Lab Report: 8.5.4 Clear the Browser Cache

Your Performance

Your Score: 7 of 7 (100%)

Pass Status: Pass

Elapsed Time: 1 minute

Required Score: 100%

Task Summary

✓ Don't preserve cookies and temporary files from your favorite websites

✓ Delete Temporary Internet Files

✓ Delete Cookies

✓ Delete History

✓ Delete Form data

✓ Delete Passwords

✓ Delete Tracking Protection, ActiveX Filtering and Do Not Track

Explanation

In this lab, your task is to delete all items from your Internet Explorer browser history, including:

- Temporary files
- Passwords
- Form data
- Cookies from your favorite websites
- ActiveX filtering data

Complete this lab as follows:

1. From the taskbar, select **Internet Explorer**.
2. Select the **Tools** icon: then select **Internet options**.
3. On the General tab, select **Delete**.
4. In Delete Browsing History, deselect **Preserve Favorites website data** to ensure that all cookies and temporary files are also deleted.
5. Select each ***type*** of browsing history you want to delete.
6. Click **Delete**.
7. Click **OK**.

Lab Report: 8.5.5 Configure IE Pop-up Blocker

Your Performance

Your Score: 3 of 3 (100%)

Pass Status: Pass

Elapsed Time: 2 minutes 26 seconds

Required Score: 100%

Task Summary

✓ Allow pop-ups from mybank.com

✓ Set the Pop-up Blocking level to High

✓ Set the Internet zone security level to High

Explanation

In this lab, you configure Internet Explorer settings as follows:

- Add **mybank.com** to the list of allowed sites for pop-ups.
- Set the pop-up blocking level to **High**.
- Set the security level for the Internet zone to **High**.

Complete this lab as follows:

1. From the taskbar, open **Internet Explorer**.
2. Configure the Pop-up Blocker settings as follows:
    a. Select the **Tools** icon; then select **Internet options**.
    b. Select the **Privacy** tab.
    c. Under Pop-up Blocker, select **Settings**.
    d. In the Address of website to allow field, enter **mybank.com**; then select **Add**.
    e. From the Blocking Level drop-down list, select **High: Block all pop-ups (Ctrl+Alt to override)**.
    f. Click **Close**.
    g. Click **Apply**.
3. Configure security zones as follows:
    a. In Internet Options, select the **Security** tab.
    b. In the Select a zone to view or change security settings field, make sure **Internet** is selected.
    c. Adjust the security level slider to **High**.
    d. Click **OK**.

Lab Report: 8.5.8 Enforce IE Settings Through GPO

Your Performance

Your Score: 5 of 5 (100%)
Elapsed Time: 9 minutes 33 seconds

Pass Status: Pass
Required Score: 100%

Task Summary

✓ Configure Internet Explorer GPO Settings Show Details

✓ Configure Internet Explorer>Internet Control Panel GPO Settings Show Details

✓ Configure Internet Explorer>Internet Control Panel>Security Page>Internet Zone GPO Settings Show Details

✓ Configure Internet Explorer>Internet Control Panel>Security Page>Restricted Sites Zone GPO Settings Show Details

✓ Configure Internet Explorer>Security Features GPO Settings Show Details

Explanation

In this lab, your task is to configure the following Internet Explorer policy settings in the WorkstationGPO:

Policy	Setting
Security Zones: Do not allow users to add/delete sites	Enabled
Security Zones: Do not allow users to change policies	Enabled
Turn on ActiveX Filtering	Enabled
Internet Control Panel > Prevent Ignoring Certificate Errors	Enabled
Internet Control Panel > Security Page > Internet Zone > Java permissions	Enabled: Disable Java
Internet Control Panel > Security Page > Internet Zone > Turn on Protected Mode	Enabled: Enable
Internet Control Panel > Security Page > Restricted Sites Zone > Allow File Downloads	Enabled: Disable
Internet Control Panel > Security Page > Restricted Sites Zone > Java permissions	Enabled: Disable Java
Internet Control Panel > Security Page > Restricted Sites Zone > Turn on Protected Mode	Enabled: Enable
Security Features > Object Caching Protection > Internet Explorer Processes	Enabled
Security Features > Protection From Zone Elevation > Internet Explorer Processes	Enabled
Security Features > Restrict ActiveX Install > Internet Explorer Processes	Enabled
Security Features > Restrict File Download > Internet Explorer Processes	Enabled

Complete this lab as follows:

1. From Server Manager, select **Tools** > **Group Policy Management**.
2. Expand **Forest: CorpNet.com** > **Domains** > **CorpNet.com** > **Group Policy Objects**.
3. Right-click **WorkstationGPO** and select **Edit**.
4. Under Computer Configuration, expand **Policies** > **Administrative Templates** > **Windows Components**.
5. Select **Internet Explorer**.
6. Browse to the ***policy*** you want to change.
7. In the right pane, double-click the ***policy***.
8. Configure the ***policy settings***.
9. Click **OK**.

10. Repeat steps 6–9 for each policy setting.

Lab Report: 8.5.9 Configure IE Preferences in a GPO

Your Performance

Your Score: 4 of 4 (100%)
Elapsed Time: 3 minutes 15 seconds

Pass Status: Pass
Required Score: 100%

Task Summary

- ✓ Create an Internet Settings policy Show Details
- ✓ Set Internet Explorer to start with the corporate intranet homepage Show Details
- ✓ Set the security level for the Local intranet zone to **Low**
- ✓ Prevent websites from requesting your physical location

Explanation

In this lab, you configure an Internet Explorer 10 policy with the following settings:

Tab	Setting	Value
General	Home page	www.corpnet.local
	Startup	Start with home page
Security	Zone: Local intranet	Low
Privacy	Location	Never allow websites to request your physical location

Complete this lab as follows:

1. From Server Manager, select **Tools > Group Policy Management**.
2. Expand **Forest: CorpNet.com > Domains > CorpNet.com > Group Policy Objects**.
3. Right-click **SalesGPO** and select **Edit**.
4. Under User Configuration, expand **Preferences > Control Panel Settings**.
5. Right-click **Internet Settings** and select **New > Internet Explorer 10**.
6. Under Home page, type the ***home page address***.
7. Under Startup, select **Start with home page**.
8. Select the **Security** tab.
9. Select **Local intranet**.
10. Move the slider down to **Low**.
11. Select the **Privacy** tab.
12. Select **Never allow websites to request your physical location**.
13. Click **OK**.

