|  |  |
| --- | --- |
| **Networking Infrastructure**  Diploma in CSF/IT  Year 2 (2020/21) Semester 3 | Week 13 |
| **1** hour |
| **Windows Server 2016 OU, User and Group Administration (CA2 5% Group)** | |

## A. Objective

To create and configure organization unit (OU), user and group objects in Active Directory based on an organizational structure.

**B. Resources**

* Machine with Microsoft Windows Server 2016 domain controller (VMware)
* Machine with Microsoft Windows 10 Pro (VMware)

### C. Lab Setup

* Windows Server 2016 Server as a **domain controller** with Domain Name: NI**T**.com where **T** is the team number.
* Form teams of 3 to 4 students. Each team will work on 1 server and at least 1 client.
* Windows 10 client to login to the domain (Windows 2016 domain controller). It is a member of the NI**T**.com domain.

Settings should be as follows:

* Windows Server 2016 Server as a **domain controller** with the following settings:

|  |  |
| --- | --- |
| TCP/IP Domain Name | NI**T**.com, T is the team number 2-9  (to be assigned by tutor) |
| Administrator Password | **p@ssw0rd** |
| Static IP address /Subnet mask | **For Server,** WinSvr2016**:**  172.16.**T**.1  **For Client PC,** NI**T**client**101**  172.16.**T**.**101**  **Subnet mask for all machines: 255.255.255.0** |

**On the PC where your Windows 2016 Server is installed on Week 11**

Start VMware Workstation Player or Pro program.

Locate and start the Windows 2016 server VM (WinSvr2016-**X** where **X** is your tutorial group number) that you have created in Week 11 practical lesson.

Login with username “administrator” and password “**p@ssw0rd**”.

**On the Windows Client machine (NITClient101):**

Login with username “administrator” and password “**p@ssw0rd**”.

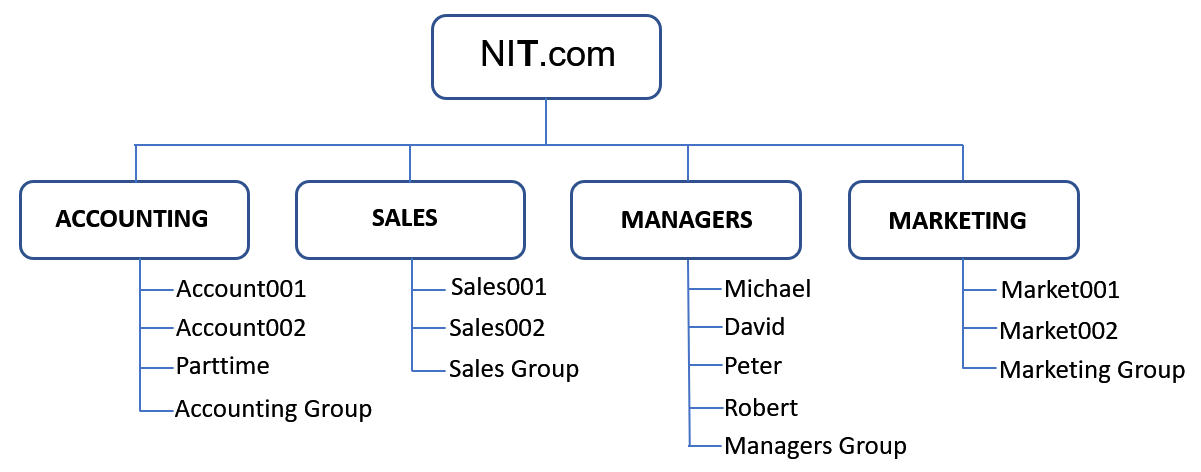
**NOTE:**

**You can logon to your AD domain server to create all users, groups or OU in this practical.**

**You can also use RSAT on Windows 10 client to create the users, group and OU in this practical.**

**D. Tasks**

The practical will lead you to create the users and group accounts based on the organizational structure as follows:



There are **4** departments (OU) in the company: **MANAGERS, ACCOUNTING**, **SALES** and **MARKETING** OU.

