Module 3

Managing Active Directory Domain Services Objects

Module Overview

AD DS can help you manage your network more effectively in many ways. For instance, it allows you to manage user and computer accounts as part of groups instead of managing one account at a time. It also provides ways to delegate administrative tasks to various people to help you distribute workloads efficiently.

Managing computer identities is becoming more and more complex as more employees bring their own devices into the workplace. As bring your own device (BYOD) programs expand you will be managing computer accounts that run on many types of personal devices which in turn are running various operating systems. AD DS has many features that can make that easier.

This module describes how to manage user accounts and computer accounts, including how to manage BYOD programs. It covers how to manage an enterprise network by managing groups, instead of managing individual identities, and how to delegate administrative tasks to designated users or groups to ensure that enterprise administration is efficient and effective.

Managing User Accounts

A user object in AD DS is far more than just properties related to the user's security identity, or account. It is the cornerstone of identity and access in AD DS. Therefore, consistent, efficient, and secure processes regarding the administration of user accounts are the cornerstone of enterprise security management.

Creating User Accounts

In AD DS, all users that require access to network resources must be configured with a user account. With this user account, users can authenticate to the AD DS domain and receive access to network resources.

In Windows Server 2012, a *user account* is an object that contains all of the information that defines a user. A user account includes the user name, user password, and group memberships. A user account also contains many other settings that you can configure based upon your organizational requirements.

Creating User Profiles

When users sign out, their desktop and app settings are saved to a subfolder that is created in the C:\Users folder on the local hard disk that matches their user name. This folder contains their user profile. Within this folder, subfolders contain documents and settings that represent the user's profile, including Documents, Videos, Pictures, and Downloads.

Using Group Policy to Manage Profiles

As an alternative to using the individual user account settings, you can also use GPOs to manage these settings. You can configure Folder Redirection settings by using the Group Policy Management Editor to open a GPO for editing, and then navigating to the User Configuration\Policies\Windows Settings node.

These settings contain the sub-nodes in the following table.

Sub-nodes in the Windows Settings node		
• AppData (Roaming) • Desktop • Start Menu • Document	• Pictures • Music • Videos • Favorites • Contacts	• Downloads • Links • Searches • Saved Games

Module 3

Lab: Managing Active Directory Domain Services Objects

Exercise 1: Delegating Administration for a Branch Office

▶ Task 1: Delegate administration for Branch Administrators

1. Switch to LON-DC1.
2. In Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
3. In Active Directory Users and Computers, click **Adatum.com**.
4. Right-click **Adatum.com**, point to **New**, and then click **Organizational Unit**.
5. In the **New Object – Organizational Unit** dialog box, in **Name**, type **Branch Office 1**, and then click **OK**.
6. Right-click **Branch Office 1**, point to **New**, and then click **Group**.
7. In the **New Object – Group** dialog box, in **Group name**, type **Branch 1 Help Desk**, and then click **OK**.
8. Repeat steps 6 and 7 using **Branch 1 Administrators** as the new group name.
9. Repeat steps 6 and 7 using **Branch 1 Users** as the new group name.
10. In the navigation pane, click **IT**.

11. In the details pane, right-click **Holly Dickson**, and then click **Move**.
12. In the **Move** dialog box, click **Branch Office 1**, and then click **OK**.
13. Repeat steps 10 through 12 for the following OU's and users:
    - **Development** and the user **Bart Duncan**
    - **Managers** and the user **Ed Meadows**
    - **Marketing** and the user **Connie Vrettos**
    - **Research** and the user **Barbara Zighetti**
    - **Sales** and the user **Arlene Huff**
14. In the navigation pane, click **Computers**.
15. In the details pane, right-click **LON-CL1**, and then click **Move**.
16. In the **Move** dialog box, click **Branch Office 1**, and then click **OK**.
17. Switch to LON-CL1.
18. Point the mouse at the lower-right corner of the screen, and then click **Settings**.
19. Click **Power**, and then click **Restart**.
20. When the computer has restarted, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
21. Switch to LON-DC1.
22. If necessary, switch to **Active Directory Users and Computers**.
23. In the navigation pane, right-click **Branch Office 1**, click **Delegate Control**, and then click **Next**.

