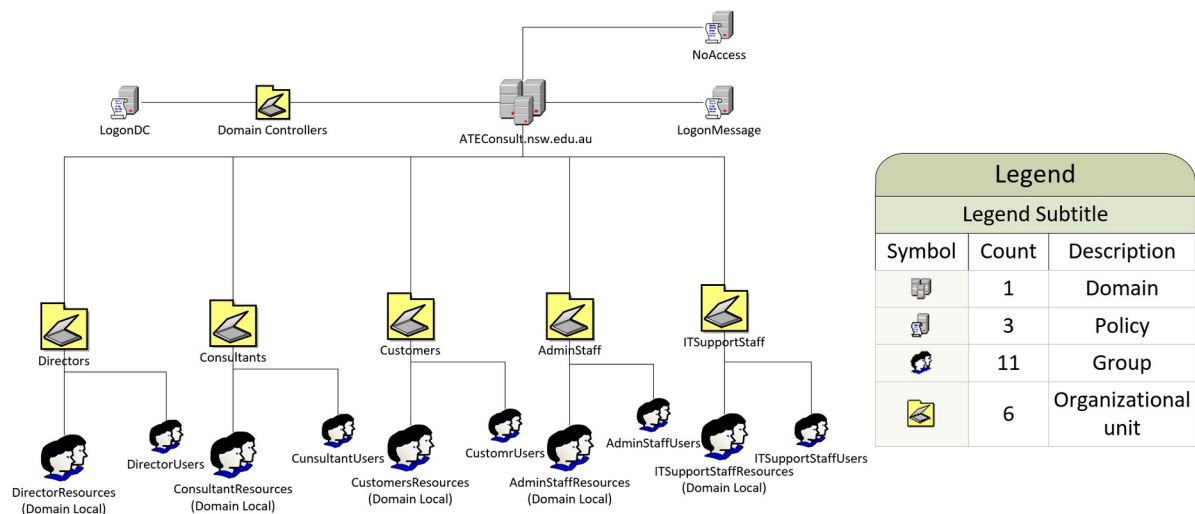Active Directory Design for ATEConsult

ASSIGNMENT/ASSESSMENT ITEM COVER SHEET

Student Name: Brock | Brinkworth

FIRST NAME | FAMILY / LAST NAME

Student Number: 3 3 3 1 9 5 2   Email: c3331952@uon.edu.au

Course Code | **Course Title**

I N F T 2 0 3 1 | Systems & Network Admin
(Example) | *(Example)*
A B C D 1 2 3 4 | Intro to University

Campus of Study: Callaghan (eg Callaghan, Ourimbah, Port Macquarie)

Assessment Item Title: Assignment 2   Due Date/Time: 28/05/2021

Tutorial Group (If applicable): _____   Word Count (If applicable): _____

Lecturer/Tutor Name: Darcy Merrick

Extension Granted: ○ Yes ◉ No   Granted Until: _____
Please attach a copy of your extension approval

NB: STUDENTS MAY EXPECT THAT THIS ASSIGNMENT WILL BE RETURNED WITHIN 3 WEEKS OF THE DUE DATE OF SUBMISSION

Please tick box if applicable

☑ *Students within the Faculty of Business and Law, Faculty of Science and Information Technology, Faculty of Engineering and Built Environment and the School of Nursing and Midwifery:*
I verify that I have completed the online Academic Integrity Module and adhered to its principles

☐ *Students within the School of Education:*
"I understand that a minimum standard of correct referencing and academic literacy is required to pass all written assignments in the School of Education; and I have read and understood the School of Education Course Outline Policy Supplement, which includes important information related to assessment policies and procedures.

I declare that this assessment item is my own work unless otherwise acknowledged and is in accordance with the University's academic integrity policy available from the Policy Library on the web at http://www.newcastle.edu.au/policylibrary/000608.html
I certify that this assessment item has not been submitted previously for academic credit in this or any other course. I certify that I have not given a copy or have shown a copy of this assessment item to another student enrolled in the course.