**Here are the user details for the 4 OUs:**

The **MANAGERS** OU consists of **4** managers as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **First Name** | **Title** | **Logon Name** | **Password** | **Access Times/Work Hours** | **Position Ends** |
| Michael | CEO | Michael | p@ssw0rd | No restriction | - |
| Robert | Sales Manager | Robert | p@ssw0rd | No restriction | - |
| Peter | Marketing Manager | Peter | p@ssw0rd | No restriction | - |
| David | Accounting Manager | David | p@ssw0rd | No restriction | - |

**In addition: Michael** will have **administrator’s rights**.

**ACCOUNTING** OU consists of **3** users as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **First Name** | **Logon Name** | **Password** | **Access Times** |
| Account001 | Account001 | p@ssw0rd | No restriction |
| Account002 | Account002 | p@ssw0rd | No restriction |

There is a **part-time** user named **Parttime** who works only on **Monday**, **Wednesday** and **Friday**. His contract with the company expires on **31/07/2020**. He is attached to the **Accounting department**.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **First Name** | **Title** | **Logon Name** | **Password** | **Access Times/Work Hours** | **Position Ends** |
| Parttime | Temp | Parttime | p@ssw0rd | Odd days only,  7am to 7pm | 31/07/2020 |

**SALES** OU consists of **2** users as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **First Name** | **Logon Name** | **Password** | **Access Times** |
| Sales001 | Sales001 | p@ssw0rd | No restriction |
| Sales002 | Sales002 | p@ssw0rd | No restriction |

**MARKETING** OU consists of **2** users as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **First Name** | **Logon Name** | **Password** | **Access Times** |
| Market001 | Market001 | p@ssw0rd | No restriction |
| Market002 | Market002 | p@ssw0rd | No restriction |

The steps to complete the above tasks are shown and explained in the following pages. You are to study the steps and complete the above tasks.

**E. Creating Organizational Units (OUs) named ACCOUNTING, MANAGERS, MARKETING and SALES,**

In this practical we will need to create **four** OUs(**MANAGERS, ACCOUNTING**, **SALES** and **MARKETING**) to represent the different departments.

To create the Organization Unit, follow the steps below.

1. Log into the Windows Server 2016 Server as “**administrator***”* to your NI**T**.com domain.
2. In the Server Manager Dashboard, at the tool bar, click the Tools tab then select **"Active Directory Users and Computers"**.
3. Right click on your created **“Domain” object**, which is NI**T**.com. Select **New** → **Organizational Unit**.
4. In the **Name** box, type a name for the new object (i.e. **MANAGERS**), and then click **OK**.
5. An icon with the appropriate name is created and inserted in the list.

**Repeat the above steps to create 3** otherOUs**: ACCOUNTING, SALES , MARKETING**.

**F. Creating User Accounts**

Create user accounts under their respective OU. Please note that all the Sales user accounts will be created under the **SALES** OU. All the Marketing user accounts will be under **MARKETING** OU…etc. to allow for **easier administration**.

1. Right click on your **SALES** OU and Select **New** → **User**.
2. In the next dialog, set the **First name** and their **log-on name** for the user to be created based on the tables given on pages 2 and 3.
3. After clicking **Next** you are presented with the password-settings screen.  Set the user's password and **Uncheck** **"User must change password at next logon".**
4. In the next dialog, we get a summary of the user to be created.  Click "**Finish**" and the user has been created.
5. Next repeat the steps to **create all the user accounts in their respective OUs** as outlined in the organizational structure on pages 2 and 3.

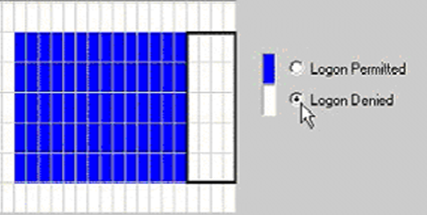
**G. Setting User Accounts Properties**

**(i) Configuring Logon Hours**

Set the **logon hours for all users** as stated in the requirements on pages 2 and 3.