24. On the **Users or Groups** page, click **Add**.
25. In the **Select Users, Computers, or Groups** dialog box, in **Enter the object names to select (examples)**, type **Branch 1 Administrators**, and then click **OK**.
26. On the **Users or Groups** page, click **Next**.
27. On the **Tasks to Delegate** page, in the **Delegate the following common tasks** list, select the following check boxes, and then click **Next**:
    - **Create, delete, and manage user accounts**
    - **Reset user passwords and force password change at next logon**
    - **Read all user information**
    - **Create, delete and manage groups**
    - **Modify the membership of a group**
    - **Manage Group Policy links**
28. On the **Completing the Delegation of Control Wizard** page, click **Finish**.
29. In the navigation pane, right-click **Branch Office 1**, click **Delegate Control**, and then click **Next**.
30. On the **Users or Groups** page, click **Add**.

31. In the **Select Users, Computers, or Groups** dialog box, in **Enter the object names to select (examples)**, type **Branch 1 Administrators**, and then click **OK**.
32. On the **Users or Groups** page, click **Next**.
33. On the **Tasks to Delegate** page, click **Create a custom task to delegate**, and then click **Next**.
34. On the **Active Directory Object Type** page, select **Only the following objects in the folder**, select the following check boxes, and then click **Next**:
    - **Computer objects**
    - **Create selected objects in this folder**
    - **Delete selected objects in this folder**
35. On the **Permissions** page, select both **General** and **Full Control**, and then click **Next**.
36. On the **Completing the Delegation of Control Wizard** page, click **Finish**.

▶ Task 2: Delegate a user administrator for the Branch Office Help Desk

1. On LON-DC1, in the navigation pane, right-click **Branch Office 1**, click **Delegate Control**, and then click **Next**.
2. On the **Users or Groups** page, click **Add**.
3. In the **Select Users, Computers, or Groups** dialog box, in **Enter the object names to select (examples)**, type **Branch 1 Help Desk**, and then click **OK**.
4. On the **Users or Groups** page, click **Next**.
5. On the **Tasks to Delegate** page, in the **Delegate the following common tasks** list, select the following check boxes, and then click **Next**:
   - **Reset user passwords and force password change at next logon**
   - **Read all user information**
   - **Modify the membership of a group**
6. On the **Completing the Delegation of Control Wizard** page, click **Finish**.

▶ Task 3: Add a member to the Branch Administrators

1. On LON-DC1, in the navigation pane, click **Branch Office 1**.
2. In the details pane, right-click **Holly Dickson**, and then click **Add to a group**.
3. In the **Select Groups** dialog box, in **Enter the object names to select (examples)**, type **Branch 1 Administrators**, and then click **OK**.
4. In the **Active Directory Domain Services** dialog box, click **OK**.
5. In the details pane, right-click **Branch 1 Administrators**, and then click **Add to a group**.
6. In the **Select Groups** dialog box, in **Enter the object names to select (examples)**, type **Server Operators**, and then click **OK**.
7. In the **Active Directory Domain Services** dialog box, click **OK**.
8. On your host computer, in the 20410C-LON-DC1 window, on the **Action** menu, click **Ctrl+Alt+Delete**.
9. On LON-DC1, click **Sign out**.
10. Sign in to LON-DC1 as **Adatum\Holly** with the password **Pa$$w0rd**.

    You can sign in locally at a domain controller because Holly belongs indirectly to the Server Operators domain local group.

11. On the taskbar, click the **Server Manager** icon.
12. In the **User Account Control** dialog box, in **User name**, type **Holly**. In **Password**, type **Pa$$w0rd**, and then click **Yes**.
13. In Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
14. In Active Directory Users and Computers, expand **Adatum.com**.
15. In the navigation pane, click **Sales**.
16. In the details pane, right-click **Aaren Ekelund**, and then click **Delete**.
17. Click **Yes** to confirm.
18. Click **OK** to acknowledge that you do not have permissions to perform this task.
19. In the navigation pane, click **Branch Office 1**.
20. In the details pane, right-click **Ed Meadows**, and then click **Delete**.
21. Click **Yes** to confirm.

    You are successful because you have the required permissions.

▶ Task 4: Add a member to the Branch Help Desk group

1. On LON-DC1, in the details pane, right-click **Bart Duncan**, and then click **Add to a group**.
2. In the **Select Groups** dialog box, in **Enter the object names to select (examples)**, type **Branch 1 Help Desk**, and then click **OK**.
3. In the **Active Directory Domain Services** dialog box, click **OK**.
4. Close Active Directory Users and Computers.
5. Close Server Manager.
6. On the desktop, click **Server Manager**. In the **User Account Control** dialog box, in **User name**, type **Adatum\Administrator**.

