BSc (Hons) Computer Networking

An Investigation into the Interoperability of Windows Enterprise Network Technologies in Heterogeneous Networks

Reece Lindsay McGowan
B00286551

29th March 2019

Supervisor: Steve Eager

Declaration

This dissertation is submitted in partial fulfillment of the requirements for the degree of BSc Computer Networking (Honours) in the University of the West of Scotland.

I declare that this dissertation embodies the results of my own work and that it has been composed by myself. Following normal academic conventions, I have made due acknowledgement to the work of others.

Name:
REECE LINDSAY MCGOWAN

Signature:

Date: 29th March 2019

Form to accompany Dissertation

To be completed in full

Surname: McGowan
First Name: Reece Lindsay **Initials RLM**
Borrower ID Number: B00286551
Course Code: COMPNAM
Course Description: BSc (Hons) Computer Networking
Project Supervisor: Steve Eager
Dissertation Title: An Investigation into the Interoperability of Windows Enterprise Network Technologies in Heterogeneous Networks.
Session 18/19

Please ensure that a copy of this form is bound with your dissertation before submission

COMPUTING HONOURS PROJECT SPECIFICATION FORM

(Electronic copy available on Moodle Computing Hons Project Site)

Project Title: An Investigation into the Interoperability of Windows Enterprise Network Technologies in Heterogeneous Networks.

Student: Reece McGowan **Banner ID: B00286551**

Supervisor: Steve Eager

Moderator: *Duncan Thomson*

Outline of Project: *(a few brief paragraphs)*

This project aims to investigate the current state of technologies that allow Linux and Windows systems to co-exist and interoperate where technologies such as Active Directory and SMB File Sharing are employed. For the scope of this project, Active Directory, SMB, Group Policy functionality and cross-platform equivalents will be explored. The project will further examine the ease of administration, network performance, cost, and support available to both platforms.

This research will aim to detail what is necessary to allow both operating systems to co-exist in a heterogeneous environment and what benefits and downsides this could bring to enterprises exploring such options. This will also explore areas where work may still need to be done in aiding seamless interoperability between them. Furthermore, this research will seek to find the most functional setup in such a heterogeneous environment given currently available technologies.

A Passable Project will:

- *Configure a Windows homogeneous network as a control, to obtain baseline results for performance.*
- *Investigate and demonstrate the performance of a Windows Server 2016 network providing common services to Linux clients.*
- *Investigate and demonstrate the performance of a Linux Server network providing common services to Windows 10 clients*

A First Class Project will:

- *Design and develop a network with a Linux Server providing extended enterprise services to heterogeneous clients to automate common tasks.*
- *Design and develop a network where Windows Server 2016 provides extended enterprise services to heterogeneous clients to automate common tasks.*
- *Implement and configure a network where both Windows and Linux Servers provide extended enterprise services to heterogeneous clients.*

Reading List:

Heslin, M. (2012) Integrating Red Hat Enterprise Linux 6 with Active Directory [online]. Available at:

http://medias.coutances.educagri.fr/proc%C3%A9dures/Administrateur/RHEL6_AD2008.pdf [Accessed October 2018].

Desmond, B., Richards, J., Allen, R., Lowe-Norris, A.G. (2011) [online]. Available at:: https://books.google.co.uk/books?hl=en&lr=&id=exlzxcsE-7QC&oi=fnd&pg=PR5&dq=active+directory&ots=JGY2K2EiI-&sig=Td-IaC3zTFLTsnoNQe_aOXvINW8#v=onepage&q=organizational%20units&f=true [Accessed October 2018].

Minasi, M., Greene, K., Booth, C., Butler, R., McCabe, J., Panek, R., Rice, M., Roth, S., (2014) [online]. Available at: https://universalflowuniversity.com/Books/Computer%20Programming/Microsoft%20Windows%20and%20Powershell/Mastering%20Windows%20Server%202012%20R2.pdf [Accessed October 2018]

Resources Required: *(hardware/software/other)*

Physical PCs to simulate the model networks and/or Virtualisation software.

Windows Server 2016 as the Server OS in both the homogeneous network and Windows Server/Linux Client network.

Windows 10 as the Client OS in both the homogeneous network and Linux Server/Windows Client network.

Linux Distributions to act as both a Server and Client OS.

Marking Scheme:

	Marks
Style and Structure	**10%**
Literature Review	**10%**
Basic Objective Completion	**40%**
Advanced Objective Completion	**30%**
Critical Reflection	**10%**

Signed:

Student	**Supervisor**	**Moderator**	**Programme Leader**

IMPORTANT:

(i) ***By signing this form all signatories are confirming that the proposed Hons Project will include the student undertaking practical work of some sort using computing technology / IT, most frequently achieved by the creation of an artefact as the focus for covering all or part of an implementation life-cycle.***

(ii) ***By signing this form all signatories are confirming that any potential ethical issues have been considered and if human participants are involved in the proposed Hons Project then ethical approval will be sought through approved mechanisms of the School of CEPS Ethics Committee.***

Contents

Acknowledgements

I would like to offer my most sincere and gracious thank you to Steve Eager, who, while being my Honours Supervisor, went above and beyond to aid me where he could in completing this project, and offered his friendship and advice from the heart where it was needed.

A heartfelt thank you must also go to my family for their unwavering support of my endeavours throughout my time at the University of the West of Scotland.

Abstract

This project will investigate the current state of technologies that allow Windows and Linux systems to co-exist and interoperate in heterogeneous environments. This project aims to fill a gap in research in this area as there is currently little in the way of academic research into the interoperability of Windows and Linux systems in such environments, with much of the existing research prone to corporate bias. Existing literature pertaining to the project will be reviewed, including literature on Windows Enterprise Technologies, such as Active Directory and Server Message Block, Linux Enterprise technologies, such as Samba and the System Security Services Daemon and Hypervisors, including the types available.

The research methodology used will be discussed, including details and justification for the technologies used to undertake the research. The development process of the networks required to undertake the research will be detailed, including how the Windows Homogeneous control, Windows Server with Linux clients and Linux server with Windows clients networks were created.

The results obtained while undertaking the research are shown in detail, including network performance benchmarks pertaining to Active Directory domain login times, transfer rates via SMB for large and small files across each network designed and details on the costs involved to license and provide commercial support to each operating system involved in the research.

The report will conclude by summarizing the results of the research, including discussion on what operating systems performed best in the benchmarks performed, the complexity of administration and implementation and an overview of the support available to each operating system involved in the research. Possible future work that could be undertaken in this area of research is proposed, and a critical reflection on the project overall is performed.

Chapter 1: Introduction

1.1 Introduction to the Project

This project investigates the current state of technologies that allow Linux and Windows systems to co-exist and interoperate in heterogeneous environments, where common Windows Enterprise network services, providing such functionality as authentication and file sharing are used. For the scope of this project, Active Directory single sign-on, SMB and cross-platform alternatives are explored. The project will further aim to investigate the requirements for implementation and administration of such a heterogeneous environment and the network performance in such an environment.

A Windows Server 2016 network with Windows 10 clients will be implemented as a control, in order to obtain baseline network performance results. Three different Linux distributions, acting as client systems, from different vendors will be used to explore the different approaches available on Linux for interoperability in such an environment, and a comparison of their approaches, including both the benefits and downsides to each individual approach, will be undertaken. These systems will interact with a Windows Server 2016 Server providing Windows Enterprise services. Another Linux distribution for a Linux server system will be chosen and an exploration of the requirements necessary to provide Windows-compatible Enterprise services to Windows 10 clients will be evaluated. The cost of implementing and administrating such environments and the support available for the systems will also be explored.

The research will aim to detail a modern best practice for what is necessary to implement in order to allow both platforms to co-exist in heterogeneous environments, and what benefits and downsides this could bring to organisations looking to implement such an environment.

1.2 Justification

Windows-focused networks have a near omnipresence in today's enterprises, with Windows clients being a ubiquitous sight, with Net Marketshare (2018) reporting a Windows desktop market share of 88.05% at the time of writing. Windows Server is a common choice to couple with Windows clients in order to provide many vital enterprise network services such as authentication, file and printer sharing, as well as enforcement of organisation-specific IT policies through Group Policy management. Linux and associated Open-Source technologies are also often found in organisations across the globe, being capable of providing many of the same services, with Linux server deployment rates rising from 65% in 2011 to 79% in 2014, compared with the decrease from 45% to a 36% deployment rate that Windows Server saw in the same period. (Vaughan-Nichols, 2014).

This rise in Linux Server adoption alongside the commonality of Windows clients, and the continued development of Open-Source software solutions, shows that there is a growing need to explore the current options available to facilitate the implementation of such a heterogeneous environment as seamlessly as possible, while providing similar network performance, features and administration options available in a Windows homogeneous environment. Despite Linux also holding a steady, sizable market share of 2.04% at the time of writing as a client operating system (Net Marketshare, 2018), there has been little exploration into the best practices of how to integrate Linux into an existing Windows environment, and with this sizable market share, there should be more investigation into integrating Linux clients into such environments utilizing Windows Enterprise technologies.

There is currently little in the way of up-to-date academic research into the current state of interoperability between Linux and Windows in such environments, which this project will tackle. Literature that currently exists on this subject is prone to corporate bias, with much of it being provided from large firms such as Red Hat, detailing one approach for their specific ecosystem. There is also little in the way of literature exploring this topic using the methods that shall be employed in this project, with little focus on performance and cost, and lack of scenarios where implementation is tested in a virtualised environment.

Chapter 2: Literature Review

2.1 Windows Enterprise Technologies

2.1.1 Active Directory

Minasi *et al.* (2014) describes Active Directory as "a central place where you store and manage all your users and computers and the behaviour of your Windows infrastructure.". Active Directory has existed in Windows Server since Server 2000 and has continued to be built upon with each subsequent version of Windows Server. Today, Active Directory now "plays a major role as a centralized identity and access solution." *(Minasi et al., 2014),* giving network administrators the facilities to globally control enterprise-wide user information from a single point. Active Directory also provides a hierarchy of administration *(Heslin, 2012)*, including;

- Forests (single Active Directory entities *(Minasi et al. 2014)),*
- Trees, (multiple domains within the same forest sharing the same database schema *(Minasi et al. 2014)),*
- Domains (a collection of objects, such as users, groups and systems, that share the same database *(Minasi et al., 2014)),*
- Organisational Units (OU) (a type of container used to organise objects within the Active Directory domain *(Minasi et al., 2014)).*

Active Directory allows for delegation of administration of objects contained within the Active Directory forest or domain through the use of Organisational Units (OU). Individual users, or a predefined group of users can be placed into a group for adding to an OU, which, when created, allows an administrator to delegate administrative tasks to that particular OU. (*Flores et al., 2017).*

Active Directory also depends on the Domain Name Service (DNS) in order to function, by using Service (SRV) DNS records in order to locate required services. Active Directory on Windows Server will, by default, attempt to configure the necessary DNS server for the administrator with the appropriate records when the Active Directory role is set up on the server. *(Minasi et al., 2014).*

2.1.2 Kerberos

Walla (2000) describes Kerberos as a protocol which "provides secure user authentication with an industry standard that permits interoperability." Kerberos (specifically version 5) has been a part of Windows Server since Windows 2000 with the inclusion of Active Directory in the same release, as Active Directory depends on Kerberos as its secure authentication protocol for domain log-ins. *(Walla, 2000).*

Kerberos is comprised of three parts; the Key Distribution Centre (KDC), the client trying to authenticate, and the server the client is trying to authenticate with. The KDC can also be broken down into two parts; the Authentication Service (AS) and the Ticket-Granting Service (TGS) *(Walla, 2000).* When a client wishes to log onto a network via Active Directory, they will provide their username and password, which will be verified by the AS against the Active Directory user database in the user's own domain. If the information provided is correct, the AS will provide the client with a Ticket-Granting Ticket (TGT), which can then be presented to the TGS when access to a network resource is required. The TGS will create a ticket and session key for the client if authentication is successful. *(Walla, 2000).*

2.1.3 Server Message Block and Common Internet File System

The Server Message Block (SMB) protocol is described by Minasi *et al (2014)* as "an application-layer network protocol that is used primarily to provide shared access to files, printers, ports and communication between machines on a network." The SMB Protocol was initially developed by IBM in the 1980s and further developed by Microsoft, with their implementation becoming the default "dialect" of SMB used on IBM's OS/2 and Microsoft's MS-DOS and Windows. *(French, 2007).*

French (2007) describes SMB/CIFS as layer 6/7 protocols according to the Open System Interconnection (OSI) 7-layer model, utilizing TCP as their Transport protocol. French (2007) also describes that SMB/CIFS are designed with "Transparency" and "Heterogeneity" in mind, where;

- The protocols will attempt to provide "local remote transparency" where users and applications will see no discernible difference between a local storage medium and a networked one. *(French, 2007).*
- The protocols are unaware of what operating systems they are interacting with nor have they any requirement to know, with clients being able to access files on a server irrespective of what file system the server's physical storage medium is using. *(French, 2007).*

2.1.4 Group Policy

Microsoft (2012) describes Group Policy as a way to enable "Active Directory-based change and configuration management of user and computer settings" on systems running Windows XP or later. Group Policy allows for such policies as security settings, software and script deployment or system preferences to be defined and implemented in Active Directory sites, domains or organisational units (OUs) *(Microsoft, 2012).*

Group Policy policies are defined through the use of Group Policy Objects (GPOs), which are managed by the Group Policy Management Console (GPMC) on the domain controller. The GPMC allows an administrator to manage GPOs and their permissions for entire Active Directory forests within an organisation *(Microsoft, 2012).*

2.2 Linux Enterprise Technologies

2.2.1 Linux in the Enterprise

McDaniel (2000) describes that Linux, in the modern day, "is being used in a wide variety of applications, from embedded systems to web servers, from software development to enterprise resource management (ERP)."

He also claims that in the corporate IT environment, Linux systems can "make excellent file and print servers for heterogeneous environments", through the use of technologies such as Samba, offering SMB/CIFS and NetBIOS name resolution support to Windows clients *(McDaniel, 2000).*

McDaniel (2000) also claims that in the corporate IT environment, reliability of the system in comparison to Windows NT is one reason the enterprise may consider implementing Linux. Linux's approach to administration primarily via a remotely accessible command-line interface (CLI) also provides ease of administration to system administrators over Windows NT's GUI-driven administration *(McDaniel, 2000).*

Dustin Kirkland (2015), former Vice President of Product at Canonical, details today's prevalence of Linux in the enterprise in the form of the Ubuntu distribution. Kirkland (2015) details that such large services as Instagram, Spotify, Netflix and Dropbox all rely on Ubuntu to provide their services.

2.2.2 Winbind

Winbind is described by Potter *et al.* (2000) as a tool which "unifies UNIX and NT account management by allowing a UNIX box to become a full member of an NT domain." Joining a UNIX system to a Windows NT domain means the UNIX system will see domain users and groups as though they were native to UNIX, with NT domain users and groups being able to be used in the same manner as their native UNIX counterparts, such as being able to take ownership of files on the UNIX system and run native UNIX applications. *(Potter et al., 2000).* Winbind also provides support for the Pluggable Authentication Modules (PAM) authentication system, meaning NT domain authentication via Winbind is possible via any UNIX application that supports the PAM system. *(Potter et al., 2000).*

Potter *et al.* (2000) details that Winbind functions by running a daemon on a UNIX system which listens on a UNIX domain socket for requests generated by the Name Service Switch (NSS) or PAM clients. Winbind then utilizes some Microsoft Remote Procedure Calls (MSRPC) to authenticate against a Windows-based domain controller.

2.2.3 System Security Services Daemon (SSSD)

Heslin (2012) details that the System Security Services Daemon (SSSD) "provides access to different identity and authentication providers", such as Microsoft's Active Directory and implementations of the Lightweight Directory Access Protocol (LDAP). SSSD functions by acting as an intermediary between the client and domain controller, allowing the client system to connect to the domain controller, with SSSD building a cache on the client of previously used user information. When used in this manner with

Active Directory, SSSD provides an alternative to the previously mentioned Winbind daemon. *(Hanzelka et al., 2018).*

SSSD has the ability to map Windows Security IDs (SIDs) for users to Linux User IDs and Group IDs (UIDs and GIDs) through a process known as ID Mapping. SSSD is able to assign a range of these IDs to a new Active Directory domain upon discovery and create entries in the SSSD cache on the client system with the Linux UIDs and GIDs of the Active Directory users logging into the system. *(Hanzelka et al., 2018).*

Much like Winbind, SSSD also has support for the PAM authentication system, meaning NT domain authentication is possible via SSSD in any application that supports PAM. *(Hanzelka et al., 2018).*

2.2.4 Pluggable Authentication Modules (PAM)

Geisshirt (2007) describes the Pluggable Authentication Modules (PAM) system as "a modular and flexible authentication management layer that sits between Linux applications and the native underlying authentication system." PAM makes it possible to utilize different authentication methods for different applications without having to recompile said applications to support them through the use of PAM modules. *(Geisshirt, 2007).* Each PAM module is tailored to the authentication method used, be it through LDAP, RADIUS or native UNIX authentication methods. PAM modules follow a typical naming convention, *pam_mechanism.so*, where mechanism is the authentication mechanism used. An example is the UNIX authentication module, named *pam_unix.so (Smørgrav, n.d.).*

2.2.5 Samba

Samba is described by Bartlett (2005) as an open-source technology which "provides Windows networking services, on a Unix-like platform", such as Linux. Samba can provide services on this platform ranging from simple file and printer sharing through SMB/CIFS, the ability to join an NT domain through Winbind, or even act as a Windows NT4-compatible Domain Controller, with such functionality being implemented in Samba v3.0. Compatibility with Windows 2000 and above Active Directory domains was implemented with Samba v4.0, with support for Kerberos authentication being included in this release. *(Bartlett, 2005).*

Bartlett (2005) also claims that the introduction of NT4-compatible domain controller features in Samba has allowed some organisations in the past "to remove Windows servers entirely from their networks", replacing their Windows-based domain controllers with UNIX/Linux-based alternatives as Samba is able to "'take over' an existing Windows network."

Samba as a server application on Linux runs two daemons *(Heslin, 2012)*:

- *smbd,* which is the primary daemon that provides SMB/CIFS file and printer server functionality *(Heslin, 2012).*
- *nmbd,* which acts as the Windows NetBIOS name server *(Heslin, 2012).*

2.2.6 Lightweight Directory Access Protocol (LDAP)

Heslin (2012) describes the Lightweight Directory Access Protocol (LDAP) as “a set of open protocols used to access centrally stored information over a network.” LDAP organizes information on a directory server in a hierarchical fashion. The directories that form this hierarchy can store a wealth of information on users within a network, and even allow said users to access their account from any client system on a network using LDAP *(Heslin, 2012).*

Heslin (2012) describes that LDAP is a client/server-based set of protocols, with an LDAP directory server containing the databases of user information, and an LDAP client, which when connected to the LDAP directory server, can query the information or modify it.

Bartlett (2007) explains that Microsoft’s Active Directory utilizes the LDAP set of protocols, with Active Directory information being exported as an LDAP tree.

2.3 Hypervisors

2.3.1 Hypervisors and the Types Available

Hypervisors are a piece of software designed to create a virtualized environment on a host system, in which a number of guest operating systems and software can be used. The hypervisor makes this possible by sharing available physical system resources between multiple guest systems, allowing them to run on the same hardware at the same time. *(Oracle, n.d.).*

Hypervisors are generally split into two categories, as defined by Goldberg and Popek; type 1 and type 2 *(Chinnaswammy, 2016).* Type 1 hypervisors are considered to be “native” or “bare-metal” hypervisors, which run directly on the physical host system’s hardware and are able to control the hardware, rather than relying on an underlying operating system, with the guest operating system running atop the base hypervisor. Common type 1 hypervisors used today include VMware’s ESXi and Microsoft’s Hyper-V *(Oracle, n.d.).*

Type 2 hypervisors are considered to be “hosted” hypervisors, which run atop an operating system running on the physical host system like any other application, with the guest operating running in a layer above the application. Common type 2 hypervisors used today include Oracle’s VM VirtualBox and VMware’s Workstation. *(Oracle, n.d.).*

2.3.2 Oracle VM VirtualBox

Oracle (2018) consider VirtualBox to be a “hosted” hypervisor, fitting the type 2 hypervisor definition by Goldberg and Popek *(Chinnaswammy, 2016).* VirtualBox, as a type 2 hypervisor, is able to run on a number of operating systems, including Windows and Linux, allowing users to run multiple different guest operating systems within at once.

Oracle (2018) detail that VirtualBox is able to virtualise a range of virtual hardware devices, including several types of disk controllers (such as the common IDE and SATA interfaces) with virtual hard disk images attached to these controllers and presented to the virtual machine as though they were physical disks, virtual network interface adapters (Fast Ethernet and Gigabit Ethernet from vendors AMD and Intel), sound cards and USB controllers. Oracle (2018) also detail that VirtualBox provides virtual machines with a share of the host system's RAM and CPU, allocated by the user according to their needs.

VirtualBox provides a wealth of network virtualisation solutions, with up to four network interface adapters being able to be presented to a virtual machine at any one time, with six different types of adapter being selectable by the user, with each type having varying degrees of support by different software and operating systems *(Oracle, 2018).* VirtualBox also allows these network adapters to configured to operate in a range of modes, including;

- Network Address Translation (NAT) mode, where a guest operating system will act "much like a real computer that connects to the Internet through a router", with VirtualBox's networking engine mapping traffic to and from the guest system. *(Oracle, 2018)*
- Bridged networking mode, where a guest operating system will connect to a physical adapter on the host system and be able to interact on a host's network *(Oracle, 2018).*
- Internal networking, where guest systems are connected together and are able to communicate on an internal VirtualBox network but are not accessible from outside this network or have access outside this network *(Oracle, 2018).*

Chapter 3: Methodology and Relevant Technologies

3.1 Research Methodology

This project was undertaken using a mostly quantitative research method; with a focus on analysing network performance statistics between the various network configurations and cost of support between the various platforms. Qualitative methods were also employed, with a focus on complexity of implementation and administration of the various enterprise network technologies on different operating systems being discussed.

3.1.1 Measuring and Analysing Network Performance

In order to analyse the performance of the networks developed in this research and ascertain the performance of the technologies employed within, several benchmarks have been devised.

1. Measuring the time taken to complete a domain login on a client system.
2. Measuring the transfer rate of a large file (1.8GB Ubuntu ISO file) from a server SMB 3 share to a client.
3. Measuring the transfer rate of a large file (1.8GB Ubuntu ISO file) from a client to the server SMB 3 share.
4. Measuring the transfer rate of a collection of smaller files (135MB folder of assorted documents and images) from a server SMB 3 share to a client.
5. Measuring the transfer rate of a collection of smaller files (135MB folder of assorted documents and images) from a client to a server SMB 3 share.

