applied to all users except the Network Manager, the Partners and IT technicians.

**Note:** **Think carefully about the placement of the policies.**

**Policies should be applied with least administrative effort.**

Indicate how many of these security settings have been configured and their Group Policy Object location in the **Evidence file**.

Record with screenshots the network Administration tasks, above, in the **Evidence file.**