Lab Report: 8.6.6 Implement Application Whitelisting with AppLocker

Your Performance

Your Score: 3 of 3 (100%) Pass Status: Pass

Elapsed Time: 6 minutes 18 seconds Required Score: 100%

Task Summary

✓ Create the default rules Show Details

✓ Allow the Support group to run the call center software

✓ Configure a publisher rule to allow for future updates from the same vendor

Explanation

In this lab, you configure AppLocker in the default domain policy as follows:

- Create the default rules.
  - Allow all files located in the Program Files folder.
  - Allow all files located in the Windows folder.
- Allow the Support group to run the call center software found in **C:\CallCenter\CallStart.exe**.
- Configure a publisher rule to allow for future updates from the same vendor.

Complete this lab as follows:

1. From Server Manager, select **Tools** > **Group Policy Management**.
2. Expand **Forest: CorpNet.com** > **Domains** > **CorpNet.com**.
3. Right-click **Default Domain Policy** and select **Edit**.
4. Under Computer Configuration, expand **Policies** > **Windows Settings** > **Security Settings** > **Application Control Policies**.
5. Select **AppLocker**.
6. In the right pane, select **Configure rule enforcement**.
7. Under Executable rules, select **Configured**.
8. Make sure **Enforce rules** is selected in the drop-down list.
9. Click **OK**.
10. Configure a Publisher rule and allow the **Support** group to run the call center software as follows:
    a. In the left pane, expand **AppLocker**.
    b. Right-click **Executable Rules** and select **Create New Rule**.
    c. Click **Next**.
    d. Make sure **Allow** is selected; then click **Select**.
    e. Enter the ***name*** of the required group; then click **OK**.
    f. Click **Next**.
    g. Make sure **Publisher** is selected; then click **Next**.
    h. Select **Browse**.
    i. Browse to and select the ***executable file***.
    j. Select **Open**.
    k. Slide the pointer from File version to **Publisher**; then click **Next**.
    l. Click **Next**.
    m. Accept the ***default name*** and select **Create**.
    n. Click **Yes** to create the default rules now.
    o. Notice that the Publisher rule was created.

Lab Report: 8.6.8 Implement Data Execution Preventions (DEP)

Your Performance

Your Score: 3 of 3 (100%)

Pass Status: Pass

Elapsed Time: 3 minutes 24 seconds

Required Score: 100%

Task Summary

✓ Enable DEP for all programs and services

✓ Add AccountWizard as an execption for DEP

✓ Restart the computer to activate DEP

Explanation

In this lab, you perform the following tasks:

- Enable DEP for all files.
- Disable DEP for **C:\Program Files\AccountWizard\AccountWizard.exe**.
- Restart the computer to activate DEP.

Enable DEP in Advanced System Properties as follows:

1. Right-click **Start** and select **System**.
2. On the left, select **Advanced System Settings**.
3. Under Performance, select **Settings**.
4. Select the **Data Execution Prevention** tab.
5. Select **Turn on DEP for all programs and services except those I select**.
6. Select **Add**.
7. Browse to **C:\Program Files\AccountWizard**.
8. Select **AccountWizard.exe**.
9. Select **Open**.
10. Make sure the ***program*** that you added is selected; then click **OK**.
11. Click **OK** to confirm that a system restart is needed.
12. Click **OK** to close System Properties.
13. Click **Restart Now** to restart the computer and activate DEP.

Lab Report: 8.8.3 Create User Accounts

Your Performance

Your Score: 4 of 4 (100%) Pass Status: Pass

Elapsed Time: 5 minutes 54 seconds Required Score: 100%

Task Summary

- ✓ Create the Juan Suarez account Show Details
- ✓ Create the Susan Smith account Show Details
- ✓ Create the Borey Chan account Show Details
- ✓ Create the Mark Burnes account Show Details

Explanation

In this lab, you use Active Directory Users and Computers to create the following user accounts:

User	Job Role	User Name	OU
Juan Suarez	Marketing manager	jsuarez	Marketing\MarketingManagers
Susan Smith	permanent sales employee	ssmith	Sales\PermSales
Borey Chan	temporary sales employee	bchan	Sales\TempSales
Mark Burnes	Sales manager	mburnes	Sales\SalesManagers

Complete this lab as follows:

1. Create a domain user account as follows:
   a. From Server Manager, select **Tools > Active Directory Users and Computers**.
   b. Browse the Active Directory structure to the appropriate ***OU***.
   c. Right-click the ***OU*** and select **New > User**.
   d. Enter the following values for the new user:
      - ***First name***
      - ***Last name***
      - ***User logon name*** (this name is required; the user will use it to log on to the domain)

   e. Click **Next**.
   f. Enter the user account's initial ***password*** and confirm it.
   g. Make sure **User must change password at next logon** is selected; then click **Next**.
   h. Click **Finish** to create the object.
   i. Repeat steps 1b-1h to create the rest of the users.
2. Modify user account restrictions for the temporary sales employee as follows:
   a. In Active Directory Users and Computers, browse to the **Borey Chan** user account.
   b. Right-click **Borey Chan** and select **Properties**.
   c. Select the **Account** tab.
   d. Select **Logon hours**.
   e. In the Logon Hours dialog, select **Logon Denied** to clear the allowed logon hours. By default, logon is always permitted (every hour box is blue).
   f. Drag the mouse to select a ***time range***.
   g. Select **Logon Permitted** to allow logon.
   h. Click **OK**.