These benchmarks have been chosen as a way of examining the performance of the technologies employed in a real-world enterprise environment scenario, where users will be regularly logging in to their domain accounts on client systems and transferring files of varying types and sizes to and from a server on the network. Each of these benchmarks will be conducted three times and an average taken of the results. The Windows homogeneous network will act as the baseline for results in these benchmarks, with the statistics obtained from the other networks compared with the baseline.

3.2 Technologies Used in the Research

3.2.1 Virtualisation

In order to facilitate the creation of the required networks, a hypervisor was deemed necessary due to available resources. Oracle VM VirtualBox was chosen for this purpose, as Oracle (2018) has described VirtualBox as a “hosted” hypervisor, meaning the hypervisor and guest operating systems within can be virtualised on an existing personal computer, rather than requiring a separate physical system to run a “bare-metal” hypervisor.

Oracle VM VirtualBox was also chosen for its cost. Currently, Oracle (2018) do not charge for personal non-commercial use of VirtualBox, in contrast to a similar product such as VMware's Workstation Pro, which currently VMware (2018) have listed for €274.95, which was considerably more than the budget available for this project. VMware (2018) do offer a free version of their Workstation product, known as VMware Workstation Player, however this product is severely limited in features in comparison to VirtualBox, with some being vital for this project including the ability to run multiple virtual machines at once, snapshotting and advanced networking settings *(VMware, 2018).*

3.2.2 Client Operating Systems

In the virtualised environments where Windows-based clients are required, Windows 10 was chosen. As the project focusses on the current state of technologies that allow interoperability between Windows and Linux, Windows 10 was selected as according to Microsoft (2018), it is the current up-to-date release of the Windows operating system and the resources are available to make use of it in this project.

Where Linux-based clients were required, three different distributions of Linux were selected; openSUSE Leap 15, CentOS 7.6, and Ubuntu 18.04 LTS.

openSUSE Leap 15 was selected as a free, binary-compatible alternative to SUSE Linux Enterprise Desktop (SLED). The Leap 15 release was selected as currently, according to openSUSE (2018), Leap 15 is the current, stable, "server ready" release of the openSUSE distribution. openSUSE (2018) detail that the openSUSE distribution is the current foundation for SUSE's enterprise offerings, with it being said that "SUSE refines and enhances openSUSE to create a hardened and supported suite of enterprise Linux products suitable for data centre deployments, edge server deployments, business desktops, and business infrastructure deployment." *(openSUSE, 2018).* In a study detailed by SUSE in 2013, with 167 respondents from organisations with at least 500 employees, 42% of respondents said Linux is either their primary server platform or plays a major role within the organisation. Among these respondents, results showed that SUSE Linux Enterprise Server was installed by one third of the respondents to the study *(SUSE, 2013)*, demonstrating the relative popularity of SUSE Linux in the enterprise.

CentOS 7.6 was selected as a free, binary-compatible alternative to Red Hat Enterprise Linux (RHEL), with CentOS (2018) detailing that CentOS 7.6 is the current up-to-date release of the distribution. Red Hat (2018) detail their leadership in the open-source world, with 100% of airlines, telecommunications companies, and commercial banks in the Fortune 500, and departments of the United States Government relying on Red Hat technologies, demonstrating the sheer prevalence of Red Hat in today's enterprise. In the same study detailed by SUSE in 2013, Red Hat Enterprise Linux was the most deployed platform among the 42% of 167 respondents who ran Linux in a major server role in their enterprise *(SUSE, 2013).* With Red Hat (2018) only providing a 30-day evaluation period for Red Hat Enterprise Linux (RHEL), a compatible alternative was required for this project, with it being detailed in a press release by Red Hat in 2014 that CentOS being endorsed by Red Hat as a community offering of the Red Hat platform.

Ubuntu 18.04 LTS was selected as one of the most popular free Linux distributions available today. 18.04 LTS was selected as it is the latest up-to-date Long-Term

Support (LTS) release of the Ubuntu distribution, with support in the form of security and maintenance being provided for five years from release, until April 2023 *(Ubuntu, 2018),* which is suitable for an enterprise environment. According to Dustin Kirkland (2015), former Vice President of Product at Canonical, Ubuntu's popularity stretches far and wide in the IT world, with, at the time of writing, at least 20 million instances of Ubuntu had been launched in cloud services such as Amazon Web Services and Microsoft Azure. Kirkland (2015) also details the prevalence of Ubuntu in social media and online content, with such large platforms as Wikipedia, Dropbox, Instagram and Spotify all making use of Ubuntu.

3.2.3 Server Operating Systems

In the virtualised environments where a Windows Server system was required, Windows Server 2016 was chosen. As the project focussed on the current state of technologies that allow interoperability between Windows and Linux, Server 2016 was selected as it was the current release of Windows Server until October 2018 *(Chapple, 2018)* and is the most up to date version available that can currently be used in this project due to available resources.

In the virtualised environments where a Linux Server system is required, Zentyal Server 6.0 was chosen. Academic research detailing Linux distribution support for the technologies being explored in this project is limited, so research was undertaken to evaluate what distributions would provide the necessary functionality. openSUSE Leap 15 was initially evaluated for the same reasons it was selected as a client operating system, as well as openSUSE (n.d.) providing a wealth of literature on configuring Leap 15 with the relevant technologies necessary to provide Windows Enterprise services to client operating systems. This literature details the options for configuration through their YaST graphical system configuration tool, which provides wizards within to ease the setup of these technologies *(openSUSE, n.d.),* thus also providing a user experience similar to that of Windows Server. However, upon testing, it was found that the literature was inconsistent with the current state of the YaST configuration tool, and the tools currently provided by YaST only allow for a domain controller to provide functionality for a Windows NT4-style domain, and not an Active Directory style domain.

Further research was conducted to find a distribution that provided support for providing Active Directory domain functionality, which yielded Zentyal Server. Zentyal (2018) describe their product as "offering an easy-to-use Linux alternative to Windows Server" and coming with "native Microsoft Active Directory interoperability, together with all the network services required in a corporate environment." Zentyal (2018) detail that Zentyal Server 6.0 is based on Ubuntu Server 18.0.4.1 LTS, which, as detailed by Kirkland (2015), has a commendable reach within the IT world, and is supported with security updates for five years from release, until April 2023 *(Ubuntu, 2018).* Upon testing, it was found that Zentyal Server did indeed provide the necessary Active Directory style domain functionality, configurable graphically through a custom web-based interface, thus satisfying the requirements for this project.

Chapter 4: Development

4.1 Designing the Virtual Network Topology

In order to begin implementing and evaluating the functionality of the named Windows Enterprise network technologies on the aforementioned operating systems, a suitable network topology had to be designed.

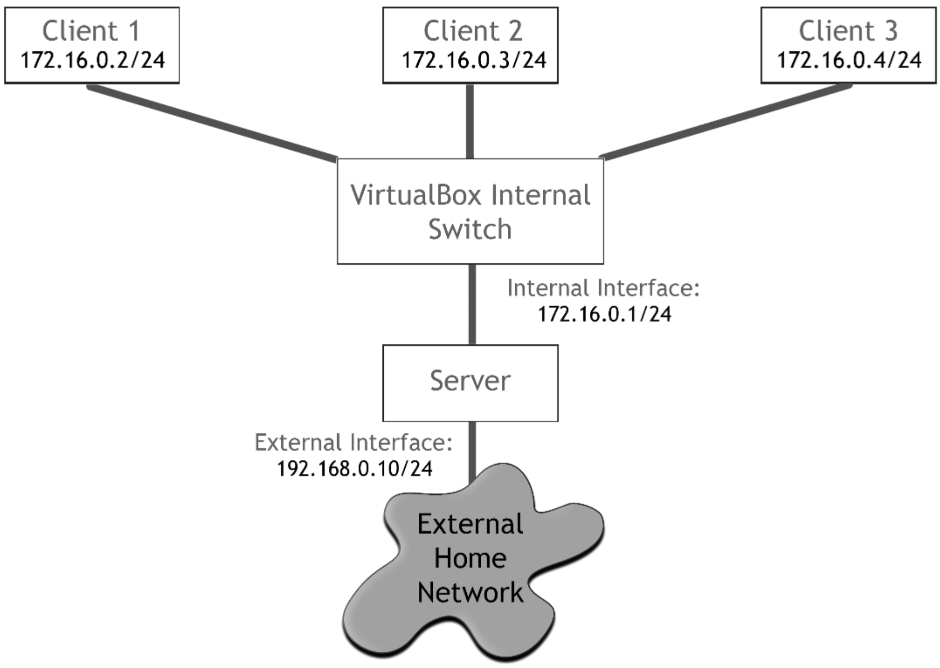


Figure 1: The basic network topology and IP addressing scheme used for the virtual machines.

Given that three different Linux distributions were to be tested as client operating systems, it was deemed fair to ensure all networks had at least three clients, even if those clients ran identical operating systems, such as in a Windows homogeneous environment. A 172.16.0.0/24 IP addressing scheme was used to differentiate from the external network the virtual machines would be connecting to. All virtual machines in their respective networks would be connected via VirtualBox's Internal Networking mode, with a name respecting the makeup of the environment. External connectivity for all virtual machines was established by using two network adapters on the server system, with one configured in VirtualBox with the Bridged Adapter networking mode, acting as the external interface. Routing functionality was then established on the server to pass traffic between the two networks.

4.2 Configuration of the Networks

4.2.1 Windows Homogeneous Network as a Control

To act as a control in this investigation, a Windows homogeneous network was created, with three Windows 10 clients connected to a Windows Server 2016 server. Baseline network performance results would be obtained from this network, as good, consistent performance would be expected when using the Windows Enterprise network technologies on their native platform.

The Windows Server 2016 server system was initially configured with the IP addresses of 172.16.0.1/24 on the internal interface, and 192.168.0.10/24 on the external interface. The server was then configured with the Routing and Remote Access, Active Directory Domain Services, and File and Storage Services roles in order to act as a router, domain controller and SMB file server for the three Windows 10 clients.

In order to act as a domain controller to the clients, the server required promotion to the domain controller role. During this process, the rmcgowanwin.net domain was established. A handful of users were subsequently added to the domain via the Active Directory Users and Computers console and contained with an Organisational Unit (OU) named Windows Homogeneous Users, as seen in Figure 2.

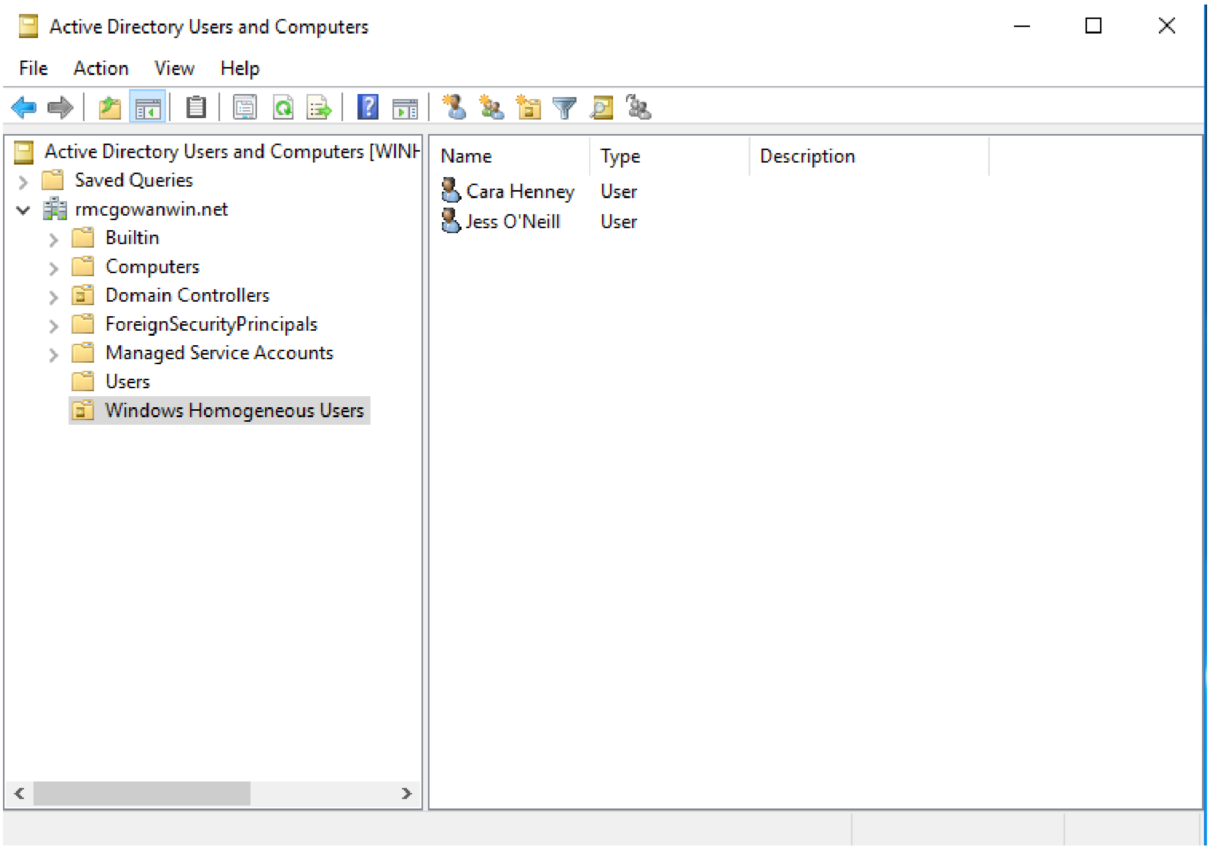


Figure 2: The Active Directory Users and Computers console showing the users within the Windows Homogeneous Users OU in the rmcgowanwin.net domain.

All three client systems were then joined to the rmcgowanwin.net domain, and domain logins were tested with one of the users shown in Figure 2, with success.

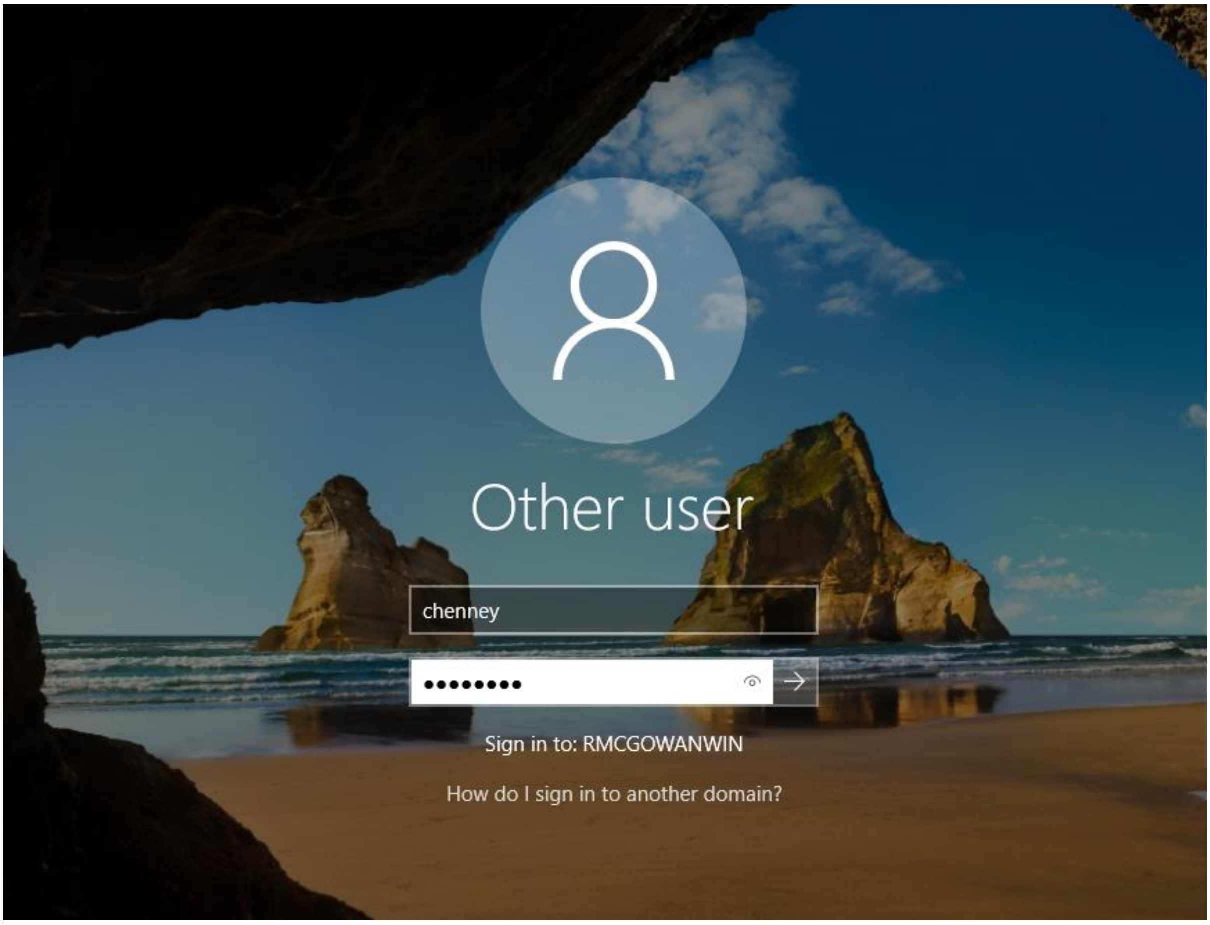


Figure 3: A Windows 10 Client login screen showing the required credentials for a domain login in the rmcgowanwin.net domain.

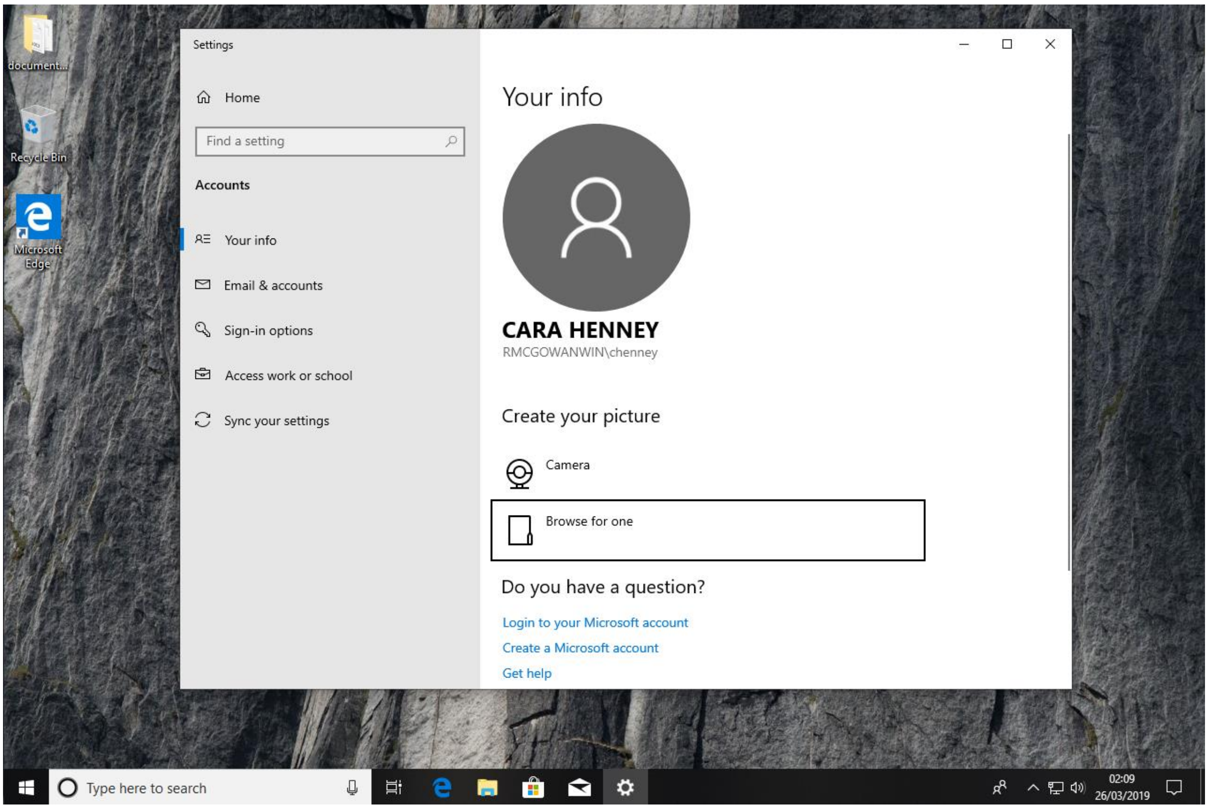


Figure 4: A Windows 10 Client showing the successful domain login of the user chenney.

A folder was then created on the server, with the path C:\Shared, which was set to be shared via SMB with the path \\WINHOMSERVER\Shared, with the Domain Users group having read/write privileges within this share, which includes the users within the Windows Homogeneous Users OU created earlier. This share was then mapped as a network drive on the client systems as drive Z:\, which remained mounted and available upon further logins.

4.2.2 Windows Server with Linux Clients Network

In this environment, a Windows Server 2016 server was set up to serve three clients running three different Linux distributions detailed in Chapter 3; namely Ubuntu 18.04 LTS, openSUSE Leap 15 and CentOS 7.6. The Windows Server 2016 Server in this network was configured in much the same way the server in the Windows Homogeneous network was configured; with the same IP addresses, server roles, users and shared folders. In this network, the server was promoted to be the domain controller of the rmcgowan.net domain, with the same users as in the previous network being created in the Active Directory Users and Computers console, within an OU named "Linux Users".