I acknowledge that the assessor of this assignment may, for the purpose of assessing this assignment:
• Reproduce this assessment item and provide a copy to another member of the Faculty; and/or
• Communicate a copy of this assessment item to a plagiarism checking service (which may then retain a copy of the item on its database for the purpose of future plagiarism checking).
• Submit the assessment item to other forms of plagiarism checking.

I certify that any electronic version of this assessment item that I have submitted or will submit is identical to this paper version.

DATE STAMP HERE

Turnitin ID: _____
(If applicable)

Insert this way

Signature: _____   Date: 27/05/2021

To copy and paste the completed form into another document use the 'snapshot' tool. | **Print Form** | THE UNIVERSITY OF NEWCASTLE AUSTRALIA

We will create a single domain for ATEConsult:

- Domain name: ATEConsult.nsw.edu.au

Parameter	Value
Fully Qualified Domain Name	ATEConsult.nsw.edu.au
Forest Functional Level	Windows Server 2019
Domain Functional Level	Windows Server 2019

Requirement: There are five major categories of users: Directors, Consultants, Customers, Admin staff and IT Support staff

First we will create separate OUs for each type of user:

Organizational Units

OU Name	Location	Description
Directors		The OU containing all directors and their resources
Consultants		The OU containing all consultants and their resources
Customers	ATEConsult.nsw.edu.au	The OU containing all customers and their resources
AdminStaff		The OU containing all admin staff and their resources
ITSupportStaff		The OU containing all it support staff and their resources

Following the AGDLP guidelines when creating groups:

Global Groups:

Group Name	Group Type	Location	Description
DirectorUsers		Directors OU	The global group will contain all Director accounts as members
ConsultantUsers		Consultants OU	The global group will contain all Consultant accounts as members
AdminStaffUsers	Global	AdminStaff OU	The global group will contain all AdminStaff accounts as members
ITSupportStaffUsers		ITSupportStaff OU	The global group will contain all ITSupportStaff accounts as members
CustomerUsers		Customers OU	The global group will contain all AdminStaff accounts as members

Domain Local:

Group Name	Location	Type	Description
DirectorResources	Directors		All permissions for Directors are assigned to this DL groups
ConsultantResources	Consultants		All permissions for Consultants are assigned to this DL groups
AdminStaffResources	AdminStaff	Domain Local	All permissions for AdminStaff are assigned to this DL groups
ITSupportStaffResources	ITSupportStaff		All permissions for ITSupportStaff are assigned to this DL groups
CustomerResources	Customers		All permissions for Customers are assigned to this DL groups

Group Membership for Domain Local Groups

Group Name	Member
DirectorResources	DirectorUsers
ConsultantResources	ConsultantUsers
AdminStaffResources	AdminStaffUsers
ITSupportStaffResources	ITSupportStaffUsers
CustomerResources	CustomerUsers

Requirement: The IT Support Staff should be able to logon to the Domain Controller:

Create a GPO called LogonDC and apply it to DomainControllers OU which contains all Domain Controllers of the domain. In LogonDC GPO, configure "Allow Logon Locally" setting in Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Management to include ITSupportUsers group

Requirement: For security reasons, all users must use complex passwords (i.e. at least 10 characters) when logging on the network:

- Edit any global policy (might aswell use LogOnMessage policy and apply it to all groups)
- Traverse Computer Settings > Policies > Windows Settings > Security Settings > Account Policies > Password Policy
- Double-click on Minimum password length, click on Explain tab and read. Finally set it to 10

Requirement: All users, except the IT Support staff, should not be able to access Control Panel or edit the registry settings on Windows:

- Login to the Doman Controller as a Domain Administrator and Open Group Policy Management Console
- Click on +'s to traverse the hierarchy and expand the domain ATEConsult
- Right-click on the domain > Create a GPO in this domain, and Link it here...
- Name the policy as NoAccess and save.
- Open Group Policy Object Folder and select NoAccess Policy and right click then edit
- To remove Control Panel from the student start menu, select User Configuration > Policies > Administrative Template > Control Panel
- Double-click on "Prohibit access to the Control Panel and PC settings" and select Enabled to enable restriction and click Apply an click OK.
- THIS DISABLES IT FOR GLOBAL, to enable for ITSupportStaff:
  - In Global Policy Objects folder, click on NoAccess Policy and select delegation tab on the right windows, then click advanced
  - Click Add and search for ITSupportStaffUsers group, then in permissions for this group selesct Deny on Apply group policy permission.
  - Click Apply and a warning will appear, click OK and click the next OK.
  - This should enable ITSupportUsers group to access control panel and registry settings.

