Edith Cowan University
School of Science

CYB6013 (CYBER PROJECT 2) – METHODOLOGY IMPLEMENTATION PLAN

STUDY PERIOD:	22AC2 March to May
STUDENT:	RAY PARKER : 10532682
PROJECT TITLE:	2STEP AUTHENTICATION SOLUTION
FACILITATOR:	BAZLUR RASHID

Written implementation plan

Description

VMWare Workstation will be used with a windows host Dell 9010 desktop computer running Microsoft Windows 10.Virtual machines will be created for 2 Windows server 2022 and 5 Microsoft Windows 11 Client computers. The DC01 Server will be promoted as a domain controller with Active directory installed to accept client requests and be setup as the authentication server for login requests.
To prepare the virtual machines mentioned in Table 1, ISO images were downloaded from Microsoft Evaluation Center. Windows Server 2022 (Insider_Preview Server) and Win11_English_x64 were downloaded. The steps documented in Table 1 and below were followed to create the network lab environment.
1. Install Vmware Workstation on the host machine.
2. Install and configure the first Domain Controller (DC01) virtual machine and add Active Directory Domain services and promote this (DC) to the Forest Domain widgetllc.internal.
3. Install and configure the second Domain Controller (DC02) and promote into thr widgetllc domain.
3. Install and configure the CLIENT virtual machines and promote these machines into the widgettllc domain using static IP addressing (Table 1.) (Mark, 2016).

Background

- The stakeholders require a more secure login system to prevent attacks from internal and external actors.
- Users will provide a password along with a pin generated by the dongle to login to the network system.
- This solution will harden the network system and help protect assets and intellectual property from attacks.
- Users will not be impacted except for an extra 5 seconds to input the pin to login.
- The only cost incurred by the stakeholders will be the purchase of the dongle
- This solution will only require existing IT personnel to implement the change necessary on the server side to include the scripting to allow authentication for user logins.

This project will be implemented over a period of 18 weeks from January 10 2022 and is expected to be completed by 26 June 2022

The resources required to complete this project include the purchasing of the dongle to be used and supplied to all users of the system. An inventory system will be integrated into the current asset inventory system to allocate the dongles to users of the network.

Current IT department employees will be provided by the company eliminating any new costs to the project.

A video presentation will be created in order to show the stakeholders how the new system will operate and the new login process will only add around 5 seconds to the current login time.

Training users will only include a short explanation of how to use the new dongle to generate the pin which expires in 5 seconds and a new pin is generated to operate in sync with the authentication server (R.Parker 2022).

Prototyping strategy

My strategy to Prototype this solution is to build a virtual network in VMware Workstation to run exhausting testing on the offered solution. This VIRTUAL network will be able to run testing in a live network environment without any impact on the company's current network configuration and will be able to be reconfigured at short notice to accommodate any changes in testing or scope creep if required.

Methodology

3) Token authentication

A virtual network environment was created in VM Ware Workstation on the Host Dell computer creating 2 domain controller servers in the widgetllc.internal domain (DC01 and DC02) with 5 client computers (Image 2) added to the domain to test the 2 step login process in a live environment not connected to the existing network. 1000 random users (Image 3) were added to a newly created _Users organisational unit in active directory. A new organisation group was created on DC01 called groups and all the existing security group entries from the generic Users group in Active directory were moved from this generic group into the newly created Users organisational group (Image 4).

Summary

Creating this virtual network to conduct extensive testing of the 2 step authentication process will allow transcend IT Services to run unlimited tests in a live virtual environment without any impact on the current network system and will not interrupt day to day operations of the company and will provide real time visual feedback to the client and show the new login solution operational.

References

References should be provided for the background literature (APA style).

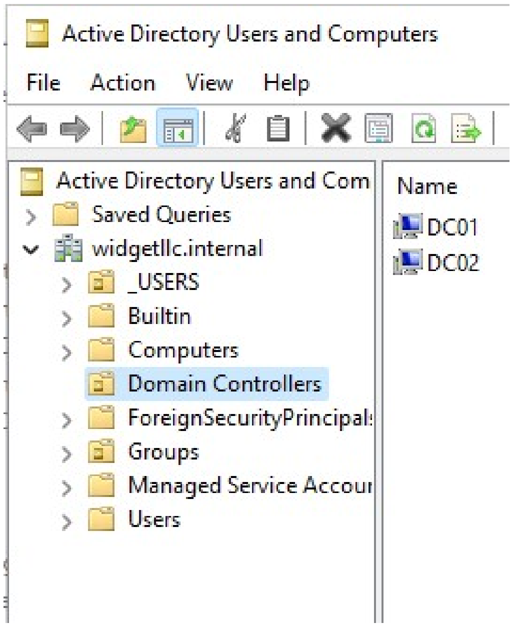
Mark, K. G. (2016). Installing and Configuring Windows Server 2016 (Hands-on Guide).