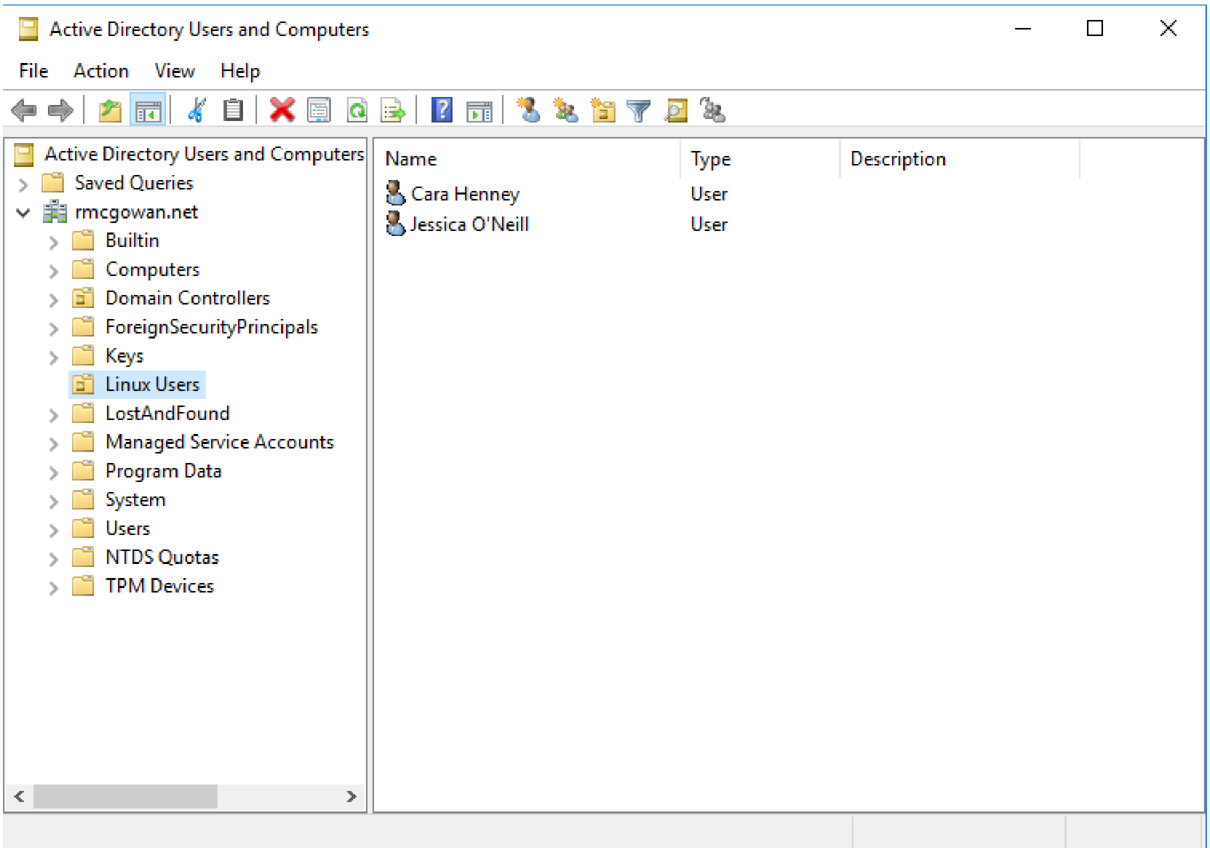


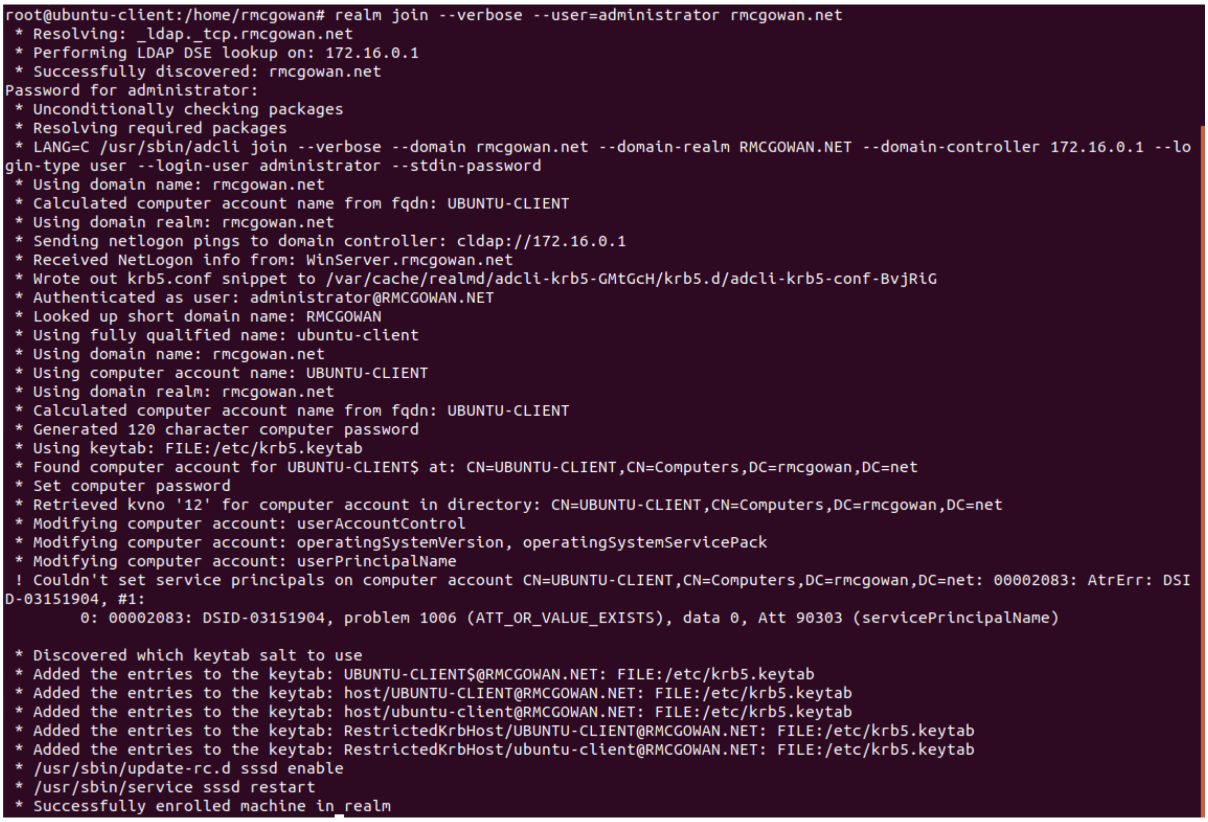
Figure 5: The Active Directory Users and Computers console showing the users within the Linux Users OU in the rmcgowan.net domain.

4.2.2.1 Ubuntu 18.04 LTS

Official Canonical (2018) documentation on integrating Ubuntu 18.04 LTS with an Active Directory domain was found to be rather vague on the setup requirements for joining an Active Directory domain, and upon testing was found to not provide a working setup. Waterman (2018) however details the process utilizing the System

Security Services Daemon (SSSD) to act as the intermediary between the client and domain controller, alongside other command line tools available in the Ubuntu software repositories that automate much of the configuration process, such as configuring Samba, SSSD and Kerberos.

In order to begin the process of joining the domain, the installation of some software packages was necessary; namely *realmd, sssd, sssd-tools, libnss-sss, libpam-sss, krb5-user, adcli, and samba-common-bin*. An attempt was then made to join the domain via the adcli utility, using the command `realm join -verbose –user=administrator rmcgowan.net`. After following the prompts, the Ubuntu client was successfully joined to the domain.



```
root@ubuntu-client:/home/rmcgowan# realm join --verbose --user=administrator rmcgowan.net
 * Resolving: _ldap._tcp.rmcgowan.net
 * Performing LDAP DSE lookup on: 172.16.0.1
 * Successfully discovered: rmcgowan.net
Password for administrator:
 * Unconditionally checking packages
 * Resolving required packages
 * LANG=C /usr/sbin/adcli join --verbose --domain rmcgowan.net --domain-realm RMCGOWAN.NET --domain-controller 172.16.0.1 --lo
gin-type user --login-user administrator --stdin-password
 * Using domain name: rmcgowan.net
 * Calculated computer account name from fqdn: UBUNTU-CLIENT
 * Using domain realm: rmcgowan.net
 * Sending netlogon pings to domain controller: cldap://172.16.0.1
 * Received NetLogon info from: WinServer.rmcgowan.net
 * Wrote out krb5.conf snippet to /var/cache/realmd/adcli-krb5-GMtGcH/krb5.d/adcli-krb5-conf-BvjRiG
 * Authenticated as user: administrator@RMCGOWAN.NET
 * Looked up short domain name: RMCGOWAN
 * Using fully qualified name: ubuntu-client
 * Using domain name: rmcgowan.net
 * Using computer account name: UBUNTU-CLIENT
 * Using domain realm: rmcgowan.net
 * Calculated computer account name from fqdn: UBUNTU-CLIENT
 * Generated 120 character computer password
 * Using keytab: FILE:/etc/krb5.keytab
 * Found computer account for UBUNTU-CLIENT$ at: CN=UBUNTU-CLIENT,CN=Computers,DC=rmcgowan,DC=net
 * Set computer password
 * Retrieved kvno '12' for computer account in directory: CN=UBUNTU-CLIENT,CN=Computers,DC=rmcgowan,DC=net
 * Modifying computer account: userAccountControl
 * Modifying computer account: operatingSystemVersion, operatingSystemServicePack
 * Modifying computer account: userPrincipalName
 ! Couldn't set service principals on computer account CN=UBUNTU-CLIENT,CN=Computers,DC=rmcgowan,DC=net: 00002083: AtrErr: DSI
D-03151904, #1:
        0: 00002083: DSID-03151904, problem 1006 (ATT_OR_VALUE_EXISTS), data 0, Att 90303 (servicePrincipalName)

 * Discovered which keytab salt to use
 * Added the entries to the keytab: UBUNTU-CLIENT$@RMCGOWAN.NET: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: host/UBUNTU-CLIENT@RMCGOWAN.NET: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: host/ubuntu-client@RMCGOWAN.NET: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: RestrictedKrbHost/UBUNTU-CLIENT@RMCGOWAN.NET: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: RestrictedKrbHost/ubuntu-client@RMCGOWAN.NET: FILE:/etc/krb5.keytab
 * /usr/sbin/update-rc.d sssd enable
 * /usr/sbin/service sssd restart
 * Successfully enrolled machine in realm
```

Figure 6: The adcli utility successfully joining the Ubuntu 18.04 client to the rmcgowan.net domain.

A graphical domain login was then attempted from the GDM login screen (the default for the GNOME interface on Ubuntu), with success. During the first-time login of a domain user, PAM is automatically configured to create a local home directory on the system, which, for the chenney user, is shown in figure 7 with the path /home/chenney@rmcgowan.net.

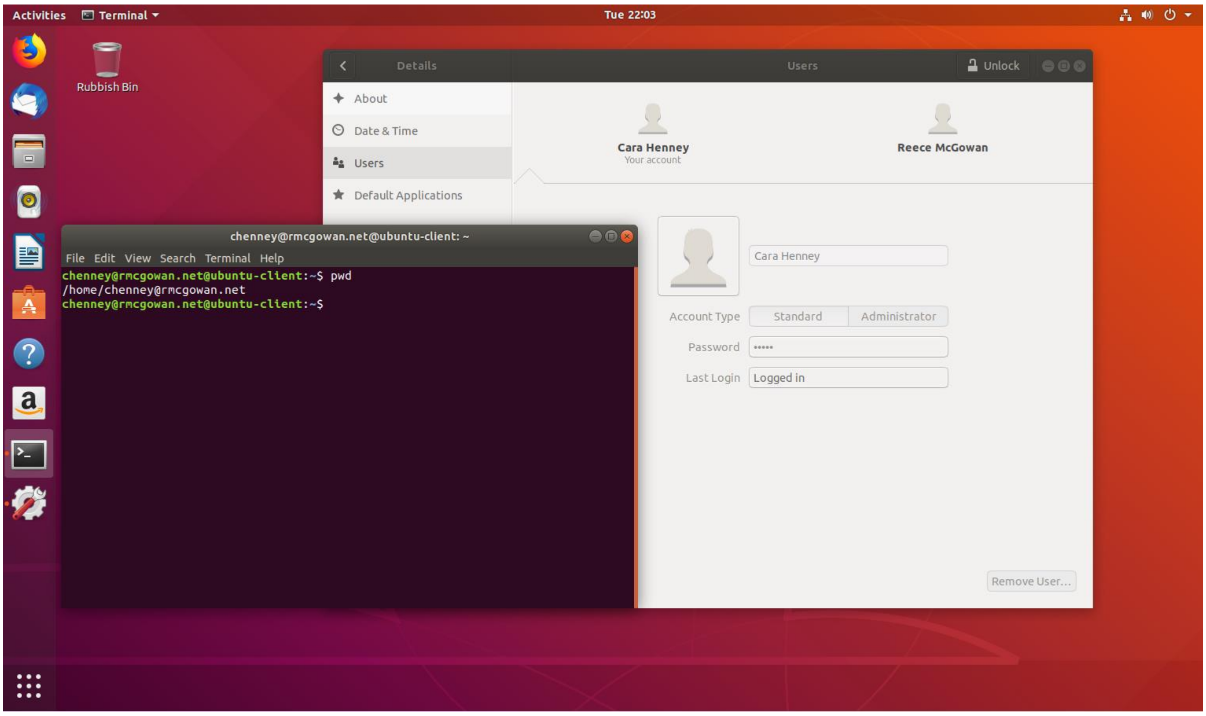


Figure 7: Ubuntu client desktop showing a successful login as the domain user chenney.

By default, SSSD is configured on Ubuntu 18.04 to use fully qualified names when logging in as domain users, meaning that if a user wished to log in with the chenney domain user, they would be required to type *chenney@rmcgowan.net* at the login prompt. This behaviour can be changed within the /etc/sssd/sssd.conf file, setting the option *use_fully_qualified_names* to *False*. This then mimics the default behaviour of Windows 10 clients, where only the domain username is required to log in, and not the fully qualified username.

In order to access the SMB network share created on Windows Server, the *Connect to Server* function in Nautilus (Ubuntu's default file manager) was used with the path *smb://172.16.0.1/Shared.* As the domain user already has access to this folder, no password was required to access it. No further attempts were made to have this folder automount, other than adding a bookmark to Nautilus, which when used, automatically mounts the share.

4.2.2.2 CentOS 7.6

Hanzelka *et al.* (2018) detail the process for joining a Red Hat Enterprise Linux (RHEL) client to an Active Directory domain. Their documentation recommends the same approach used on the Ubuntu 18.04 client; using SSSD as an intermediary between the client and domain controller, and the adcli tool and realmd to configure the underlying components, such as Samba, SSSD and Kerberos, and to join the client to the domain. Given that CentOS is a binary compatible and functionally similar derivative of RHEL, this guide was found also to apply to CentOS, however extra software packages were required to be installed. In order to begin the domain join process, the packages *sssd, realmd, oddjob, oddjob-mkhomedir, adcli, samba-common, samba-common-tools, krb5-workstation, openldap-clients, and policycoreutils-python* had to be installed on the client. An attempt was then made to join the domain via the adcli utility, using the command realm join –verbose –user=administrator rmcgowan.net. After following the prompts, the CentOS client was also successfully joined to the domain.

```
[root@centos-client rmcgowan]# realm join --verbose --user=administrator rmcgowan.net
 * Resolving: _ldap._tcp.rmcgowan.net
 * Performing LDAP DSE lookup on: 192.168.0.10
 * Performing LDAP DSE lookup on: 172.16.0.1
 * Successfully discovered: rmcgowan.net
Password for administrator:
 * Required files: /usr/sbin/oddjobd, /usr/libexec/oddjob/mkhomedir, /usr/sbin/sssd, /usr/bin/net
 * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-conf.3JZVYZ -U administrator ads join rmcgow
an.net
Enter administrator's password:DNS update failed: NT_STATUS_INVALID_PARAMETER

Using short domain name -- RMCGOWAN
Joined 'CENTOS-CLIENT' to dns domain 'rmcgowan.net'
No DNS domain configured for centos-client. Unable to perform DNS Update.
 * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-conf.3JZVYZ -U administrator ads keytab crea
te
Enter administrator's password:
 * /usr/bin/systemctl enable sssd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/sssd.service to /usr/lib/systemd/system/sssd.se
rvice.
 * /usr/bin/systemctl restart sssd.service
 * /usr/bin/sh -c /usr/sbin/authconfig --update --enablesssd --enablesssdauth --enablemkhomedir --nostart && /us
r/bin/systemctl enable oddjobd.service && /usr/bin/systemctl start oddjobd.service
 * Successfully enrolled machine in realm
```

Figure 8: The adcli utility successfully joining the CentOS 7.6 client to the rmcgowan.net domain.

A graphical login was then attempted from the GDM login screen (the default for the GNOME interface on CentOS), with success. PAM, much like on Ubuntu, is configured to automatically create a local home folder on the client for the domain user. Fully qualified names for domain logins is also enabled by default in /etc/sssd/sssd.conf, meaning that, much like Ubuntu, if a user wished to login with the chenney user, they would have to enter chenney@rmcgowan.net at the login prompt. This also means PAM will name the domain user’s home folder in this fully qualified manner. This behaviour can be disabled by setting the *use_fully_qualified_names* option in /etc/sssd/sssd.conf to *False*.

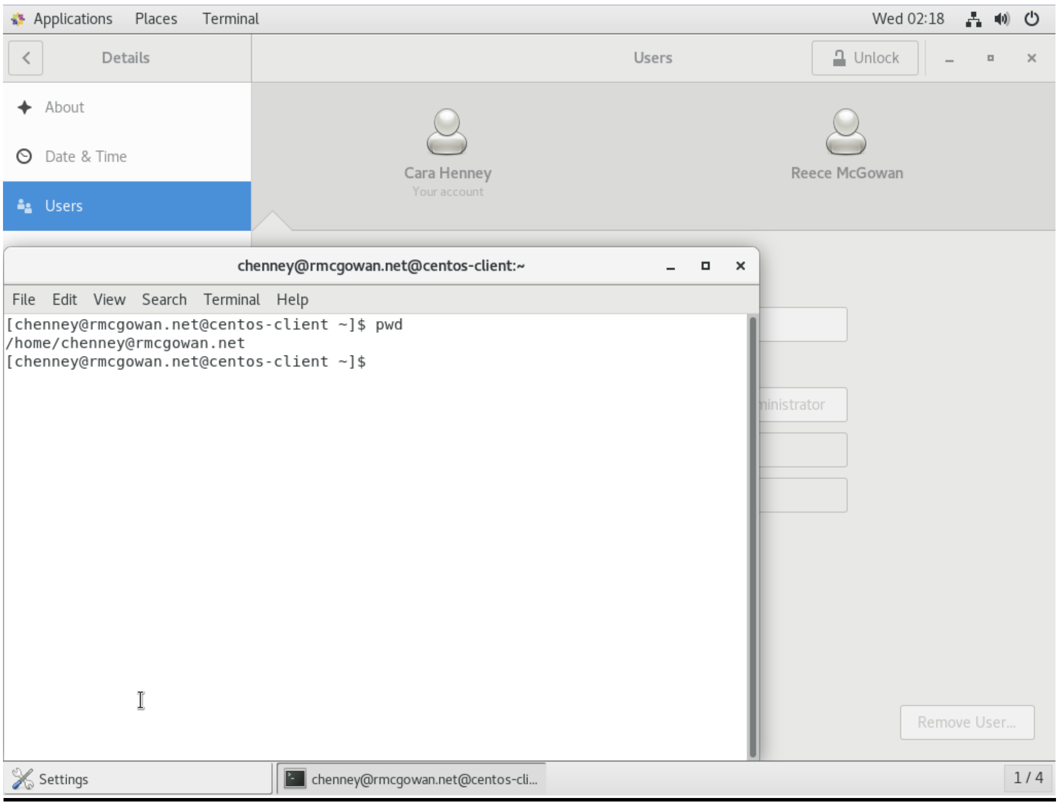


Figure 9: CentOS client desktop showing a successful login as the domain user chenney.

In order to access the SMB network share created on Windows Server, the same *Connect to Server* function in Nautilus (CentOS' default file manager) was used with the path *smb://172.16.0.1/Shared.* As the domain user already has access to this folder, no password was required to access it. No further attempts were made to have this folder automount, other than adding a bookmark to Nautilus, which when used, automatically mounts the share.

4.2.2.3 openSUSE Leap 15

openSUSE (n.d.) detail joining an openSUSE Leap 15 client to an Active Directory domain through the YaST graphical system configuration tool. YaST provides three graphical tools, known as modules, for joining openSUSE to an Active Directory domain:

1. The *User Logon Management* module, which utilizes the System Security Services Daemon (SSSD) as the intermediary between the client and domain controller to enable openSUSE to use a range of identity services (such as Active Directory or other LDAP implementations) and an authentication service such as Kerberos *(openSUSE, n.d.).* openSUSE (n.d.) say this is "best suited for joining Active Directory domains".
2. The *Windows Domain Membership* module, which is tailored to join openSUSE to an Active Directory domain, but instead utilizes winbind as the intermediary between the client and domain controller rather than SSSD *(openSUSE, n.d.).* openSUSE (n.d.) say this is better suited if there is a requirement for using the older NTLM method of authentication rather than Kerberos, or if cross-forest trusts are necessary.

3. The *LDAP and Kerberos Authentication* module, which facilitates the configuration of LDAP identities and Kerberos authentication independently from one another, though provides fewer configuration options than the previous two modules *(openSUSE, n.d.).* This module also utilizes SSSD, however openSUSE (n.d.) say it is “not as well suited for connecting to Active Directory” as the other modules.

Given that openSUSE (n.d.) detail that the *User Logon Management* module is recommended for Active Directory domains, it was decided that the client would be joined to the domain through that module. The YaST utility will install any extra packages required for the domain join process automatically, if necessary. Once launched, the module will give the user an overview of the system’s current configuration, which can be modified by clicking the “change settings” button.

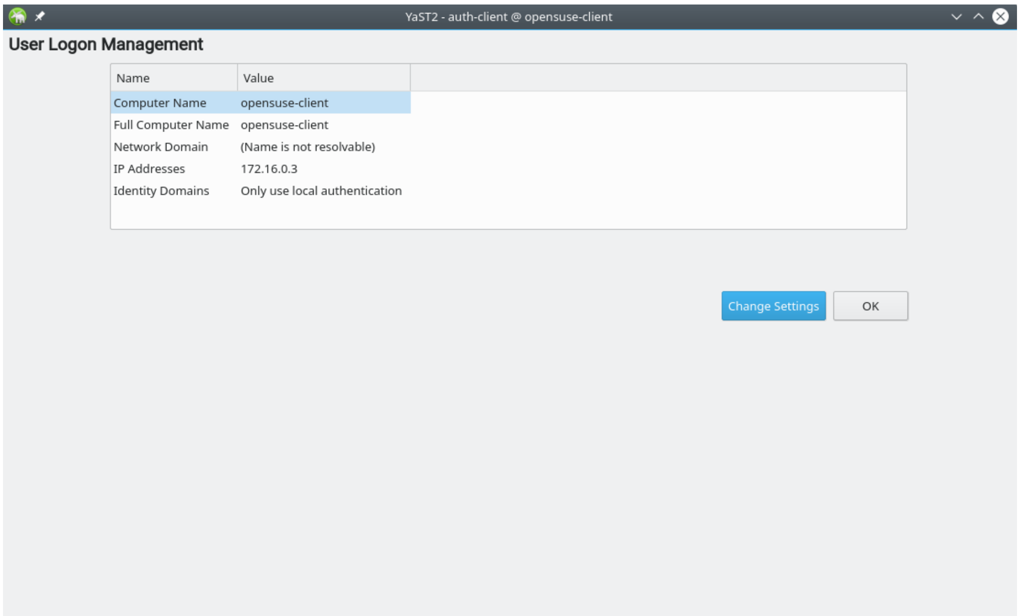


Figure 10: The User Logon Management module overview prior to joining a domain.