3. Under Account expires, select **End of**.
4. In the Date field, enter **12/31** of the current year.
5. Click **OK**.

Lab Report: 8.8.4 Manage User Accounts

Your Performance

Your Score: 5 of 5 (100%) Pass Status: Pass

Elapsed Time: 8 minutes 31 seconds Required Score: 100%

Task Summary

✓ Disable the Mark Woods user account

✓ Enable the Pat Benton user account

✓ Modify the Andrea Simmons user account Show Details

✓ Unlock the Mary Barnes user account Show Details

✓ Restrict Janice Rons and Tom Plask to use only the Support computer

Explanation

In this lab, you perform the following tasks:

- In the Accounting department, Mark Woods has been fired. Disable his account.
- In the Research-Dev department, Pat Benton is returning from maternity leave. Her account is disabled to prevent logon. Enable her account.
- Andrea Simmons in the Research-Dev department has recently married:
    - Rename the account **Andrea Socko**.
    - Change the last name to **Socko**.
    - Change the display name to **Andrea Socko**.
    - Change the user logon and the pre-Windows 2000 user logon name to **asocko**.
- In the Accounting department, Mary Barnes has forgotten her password, and now her account is locked:
    - Reset the password to **1234abcd$**.
    - Require a password change at the next logon.
    - Unlock the account.
- Allow all users in the Support OU to log on only to the Support computer. Do not restrict the users in the SupportManagers OU.

Complete this lab as follows:

1. Disable a user account as follows:
    a. From Server Manager on CorpDC, select **Tools > Active Directory Users and Computers**.
    b. Browse the Active Directory structure and select the **Accounting** OU.
    c. Right-click **Mark Woods** and select **Disable Account**.
    d. Click **OK** to apply the changes.
2. Enable a user account as follows:
    a. Select the **Research-Dev** OU.
    b. Right-click **Pat Benton** and select **Enable Account**.
    c. Click **OK**.
3. Rename the user account as follows:
    a. In the Research-Dev OU, right-click **Andrea Simmons** and select **Rename**.
    b. Enter **Andrea Socko**.
    c. Click outside the Name field to open the Rename User dialog.
    d. In the Last name field, enter **Socko**.
    e. In the Display name field, enter **Andrea Socko**.
    f. In the User logon name field, enter **asocko**.
    g. Verify that the pre-Windows 2000 user logon name is **asocko**.

   h. Click **OK**.

4. Unlock a user account as follows:
   a. In the Accounting OU, right-click **Mary Barnes** and select **Reset Password**.
   b. In the New password field, enter the **1234abcd$**.
   c. In the Confirm password field, enter **1234abcd$**.
   d. Make sure that **User must change password at next logon** is selected.
   e. Make sure that **Unlock the user's account** is selected.
   f. Click **OK**.
5. Configure user account restrictions as follows:
   a. Navigate to and select the **Support** OU.
   b. Press **Ctrl** and select both the **Tom Plack** and **Janice Rons** users to edit multiple users at the same time.

      In Safari, press **Command** and select each user.

   c. Right-click the ***user accounts*** and select **Properties**.
   d. Select the **Account** tab.
   e. Mark **Computer restrictions**.
   f. Select **Log on to**.
   g. Select **The following computers**.
   h. In the Computer name field, enter **Support**; then select **Add**.
   i. Click **OK**.
6. Click **OK**.

Lab Report: 8.8.6 Create a Group

Your Performance

Your Score: 2 of 2 (100%) Pass Status: Pass

Elapsed Time: 6 minutes 23 seconds Required Score: 100%

Task Summary

✓ Create a security group named Managers in the Users container

✓ Make users members of the Managers group Show Details

Explanation

In this lab, you use Active Directory Users and Computers to complete the following tasks on the CorpDC server:

- In the Users container, create a group named **Managers**.
  - Under group scope, select **Global**.
  - Under the group type, select **Security**.
- Make the following users members of the Managers group:
  - **Mark Woods** in the Accounting OU
  - **Pat Benton** in the Research-Dev OU
  - **Juan Suarez** in the Marketing\MarketingManagers OU
  - **Arlene Kimbly** in the Research-Dev\ResearchManagers OU
  - **Mark Burnes** in the Sales\SalesManagers OU
  - **Shelly Emery** in the Support\SupportManagers OU

Use Active Directory Users and Computers on CorpDC to create groups and add members to the groups as follows:

1. From Server Manager, select **Tools** > **Active Directory Users and Computers**.
2. Expand **CorpNet.com**.
3. Select **Users**.
4. From the menu, select the **Create a new group in the current container** icon.
5. In the Groups name field, enter **Managers**.
6. Under Group scope, make sure **Global** is selected.
7. Under Group type, make sure **Security** is selected and then click **OK**.
8. Add user accounts to the Managers group as follows:
   a. Navigate to each ***user***.
   b. Right-click ***user*** and select **Add to a group**.
   c. In the Enter the object names to select field, enter **Managers**.

      You can also browse to the Managers group as follows:
      1. Select **Advanced**.
      2. Select **Find Now**.
      3. Select the ***group***.
      4. Click **OK** twice.

   d. Click **OK** twice.
   e. Repeat steps 8a–8d to add additional users to the group.