(N-able, April 2019)

Visual implementation plan

Log No.	Action	Steps Performed	Results (if Any)
1.	Open VMWare on the host machine	Create windows Server 2022 Virtual Machine	Autounattend.xml file was used to install server 2022 software from an ISO image file. Set password: J388ica* across this working Lab environment
		Promote DC01 to the forest widgetllc.internal	DC01 promoted to the forest and active directory services installed correctly. The network address chosen for this Lab environment will utilise 10.0.0.0 The DC01 will use a static IP address with subnet and default gateway as set below IP: 10.0.0.100 Subnet: 255.0.0.0 Gateway:10.0.0.1 DNS: 10.0.0.100 (Mark, 2016)
2.		Create windows 11 workstation Virtual Machine.	Autounattend.xml file was used to install windows 11 pro workstation from an ISO image file.
3.		Change the computer name to Client1 and add it to the widgetllc domain	IP: 10.0.0.102 Subnet: 255.0.0.0 Gateway:10.0.0.1 DNS: 10.0.0.100 (Mark, 2016)
4.	Ad Users to domain	A Powershell script was used to add 1000 users to the domain	

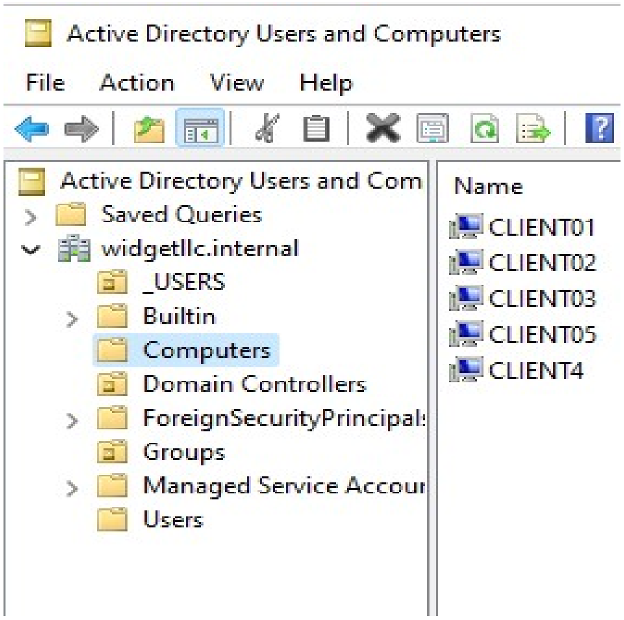
Table 1. Visual Implementation Plan(Mark, 2016).



Active Directory Users and Com
Saved Queries
widgetllc.internal
_USERS
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Groups
Managed Service Accour
Users

Name
DC01
DC02

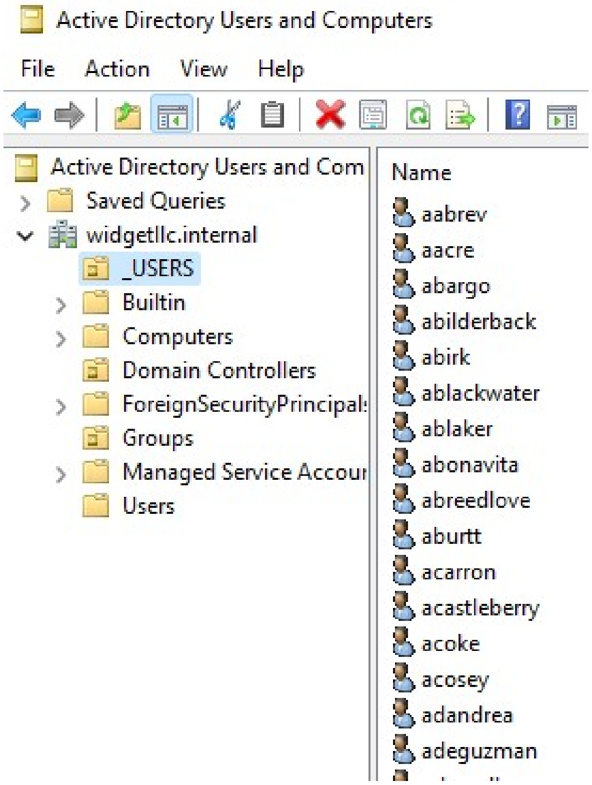
Image 1.