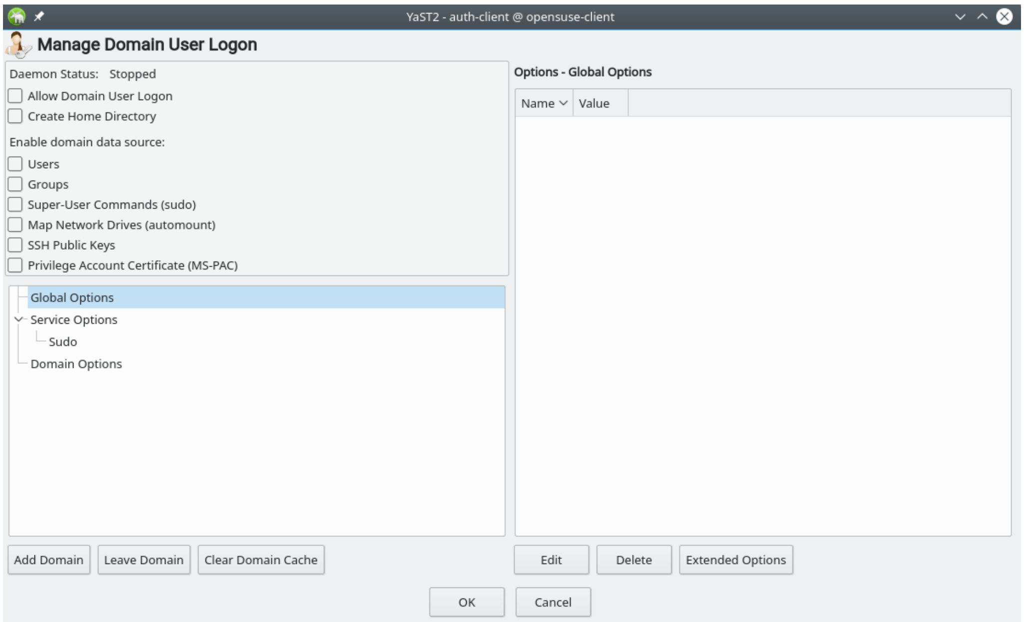


Figure 11: The User Logon Management module configuration interface prior to joining a domain.

In order to begin the domain join process, the “Allow Domain User Logon” button was checked. To maintain consistency between all the Linux clients, the “Create Home Directory” option was also checked, so that PAM will create a local home directory upon a first-time login of a domain user. To join the domain, the “Add Domain” button was clicked which opened the wizard to begin the process. In the initial dialog presented, the name of the domain the client would be joining was entered, and Microsoft Active Directory was specified as both the service that provides identity data, and authentication.

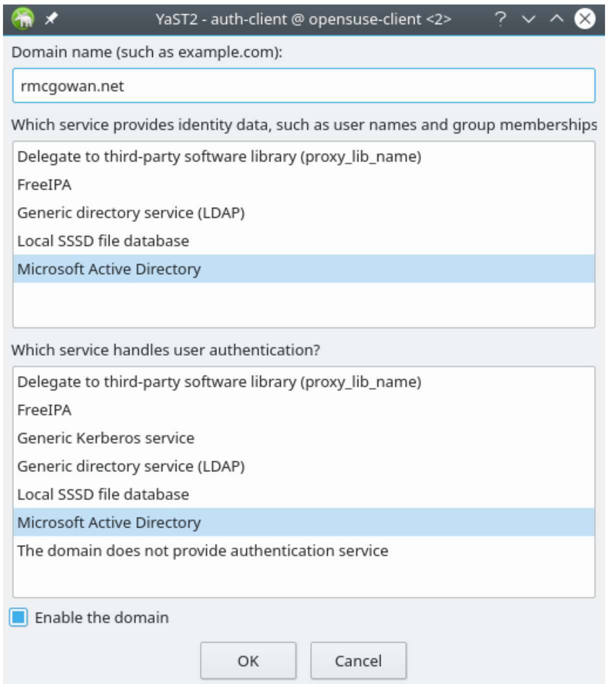


Figure 12: The first step of the domain join process.

In the second part of the wizard, no criteria were required, however “Cache credentials for offline use” was checked, in keeping with the default behaviour of the other Linux distributions, meaning that if the domain controller were to become unavailable, users would still be able to log in if they had done so previously on the same client.

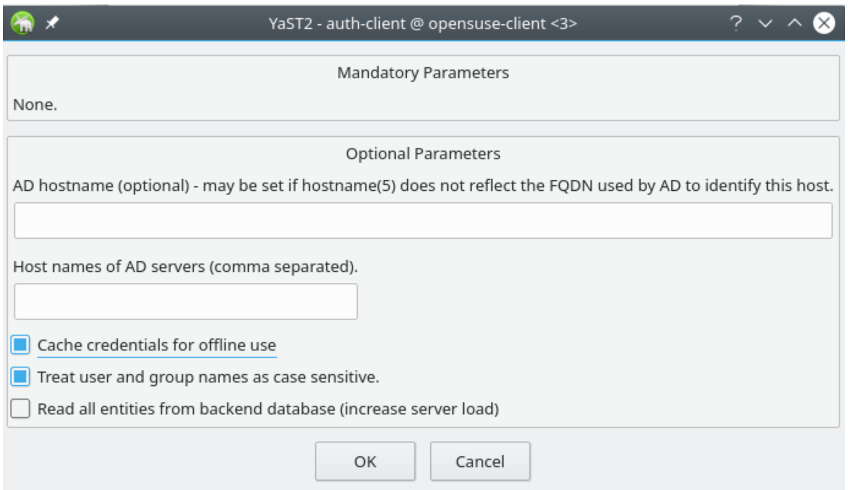


Figure 13: The second step of the domain join process.

The third prompt required the credentials of a user in the domain with the privileges to enrol a system in the domain, after having found the domain controller in the network via a DNS lookup of the domain name of the Active Directory domain. In this case, the server’s Administrator account was used. The “Overwrite Samba configuration to work with this AD” was also checked to ensure that no previous Samba configuration on the client system would interfere with the domain join process.

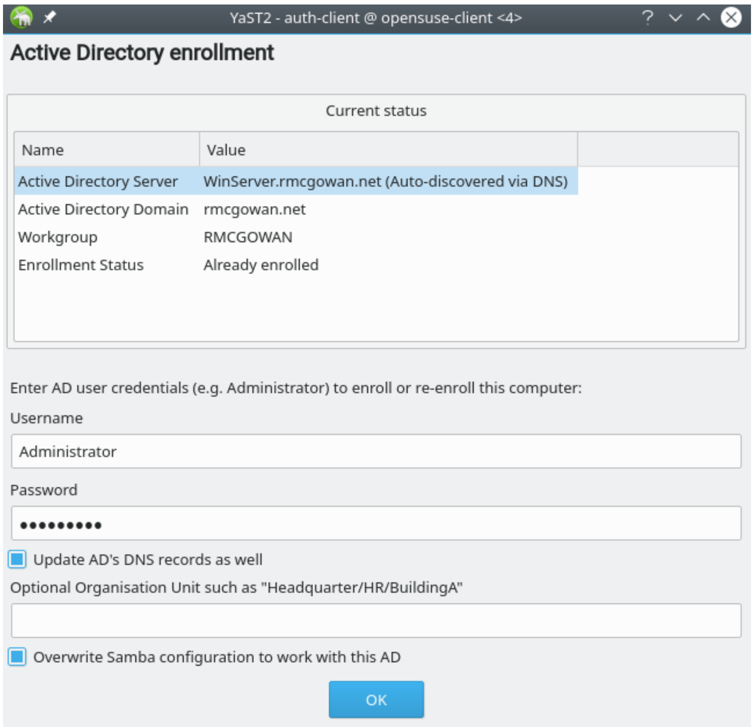


Figure 14: The third step of the domain join process, requiring user credentials of a domain user with the privileges to join the system to the domain.

With the credentials verified, the openSUSE client was joined to the rmcgowan.net domain.

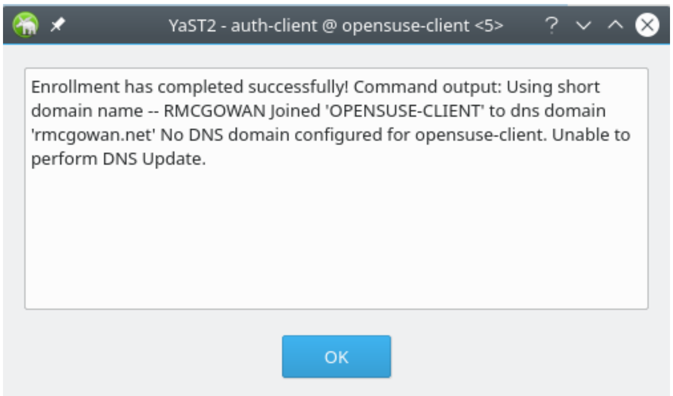


Figure 15: Confirmation of the client being successfully enrolled in the rmcgowan.net domain.

With the openSUSE client now joined to the domain, the User Logon Management module’s configuration interface is updated to reflect this, including the ability to modify and add SSSD options, rather than having to manually edit the /etc/sssd/sssd.conf file, as was required in CentOS and Ubuntu. Fully qualified names when logging in as a domain user are not required by default on openSUSE Leap 15, in contrast with Ubuntu and CentOS. However, this functionality can be enabled if desired by adding the option through the “Extended options” interface, accessible from the User Logon Management configuration interface.

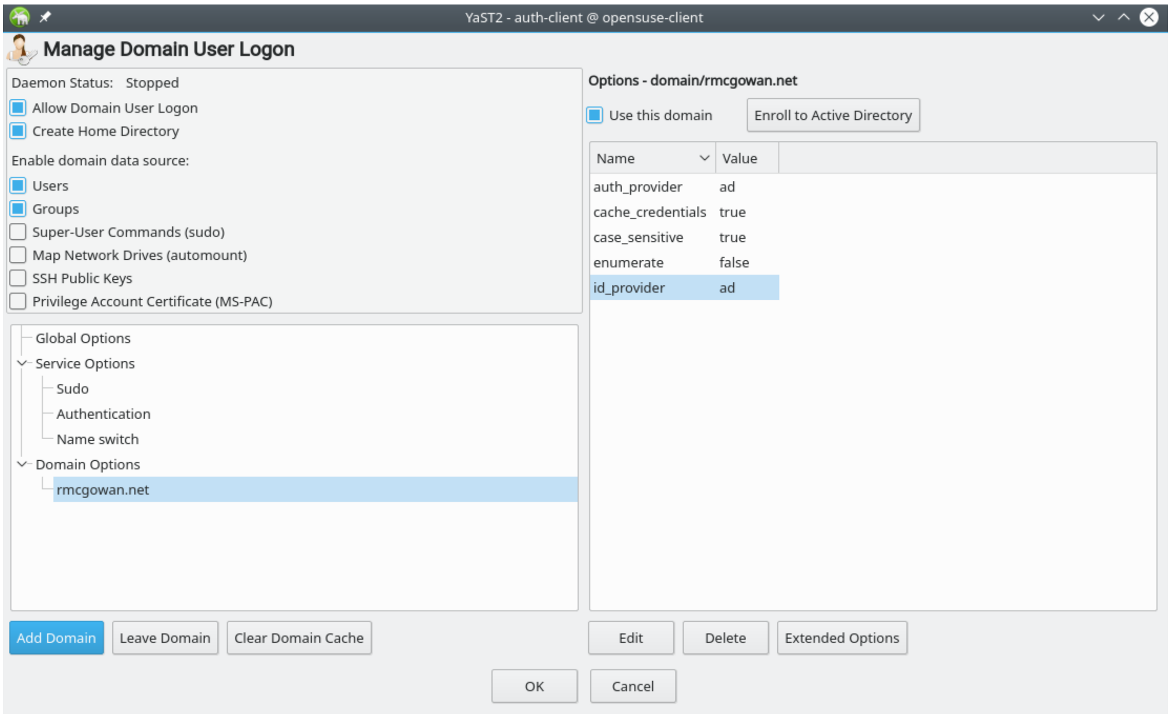


Figure 16: The User Logon Management module configuration interface updated with options for the newly joined domain.

A graphical domain login was then attempted via the SDDM login screen (the default for the KDE interface on openSUSE Leap 15), which initially was unsuccessful, resulting in a black screen and the system hanging. However, in a recent system update, this issue seems to have been rectified, and graphical logins through SSSD are now functional.

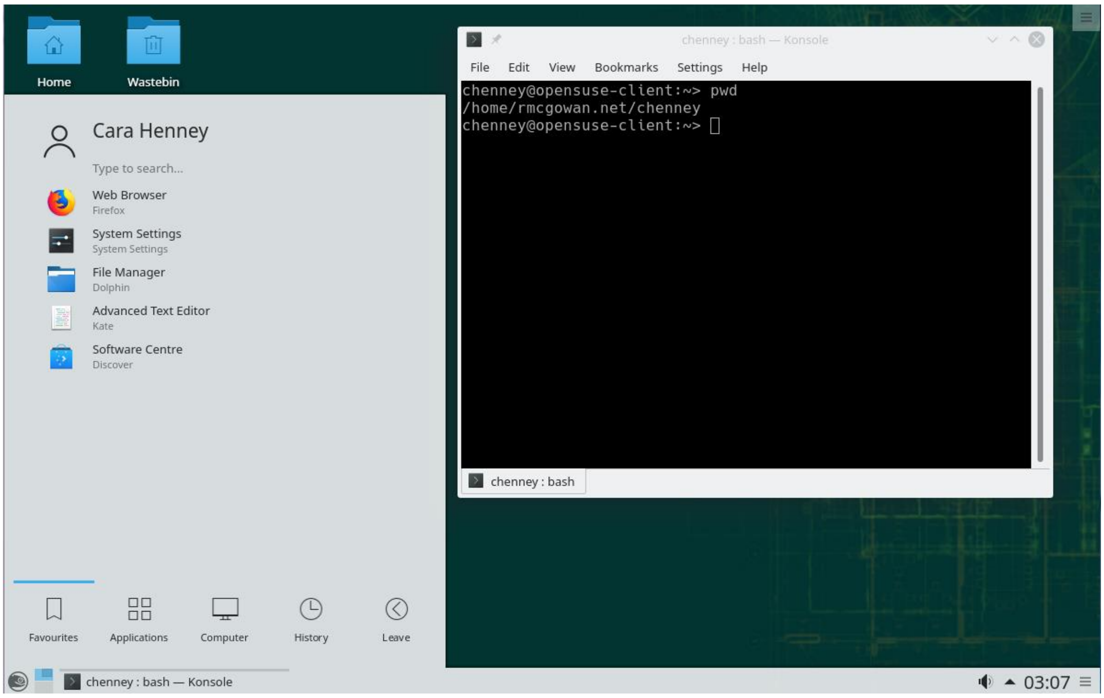


Figure 17: openSUSE Leap client desktop showing a successful login as the chenney domain user.

In order to access the SMB network share created on Windows Server graphically, the address bar in Dolphin (openSUSE's default file manager) was used by entering the path *smb://172.16.0.1/Shared.* As the domain user already has access to this folder, no password was required to access it. No further attempts were made to have this folder automount, other than adding it to the list of *Places* in Dolphin, which when used, automatically mounts the share.

4.2.2.4 The Network after the Enrolment of Linux Clients to the Domain

With the Ubuntu, CentOS and openSUSE Leap clients joined to the domain, the Active Directory Users and Computers console is updated to reflect this, with all three clients now showing as individual computer objects in this console.

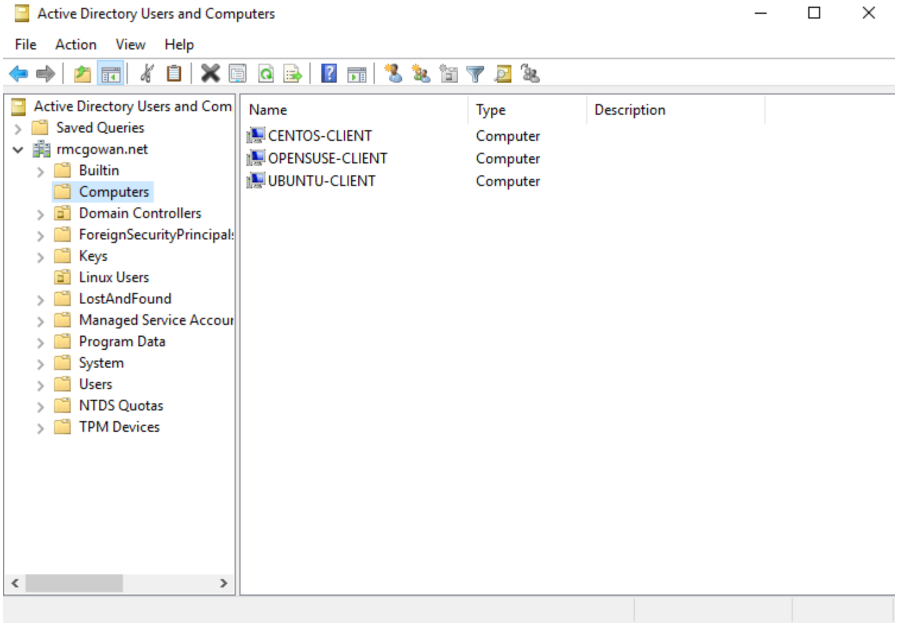


Figure 18: The Active Directory Users and Computers console reflecting the enrolment of all three clients to the domain.

4.2.3 Linux Server with Windows Clients Network

In this environment, a Linux server was configured to serve three Windows 10 clients; providing routing functionality and acting as an Active Directory compliant domain controller. Much like the previous two Windows Server servers, the Linux server was configured with the same IP addresses, services equivalent to that of the roles configured on Windows Server, domain users and shared folders.

4.2.3.1 Zentyal Server 6.0

As mentioned in chapter 3, Zentyal Server 6.0's server functions are generally configured by a custom web interface, accessible on this network by navigating to *https://172.16.0.1:8443* in a web browser. To modify settings on the server from this interface, you must log in with either a domain account or local account that has privileges to make configuration changes to the system.

When Zentyal Server is first installed, the user is presented with a web browser with the Zentyal web interface loaded. Zentyal Server provides a first-run setup wizard that allows an administrator to configure the server with the required roles. For the purposes of this network, the *Domain Controller and File Sharing* and *Firewall* roles were selected, with Zentyal opting to install the *DNS Server* role as a dependency.

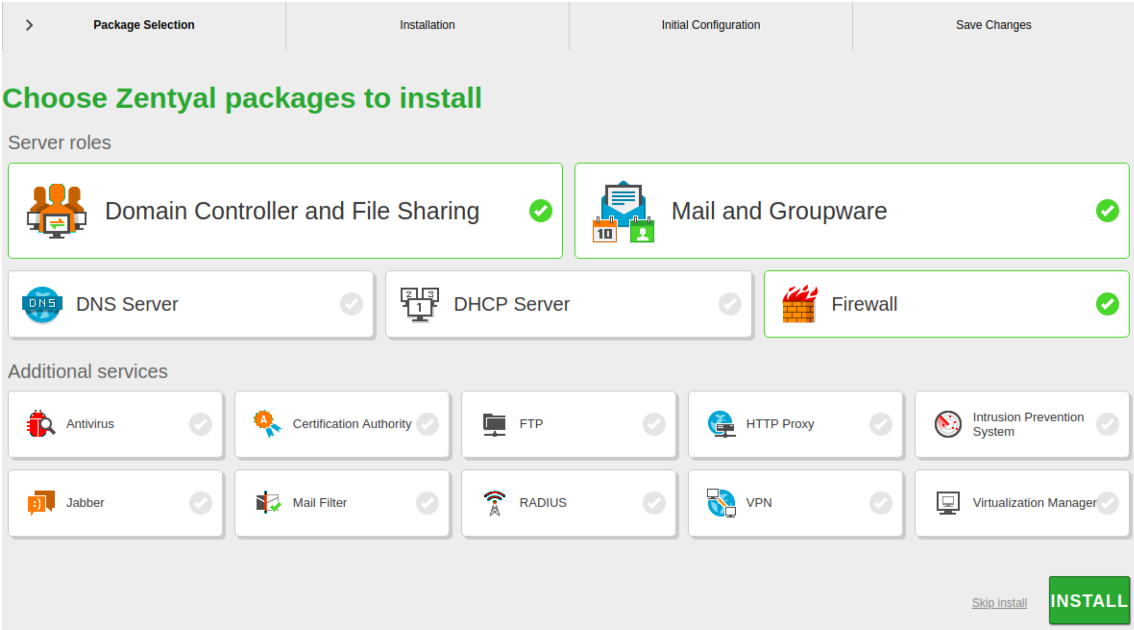


Figure 19: The Zentyal Server 6.0 first-run wizard asking what roles are to be configured on the server (Zentyal, n.d.).

Once these roles have been installed by the wizard, the user is then presented with the network interface configuration, where IP addresses and the interface “type” can be set. On the server in this environment, eth0 was set to External with the IP 192.168.0.10/24, and eth1 was set to Internal with the IP 172.16.0.1/24.