1. To set user’s logon hours, **right click** on the **specific users** and select **Properties**. Select the **Account Tab**. Click on the **Logon Hours button** to restrict the logon hours.
2. Set the valid and invalid logon hours using the **Logon Hours** dialog box. In this box each hour of the day or night is a field that can be turned on and off. To change the setting for an hour, click it. Then select either the **Logon Permitted** or **Logon Denied** option button.

* Hours that are allowed are filled in with a dark bar.
* Hours that are disallowed are blank.



Set the logon hours for all user(s) based on the stated requirements. Note: You can also restrict the computers that the user(s) can use to logon by clicking on the Log on To button.

**(ii) Configuring Account Expiration Date (for partime users)**

1. To set Parttime’s account expiry date, **right click** on Parttime’s user account and select **Properties**. Select the **Account Tab**.

Under **Account expires**, select the **End of:** radio button.

In the date drop down menu box, select the drop down arrow. A calendar window will appear showing the current date. Use the calendar to select the date the account is to expire on by using the forward arrow (right side arrow) to select a future month, and then clicking on the desired day within the calendar. You can set the account to expire by a certain date (e.g. 31/07/2020). Click the **Apply** button and click **OK** to close user's **Properties** dialog box.

**Answers for E to G: Creating OUs and User Accounts**

Paste your captured screens to **Answers for E to G: Creating OUs and User Accounts** in **CA2 Answer Document** for the following tasks**:**

1. **Task 1 - Are all OUs created correctly?**
2. **Task 2 -** **Are all user account(s) with restrictions (if any) created correctly in their respective OU?**

(c) **Task 3 –** **How Michael is assigned administrator’s rights?**

**H. Creating Group Accounts**

The main purpose of a group is to simplify administration by allowing permissions to be assigned to a collection of users instead of individual users. A group can **contain user accounts, computer accounts, or contacts, as its members.**  A group can also contain other groups.

Next, we will create 4 user groups: Managers Group, Accounting Group, Sales Group Marketing Group and under **MANAGERS** OU, **ACCOUNTING** OU, **SALES** OU and **MARKETING** OU respectively.

1. To create an Accounting Group, right click on the **ACCOUNTING** OU(or object in which you want to add a new group) and point to **New** and then click **Group.**
2. Type the name of the new group. By default, the name you type is also entered as the pre-Windows 2000 name of the new group. In **Group scope**, choose **Global** and in **Group type**, choose **Security** and then click **OK.**

3. The next step is to **add the users to the correct groups**. To add all the Accounting users to the Accounting Group, right click on the Accounting Group and then click **Properties.**

4. Click the **Members** tab, and then do one of the following:

* To add a member to a group, click **Add**. In "**Enter the object names to select" box**, type the name of the user, group, or computer that you want to add to the group, (e.g. **Account001**). Click the “**Check Names**” box to verify the name is valid. Click **OK**.
* To remove a member from a group, click the member you want to remove, and then click **Remove**.

Add all the Accounting users **including Accounting manager’s account** into the Accounting Group.

5. **Repeat the above steps** to add other users (Managers, Marketing and Sales) into the correct groups (Managers Group, Marketing Group and Sales Group).

**I. Testing User Accounts**

1. Test the created user accounts by using the **Windows 10 client** to log into the Windows domain using the created accounts.
2. Test on the **configured log-on hours**:

Change the computer time on the Windows 2016 domain controller to an invalid logon time and try to log in with the Windows 10 client using a suitable user account.

1. Test on the configured **parttime’s account expiration**:

Set the computer time on the Windows 2016 domain controller to a date that is beyond the expiry date and try to log in.

You are to **demonstrate** to your tutor on the above tasks by capturing the appropriate screenshots.

**Answers for I. Testing User Accounts**

Paste your captured screens to **I. Testing User Accounts** in **CA2 Answer Document for the following tasks:**

(a) **Task 1 - Creation and testing on the users account. Is your user, “Market001” able to** **to log in to domain?** Open a powershell and type the command, “whoami” to indicate who is the user.