7. In **Password**, type **Pa$$w0rd**, and then click **Yes**.

Note: To modify the Server Operators membership list, you must have permissions beyond those available to the Branch 1 Administrators group.

8. In Server Manager, click **Tools**.
9. In the Tools list, click **Active Directory Users and Computers**.
10. In Active Directory Users and Computers, expand **Adatum.com**.
11. In the navigation pane, click **Branch Office 1**.
12. In the details pane, right-click **Branch 1 Help Desk**, and then click **Add to a group**.
13. In the **Select Groups** dialog box, in **Enter the object names to select (examples)**, type **Server Operators**, and then click **OK**.
14. In the **Active Directory Domain Services** dialog box, click **OK**.
15. On your host computer, in the 20410C-LON-DC1 window, on the **Action** menu, click **Ctrl+Alt+Delete**.

16. On LON-DC1, click **Sign out**.
17. Sign in as **Adatum\Bart** with the password **Pa$$w0rd**.

    You can sign in locally at a domain controller because Bart belongs indirectly to the Server Operators domain local group.
18. On the desktop, click **Server Manager**.
19. In the **User Account Control** dialog box, in **User name**, type **Bart**. In **Password**, type **Pa$$w0rd**, and then click **Yes**.
20. In Server Manager, click **Tools**.
21. Click **Active Directory Users and Computers**.
22. In Active Directory Users and Computers, expand **Adatum.com**.
23. In the navigation pane, click **Branch Office 1**.
24. In the details pane, right-click **Connie Vrettos**, and then click **Delete**.
25. Click **Yes** to confirm.

    You are unsuccessful because Bart lacks the required permissions.
26. Click **OK**.
27. Right-click **Connie Vrettos**, and then click **Reset Password**.
28. In the **Reset Password** dialog box, in **New password** and **Confirm password**, type **Pa$$w0rd**, and then click **OK**.
29. Click **OK** to confirm the successful password reset.
30. On your host computer, in the 20410C-LON-DC1 window, on the **Action** menu, click **Ctrl+Alt+Delete**.
31. On LON-DC1, click **Sign out**.
32. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa$$w0rd**.

Exercise 2: Creating and Configuring User Accounts in AD DS

▶ Task 1: Create a user template for the branch office

1. On LON-DC1, on the taskbar, click the **File Explorer** icon.
2. Double-click **Local Disk (C:)**.
3. On the menu, click **Home**, and then click **New folder**.
4. Type **branch1-userdata**, and then press **Enter**.
5. Right-click **branch1-userdata**, and then click **Properties**.
6. In the **branch1-userdata Properties** dialog box, on the **Sharing** tab, click **Advanced Sharing**.
7. Select **Share this folder**, and then click **Permissions**.
8. In the **Permissions for branch1-userdata** dialog box, for the **Full Control** permission select the **Allow** check box, and then click **OK**.
9. In the **Advanced Sharing** dialog box, click **OK**, and then in the **branch1-userdata Properties** dialog box, click **Close**.
10. In Server Manager, click **Tools**, and then click **Active Directory Users and Computers**, and then expand **Adatum.com**.
11. Right-click **Branch Office1**, point to **New**, and then click **User**.
12. In the **New Object – User** dialog box, in **Full name**, type **_Branch_template**.
13. In **User logon name**, type **_Branch_template**, and then click **Next**.
14. In **Password** and **Confirm password**, type **Pa$$w0rd**.
15. Select the **Account is disabled** check box, and then click **Next**.
16. Click **Finish**.

▶ Task 2: Configure the template settings

1. On LON-DC1, from within the **Branch Office 1** OU, right-click **_Branch_template**, and then click **Properties**.
2. In the **_Branch_template Properties** dialog box, on the **Address** tab, in **City**, type **Slough**.
3. Click the **Member Of** tab, and then click **Add**.
4. In the **Select Groups** dialog box, in **Enter the object names to select (examples)**, type **Branch 1 Users**, and then click **OK**.
5. Click the **Profile** tab.
6. Under Home folder, click **Connect**, and in the **To** box, type **\\lon-dc1\branch1-userdata\%username%**.
7. Click **Apply**, and then click **OK**.