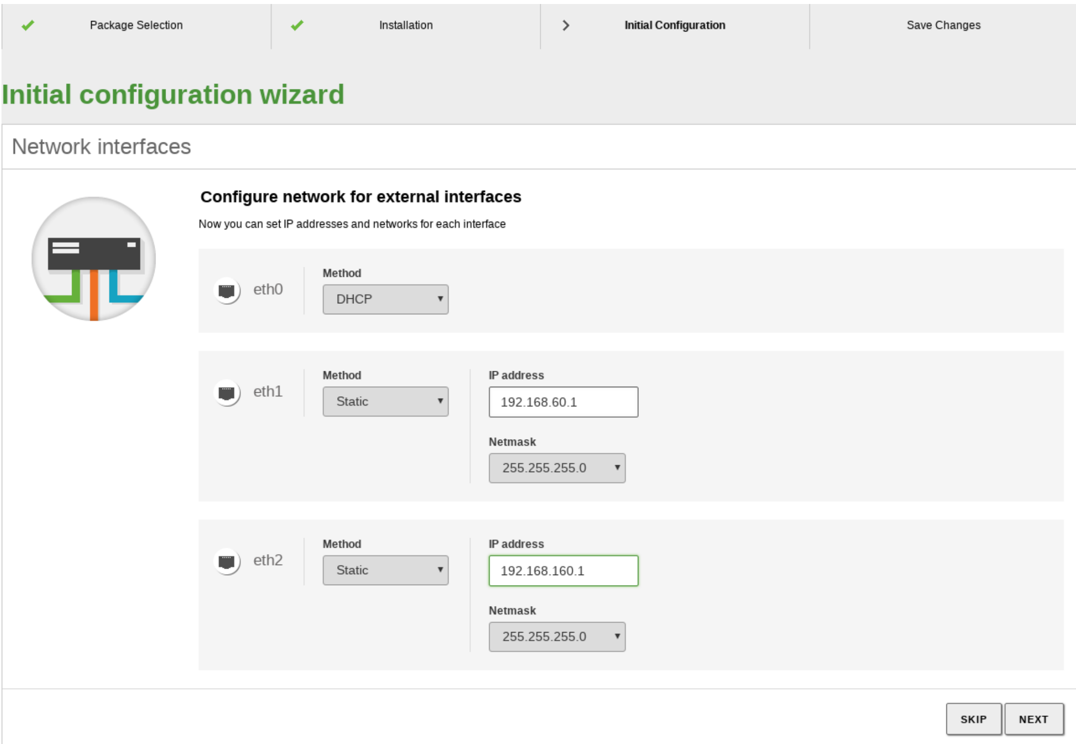


Figure 20: The Zentyal Server 6.0 first-run wizard IP configuration step for all network interfaces on the server. (Zentyal, n.d.).

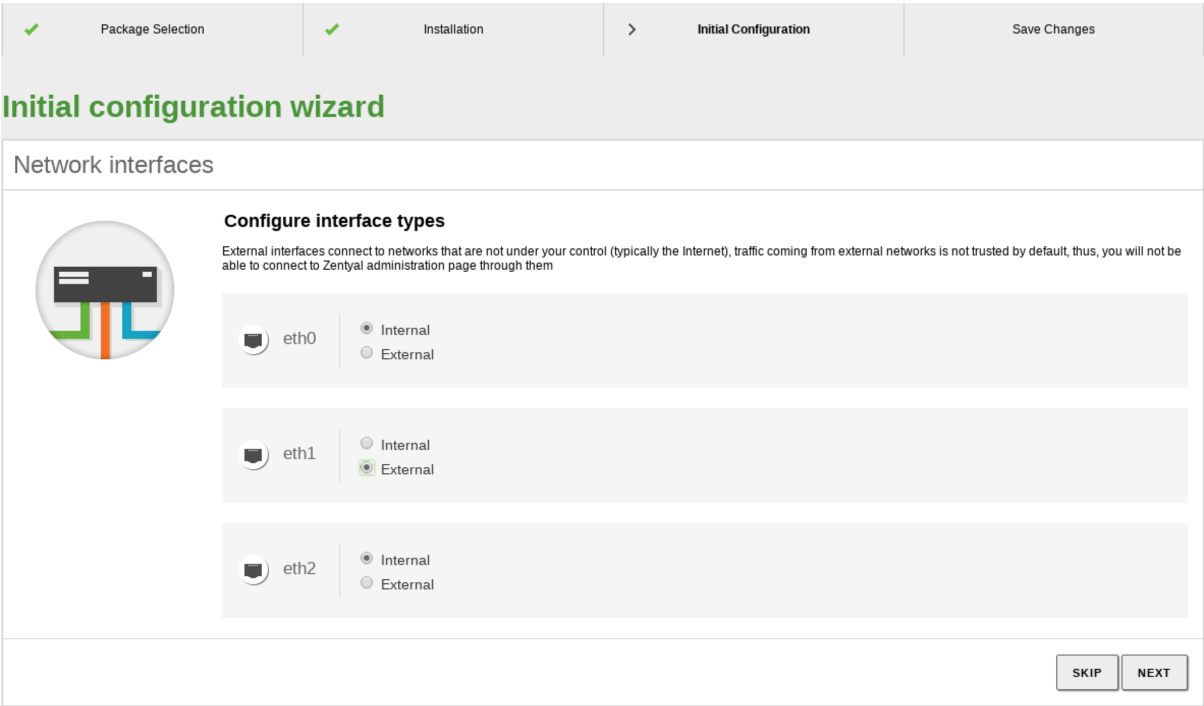


Figure 21: The Zentyal Server 6.0 first-run wizard interface type configuration step for all network interfaces on the server. (Zentyal, n.d.).

With the network interfaces configured, the wizard moves onto configuring the basic parameters of the domain controller; asking if the server is to be a *Standalone*, or primary, domain controller, or an *Additional*, or backup, domain controller, as well as the domain name to be used for the domain. In this environment, the server was configured to be a “Standalone” server, and the domain name was set to rmcgowanlin.net.

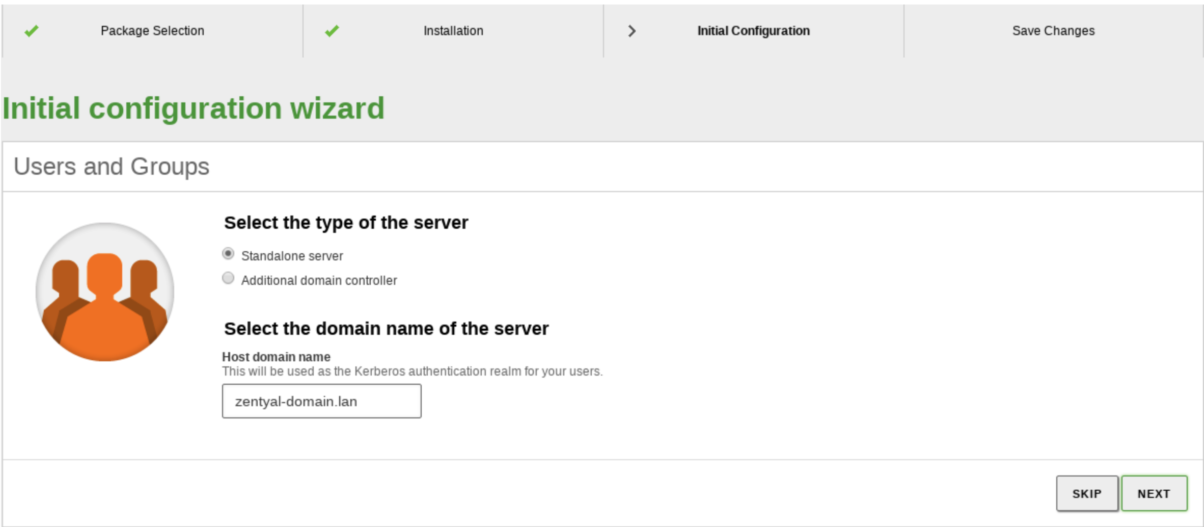


Figure 22: The Zentyal Server 6.0 first-run wizard configuration step for the domain controller role. (Zentyal, n.d.).

With all the required settings specified in the first-run wizard, the wizard will then take the time to set up and start running the required system services. With this complete, the user will be presented with the *Dashboard,* which shows an overview of the status of the system, what services are currently running and network interface statistics.

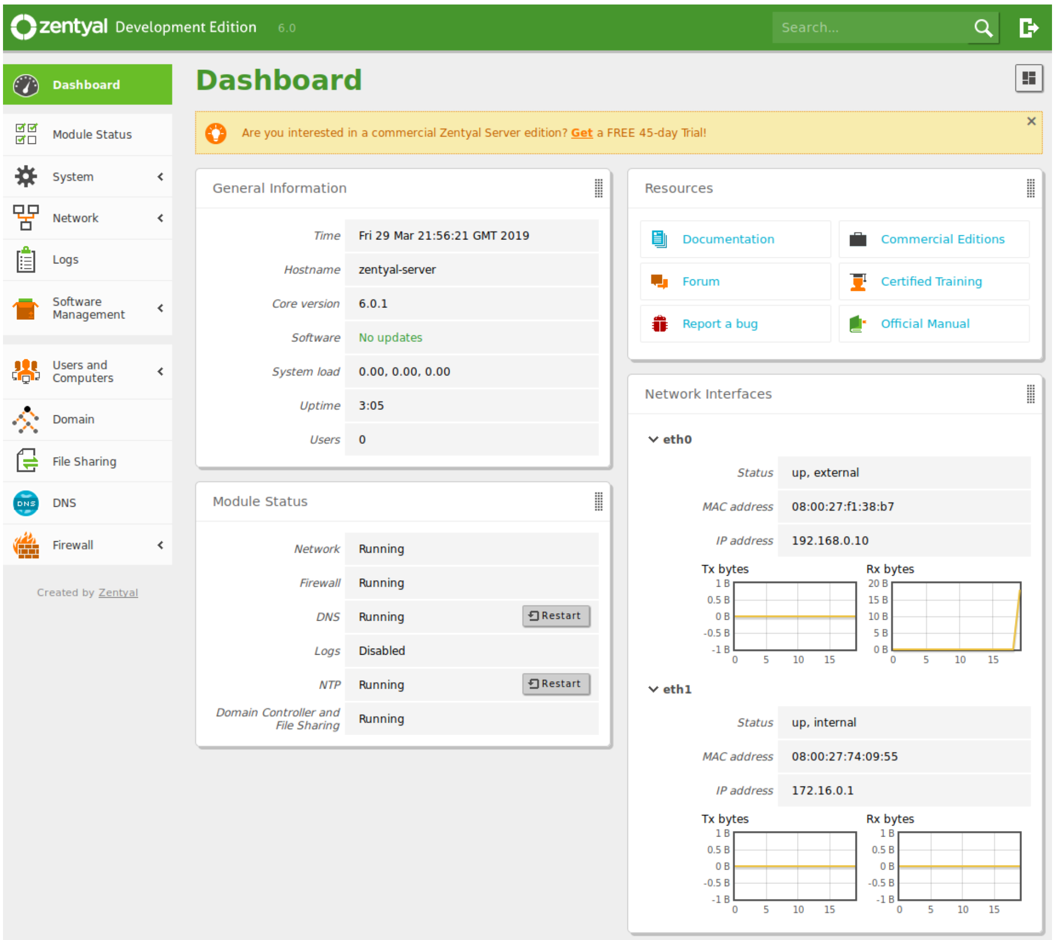


Figure 23: The Zentyal Server 6.0 dashboard after initial setup.

In order to verify settings for the domain controller service, the *Domain* settings interface was accessed. From here, roaming profiles were enabled, and a Home drive to be mounted as H: on Windows was enabled, meaning all users in the domain had an automatically mounted personal shared folder upon login.

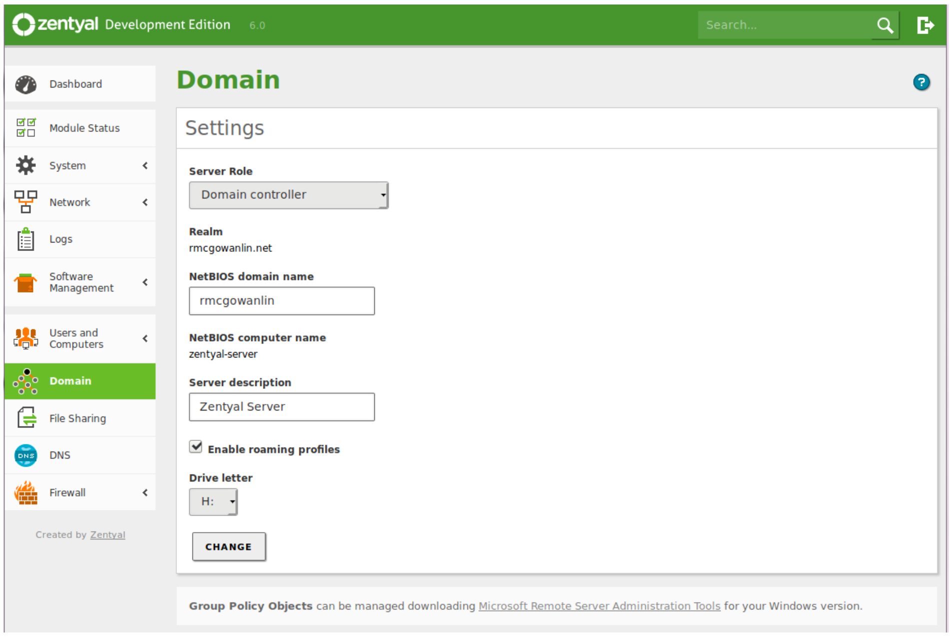


Figure 24: The Zentyal Server 6.0 Domain settings interface.

The Zentyal Server web interface provides an equivalent to the Active Directory Users and Computers console found on Windows Server, providing much of the functionality found in the Windows Server equivalent. Much like on Windows Server on the previous networks, an Organisational Unit (OU) was created named “Windows Users”, where two domain users were created. An Administrator account was also created and added to the *Domain Admins* group, to function like the default Administrator account found on Windows Server to be used during the domain join process on the clients.

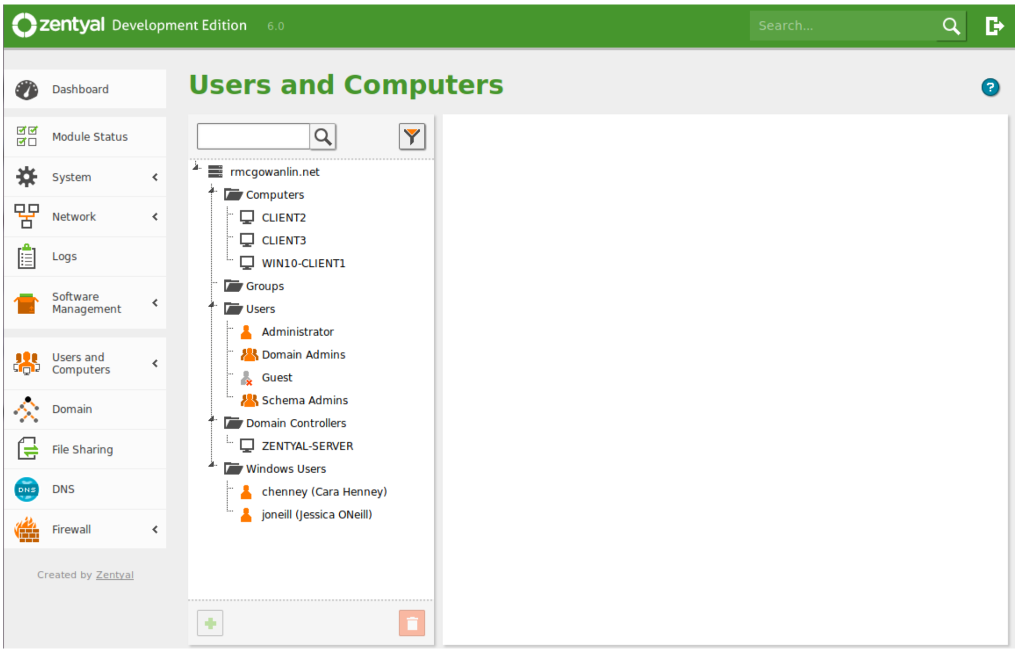


Figure 25: The Zentyal Server 6.0 Users and Computers configuration interface, provided as an equivalent to the Active Directory Users and Computers console found on Windows Server.

4.2.3.2 Windows 10 Clients

With the Linux-based domain controller now running in this network, the Windows 10 clients were joined to the rmcgowanlin.net domain. This was accomplished using the same process the Windows 10 clients were previously joined to the rmcgowanwin.net domain in the Homogeneous network; through the Computer Name/Domain Changes dialogue in System Properties. With the clients now joined, they were now listed as members of the domain in Zentyal Server’s Users and Computers configuration interface, as shown in Figure 25. This also resembles the way in which member clients of the domain would be shown in the Active Directory Users and Computers console on Windows Server.

Graphical logins were then tested on the Windows 10 clients with one of the users shown in Figure 25, with success. As configured in Zentyal Server, domain users had an automatically mounted network drive, H:, accessible in Windows Explorer.

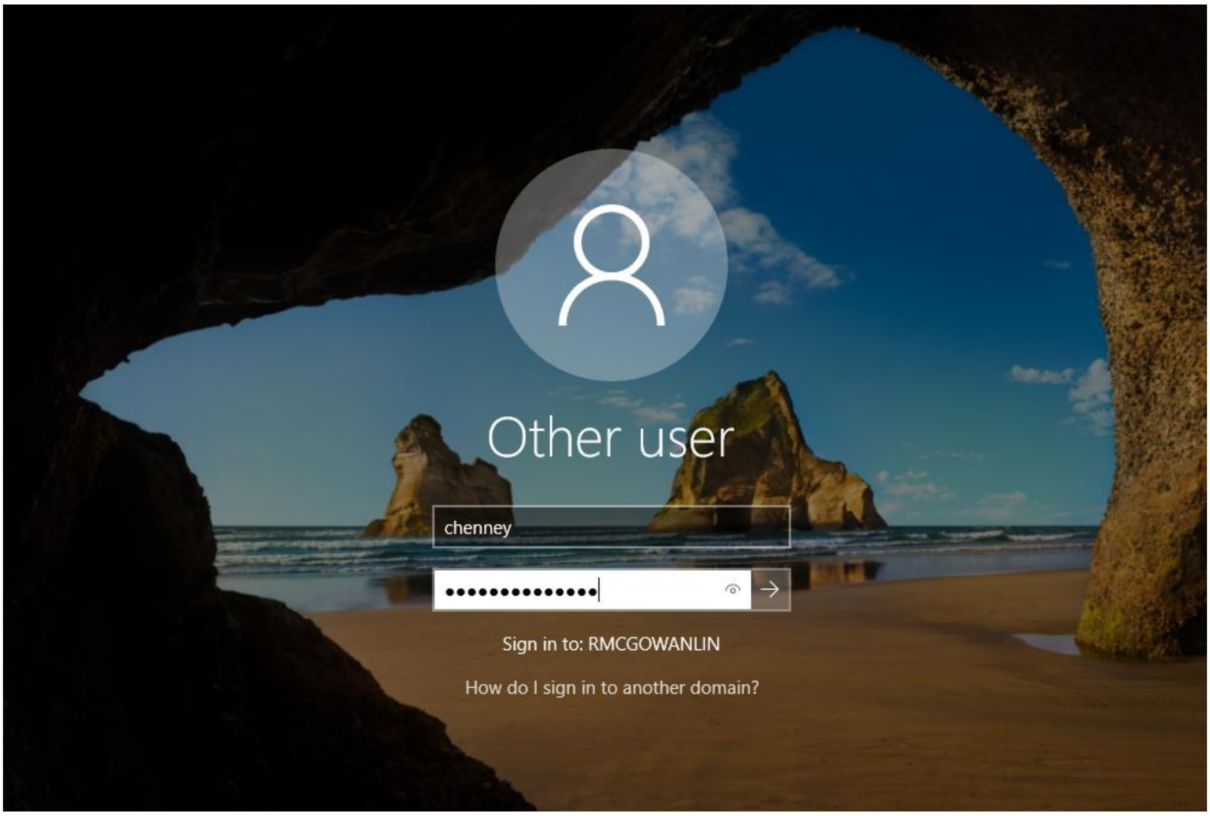


Figure 26: A Windows 10 Client login screen showing the required credentials for a domain login in the rmcgowanlin.net domain, authenticating against the Zentyal Server domain controller.

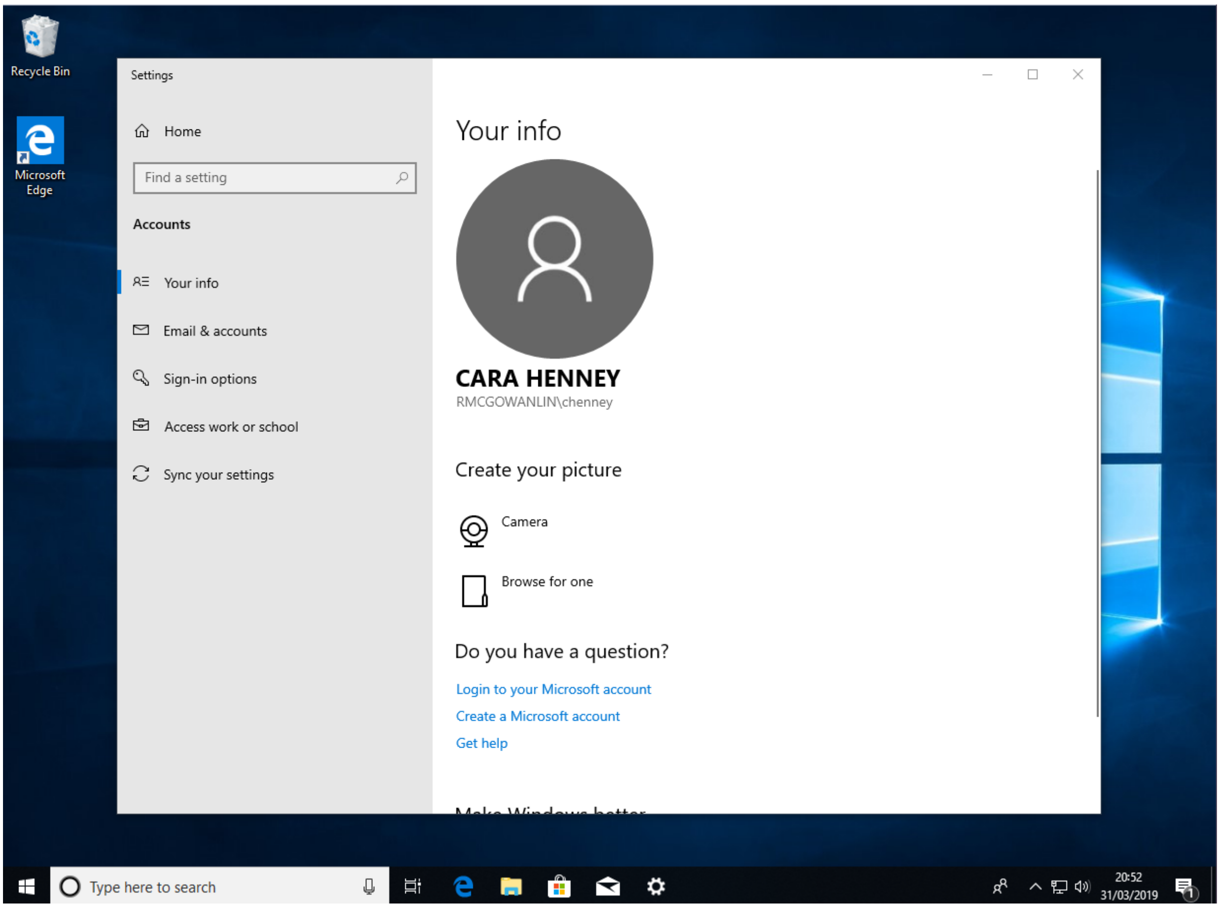


Figure 27: A Windows 10 Client showing the successful domain login of the user chenney in the rmcgowanlin.net domain.