Lab Report: 8.8.7 Create Global Groups

Your Performance

Your Score: 6 of 6 (100%) Pass Status: Pass

Elapsed Time: 5 minutes 59 seconds Required Score: 100%

Task Summary

✓ Create a global security group named Accounting in the Accounting OU

✓ Add the correct employees as members of the Accounting group Show Details

✓ Create a global security group named Research-Dev in the Research-Dev OU

✓ Add the correct employees as members of the Research-Dev group Show Details

✓ Create a global security group named Sales in the Sales OU

✓ Add the correct employees as members of the Sales group Show Details

Explanation

In this lab, you complete the following tasks:

- Create a global security group named **Accounting** in the Accounting OU.
- Create a global security group named **Research-Dev** in the Research-Dev OU.
- Create a global security group named **Sales** in the Sales OU.
- Add all user accounts in the corresponding OUs and sub-OUs as members of the newly-created groups.

Following are steps an expert might take to complete this lab:

1. From Server Manager, select **Tools** > **Active Directory Users and Computers**.
2. Browse the Active Directory structure to the appropriate ***OU***.
3. Right-click the ***OU*** you want to create the group in and select **New** > **Group**.
4. In the Group name field, enter the ***name*** of the group.
5. Select the ***group scope***.
6. Select the ***group type***; then click **OK**.
7. Add a user account to a group as follows:
   a. Right-click the ***user account*** and select **Add to a group**. (Use the Ctrl or Shift keys to select and add multiple user accounts to a group at the same time.)
   b. In the Enter the object names to select, enter the ***name*** of the group.
   c. Select a group scope and a group type, and then click **OK**.
   d. Select **Check Names**.
   e. Click **OK**.
   f. Click **OK**.
   g. Repeat step 7 to add users to the group.
8. Repeat steps 6-8 to add additional users to the group.

Lab Report: 8.9.4 Create a User Account

Your Performance

Your Score: 3 of 3 (100%) Pass Status: Pass

Elapsed Time: 2 minutes 45 seconds Required Score: 100%

Task Summary

✓ Create the pwilson user account

✓ Add Paul Wilson as a comment for the user account

✓ Set i8cer3al as the password

Explanation

In this lab, you perform the following:

- Create the **pwilson** user account.
- Include the full name, **Paul Wilson**, as a comment for the user account.
- Set the password to **i8cer3al**.
- View the **/etc/passwd** file to verify the creation of the account.

Complete this lab as follows:

1. At the command prompt, type **useradd -c "Paul Wilson" pwilson** and press **Enter** to create the user and set the comment in a single command.
2. Type **passwd pwilson** and press **Enter**.
3. Type **i8cer3al** and press **Enter** to set the password for the user account.
4. Type **i8cer3al** and press **Enter** to confirm the password.
5. Type **cat /etc/passwd** and press **Enter** to view the passwd file and verify that the account was created.

Lab Report: 8.9.5 Rename a User Account

Your Performance

Your Score: 4 of 4 (100%)
Pass Status: Pass
Elapsed Time: 2 minutes 25 seconds
Required Score: 100%

Task Summary

- ✓ Rename the bmiller user account bpalmer
- ✓ Change the comment field to Brenda Palmer
- ✓ Change the home directory to /home/bpalmer
- ✓ Move the home directory contents

Explanation

In this lab, your task is to do the following:

- Rename the user account **bpalmer**.
- Change the comment field to read **Brenda Palmer**.
- Change the home directory to **/home/bpalmer**, moving the contents of the old home directory to the new location.
- View the **/etc/passwd** file and **/home** directory to verify the modification of the account.

Do the following:

- At the command prompt, type **usermod -l bpalmer bmiller** and press **Enter** to rename the user account.
- Type **usermod -c "Brenda Palmer" bpalmer** and press **Enter** to change the comment field to read Brenda Palmer.
- Type **usermod -d /home/bpalmer -m bpalmer** and press **Enter** to change the home directory to /home/bpalmer and to move the contents of the old home directory to the new location.
- Type **cat /etc/passwd** and **ls /home** and press **Enter** to verify that the account was modified.

> To complete the tasks in the lab using a single command, use **usermod -c "Brenda Palmer" -d /home/bpalmer -m -l bpalmer bmiller**.

Lab Report: 8.9.6 Delete a User

Your Performance

Your Score: 2 of 2 (100%)
Elapsed Time: 55 seconds

Pass Status: Pass
Required Score: 100%

Task Summary

✓ Delete the tbrown user

✓ Delete the tbrown home directory

Explanation

In this lab, you perform the following:

- Remove the tbrown user account.
- Remove the tbrown home directory.
- View the **/etc/passwd** file and **/home** directory to verify that the account has been removed.

Complete this lab as follows:

1. At the command prompt, type **userdel -r tbrown** and press **Enter** to remove the user account and the home directory. (The **-r** switch removes the home directory when the user account is removed.)
2. Type **cat /etc/passwd** and **ls /home** to verify that the account was removed.

Lab Report: 8.9.7 Change Your Password

Your Performance

Your Score: 1 of 1 (100%) Pass Status: Pass

Elapsed Time: 1 minute 8 seconds Required Score: 100%

Task Summary

✓ Change the administrator user password to r8ting4str

Explanation

In this lab, you change your administrator password from **7hevn9jan** to **r8ting4str** as follows:

1. At the command prompt, type **passwd** and press **Enter**.
2. Enter **7hevn9jan** and press **Enter** for the UNIX password.
3. Enter **r8ting4str** and press **Enter** for the new password.
4. When prompted to retype the new password, enter **r8ting4str** and press **Enter**.