(b) **Task 2 - Testing on the user’s configured log-on hours.**

(c) **Task 3 - Testing on the configured Parttime’s account expiration.**

**J. OU Delegation**

One of the benefits of using OUs is delegation. When you establish OU's and delegation, a local administrator or power user can reset the password and leave you to get on with more interesting work.  You decide which administrators have control over which tasks.  For the more experienced, you could allow them to create user accounts for new joiners, and disable accounts for those who resigned.

**For this practical, we will delegate the tasks of resetting passwords, disabling accounts and creating accounts to the respective departmental manager.** For example, Sales manager will have power of create account, delete account and resetting passwords for users under the **SALES** OU.

The steps in OU delegation are as follows:

1. Right click on **SALES** OU and then click **Delegate control**.
2. The Delegation of Control wizard appears. Click **Next**.
3. On the **Users or Groups** page, click **Add**, and enter **Robert** (since **Robert** is the Sales Manager that we want to delegate the tasks to under **SALES** OU) then click **OK**. Click **Next** to continue.
4. On the **Tasks to Delegate** page, under Delegate the following common tasks, select:

- (**Create, delete, and manage user accounts**),

**- (Reset user passwords and force password change at next logon)** and

**-** **(Create, delete and manage groups)**.

Click **Next** to continue.

1. Click **Finish**.

**Testing the Delegation**

1. Log in to the NI**T**.com domain from your Windows 10 client using “**Robert**” account.
2. In Active Directory Users and Computer Tool (RSAT on Windows 10):

Assuming a Sales user (i.e Sales001) has forgotten his password, **right click** this user account under **SALES** OU and reset the password to **Password123**.

Logout Robert from the Windows 10 client and log to the NIT.com domain using this Sales user (i.e. Sales001) account with the password, **Password123**.

**Answers for J. Testing the Delegation**

Paste your captured screens to **J. Testing the Delegation** in **CA2 Answer Document** for the following tasks:

(a) **Task 1 - Is Robert able to perform certain tasks for Sales users (as delegated)?**

Using **Robert’s account**, are you able to reset password of other user accounts in **SALES** OU? Open a PowerShell and type the command, “whoami” to indicate who is the user.

(b) **Task 2 - Is Robert able to perform certain tasks for Accounting users?**

Using **Robert’s account**, are you able to reset password for user accounts in other OU such as **ACCOUNTING**? Open a PowerShell and type the command, “whoami” to indicate who is the user.

**\*\*\*\* End of Practical \*\*\*\***

**Appendix A: Reference Materials**

**OU (Organizational Units**

**OUs are Active Directory objects that serve as containers for other objects**. For example, you can create an OU named “**ACCOUNTING**” and then place Active Directory objects such as Accounting users, computers and groups within this OU. This would allow administrators to easily organize and manage AD objects.

The benefit of OUs is that they allow you to classify users by department or site.  There are two advantages of this arrangement:

* You can **delegate** within organizational units. For example, you can give managers complete controls of users their own department. With this arrangement, managers can create new users, groups and computer objects but only in their own OU.
* You can create **different Group Policies for each OU**. Each department designated by different OU can be assigned different group policy.

****Group Types****

* **Security Groups** – Security Groups are used to gather a specific set of users for the specific reason of assigning access rights and permissions via the group rather than individually to each user object. Used for assigning permissions for directory objects and resources such as shared folders and printers. Security groups are also used for assigning right to users.
* **Distribution Groups** – Used for creating e-mail distribution lists (i.e. for MS Exchange Server). It allows a user to send e-mail to all the members by using a single address. Distribution groups are **NOT** used to assign rights and permissions.

###### Group Scope

* **Domain local Group** – Used to assign permissions to resources only within the domain in which it is created.
* **Global Group** – Global groups can only contain members from a single domain. However, global groups can be assigned permissions to resources located in any domain within an Active Directory forest. Used when a group of users that all reside in a single domain require access to resources in other domains.
* **Universal Group** - Most inclusive of all group scopes. Can contain members from multiple domains. Can be granted permissions to resources that are located in any domain of an Active Directory forest.