4.2.4 Fully Heterogeneous Networks

4.2.4.1 Windows Server with Heterogeneous Clients

In this environment, a Windows 10 client was added to the existing Windows Server with Linux Clients network. This client was set up with an IP address of 172.16.0.5/24 and joined to the existing rmcgowan.net domain. With the Windows client joined to the domain, it was listed alongside the existing Linux clients in the Active Directory Users and Computers console on Windows Server.

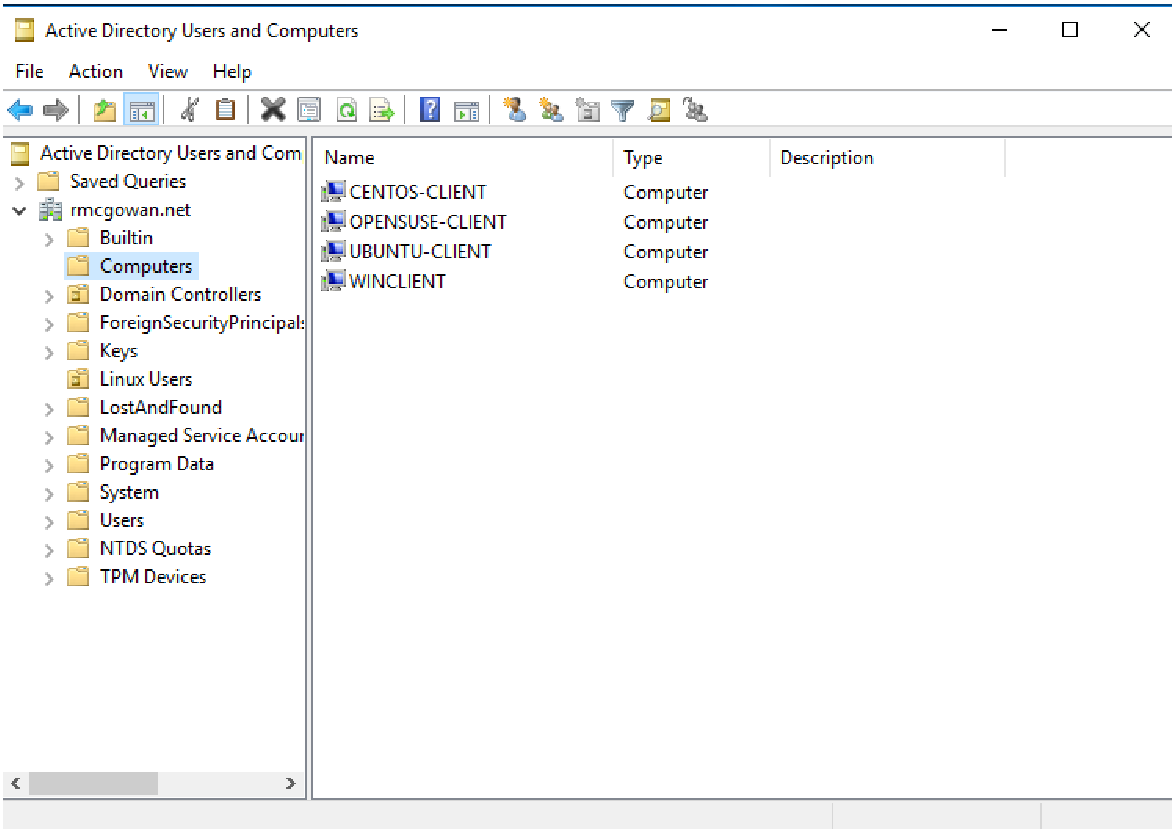


Figure 28: The Active Directory Users and Computers console on Windows Server showing the new Windows Client joined to the domain alongside the existing Linux clients.

A domain login was then attempted on the Windows 10 client with a domain user from the Linux Users OU, with success, as shown in figure 30.

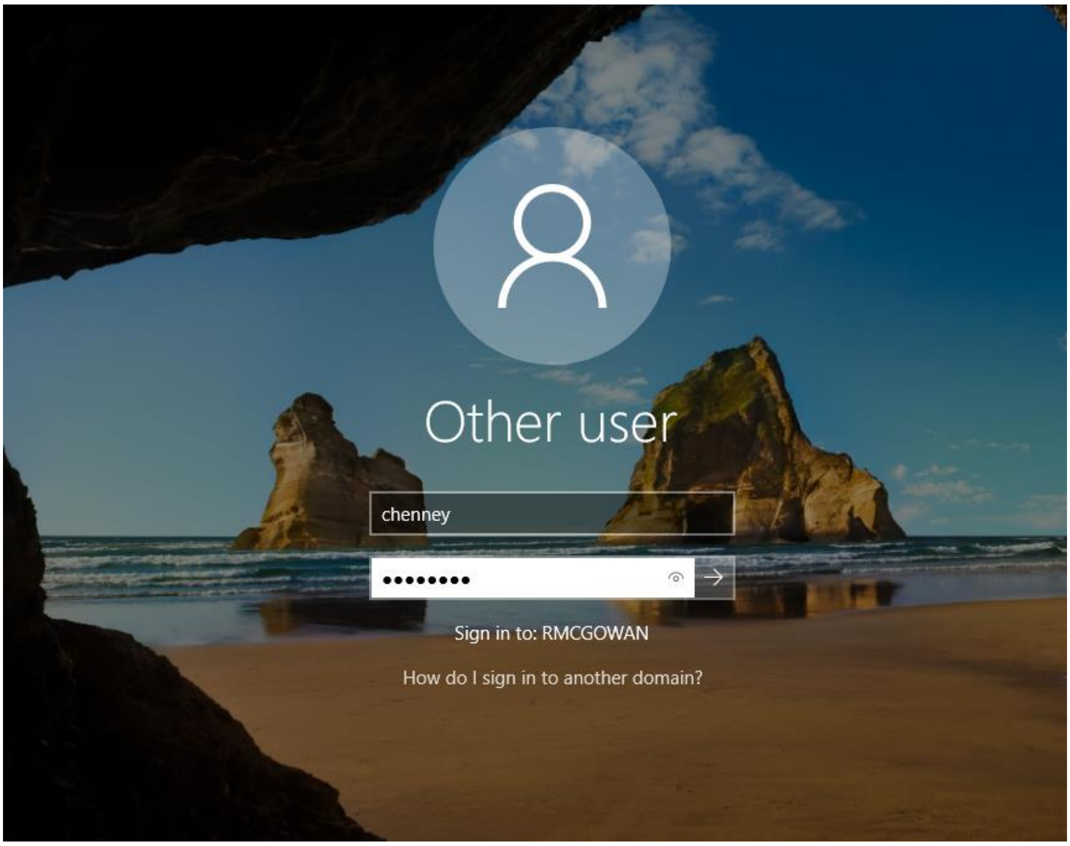


Figure 29: The Windows 10 client login screen showing the required credentials to log in as the domain user chenney in the rmcgowan.net heterogeneous domain.

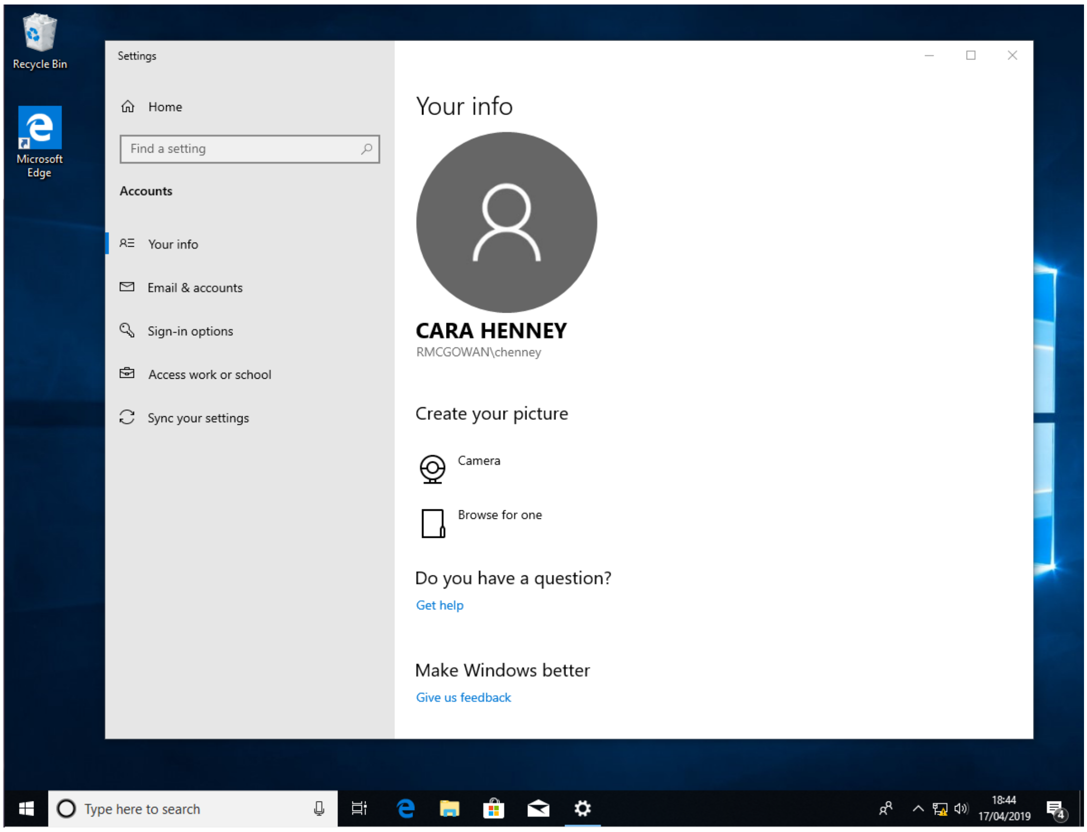


Figure 30: The Windows 10 client showing the successful login of the domain user chenney in the rmcgowan.net heterogeneous domain.

In order to access the SMB share \\WINSERVER\Shared, configured on Windows Server that the existing Linux clients all had access to, a network drive was mapped to drive Z:, which remained accessible upon further logins.

4.2.4.2 Linux Server with Heterogeneous Clients

In this environment, a single Linux client (namely Ubuntu 18.04 LTS) was added to the existing Linux Server with Windows clients network. This client was set up with an IP address of 172.16.0.5/24 and joined to the existing rmcgowanlin.net domain using the methods detailed in section 4.2.2.1. Initially when joining the Ubuntu client to the domain, the Zentyal Server domain controller would not allow the client to join the domain, citing that the Administrator domain user had insufficient privileges to join the client to the domain. In order to overcome this issue, the option `rdns = false` had to be inserted into the `/etc/krb5.conf` Kerberos configuration file on the client, disabling Reverse DNS resolution. With the Ubuntu client joined to the domain, it was listed alongside the existing Windows clients in Zentyal Server's Users and Computers configuration interface.

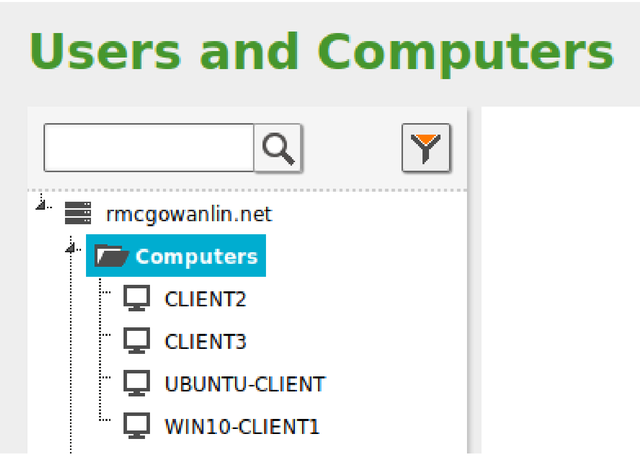


Figure 31: The Zentyal Server Users and Computers configuration interface showing the Ubuntu client joined to the domain alongside the existing Windows clients.

A domain login was then attempted on the Ubuntu client with a domain user from the Windows Users OU, with success, as shown in figure 32. During the first-time login of a domain user, PAM is automatically configured to create a local home directory on the system, which, for the chenney user is shown in figure 32 with the path /home/chenney@rmcgowanlin.net.

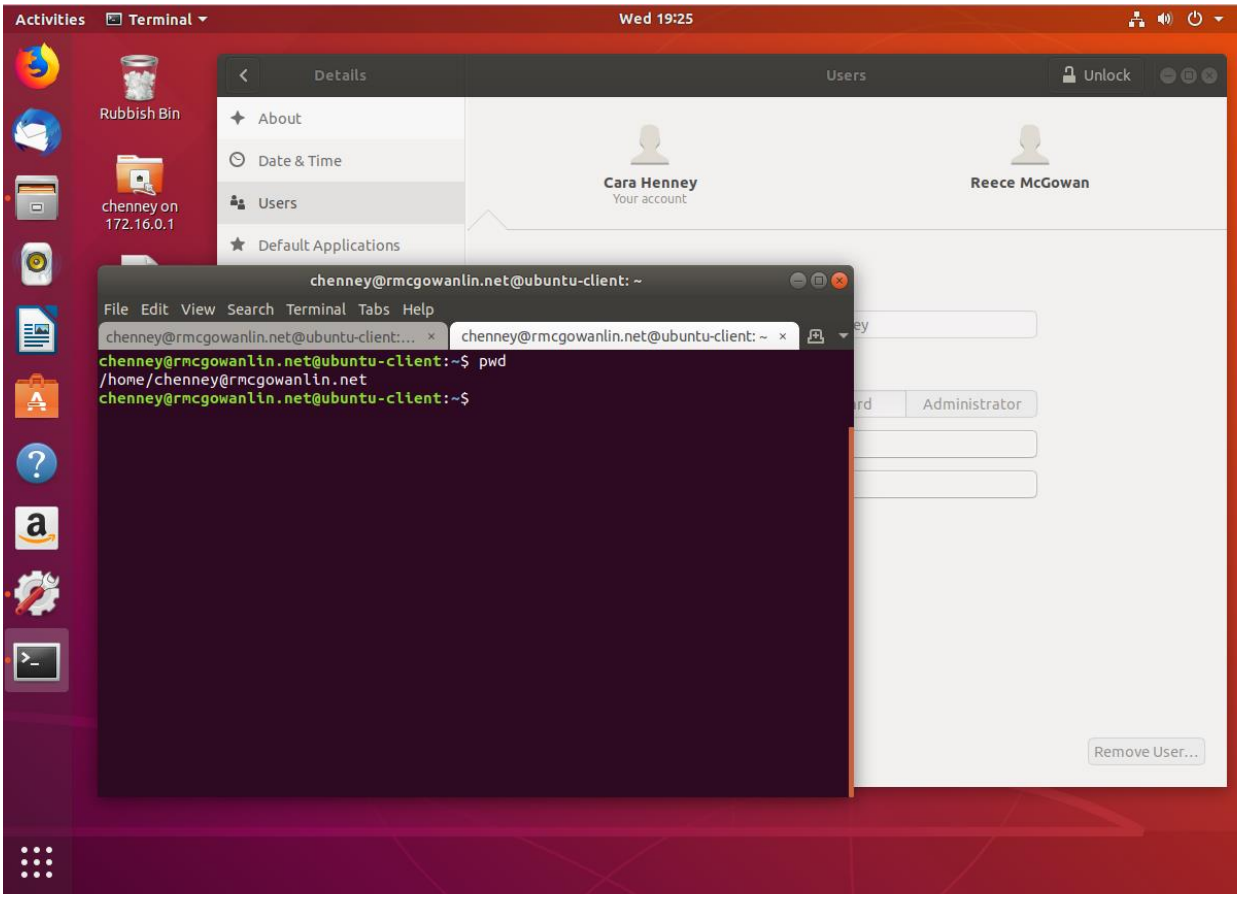


Figure 32: The Ubuntu 18.04 LTS client showing the successful domain login of the user chenney in the rmcgowanlin.net domain.

Despite Zentyal Server being configured to mount a personal network shared folder for domain users upon login, this did not function on Ubuntu. Instead, the domain user chenney's personal network shared folder had to be accessed via the *Connect to Server* option in the Nautilus file manager with the path *smb://172.16.0.1/chenney*. This share was bookmarked in Nautilus so it could be accessed in the future.

Chapter 5: Network Performance Statistics

5.1 Windows Homogeneous Network – Baseline Results

5.1.1 Active Directory Domain Login Times

In order to assess native Active Directory performance, login times on the Windows clients authenticating against a Windows server were measured. The results shown are measured from clicking the "submit" button on the login screen to the desktop appearing. The benchmark was conducted three times; once on each client in the network.

Table 1

Client System	***Time (s)***
Client 1	4.02
Client 2	3.59
Client 3	7.14
Average time	4.92

5.1.2 SMB3 Large File Transfer

In order to assess native SMB file transfer performance, several file transfers were conducted between the clients and server. The first benchmark involved transferring a large file (a 1.8GB Ubuntu ISO file named *ubuntu.iso*) between the clients and server. The large file was placed in the share \\WINHOMSERVER\Shared (or drive Z: on the client systems) and transfers from this share to the client were measured first. In order to conduct the transfer and obtain an average result in each run, the robocopy tool in Powershell was used, as shown in figure 28, with the command: `Robocopy.exe \\WINHOMSERVER\Shared C:\Users\chenney\Desktop ubuntu.iso.`

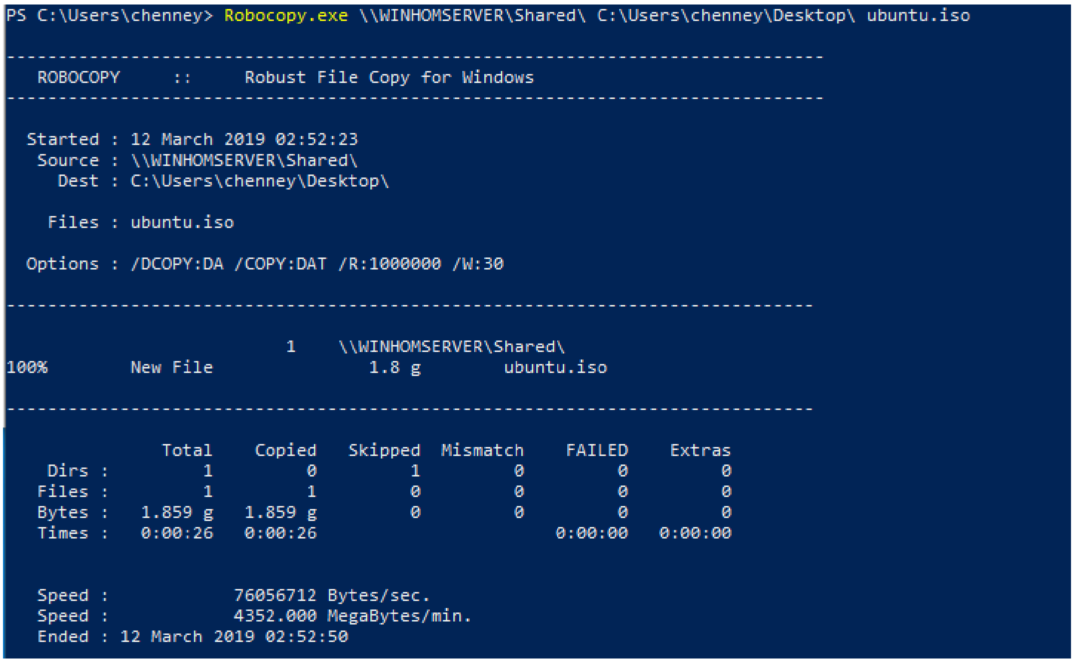


Figure 33: An example of the use of the robocopy Powershell tool used in the benchmarks on this network.

Table 2

Transfer (Server>Client)	***Speed (MB/s)***
1	78.10
2	76.74
3	76.06
Average	76.97

The file transferred to the client was then renamed to *ubuntu2.iso* and, using robocopy, was transferred from the client to the server, using the command: `Robocopy.exe C:\Users\chenney\Desktop \\WINHOMSERVER\Shared ubuntu2.iso.`

Table 3

Transfer (Client>Server)	*Speed (MB/s)*
1	70.32
2	72.23
3	70.97
Average	71.17

5.1.3 SMB3 Small Files Transfer

The second SMB3 benchmark involved transferring a collection of assorted documents and images of varying sizes; from as small as one kilobyte in size to several megabytes, totalling a folder size of 135MB. Much like the large file, this folder, named *documents*, was placed in the share \\WINHOMSERVER\Shared and transfers from this share to the client were measured first. Just like the large file, the folder was transferred using the robocopy Powershell tool, which was able to provide an average transfer rate in each transfer of all the files within the folder together. However, since a directory was being copied and not a single file, the /MIR robocopy switch was required, resulting in the command: `Robocopy.exe \\WINHOMSERVER\Shared\documents C:\Users\chenney\Desktop\documents /MIR.`

Table 4

Transfer (Server>Client)	*Speed (MB/s)*
1	47.36
2	44.09
3	49.25
Average	46.90

The folder transferred to the client was then renamed to *documents2* and transferred using robocopy from the client to the server with the command: `Robocopy.exe C:\Users\chenney\Desktop\documents2 \\WINHOMSERVER\Shared\documents2 /MIR.`

Table 5

Transfer (Client>Server)	*Speed (MB/s)*
1	16.18
2	13.87
3	15.15
Average	15.07

5.2 Windows Server with Linux Clients Benchmark Results

5.2.1 Active Directory Login Times

In order to assess each Linux distribution's configuration and implementation of technologies allowing them to authenticate against Active Directory, login times on each distribution were measured. The results shown are measured from clicking the "submit" button on the login screen to the desktop appearing. The benchmark was conducted three times on each distribution and an average taken for each distribution.