Lab Report: 8.9.8 Change a User's Password

Your Performance

Your Score: 1 of 1 (100%)

Pass Status: Pass

Elapsed Time: 1 minute 35 seconds

Required Score: 100%

Task Summary

✓ Set the password for user sgarcia to G20oly04

Explanation

In this lab, you perform the following:

- Change the password for the sgarcia user account to **G20oly04**.
- Make sure the password is encrypted in the shadow file.

Complete this lab as follows:

1. At the command prompt, type **su -c "passwd sgarcia"** and press **Enter** to complete this task using a single command.
2. Type **1worm4b8** and press **Enter** for the root user password.
3. Type **G20oly04** and press **Enter** to assign the new password to the sgarcia user account.
4. Re-type **G20oly04** and press **Enter** to confirm the new password to the sgarcia user account.

Do not use the **usermod -p** command to change the password, as this stores the unencrypted version of the password in the **/etc/shadow** file.

Lab Report: 8.9.9 Lock and Unlock User Accounts

Your Performance

Your Score: 2 of 2 (100%) Pass Status: Pass

Elapsed Time: 2 minutes 50 seconds Required Score: 100%

Task Summary

✓ Lock the user accounts Show Details

✓ Unlock the user accounts Show Details

Explanation

In this lab, you perform the following:

- Lock the following user accounts:
  - **vedwards**
  - **cflynn**
  - **bkahn**
- Unlock the following user accounts:
  - **mbrown**
  - **bpalmer**
  - **aespinoza**
- View the **/etc/shadow** file to verify changes.

Complete this lab as follows:

1. At the command prompt, type **usermod -L** or **passwd -l** followed by the ***user account name*** and press **Enter** to lock the user accounts.
2. Repeat step 1 for each user account.
3. Type **usermod -U** or **passwd -u** followed by the ***user account name*** and press **Enter** to unlock the user accounts.
4. Repeat step 2 for each user account.
5. Type **cat /etc/shadow** to verify the changes. The inclusion of the exclamation point (!) in the password field indicates that the account is disabled.

Lab Report: 8.10.3 Rename and Create Groups

Your Performance

Your Score: 4 of 4 (100%)
Pass Status: Pass

Elapsed Time: 2 minutes 14 seconds
Required Score: 100%

Task Summary

- ✓ Rename the sales group to western_sales
- ✓ Create the eastern_sales group
- ✓ Remove aespinoza from the western_sales group
- ✓ Add aespinoza to the eastern_sales group

Explanation

In this lab, you perform the following:

- Rename the sales group **western_sales**.
- Create the **eastern_sales** group.
- Assign **aespinoza** as the only member of the **eastern_sales** group and remove **aespinoza** from all other groups.
- Verify the changes by viewing the **/etc/group** file or using the **groups** command.

Complete this lab as follows:

1. At the command prompt, type **groupmod -n western_sales sales** and press **Enter** to rename the sales group western_sales.
2. Type **groupadd eastern_sales** and press **Enter** to create the eastern_sales group.
3. Type **usermod -G eastern_sales aespinoza** and press **Enter** to modify group membership. When you assign aespinoza to the eastern_sales group with the **usermod -G** option, the user account is removed from the western_sales group.
4. Type **cat /etc/group** or **groups *username*** and press **Enter** to verify the user account's group membership.

Lab Report: 8.10.4 Add Users to a Group

Your Performance

Your Score: 2 of 2 (100%)

Pass Status: Pass

Elapsed Time: 1 minute 54 seconds

Required Score: 100%

Task Summary

✓ Make mjones a secondary member of the hrgroup Show Details

✓ Make cjohnson a secondary member of the hr group Show Details

Explanation

In this lab, your task is to perform the following:

- Append the **hr** group as a secondary group for the **mjones** and **cjohnson** user accounts.
- View the **/etc/group** file or use the **groups** command to verify the changes.

Complete this lab as follows:

1. At the command prompt, type **usermod -aG hr mjones** and press **Enter** to add mjones as member of the hr group.
2. Type **usermod -aG hr cjohnson** and press **Enter** to add cjohnson as member of the hr group.
3. Type **groups *username*** and press **Enter** to verify the user account's group membership.
4. Repeat step 3 for the other user.

Lab Report: 8.10.5 Remove a User from a Group

Your Performance

Your Score: 3 of 3 (100%)
Elapsed Time: 1 minute 32 seconds

Pass Status: Pass
Required Score: 100%

Task Summary

✓ Remove cflynn from the hr group

✓ Keep cflynn as a member of the it group

✓ Keep cflynn as a member of the mgmt1 group

Explanation

In this lab, you perform the following tasks:

- Remove **cflynn** from the hr group.
- Preserve cflynn's other group memberships.
- Verify the changes using the **groups** command or by viewing the **/etc/group** file.

Complete this lab as follows:

1. At the command prompt, type **groups cflynn** and press **Enter** to view a list of all groups to which the user belongs. You will see that cflynn currently belongs to the mgmt1, it, and hr secondary groups.

   The cflynn group is the user's primary group.

2. Type **usermod -G mgmt1,it cflynn** and press **Enter** to change group membership. To preserve existing group membership, use the **usermod -G** command listing all groups to which the user must belong. Do not include the primary group name in the list of groups.
3. Type **groups cflynn** and press **Enter** to verify the user account's group membership.

Lab Report: 8.12.5 Create and Link a GPO

Your Performance

Your Score: 5 of 5 (100%)
Pass Status: Pass

Elapsed Time: 5 minutes 49 seconds
Required Score: 100%

Task Summary

✓ Create the Workstation Settings GPO

✓ Link the GPO to the TempMarketing OU

✓ Link the GPO to the TempSales OU

✓ Link the GPO to the Support OU

✓ Import the policy from C:\Templates\ws_sec.inf

Explanation

In this lab, you perform the following on CorpDC:

- Create a GPO named **Workstation Settings**.
- Link the GPO to the following organizational units (OUs):
  - **TempMarketing OU** in the Marketing OU
  - **TempSales OU** in the Sales OU
  - **Support OU**
- Import the **ws_sec.inf** template file located in C:\Templates.