Active Directory Users and Com
Saved Queries
widgetllc.internal
_USERS
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Groups
Managed Service Accour
Users

Name
CLIENT01
CLIENT02
CLIENT03
CLIENT05
CLIENT4

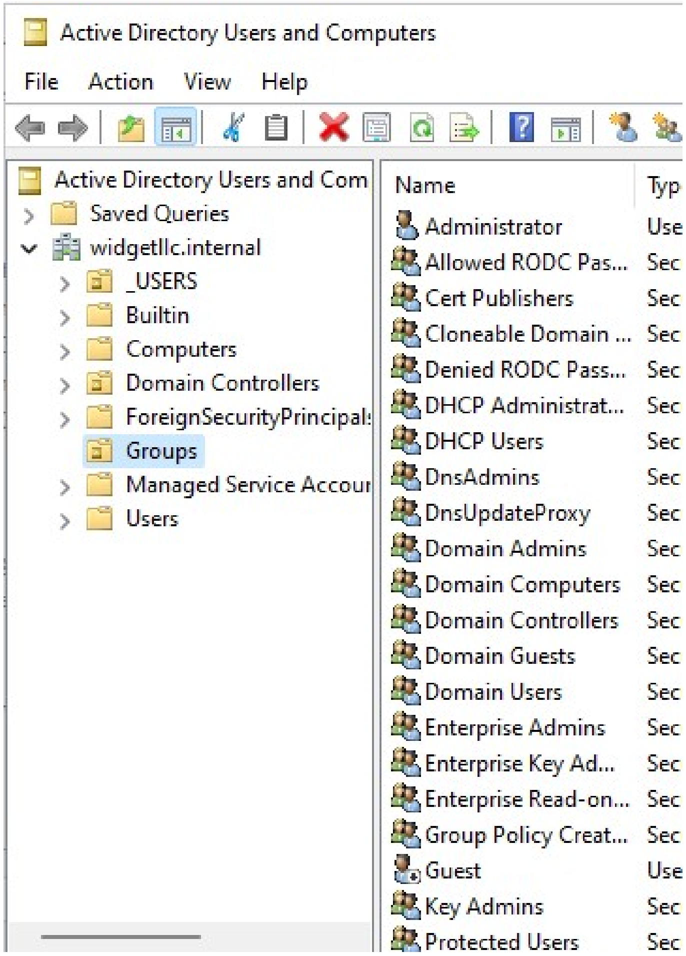
Image 2.



Active Directory Users and Com
Saved Queries
widgetllc.internal
_USERS
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Groups
Managed Service Accour
Users

Name
aabrev
aacre
abargo
abilderback
abirk
ablackwater
ablaker
abonavita
abreedlove
aburtt
acarron
acastleberry
acoke
acosey
adandrea
adeguzman

Image 3



Active Directory Users and Com
- Saved Queries
- widgetllc.internal
  - _USERS
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipal:
  - Groups
  - Managed Service Accour
  - Users

Name	Typ
Administrator	Use
Allowed RODC Pas...	Sec
Cert Publishers	Sec
Cloneable Domain ...	Sec
Denied RODC Pass...	Sec
DHCP Administrat...	Sec
DHCP Users	Sec
DnsAdmins	Sec
DnsUpdateProxy	Sec
Domain Admins	Sec
Domain Computers	Sec
Domain Controllers	Sec
Domain Guests	Sec
Domain Users	Sec
Enterprise Admins	Sec
Enterprise Key Ad...	Sec
Enterprise Read-on...	Sec
Group Policy Creat...	Sec
Guest	Use
Key Admins	Sec
Protected Users	Sec

Image 4

Mark, K. G. (2016). Installing and Configuring Windows Server 2016 (Hands-on Guide).

N-able. (April 2019). Common Network Authentication Methods. https://www.n-able.com/blog/network-authentication-methods