Requirement: Shared folders are maintained in the file server. Two folders "Consultant-Shared" and "SupportStaff-Documents" needs to be maintained where Consultants and General Support staff members have read and write access to the folders respectively. Also, the shared folders must be mapped as network drives to be easily accessible for users when they log in:

- First we need a server, to create a server:
    o In server manager click configure this local server
    o Click on the computer name and change computer name and workgroup to: ATEConsult-Server, and then the workgroup name to: ATEConsult
    o Install DHCP server role, using server manager
    o Click Add roles and features, click next
    o Select Role-based or feature-based installation and click next
    o Select ATEConsult-Server to install and click next
    o Click next and select DHCP server and you will be prompted to asked whether you require management tools for DHCP Server management. Ensure that you have Include management tools check box selected and click Add Features button
    o Click Next and Leave the defaults for Select Features windows and click Next, Then click Next
    o Select Restart the designation server automatically if required box and click Yes
    o Click Install in the Confirm installation selections. This will start installing the DHCP Server role
- To create the folders open server manager > File and storage services > shares in right pane
- In shares, right click and select New Share
- Select C:\ Drive as location for the shared folder and click Next
- Enter Consultant-Shared as the name and click Next
- Leave the defaults for the configure share settings window and click next
- In permissions configs, you want to provide read and write by:
    o Click customize perms, click disable inheritance to permission inheritance then select convert inherited permissions into explicit permissions on this object
    o Remove Users group from all perms to disallow others access to this shared folder
    o Click Add and select ConsultantUsers and provide read and write permissions to it, leave default permissions for creator, administrator and SYSTEM security principles
    o Click OK, Apply and OK
- Click Next and then click Create to create the shared folder
- Finally click Close
- Now to create the SupportStaff-Documents, follow the same instructions but change the names and Users group according to the ITSupportStaffUsers group.

- To map these, create a GPO called NetworkDrivesMappings and link it to this domain
- Click on NetworkDrivesMappings GPO in Group Policy Management window. Click on Delegation tab and then select Advanced
- In Advanced select Authenticated Users and uncheck Apply group policy and click OK
- Then you should add any users or computers to a security group that you need this applied, and add that group to the delegation with read and apply rights
- Next add ConsultantUsers and ITSupportStaffUsers group to Security Filtering.
- Right-click on NetworkDrivesMappings GPO and select Edit… to edit the NetworkDrivesMappings GPO.
- Select User Configuration > Preferences > Windows Settings > Drive Maps
- To create a Drive Map
  o Right-click on Drive Maps > New > Mapped Drive to create a new mapped drive
  o In the New Drive Properties window, fill the following
    ▪ Action: Create
    ▪ Location: \\ATEConsult-Server\Consultant-Shared
    ▪ Drive Letter > Use: S
    ▪ Hide/Show this drive: Show this drive
  o Create another Drive Map in the NetworkDrivesMappings GPO for SupportStaff-Documents folder with the following information.
    ▪ Action: Create
    ▪ Location: \\ATEConsult-Server\SupportStaff-Documents
    ▪ Drive Letter > Use: T
    ▪ Hide/Show this drive: Show this drive

Requirement: Directors have permissions of all resources of staff and customers except IT Support staff (i.e. Consultants, Customers and General Support staff):

In server manager go: Tools > Active Directory Users and Computers. Then in the ATEConsult domain we want to open Consultants OU and right click ConsultantResources > properties > Members > add… > and add "Directors" > Click OK, Click Apply, Click OK.

Then do that again for AdminStaff OU, ITSupportStaff OU and Customers OU.

Requirement: The IT Support Staff are able to manage user accounts and reset passwords for Directors, Consultants, Clients and General Support Staff:

Delegate Control over Directors OU, Consultants OU, AdminStaff OU and Customers OU to ITSupportStaffUsers global group for resetting passwords.