Complete this lab as follows:

1. From Server Manager, select **Tools > Group Policy Management**.
2. Expand **Forest: CorpNet.com > Domains > CorpNet.com**.
3. Right-click the ***OU*** where the policy will be linked and select **Create a GPO in this domain, and link it here**.
4. In the Name field, enter the ***GPO name***; then click **OK**.
5. Link the GPO to additional OUs as follows:
   a. Right-click the next ***OU*** and select **Link an Existing GPO** to link the GPO to another OU.
   b. Under Group Policy objects, select **Workstation Settings** from the list; then click **OK**.
   c. Repeat step 5 to link additional OUs.
6. Import a security policy template as follows:
   a. Expand **Group Policy Objects**.
   b. Right-click **Workstation Settings** and select **Edit**.
   c. Under Computer Configuration, expand **Policies > Windows Settings**.
   d. Right-click **Security Settings** and select **Import Policy**.
   e. Browse to the **C:\Templates**.
   f. Select **ws_sec.inf**; then click **Open**.

Lab Report: 8.13.3 Configure User Account Restrictions

Your Performance

Your Score: 4 of 4 (100%) Pass Status: Pass

Elapsed Time: 4 minutes 29 seconds Required Score: 100%

Task Summary

✓ Add restrictions for Borey Chan Show Details

✓ Disable the Pat Benton account

✓ Enable the Wendy Pots account

✓ Restrict computers for Support users Show Details

Explanation

In this lab, your task is to perform the following:

- Borey Chan is a temporary sales account assistant in the Sales/TempSales OU.
  - Allow logon **Monday–Friday**, **9:00 am–5:00 pm** only.
  - Expire the user account on **December 31st**.
- Pat Benton has been fired from the Research-Dev department. Disable her account until her replacement is found.
- Wendy Pots in the Research-Dev department is returning from maternity leave. While she was gone, you disabled her account to prevent logon. Enable her account to allow logon.
- For all users in the Support OU (but not the SupportManagers OU), allow logon only to the **Support** computer.

Complete this lab as follows:

1. From Server Manager, select **Tools** > **Active Directory Users and Computers**.
2. Expand **CorpNet.com**.
3. To configure logon hour restrictions for Borey Chan:
   a. Browse to the **Sales/TempSales** OU.
   b. In the right pane, right-click **Borey Chan** and select **Properties**.
   c. Select the **Account** tab.
   d. Select **Logon Hours**.
   e. Select **Logon Denied** because logon is allowed for all hours (indicated by blue boxes) by default.
   f. Click and drag the mouse to highlight the ***boxes*** that correspond to hours of permitted logon.
   g. Select **Logon Permitted**. The selected boxes turn blue, indicating that logon is allowed during those times.
   h. Click **OK**.
   i. Under Account expires, select **End of**.
   j. Enter the ***date*** that the user's account will expire.
   k. Click **OK**.
4. Disable Pat Benton's account as follows:
   a. Select the **Research-Dev** OU.
   b. Right-click **Pat Benton** and select **Disable Account**.
   c. Click **OK** to apply the changes.
5. Enable Wendy Pots's account as follows:
   a. In the Research-Dev OU, right-click **Wendy Pots** and select **Enable Account**.
   b. Click **OK**.
6. Configure user account restrictions as follows:
   a. Navigate to the **Support** OU.
   b. Press **Ctrl** and select both the **Tom Plack** and **Janice Rons** users to edit multiple users at the same time.

In Safari, press **Command** and select each user.

- c. Right-click the ***user accounts*** and select **Properties**.
- d. Select the **Account** tab.
- e. Mark **Computer restrictions**.
- f. Select **Log On To**.
- g. Select **The following computers**.
- h. In the Computer name field, enter **Support**.
- i. Click**Add**.
- j. Click **OK**.

7. Click **OK**.

Lab Report: 8.13.5 Configure Account Policies

Your Performance

Your Score: 8 of 8 (100%)

Elapsed Time: 5 minutes 14 seconds

Pass Status: Pass

Required Score: 100%

Task Summary

- ✓ Set the minimum password length to 10
- ✓ Enforce password complexity
- ✓ Set the maximum password age to 90
- ✓ Set the minimum password age to 14
- ✓ Enforce password history to remember 10 passwords
- ✓ Set the account lockout threshold to 5
- ✓ Set the reset account lockout after policy to 10
- ✓ Set the account lockout duration to 60

Explanation

In this lab, you configure the account policy settings in the default domain policy using Group Policy Management to meet the following requirements:

Policy	Security Setting	Value
Password Policy	Enforce password history	10 passwords remembered
	Maximum password age	90 days
	Minimum password age	14 days
	Minimum password length	10 characters
	Password must meet complexity requirements	Enabled
Account Lockout Policy	Account lockout duration	60 minutes
	Account lockout threshold	5 incorrect passwords
	Reset account lockout counter after	10 minutes

Following are steps that an expert might take to complete lab:

1. From Server Manager, select **Tools > Group Policy Management**.
2. Expand the ***domain***.
3. Right-click **Default Domain Policy** and select **Edit**.
4. Under Computer Configuration, expand **Policies > Windows Settings >Security Settings > Account Policies**.
5. Select **Password Policy**.
6. On the right, right-click the ***policy*** you want to edit and select **Properties**.