▶ Task 3: Create a new user for the branch office, based on the template

1. On LON-DC1, right-click **_Branch_template**, and then click **Copy**.
2. In the **Copy Object – User** dialog box, in **First name**, type **Ed**.
3. In **Last name**, type **Meadows**.
4. In **User logon name**, type **Ed**, and then click **Next**.

5. In **Password** and **Confirm password**, type **Pa$$w0rd**.
6. Clear the **User must change password at next logon** check box.
7. Clear the **Account is disabled** check box, and then click **Next**.
8. Click **Finish**.
9. Right-click **Ed Meadows**, and then click **Properties**.
10. In the **Ed Meadows Properties** dialog box, on the **Address** tab, notice that the City is already configured.
11. Click the **Profile** tab.

    Notice that the home folder location is already configured.
12. Click the **Member Of** tab.

    Notice that Ed belongs to the Branch 1 Users group. Click **OK**.
13. On your host computer, in the 20410C-LON-DC1 window, on the **Action** menu, click **Ctrl+Alt+Delete**.
14. On LON-DC1, click **Sign out**.

▶ Task 4: Sign in as a user to test account settings

1. Switch to LON-CL1.
2. On your host computer, in the 20410C-LON-CL1 window, on the menu, click **Ctrl+Alt+Delete**.
3. On LON-CL1, click **Switch User**.
4. Sign in to LON-CL1 as **Adatum\Ed** with the password **Pa$$w0rd**.
5. On the Start screen, type **File Explorer** and then press **Enter**.
6. Verify that drive Z is present.
7. Double-click **Ed (\\lon-dc1\branch1-userdata) (Z:)**.
8. If you receive no errors, you have been successful.
9. On your host computer, in the 20410C-LON-CL1 window, on the **Action** menu, click **Ctrl+Alt+Delete**.
10. On LON-CL1, click **Sign out**.

Results: After completing this exercise, you will have successfully created and tested a user account created from a template.

Exercise 3: Managing Computer Objects in AD DS

▶ Task 1: Reset a computer account

1. On LON-DC1, sign in as **Adatum\Holly** with the password **Pa$$w0rd**.
2. On the taskbar, click the **Server Manager** icon.
3. In the **User Account Control** dialog box, in **User name**, type **Holly**.
4. In **Password**, type **Pa$$w0rd**, and then click **Yes**.
5. In Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
6. In Active Directory Users and Computers, expand **Adatum.com**.
7. In the navigation pane, click **Branch Office 1**.
8. In the details pane, right-click **LON-CL1**, and then click **Reset Account**.
9. In the **Active Directory Domain Services** dialog box, click **Yes**, and then click **OK**.

▶ Task 2: Observe the behavior when a client logs on

1. Switch to LON-CL1.
2. Sign in as **Adatum\Ed** with the password **Pa$$w0rd**.

   A message appears stating that **The trust relationship between this workstation and the primary domain failed**.
3. Click **OK**.

▶ Task 3: Rejoin the domain to reconnect the computer account

1. On LON-CL1 click the back arrow and switch to **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the Start screen, right-click the display, click **All apps**, and in the Apps list, click **Control Panel**.
3. In Control Panel, in the **View by** list, click **Large icons**, and then click **System**.
4. In the navigation list, click **Advanced system settings**.
5. In System Properties, click the **Computer Name** tab, and then click **Network ID**.
6. On the **Select the option that describes your network** page, click **Next**.
7. On the **Is your company network on a domain?** page, click **Next**.
8. On the **You will need the following information** page, click **Next**.
9. On the **Type your user name, password, and domain name for your domain account** page, in **Password**, type **Pa$$w0rd**. Leave the other boxes completed, and then click **Next**.
10. In the **User Account and Domain Information** dialog box, click **Yes**.
11. On the **Do you want to enable a domain user account on this computer?** page, click **Do not add a domain user account**, and then click **Next**.
12. Click **Finish**, and then click **OK**.

13. In the **Microsoft Windows** dialog box, click **Restart Now**.
14. Sign in as **Adatum\Ed** with the password **Pa$$w0rd**.

    You are successful because the computer had been successfully rejoined.

Results: After completing this exercise, you will have successfully reset a trust relationship.

▶ Prepare for the next module

When you have completed the lab, revert the virtual machines back to their initial state.

To do this, complete the following steps:

1. On the host computer, start Hyper-V® Manager.
2. In the **Virtual Machines** list, right-click **20410C-LON-CL1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for 20410C-LON-DC1.