5.2.1.1 Ubuntu 18.04 LTS

Table 6

Login	***Time (s)***
1	7.43
2	5.48
3	5.14
Average	6.02

5.2.1.2 CentOS 7.6

Table 7

Login	***Time (s)***
1	11.24
2	10.17
3	9.92
Average	10.44

5.2.1.3 openSUSE Leap 15

Table 8

Login	***Time (s)***
1	6.89
2	6.69
3	6.73
Average	6.77

5.2.2 SMB3 Large File Transfer

In order to assess the performance of Samba on the Linux clients interacting with native SMB on Windows Server, the same file transfers conducted on the Windows homogeneous network were conducted between the Linux distributions and Windows Server. The same large file (1.8GB Ubuntu ISO file) was used in this benchmark, stored on the share \\WINSERVER\Shared. As an alternative to robocopy used on Windows, the smbclient command line tool was used which, much like robocopy, provides an average transfer rate at the end of the file transfer. In order to transfer the file, the following smbclient command was used: `smbclient -m smb3 //winserver/Shared -c “get ubuntu.iso /home/chenney/Desktop/ubuntu.iso”`. This command was used on every Linux distribution for every server to client transfer.

5.2.2.1 Ubuntu 18.04 LTS

Table 9

Transfer (Server>Client)	***Speed (MB/s)***
1	77.67
2	97.12
3	96.09
Average	90.29

The file transferred to the client was renamed to *ubuntu2.iso* and transferred using smbclient back to the server. In order to transfer the file, the following smbclient command was used: `smbclient -m smb3 //winserver/Shared -c “put /home/chenney/Desktop/ubuntu2.iso ubuntu2.iso”`. This command was also used on every Linux distribution for every client to server transfer.

Table 10

Transfer (Client>Server)	***Speed (MB/s)***
1	107.01
2	108.17
3	109.48
Average	108.22

5.2.2.2 CentOS 7.6

Table 11

Transfer (Server>Client)	***Speed (MB/s)***
1	42.19
2	45.24
3	37.66
Average	41.70

Table 12

Transfer (Client>Server)	***Speed (MB/s)***
1	128.03
2	137.14
3	132.25
Average	132.47

5.2.2.3 openSUSE Leap 15

Table 13

Transfer (Server>Client)	*Speed (MB/s)*
1	78.82
2	106.78
3	107.13
Average	97.58

Table 14

Transfer (Client>Server)	*Speed (MB/s)*
1	108.05
2	110.85
3	109.31
Average	109.40

5.2.3 SMB3 Small Files Transfer

The same collection of documents and images of varying sizes totalling 135MB was used in this benchmark as used previously. The folder named *documents* was placed in the share \\WINSERVER\Shared and transfers from this share to the clients was measured first. Smbclient was used to transfer the folder, however the command had to be amended slightly in order to transfer the folder including all files and subdirectories, resulting in the command: `smbclient -m smb3 //winserver/Shared -c “recursive; prompt; mget documents /home/chenney/Desktop/documents”`. This command was used on all the Linux distributions for transferring the folder from the server to the client.

5.2.3.1 Ubuntu 18.04 LTS

Table 15

Transfer (Server>Client)	*Speed (MB/s)*
1	61.93
2	59.96
3	61.51
Average	61.13

The folder transferred to the client was renamed to *documents2* and transferred back to the server using smbclient. The following smbclient was used to achieve this: `smbclient -m smb3 //winserver/Shared -c “recursive; prompt; mput /home/chenney/Desktop/documents2 documents2”`. This command was used on all the Linux distributions for transferring the folder from the client to the server.

Table 16

Transfer (Client>Server)	*Speed (MB/s)*
1	52.15
2	52.07
3	50.69
Average	51.64

5.2.3.2 CentOS 7.6

Table 17

Transfer (Server>Client)	*Speed (MB/s)*
1	22.46
2	27.45
3	26.88
Average	25.60

Table 18

Transfer (Client>Server)	*Speed (MB/s)*
1	41.66
2	42.98
3	43.98
Average	42.87

5.2.3.3 openSUSE Leap 15

Table 19

Transfer (Server>Client)	*Speed (MB/s)*
1	41.44
2	62.64
3	63.53
Average	55.87

Table 20

Transfer (Client>Server)	*Speed (MB/s)*
1	46.04
2	42.82
3	46.39
Average	45.08

5.3 Linux Server with Windows Clients Benchmark Results

5.3.1 Zentyal Domain Controller (Samba) Login Times

In order to assess Zentyal Server's claim of "native compatibility with Microsoft Active Directory" (Zentyal, n.d.) and the performance of their implementation of this, login times from the Windows clients were measured. The results shown are measured from clicking the "submit" button on the login screen to the desktop appearing. The benchmark was conducted three times, once on each client system.

Table 21

Login	***Time (s)***
Client 1	9.67
Client 2	5.27
Client 3	4.16
Average	6.37

5.3.2 SMB3 Large File Transfer

In order to assess the performance of Samba on Zentyal Server interacting with native SMB on the Windows clients, the same file transfers conducted on the previous networks were conducted between the Windows clients and Zentyal Server. The same large file (1.8GB Ubuntu ISO file) named *ubuntu.iso* was used in this benchmark, with it being stored instead on the domain user's personal share, H: (or \\ZENTYAL-SERVER\chenney). The robocopy Powershell tool was used on the Windows clients to transfer in order to obtain an average transfer rate for each transfer, with the command: `Robocopy.exe \\zentyal-server \chenney C:\Users\chenney\Desktop ubuntu.iso.`

Table 22

Transfer (Server>Client)	***Speed (MB/s)***
Client 1	64.72
Client 2	90.81
Client 3	138.92
Average	98.15

The file transferred to the client was then renamed to *ubuntu2.iso* and transferred back to the client using robocopy with the command: `Robocopy.exe C:\Users\chenney\Desktop \\zentyal-server\chenney ubuntu2.iso.`

Table 23

Transfer (Client>Server)	***Speed (MB/s)***
Client 1	159.71
Client 2	215.81
Client 3	148.88
Average	174.80

5.3.3 SMB3 Small Files Transfer

The same collection of documents and images of varying sizes totalling 135MB was used in this benchmark as used previously. The folder named *documents* was placed in the domain user chenney's H: drive (or \\ZENTYAL-SERVER\chenney) and transfers from this share to the clients were measured first. The robocopy Powershell tool was used on the Windows clients to transfer the folder, with the /MIR switch to copy the entire directory structure, resulting in the command: `Robocopy.exe \\zentyal-server\chenney\documents C:\Users\chenney\Desktop\documents /MIR`.

Table 24

Transfer (Server>Client)	***Speed (MB/s)***
Client 1	36.65
Client 2	49.53
Client 3	51.17
Average	45.78

The folder transferred to the client was then renamed to *documents2* and transferred back to the server using robocopy, with the command: `Robocopy.exe C:\Users\chenney\Desktop\documents2 \\zentyal-server\chenney\documents2 /MIR`

Table 25

Transfer (Client>Server)	***Speed (MB/s)***
Client 1	41.41
Client 2	39.83
Client 3	64.55
Average	48.60

5.4 Fully Heterogeneous Networks

5.4.1 Windows Server with Heterogeneous Clients Network

5.4.1.1 Active Directory Login Times

In order to measure whether including Windows clients into a fully heterogeneous network would have any effect on Active Directory login times, the time to complete domain login attempts were measured. These results can be compared with those of the Linux clients in this network in section 5.2. The results shown are measured from clicking the “submit” button on the login screen to the desktop appearing. The benchmark was conducted three times, once on each client system.

Table 26

Login Attempt	***Time (s)***
1	3.70
2	3.40
3	3.45
Average	3.52

5.4.1.2 SMB3 Large File Transfer

In order to assess native SMB file transfer performance between Windows 10 and Windows Server in a fully heterogeneous network, the same file transfer benchmark as used previously was used, with the same 1.8GB Ubuntu ISO file named *ubuntu.iso* used for the large file transfers between the client and server. The large file was placed in the share \\WINSERVER\Shared (or drive Z: on the client system) and transfers from this share to the client were measured first. In order to conduct the transfer and obtain an average result in each run, the robocopy tool in Powershell was again used, with the command: `Robocopy.exe \\WINSERVER\Shared C:\Users\chenney\Desktop ubuntu.iso`.

Table 27

Transfer (Server>Client)	*Speed (MB/s)*
1	105.34
2	93.60
3	98.44
Average	99.13

The Ubuntu ISO file was then renamed to *ubuntu2.iso* and transferred back to the server using Robocopy with the command: `Robocopy.exe C:\Users\chenney\Desktop \\WINSERVER\Shared ubuntu2.iso`.

Table 28

Transfer (Client>Server)	*Speed (MB/s)*
1	117.65
2	125.77
3	162.13
Average	135.18

5.4.1.3 SMB3 Small Files Transfer

The same collection of documents and images of varying sizes totalling 135MB was used in this benchmark as used previously, with the folder *documents* placed in the \\WINSERVER\Shared shared folder (or drive Z: for the client system). The robocopy powershell tool was again used to facilitate the transfer with the command: `Robocopy.exe \\WINSERVER\Shared\documents C:\Users\chenney\Desktop\documents /MIR`.

Table 29

Transfer (Server>Client)	*Speed (MB/s)*
1	25.97
2	48.84
3	48.47
Average	41.09

The *documents* folder was then renamed to *documents2* and transferred back to the server using Robocopy with the command: `Robocopy.exe C:\Users\chenney\Desktop\documents2 \\WINSERVER\Shared\documents2 /MIR`.

Table 30

Transfer (Client>Server)	***Speed (MB/s)***
1	28.88
2	31.81
3	25.87
Average	28.85

5.4.2 Linux Server with Heterogeneous Clients Network

5.4.2.1 Zentyal Domain Controller (Samba) Login Times

In order to assess the performance of a Linux client authenticating against the Zentyal Server Samba-based domain controller in a network where Windows clients are already in use, the time to complete domain login attempts were measured. The results shown are measured from clicking the "submit" button on the login screen to the desktop appearing. The benchmark was conducted three times, once on each client system. These results can be compared with that of the Windows clients in this network as shown in section 5.3.1.

Login Attempt	***Time (s)***
1	5.42
2	4.46
3	4.33
Average	4.74

5.4.2.2 SMB3 Large File Transfer

In order to assess the performance of Samba on Zentyal Server interacting with Samba on the Linux client, as well as to compare this performance with that of native SMB on Windows in this network, the same file transfers conducted on the previous networks were conducted between the Linux client and Zentyal Server. The same large file (1.8GB Ubuntu ISO file) named *ubuntu.iso* was used in this benchmark, with it being stored instead on the domain user's personal share (\\ZENTYAL-SERVER\chenney). The smbclient tool was used to transfer the file from the server to the client, with the following command: `smbclient -m smb3 //winserver/Shared -c "get ubuntu.iso /home/chenney/Desktop/ubuntu.iso"`.

Transfer (Server>Client)	***Speed (MB/s)***
1	68.37
2	73.99
3	78.35
Average	73.57

The Ubuntu ISO file was then renamed to *ubuntu2.iso* and copied back to the server using smbclient with the following command: `smbclient -m smb3 //winserver/Shared -c “put /home/chenney/Desktop/ubuntu2.iso ubuntu2.iso”`.

Transfer (Client>Server)	***Speed (MB/s)***
1	160.02
2	158.65
3	156.98
Average	158.55

5.4.2.3 SMB Small Files Transfer

The same collection of documents and images of varying sizes totalling 135MB was used in this benchmark as used previously, with the folder *documents* placed in the domain user’s personal network share (\\ZENTYAL-SERVER\chenney). The smbclient tool was used to complete the transfer with the following command: `smbclient -m smb3 //zentyal-server/chenney -c “recursive; prompt; mget documents2 /home/chenney/Desktop/documents2”`.

Transfer (Server>Client)	***Speed (MB/s)***
1	54.11
2	78.45
3	80.94
Average	71.17

The *documents* folder was then renamed to *documents2* and transferred back to the server using smbclient with the command: `smbclient -m smb3 //zentyal-server/chenney -c “recursive; prompt; mput /home/chenney/Desktop/documents2 documents2”`.

Transfer (Client>Server)	***Speed (MB/s)***
1	127.13
2	128.67
3	133.16
Average	129.65

5.5 Licensing and Support Costs

5.5.1 Windows Server 2016

Horwitz (2016) details the licensing price for several editions of Windows Server 2016:

Table 26 adapted from Horwitz (2016).

License	***Version 2016 Pricing (USD)***
Windows Server Datacenter Edition	$770 per two cores
Windows Server Standard Edition	$110 per two cores

Microsoft (n.d.) further detail that all physical cores of a server must be licensed, with licenses sold in packs of two as detailed by Horwitz (2016), and all physical processors within a server must be licensed with a minimum of eight cores per license.

Further to this, Horwitz (2016) specifies that the annual cost of Microsoft's Software Assurance program for Server 2016 is 25% of the underlying license price. Microsoft (n.d.) explain that Software Assurance provides luxuries such as "24/7 Problem Resolution Support", however, this is only available through a Volume Licensing Agreement with Microsoft *(Microsoft, n.d.).*

5.4.2 Windows 10

Microsoft (n.d.) currently have Windows 10 Pro available for purchase for £219.99 (including VAT), with this license being usable on one system at any one time. Further information regarding Windows 10 Enterprise licensing costs and costs in a Volume Licensing Agreement are subject to evaluation from Microsoft according to the size of the company enquiring.

5.4.3 Ubuntu 18.04 LTS

While Ubuntu 18.04 LTS is available to download and use for free with no licensing requirements, Canonical (2018) offer commercial support through the "Ubuntu Advantage" program. This program offers luxuries such as phone and web ticket support and live patching of the kernel to minimize downtime. Canonical offer two tiers of support to the desktop variant of the distribution used in this research:

Table 27 adapted from Canonical (2018).

Desktop Support	***Cost per annum (USD)***
Standard	$150
Advanced	$300

Where the Standard tier offers phone and web ticket support from 8am-6pm on weekdays, with Advanced offering 24/7 support.

5.4.4 CentOS 7.6/Red Hat Enterprise Linux 7

CentOS 7.6 was used in this research as a binary-compatible free alternative to Red Hat Enterprise Linux 7 (RHEL). Due to CentOS being a free alternative to RHEL, no commercial support is offered directly for the distribution. Instead, using RHEL would offer the ability of obtaining commercial support for the system.

Red Hat (n.d.) offer two subscription types for their desktop, or "Workstation" variant of RHEL;

Table 28 adapted from Red Hat (n.d.).

Subscription Type	***Cost per annum (USD)***
Professional	$299
Enterprise	$449

Where a Professional subscription provides a license for RHEL Developer Workstation and support for an "unlimited number of incidents and a 2-business-day response service level agreement" (Red Hat, n.d.), and Enterprise providing the same license and support for the same number of incidents, but with a "4-business-hour response service level agreement" (Red Hat, n.d.).

5.4.5 openSUSE Leap 15/SUSE Linux Enterprise Desktop 15

openSUSE Leap 15 was used in this research as a binary-compatible free alternative to SUSE Linux Enterprise Desktop 15 (SLED). openSUSE (2018) detail that the openSUSE distribution is the current foundation for SUSE's enterprise offerings, meaning that no commercial support is offered directly to openSUSE. Instead, using SLED would offer the ability of obtaining commercial support for the system.

SUSE (n.d.) offer several subscription tiers for the SLED distribution:

Table 29 adapted from SUSE (n.d.).

Subscription Tier	***Subscription Term***	***Cost (USD)***
Self Support	1 year	$50
	3 year	$135
Standard	1 year	$120
	3 year	$324
Priority	1 year	$220
	3 year	$600

Where:

- Self Support offers no commercial support and simply offers a license for the system to receive maintenance updates. (SUSE, n.d.).
- Standard offers maintenance updates and commercial support twelve hours a day, five days a week, with a response time of four hours. (SUSE, n.d.).
- Priority offers the same as Standard but with twenty-four hour, seven days a week support and a one-hour response time for high severity issues. (SUSE, n.d.).

5.4.6 Zentyal Server 6.0

Zentyal (2018), in a direct enquiry to the company, provided a comprehensive list of typical commercial licensing and support pricing for Zentyal Server 6.0. Zentyal offer the following commercial licenses by organization size:

Table 30 adapted from Zentyal (2018).

	Micro	***Small***	***Medium***	***Enterprise***
Users	<25	<75	<300	Unlimited
Features	All	All	All	All
SW/Security Updates	Yes	Yes	Yes	Yes
Price (no VAT)	€195	€495	€995	€2995

Zentyal Server commercial licenses are purchased by server instance, valid for the version they are purchased for, perpetual and ensure the edition of Zentyal receives software and security updates until End Of Life (Zentyal, 2018).

Alongside Zentyal commercial licenses, commercial support packages are offered to customers who purchase licenses on a yearly subscription basis:

Table 31 adapted from Zentyal (2018).

	Professional	***Business***	***Premium***
Technical Support	5 tickets	10 tickets	Unlimited
Max response time	2 business days	1 business day	4 h on business days
Version Upgrade	Yes	Yes	Yes
No. servers (max)	3	3	3
Duration	1 year	1 year	1 year
Price (no VAT)	€495	€795	€1495

Alongside their subscription model, Zentyal also offer a "pay-as-you-go" support option, where customers with a valid license can pay per support ticket.

Table 32 adapted from Zentyal (2018).

	Pay-as-you-go
Technical Support	Pay per ticket
Max response time	2 business days
Version upgrade	No
No. of servers (max)	1
Duration of ticket	1 year
Price/ticket	€295

Chapter 6: Discussion and Conclusion

6.1 Complexity of Implementation and Administration

6.1.1 Joining Linux Clients to an Active Directory Domain

Each Linux distribution that was joined to an Active Directory domain offered a different experience and level of complexity in doing so. Each distribution’s vendor offers documentation detailing different methods, software and required packages to facilitate this method of authentication, with this documentation having varying degrees of accuracy against the current state of their distributions.

Ubuntu 18.04 LTS presented a number of challenges, including official documentation from Canonical (2018) on the matter proving to be vague and delivering a non-functional result, thus further research was required on a process to join an Ubuntu client to an Active Directory domain. Waterman (2018) details the required packages and command line process necessary to join Ubuntu to the domain, however it could be argued that this is a major step up in complexity versus the methods used on Windows 10, where all the required components are preinstalled with the system and the system can be joined to the domain graphically.

CentOS 7.6 presented similar challenges to Ubuntu, although official Red Hat documentation from Hanzelka *et al.* (2018) detailed a working process similar to that of Ubuntu. However, as the method used was much like that used on Ubuntu, it also suffers from the same caveats, including the possibility of it being considered a major step up in complexity of implementation versus the methods used on Windows 10, and CentOS requiring that several extra packages were necessary to facilitate joining the domain.

openSUSE Leap 15 provided a very different experience in joining the system to an Active Directory domain, with openSUSE (n.d.) detailing several processes through openSUSE’s YaST graphical system configuration tool. While the method of using the *User Logon Management* module in YaST to join the system to the domain is arguably more involved than on Windows, it provides an arguably simpler way of joining the system to the domain, akin to Windows. The *User Logon Management* module may even benefit some administrators by offering several configuration options from one central interface, unlike Windows, where many options pertaining to domain membership must be configured through Group Policy.

6.1.2 Using a Linux-based Active Directory Compliant Domain Controller

Implementing an Active Directory compliant domain controller based on Linux initially proved to be significantly complex, with literature from openSUSE (2018) not reflecting the current state of the distribution and the YaST graphical system configuration tool. However, Zentyal Server 6.0 lived up to the claims of Zentyal (n.d.) that it could provide an Active Directory compliant domain controller configurable through a graphical interface, thus reflecting the methods of configuration on Windows Server. The first-run setup wizard made installing the relevant roles a similar experience to that of Windows Server, where roles are managed through Server Manager, and Zentyal’s web-based configuration interface provided alternatives to Active Directory configuration consoles such as the Active Directory Users and Computers console. It can be argued that with this web interface, there is little extra administration complexity with no dramatic learning curve, unlike joining Linux clients to an Active Directory domain. However, as Zentyal's web-based configuration interface does not manage all aspects of the underlying Linux system, some Linux knowledge would still be required in the event of more advanced system configuration being necessary.

Windows 10 clients joined to the domain controlled by Zentyal seamlessly, in much the same way they would if joined to a Windows Active Directory domain. Domain logins on Windows visually functioned in the same way as they would if authenticating against a Windows Server.

6.1.3 SMB Interoperability

Both Windows and Linux, regardless of what role they played in the network, were able to share files with one another via SMB without issue. All three Linux distributions tested provided methods in their respective graphical file managers to connect to an SMB share on the network using the underlying Samba technology to interoperate seamlessly with the SMBv3 share on Windows Server. Windows clients also had no issues using native SMB to interoperate with a Samba share, with Zentyal using Samba being able to configure domain accounts on Windows to have an automatically mounted network drive with letter H:.

6.2 Benchmark Results

6.2.1 Active Directory Domain Login Times

6.2.1.1 Windows Server with Linux Clients Network

When comparing the measured login times of the distributions against that of the Windows homogeneous control network, all of the Linux distributions were measured to be slower.

Table 31

Operating System	***Average Login Time (s)***
Windows 10	4.92
Ubuntu 18.04 LTS	6.02
CentOS 7.6	10.44
openSUSE Leap 15	6.77

Ubuntu 18.04 LTS and openSUSE Leap 15 were measured to be slower than Windows 10, with all results shown in chapter 5 to be slower than Windows' average time. However, with this only being an extra second, it can be argued that this isn't a significant real-world difference and would have little if any impact on day to day usage. CentOS 7.6 on the other hand was noticeably slower than Windows 10 and the other two Linux distributions. It is not known why this is, and further research would be required into why CentOS was consistently much slower.

6.2.1.2 Linux Server with Windows Clients Network

When comparing the measured login times of Windows 10 clients authenticating against a Linux-based domain controller versus a Windows-based one in the Windows homogeneous control network, all three clients were measured to log in slower than on the homogeneous network, with the average being slower than this network also.

Table 32

Network	***Average Login Time (s)***
Windows Homogeneous	4.92
Linux Server/Windows Clients	6.37

It is not known at this time why Windows clients authenticating against a Linux-based domain controller is slower than authenticating against a Windows-based domain controller. Further research would be required to ascertain this. However, with the average time for the Linux server not being much longer than that of the homogeneous network, it could be argued that this would again have little if any impact on day to day usage in the real world.

6.2.1.3 Windows Server with Heterogeneous Clients

In this environment, the Windows 10 client added to the network authenticating against a Windows Server was measured to be faster to login than any of the existing Linux clients, and faster than the times observed in the homogeneous control network.

Operating System	***Average Login Time (s)***
Windows 10 (homogeneous control)	4.92
Windows 10 (heterogeneous)	3.52
Ubuntu 18.04 LTS	6.02
CentOS 7.6	10.44
openSUSE Leap 15	6.77

It is not known at this time why the newly added Windows 10 client outperformed both the Linux clients and the homogeneous control network, with a difference of over a second observed between the heterogeneous and homogeneous networks. Further research would be required to ascertain this.