7. Edit the ***value*** for the policy.
8. Click **OK**.
9. Repeat steps 6–9 for each password policy that needs to be configured.
10. Select **Account Lockout Policy**.
11. Browse to the domain. Right-click **Default Domain Policy** and select **Edit**.
12. On the right, right-click the ***policy*** you want to edit and select **Properties**.
13. If the policy is undefined, select **Define this policy setting**.
14. Edit the ***value*** for the policy.
15. Click **OK**.
16. Repeat steps 12–15 for each password policy that needs to be configured.
17. Edit the value for the policy, and then click **OK**.

Lab Report: 8.13.7 Restrict Local Accounts

Your Performance

Your Score: 5 of 5 (100%) Pass Status: Pass

Elapsed Time: 3 minutes 29 seconds Required Score: 100%

Task Summary

- ✓ Create the Administrators (built-in) local group
- ✓ Select Delete all member users
- ✓ Select Delete all member groups
- ✓ Add BUILTIN\Administrator to the group
- ✓ Add %DOMAINNAME%\Domain Admins to the group

Explanation

In this lab, you edit the Default Domain policy and configure the Local Users and Groups policy settings as follows:

- Create a policy to update the built-in Administrator local group.
- Delete all member users.
- Delete all member groups.
- Add BUILTIN\Administrator to the group.
- Add %DOMAINNAME%\Domain Admins to the group.

Complete this lab as follows:

1. From Server Manager, select **Tools > Group Policy Management**.
2. Expand **Forest: CorpNet.com > Domains > CorpNet.com**.
3. Right-click **Default Domain Policy** and select **Edit**.
4. Under Computer Configuration, expand **Preferences > Control Panel Settings**.
5. Right-click **Local Users and Groups** and select **New > Local Group**.
6. In the Group name field, select **Administrators (built-in)** from the drop-down list.
7. Select **Delete all member users** to remove all member users.
8. Select **Delete all member groups** to remove all member groups.
9. Click **Add**.
10. In the Name field, enter **BUILTIN\Administrator**; then click **OK**.
11. Click **Add**.
12. In the Name field, enter **%DOMAINNAME%\Domain Admins**; then click **OK**.
13. Click **OK** to save the policy.

Lab Report: 8.13.8 Secure Default Accounts

Your Performance

Your Score: 4 of 4 (100%) Pass Status: Pass

Elapsed Time: 2 minutes 56 seconds Required Score: 100%

Task Summary

✓ Rename Administrator to xAdmin

✓ Disable the Guest account

✓ Deselect Password never expires for the Susan account

✓ Delete the Sam account, which has not been used

Explanation

In this lab, your task is to perform the following on the Office 1 computer:

- Rename the Administrator account **xAdmin**.
- Disable the **Guest** account.
- Verify that Password never expires is not selected for local users so they must change their passwords regularly.
- Delete user accounts with User must change password at next logon selected, which indicates that a user has never logged in.

Complete this lab as follows:

1. Right-click **Start** and select **Computer Management**.
2. Under System Tools, expand **Local Users and Groups**.
3. Select **Users**.
4. Right-click **Administrator** and select **Rename**.
5. Enter the new ***name***.
6. Right-click **Guest** and select **Properties**.
7. Select **Account is disabled** and click **OK**.
8. Right-click a ***user*** and select **Properties**.
9. Deselect **Password never expires** (if selected).
10. Click **OK**.
11. Repeat step 8–10 for each user.
12. Right-click the ***user*** that has User must change password at next logon selected and select **Delete**.
13. Click **Yes** to confirm deletion of the account.

Lab Report: 8.13.9 Enforce User Account Control

Your Performance

Your Score: 10 of 10 (100%) Pass Status: Pass

Elapsed Time: 2 minutes 43 seconds Required Score: 100%

Task Summary

- ✓ Admin Approval Mode for the Built-in Administrator account: Enabled
- ✓ Allow UIAccess applications to prompt for elevation without using the secure desktop: Disabled
- ✓ Behavior of the elevation prompt for administrators in Admin Approval mode: Prompt for credentials
- ✓ Behavior of the elevation prompt for standard users: Automatically deny elevation requests
- ✓ Detect application installations and prompt for elevation: Enabled
- ✓ Only elevate executables that are signed and validated: Disabled
- ✓ Only elevate UIAccess applications that are installed in secure locations: Enabled
- ✓ Run all administrators in Admin Approval Mode: Enabled
- ✓ Switch to the secure desktop when prompting for elevation: Enabled
- ✓ Virtualize file and registry write failures to per-user locations: Enabled

Explanation

In this lab, your task is to set the following UAC settings in the Default Domain policy:

User Account Control Category	Setting
Admin Approval Mode for the Built-in Administrator account	Enabled
Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
Behavior of the elevation prompt for administrators in Admin Approval mode	Prompt for credentials
Behavior of the elevation prompt for standard users	Automatically deny elevation requests
Detect application installations and prompt for elevation	Enabled
Only elevate UIAccess applications that are installed in secure locations	Enabled
Only elevate executables that are signed and validated	Disabled
Run all administrators in Admin Approval Mode	Enabled
Switch to the secure desktop when prompting for elevation	Enabled
Virtualize file and registry write failures to per-user locations	Enabled

Complete this lab as follows:

1. From Server Manager, select **Tools** > **Group Policy Management**.
2. Expand **Forest: CorpNet.com** > **Domains** > **CorpNet.com**.
3. Right-click **Default Domain Policy** and select **Edit**.
4. Under Computer Configuration, expand **Policies** > **Windows Settings** > **Security Settings** > **Local Policies**.
5. Select **Security Options**.
6. In the right pane, double-click the ***policy*** you want to edit.

7. If the policy is undefined, select **Define this policy setting**.
8. Select the ***policy setting***; then click **OK**.
9. Repeat steps 6–8 for each policy setting.