6.2.1.4 Linux Server with Heterogeneous Clients

In this environment, the Ubuntu 18.04 LTS client added to the network authenticating against a Zentyal Server Samba-based domain controller was measured to be faster on average to login than the Windows homogeneous control network, the Windows clients already existing in this network, and the Linux clients in the networks utilizing Windows Server.

Operating System	Average Login Time (s)
Windows 10 (homogeneous control)	4.92
Windows 10 (heterogeneous)	3.52
Ubuntu 18.04 LTS (Windows Server)	6.02
CentOS 7.6	10.44
openSUSE Leap 15	6.77
Ubuntu 18.04 LTS (Linux Server)	4.74

It is not known why the Ubuntu client authenticated much faster in this network than any of the others. Further research would be required to ascertain this.

6.2.1.5 Summary

While any scenario involving Linux, be it as a client operating system or the domain controller, resulted in longer domain login times than that observed in the homogeneous control network (with the exception of Ubuntu in the Linux Server with heterogeneous clients network), the times observed can be argued to have little to no impact on real-world operation. Apart from CentOS, the difference between Linux and Windows environments in this regard is minor enough to not be considered a drawback to implementation of Linux as either a client operating system or a server.

6.2.2 SMB File Transfer

6.2.2.1 Windows Server with Linux Clients Network

SMB Large File Transfer

When comparing the average SMB transfer rates of a large file in the Windows homogeneous network against that of the Windows Server with Linux clients network, the average transfer rates on Linux were generally higher than that observed on Windows.

Table 33

OS	Server>Client (MB/s)	Client>Server (MB/s)
Windows (homogeneous)	76.97	71.17
Ubuntu	90.29	108.22
CentOS	47.70	132.47
openSUSE	97.58	109.40

With the exception of CentOS in the transfer from the server to the client, the average transfer rates measured on the Linux clients were faster than native SMB transfers between Windows Server and Windows 10. For client to server transfers, all three Linux clients were observed to be considerably faster on average than native SMB transfers on Windows. It is unknown why transfer rates on Linux were observed to be considerably faster, with further testing of Samba and SMB configuration on their respective operating systems being required to ascertain this. It is also not known why CentOS produced dramatically different results, with a server to client transfer rate far below any of the rest of the operating systems tested, and a client to server transfer rate exceeding that of Gigabit networking standards.

This exceedingly fast transfer rate could be explained by an abnormality caused by virtualization, however further testing between a virtualized network and a physical network would be required to examine this.

SMB Small Files Transfer

When comparing the average SMB transfer rates of a collection of small files in the Windows homogeneous network against that of the Windows Server with Linux clients network, the average transfer rates on Linux were observed to be somewhat faster than observed on Windows.

Table 34

OS	***Server>Client (MB/s)***	***Client>Server (MB/s)***
Windows	46.90	15.07
Ubuntu	61.13	51.64
CentOS	25.60	42.87
openSUSE	55.87	45.08

Again, with the exception of CentOS, server to client average transfer rates on Linux were on average faster than that of native SMB on Windows. It is unknown why CentOS produced a noticeably slower result than any of the other Linux distributions in this benchmark. With client to server transfers, all three Linux distributions were again observed to be noticeably faster on average than native SMB transfers on Windows. It is unknown at this stage why this is the case, and further testing and exploration of Samba and SMB configuration on their respective operating systems would be required to ascertain this.

6.2.2.2 Linux Server with Windows Clients Network

SMB Large File Transfer

When comparing the average SMB transfer rates of a large file in the Windows homogeneous network against that of the Linux server with Windows clients network, the average transfer rates were observed to be considerably higher than that seen in the homogeneous network.

Table 35

Network	***Server>Client (MB/s)***	***Client>Server (MB/s)***
Windows Homogeneous	76.97	71.17
Linux Server	98.15	174.80

It is unknown why transfer rates to and from a Linux server (using Samba as it’s SMB implementation) on Windows were observed to be considerably higher. Virtualisation abnormalities may be responsible the exceedingly high client to server average transfer rate, which exceeds Gigabit networking standards, however further testing between a virtual network and physical network would be required to assess this.

SMB Small Files Transfer

When comparing the average SMB transfer rates of a collection of small files in the Windows homogeneous network against that of the Linux server with Windows clients network, the average transfer rates were observed to be similar, if not slightly faster, than that seen in the homogeneous network.

Table 36

Network	**Server>Client (MB/s)**	**Client>Server (MB/s)**
Windows Homogeneous	46.90	15.07
Linux Server	45.78	48.60

In this scenario, the average transfer rate from the server to the clients was on par with that observed with native SMB in the homogeneous network. However, it is unknown why the client to server average transfer rate is considerably faster with a Linux server using Samba. Further testing of Samba and SMB configurations on their respective operating systems would be required to ascertain this.

6.2.2.3 Windows Server with Heterogeneous Clients

SMB Large File Transfer

In this scenario, the newly added Windows 10 client transferring a large file between itself and Windows Server via native SMB was measured to be faster than either Windows in the homogeneous control network, or any of the existing Linux clients in the heterogeneous network.

OS	**Server>Client (MB/s)**	**Client>Server (MB/s)**
Windows (homogeneous)	76.97	71.17
Windows (heterogeneous)	99.13	135.18
Ubuntu	90.29	108.22
CentOS	47.70	132.47
openSUSE	97.58	109.40

It is unknown why Windows 10 in the heterogeneous network is much faster when transferring large files via native SMB, with further research being required to ascertain this.

SMB Small Files Transfer

In this scenario, the newly added Windows 10 client transferring a collection of small files between itself and Windows Server was measured to perform roughly similarly to that of Windows in the homogeneous control network, and somewhat slower than that of the existing Linux clients in this network (with the exception of CentOS 7.6).

OS	**Server>Client (MB/s)**	**Client>Server (MB/s)**
Windows (homogeneous)	46.90	15.07
Windows (heterogeneous)	41.09	28.85
Ubuntu	61.13	51.64
CentOS	25.60	42.87

openSUSE	55.87	45.08

It would be expected that Windows would perform roughly similar in both the homogeneous and heterogeneous networks, however it is unknown why Windows with native SMB performs slower than that of Linux interacting with Windows Server via Samba. Further research would be required to ascertain this.

6.2.2.4 Linux Server with Heterogeneous Clients

SMB Large File Transfer

In this scenario, the newly added Ubuntu 18.04 LTS client was measured to perform on average slower than that of the existing Windows clients in this network.

OS	***Server>Client (MB/s)***	***Client>Server (MB/s)***
Windows (Homogeneous)	76.97	71.17
Ubuntu 18.04 LTS (Het.)	73.57	158.55
Windows (Heterogeneous)	98.15	174.80

It is unknown why the Ubuntu client performed on average slower than the existing Windows clients in this network, however the same possible virtualization abnormality was observed on Ubuntu as observed on Windows; with exceedingly fast client to server file transfers. Further testing between a physical and virtual network would be required to ascertain why this is, with further testing also needed to ascertain why Ubuntu in this scenario performed worse than Windows yet has previously been seen to outperform Windows in the same transfer (as shown in section 6.2.2.3).

SMB Small Files Transfer

6.2.2.5 Summary

While it is unknown why transfer rates were almost always considerably higher with Linux involved than in the Windows homogeneous network, the increase in throughput could be a potential benefit for using Linux as either a client operating system or a file server. In enterprises where users rely on and utilize SMB shares daily, faster transfer rates obtained through using Linux could be an advantage to implementing and integrating Linux into an existing Windows-oriented environment.

6.3 Conclusion and Further Work

6.3.1 Conclusion

To conclude, there is much to consider in an environment where Windows and Linux must interoperate while utilizing Windows Enterprise technologies like Active Directory Single Sign-On and SMB.

With these technologies being originally designed for and native to Windows, it would be expected that the implementation and administration of these technologies would be simplest on their native platform. However, solutions now exist in the Linux eco-system that dramatically reduce the complexity of these tasks; as evidenced by openSUSE with its YaST graphical system configuration tool, and Zentyal Server, providing a web-based interface akin to those found on Windows Server to work with these technologies. While the implementation and administration experience is different and arguably more complex on these solutions than on Windows, it shows that incorporating Linux into an existing Windows-oriented environment need not be as disruptive and detrimental as some may fear.

The performance of these technologies would also be expected to be best on their native platform. While this is true with regards to Active Directory domain logins, where login times were observed to be fastest in a Windows homogeneous environment, SMB implemented through Samba on Linux proved to be faster. While marginally slower domain login times may have little real impact for users, faster network file transfers could prove to be beneficial in environments which rely heavily on networked storage, and present Linux as either a client or an SMB file server as a viable option.

With a range of licensing and commercial support options available to every operating system featured, enterprises can consider whether cost is worth convenience. With Windows Server 2016 being costly to license (where licenses are sold according to the number of physical CPU cores in a system) and Windows 10 licenses not being considerably cheaper, with neither of these including the cost of commercial support, enterprises must consider whether the ease of implementation, administration and mediocre performance is worth the cost. With the Linux distributions tested being either freely available for download, licensed on a subscription basis including commercial support, or presenting flexible options for commercial support, there could be a financial incentive for enterprises to consider utilizing Linux in their existing Windows-oriented environments.

While this report initially set out to find what the most functional setup is in such heterogeneous environments given currently available technologies, this is not possible with so many factors to consider and future work still being required to investigate abnormalities found in the research.

6.3.2 Future Work

It was not possible to cover Group Policy functionality in heterogeneous environments in this research. Future work could perhaps focus on how to implement this on Linux clients, and how to administer Group Policy from a Linux server.

It was also not possible in this research to cover utilizing Linux as a server in a multi-server network, where a Windows Server may also be deployed acting as either a primary domain controller, or a backup domain controller. Future work could perhaps explore the functionality of using a Linux server in such an environment and in such roles.

This research found abnormalities in the observed file transfer rates through SMB, with some rates exceeding that of Gigabit network specifications. Future work could explore whether these abnormalities are caused by networking in virtualisation, issues found in SMB or Samba configuration or other unforeseen causes. Abnormalities were also found in the performance of all the implemented network technologies on CentOS, with it often being considerably slower than all other operating systems tested despite near identical configuration performed on the system. Future work could explore why CentOS' performance differed so much from that of the other operating systems tested.

Future work could also explore what other Windows Enterprise technologies can be implemented on Linux systems, and whether existing alternatives to these provide similar, if not better, performance.

Chapter 7: Critical Reflection

This project has proved to be an immensely valuable experience; having taught me a number of lessons with regards to working on something as important and substantial as this project. While my time management has dramatically improved during my time at University and aided in the completion of this project, there were still instances where I feel time could have been used in a considerably more productive manner.

Several unfortunate circumstances in my personal life impacted the completion of this project at several key points. It is regrettable that due to these, the project was unable to reach its full completion as specified on the specification sheet at the start of the project. However, I feel taking the time to organise and handle my personal life was beneficial to me in terms of my mental health and overall focus on the work at hand. I am pleased with the project I have produced despite these circumstances and I am rather proud of myself for overcoming and working round these circumstances to complete such a substantial piece of work.

Planning of the project was a challenge from the start, as for much of what I was undertaking, I had to teach myself how many of the technologies I worked with functioned and deal with poor documentation. Attempts were made to plan my time with regards to setting up what was required to undertake the research (as shown by appendix 9.1); however, it was found that this took considerably longer than originally estimated. I have learned that I must always estimate and expect possible setbacks, and to always expect the unexpected when working with information on technologies that others have produced.

8 References

[1] *Flores, J., Mathers, B., Kumar, S., Plett, C., "yishengjin1413" (2017) Delegating Administration by Using OU Objects* [online]. [Accessed November 2018]. Available at: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/delegating-administration-by-using-ou-objects

[2] *Heslin, M. (2012) Integrating Red Hat Enterprise Linux 6 with Active Directory* [online]. [Accessed November 2018]. Available at: https://docplayer.net/3591694-Integrating-red-hat-enterprise-linux-6-with-active-directory-mark-heslin-principal-software-engineer.html

[3] *Walla, M. (2000) Kerberos Explained* [online]. [Accessed November 2018]. Available at: http://tomax7.com/asecplus/vpn-cloud/Kerberos%20Explained.docx

[4] *Microsoft (2012) Group Policy Planning and Deployment Guide* [online]. [Accessed November 2018]. Available at: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754948(v=ws.10)

[5] *Microsoft (2012) Group Policy for Beginners* [online]. [Accessed November 2018]. Available at: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/hh147307(v=ws.10)

[6] *French, S.M. (2007) A New Network File System is Born: Comparison of SMB2, CIFS and NFS* [online]. pp. 131-134.[Accessed November 2018]. Available at: https://ols.fedoraproject.org/OLS/Reprints-2007/OLS2007-Proceedings-V1.pdf#page=131

[7] *Potter, T., Tridgell, A. (2000) Unified Logons between Windows NT and UNIX using Winbind* [online]. [Accessed November 2018]. Available at: http://wireless.ictp.it/school_2001/labo/linux/linux_guides/winbind.pdf

[8] *Hanzelka, F., Maňásková, L., Petrová, A.S., Muehlfeld, M., Čapek, T., Ballard, E.D. (2018) Red Hat Enteprise Linux 7 Windows Integration Guide: Integrating Linux Systems with Active Directory Environments* [online]. [Accessed November 2018]. Available at: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/pdf/windows_integration_guide/Red_Hat_Enterprise_Linux-7-Windows_Integration_Guide-en-US.pdf

[9] *Smørgrav, D. (n.d.) Pluggable Authentication Modules* [online]. [Accessed November 2018]. Available at: https://www.freebsd.org/doc/en/articles/pam/article.html

[10] *Geisshirt, K. (2007) Pluggable Authentication Modules: The Definitive Guide to PAM for Linux SysAdmins and C Developers* [online]. *Publisher: Packt Publishing* [Accessed November 2018]. Available at: https://books.google.co.uk/books?hl=en&lr=&id=LQXSAQAAQBAJ&oi=fnd&pg=PT12&dq=linux+pluggable+authentication+modules&ots=rJfZbcDwOp&sig=m0Nn2bQL2deFCpT6taFaFsKM5sY#v=onepage&q=linux%20pluggable%20authentication%20modules&f=false

[11] *Hanzelka, F., Maňásková, L., Petrová, A.S., Muehlfeld, M., Čapek, T., Ballard, E.D. (2018) Red Hat Enteprise Linux 7 System-Level Authentication Guide: About System-Level Services for Authentication and Identity Management* [online]. [Accessed November 2018]. Available at: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/pdf/system-level_authentication_guide/Red_Hat_Enterprise_Linux-7-System-Level_Authentication_Guide-en-US.pdf

[12] *Bartlett, A. (2005) Samba 4- Active Directory* [online]. [Accessed November 2018]. Available at: https://cvs.samba.org/samba/news/articles/abartlet_thesis.pdf

[13] *Oracle (n.d.) 1.3 What are Hypervisors?* [online]. [Accessed November 2018]. Available at: https://docs.oracle.com/cd/E50245_01/E50249/html/vmcon-hypervisor.html

[14] *Chinnaswammy, M.M. (2016) A Comprehensive Review on Embedded Hypervisors* [online]. [Accessed November 2018]. Available at: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-5-ISSUE-5-1546-1550.pdf

[15] *Chapple, E. (2018) Windows Server 2019 – Announcing general availability in October!* [online]. [Accessed November 2018]. Available at: https://cloudblogs.microsoft.com/windowsserver/2018/09/24/windows-server-2019-announcing-general-availability-in-october/

[16] *VMware (2018) Virtual Machine for Business – Buy Workstation Pro* [online]. [Accessed November 2018]. Available at: https://store.vmware.com/store/vmwde/en_GB/DisplayProductDetailsPage/ThemeID.29219600/productID.5223188000

[17] *Microsoft (2018) Windows | Official Site for Microsoft Windows 10 Home and Pro OS, laptops, PCs, tablets & more* [online]. [Accessed November 2018]. Available at: https://www.microsoft.com/en-gb/windows

[18] *SUSE (2013) Linux Continues to Gain Momentum in Enterprise Server Market* [online]. [Accessed November 2018]. Available at: https://www.suse.com/media/brief/linux_gains_momentum.pdf

[19] *Red Hat (2018) Tried. Tested. Trusted. From the leader in open source, for the leaders in I.T.* [online]. [Accessed November 2018]. Available at: https://www.redhat.com/en/about/trusted

[20] *openSUSE (2018) Portal: 15.0* [online]. [Accessed November 2018]. Available at: https://en.opensuse.org/Portal:15.0

[21] *Red Hat (2014) Red Hat and the CentOS Project Join Forces to Speed Open Source Innovation* [online]. [Accessed November 2018]. Available at: https://www.redhat.com/en/about/press-releases/red-hat-and-centos-join-forces

[22] *CentOS (2018) CentOS-7 (1804) Release Notes* [online]. [Accessed November 2018]. Available at:

https://wiki.centos.org/Manuals/ReleaseNotes/CentOS7.1804?action=show&redirect=Manuals%2FReleaseNotes%2FCentOS7

[23] *Red Hat (2018) Evaluate Red Hat Enterprise Linux* [online]. [Accessed November 2018]. Available at: https://access.redhat.com/products/red-hat-enterprise-linux/evaluation?extIdCarryOver=true&sc_cid=701f2000001Css5AAC

[24] *Kirkland, D. (2015) How many people in the world use Ubuntu? More than anyone actually knows!* [online]. [Accessed November 2018]. Available at: http://blog.dustinkirkland.com/2015/12/more-people-use-ubuntu-than-anyone.html

[25] *Ubuntu (2018) Download Ubuntu Desktop* [online]. [Accessed November 2018]. Available at: https://www.ubuntu.com/download/desktop

[26] *VMware (2018) Workstation Player* [online]. [Accessed November 2018]. Available at: https://www.vmware.com/products/workstation-player.html

[27] *Net Marketshare (2018) Linux Market Share* [online]. [Accessed November 2018]. Available at: https://netmarketshare.com/linux-market-share

[28] *Net Marketshare (2018) Windows Market Share* [online]. [Accessed November 2018]. Available at: https://netmarketshare.com/windows-market-share

[29] *openSUSE (n.d.). Setting Up Authentication Servers and Clients Using YaST* [online]. [Accessed November 2018]. Available at: https://doc.opensuse.org/documentation/leap/security/html/book.security/cha.security.auth.html

[30] *Oracle (2018) Oracle VM VirtualBox User Manual* [online]. [Accessed October 2018]. Available at: https://www.virtualbox.org/manual/

[31] *Minasi, M., Greene, K., Booth, C., Butler, R., McCabe, J., Panek, R., Rice, M., Roth, S. (2014) Mastering Windows Server 2012 R2. Publisher: Sybex.* pp. 257-266, 688.

[32] *Zentyal (2018) Zentyal Server 6.0 Commercial now available* [online]. [Accessed February 2019]. Available at: https://zentyal.com/news/zentyal-server-6-0-commercial-now-available/

[33] *Waterman, M. (2018) Join Ubuntu 18.04 to Active* Directory [online]. [Accessed January 2019]. Available at: https://bitsofwater.com/2018/05/08/join-ubuntu-18-04-to-active-directory/

[34] *Jarrod (2016) How To Join CentOS Linux To An Active Directory Domain* [online]. [Accessed January 2019] Available at: https://www.rootusers.com/how-to-join-centos-linux-to-an-active-directory-domain/

[35] *openSUSE (n.d.) Active Directory Support* [online]. [Accessed January 2019]. Available at:

https://doc.opensuse.org/documentation/leap/security/html/book.security/cha.security.ad.html#sec.security.ad.sssd

[36] *Zentyal (n.d.) Installation* [online]. [Accessed March 2019]. Available at: https://doc.zentyal.org/en/installation.html

[37] *Microsoft (n.d.) Windows Server 2016 Licensing Editions* [online]. [Accessed March 2019]. Available at: https://www.microsoft.com/en-us/licensing/product-licensing/windows-server-2016

[38] *Microsoft (n.d.) Software Assurance Overview* [online]. [Accessed March 2019]. Available at: https://www.microsoft.com/en-us/Licensing/licensing-programs/software-assurance-default?activetab=software-assurance-default-pivot:primaryr4

[39] *Horwitz, R. (2016) Windows Server Pricing* [online]. [Accessed March 2019]. Available at: https://www.directionsonmicrosoft.com/secured/2016/10/windows-server-pricing

[40] *Microsoft (n.d.) Windows 10 Pro Download* [online]. [Accessed March 2019]. Available at: https://www.microsoft.com/en-gb/p/windows-10-pro/df77x4d43rkt/48DN

[41] *Canonical (2018) Ubuntu Advantage* [online]. [Accessed March 2019]. Available at: https://assets.ubuntu.com/v1/63deda69-canonical-ua-datasheet-2018-09-14.pdf

[42] *Red Hat (n.d.) Red Hat Enterprise Linux Developer Workstation* [online]. [Accessed March 2019]. Available at: https://www.redhat.com/en/store/red-hat-enterprise-linux-developer-workstation#?sku=RH3482727

9 Appendices

Appendix 9.1: Gantt Chart showing time planning for practical work that was to be undertaken to conduct the research.

Honours Project	start	end	0h	0%
Windows Homogeneous Network	**28/12/18**	**30/12/18**	**0h**	**0%**
Install operating systems	28/12	28/12	0	0%
Configure basic networking/system settings	28/12	28/12	0	0%
Implement SMB and Active Directory	28/12	30/12	0	0%
Obtain network performance baseline results	30/12	30/12	0	0%
Windows Server/Linux Clients Network	**28/12/18**	**03/01/19**	**0h**	**0%**
Install operating systems	28/12	28/12	0	0%
Configure basic networking/system settings	28/12	28/12	0	0%
Implement SMB and Active Directory	01/01	03/01	0	0%
Obtain network performance results	03/01	03/01	0	0%
Linux Server/Windows Clients Network	**08/01/19**	**14/01/19**	**0h**	**0%**
Install operating systems	08/01	08/01	0	0%
Configure basic networking/system settings	08/01	08/01	0	0%
Implement SMB and Active Directory	10/01	14/01	0	0%
Obtain network performance results	14/01	14/01	0	0%
1st Class Linux/Windows Fully Heterogeneou...	**17/01/19**	**30/01/19**	**0h**	**0%**
Install operating systems	17/01	17/01	0	0%
Configure basic networking/system settings	17/01	17/01	0	0%
Implement SMB and Active Directory	22/01	24/01	0	0%
Implement extended enterprise services	25/01	30/01	0	0%