Lab Report: 8.14.2 Configure Smart Card Authentication

Your Performance

Your Score: 2 of 2 (100%) Pass Status: Pass

Elapsed Time: 2 minutes 48 seconds Required Score: 100%

Task Summary

✓ Set the Research-DevGPO to Enforced

✓ Configure smart card enforcement in the GPO Show Details

Explanation

In this lab, you perform the following in the Research-Dev GPO on CorpDC:

- Set the GPO to **Enforced**.
- **Enable** the Interactive logon: Require smart card policy.
- Set the Interactive logon: Smart card removal behavior policy to **Force logoff**.

Complete this lab as follows:

1. From Server Manager, select **Tools** > **Group Policy Management**.
2. Expand **Forest: CorpNet.com** > **Domains** > **CorpNet.com** > **Research-Dev**.
3. Right-click **Research-DevGPO** and select **Enforced**
4. Right-click **Research-DevGPO** and select **Edit**.
5. Under Computer Configuration, expand **Policies** > **Windows Settings** > **Security Settings** > **Local Policies**.
6. Select **Security Options**.
7. In the right pane, double-click the ***policy*** you want to edit.
8. Select **Define this policy setting**.
9. Select the ***policy setting***; then click **OK**.
10. Repeat steps 7–9 for each policy setting.

Lab Report: 8.14.6 Create a Fine-Grained Password Policy

Your Performance

Your Score: 9 of 9 (100%) Pass Status: Pass

Elapsed Time: 5 minutes 40 seconds Required Score: 100%

Task Summary

- ✓ Create the AccountingPasswords PSO Show Details
- ✓ Enforce a minimum password length (12 characters)
- ✓ Enforce password history (15 remembered passwords)
- ✓ Password must meet complexity requirements
- ✓ Do not store passwords using reversible encryption
- ✓ Protect from accidental deletion
- ✓ Set Password age options Show Details
- ✓ Enforce account lockout policy Show Details
- ✓ Apply the PSO to the Accounting group

Explanation

In this lab, you should have created a new password settings object using Active Directory Administrative Center with the following settings:

Create the PSO in the System > Password Settings Container with the following settings:

Setting	Value
Name	**AccountingPasswords**
Precedence	1
Enforce minimum password length	**12** characters
Enforce password history	**15** remembered
Password should meet complexity requirements	Checked
Store passwords using reversible encryption	Unchecked
Protect the object from accidental deletion	Checked
Enforce minimum password age	**2** days
Enforce a maximum password age	**30** days
Enforce account lockout policy: ▪ Number of failed attempts allowed ▪ Reset failed logon attempts count after (mins) ▪ Account will be locked out	**3** **30** Until an administrator manually unlocks the account

Directly Applies To	**Accounting**

Do the following:

1. From Server Manager, select **Tools > Active Directory Administrative Center**.
2. In the left pane, select **CorpNet.com (local)**.
3. In the center pane, double-click **System**.
4. Select, then Right-click **Password Settings Container** and select **New > Password Settings**.
5. Under Password Settings, enter the ***password settings***.
6. Under Directly Applies To, select **Add**.
7. Enter the ***name*** of the user or group; then click **OK**.
8. Click **OK**.

Lab Report: 9.7.3 Encrypt Files with EFS

Your Performance

Your Score: 2 of 2 (100%) Pass Status: Pass

Elapsed Time: 2 minutes 36 seconds Required Score: 100%

Task Summary

✓ Encrypt the D:\Finances folder and its contents

✓ Add Susan as an authorized user of the 2017report.xls

Explanation

In this lab, you perform the following tasks:

- Encrypt the **D:\Finances** folder and all of its contents.
- Add **Susan** as an authorized user for the **D:\Finances\2017report.xls** file.

Complete this lab as follows:

1. From the taskbar, select **File Explorer**.
2. Select the **D:** volume.
3. Right-click the **Finances** folder and select **Properties**.
4. On the General tab, select **Advanced**.
5. Select **Encrypt contents to secure data**.
6. Click **OK**.
7. Click **OK**.
8. Make sure **Apply changes to this folder, subfolder and files** is selected; then click **OK**.
9. Double-click the **Finances** folder to authorize additional users for a file.
10. Right-click the ***file*** and select **Properties**.
11. On the General tab, select **Advanced**.
12. Select **Details**.
13. Select **Add**.
14. Select the ***user*** and click **OK**.
15. Click **OK**.
16. Click **OK** to close the Advanced Attributes dialog.

Lab Report: 9.7.8 Configure BitLocker with a TPM

Your Performance

Your Score: 5 of 5 (100%)
Pass Status: Pass
Elapsed Time: 4 minutes 51 seconds
Required Score: 100%

Task Summary

✓ Enable the TPM

✓ Activate the TPM

✓ Turn On BitLocker for the System (C:) drive

✓ Save the recovery key on CorpServer

✓ Perform a BitLocker system check

Explanation

In this lab, you configure BitLocker drive encryption as follows:

- Turn on TPM in the BIOS.
- Activate TPM in the BIOS.
- Turn on BitLocker for the Local Drive (C:) drive.
- Save the recovery key to **\\CorpServer\BU-Office1**.
- Run the BitLocker system check.
- Encrypt the entire **Local Drive (C:)** drive.

Complete this lab as follows:

1. Right-click **Start** and select **Control Panel**.
2. Select **System and Security**.
3. Select **BitLocker Drive Encryption**.
4. Select **Turn on BitLocker** next to C:.
5. Notice, at the bottom of the window, that Windows indicates that a TPM was not found.
6. Click **Cancel**.
7. Click **Start**.
8. Click **Power**.
9. Click **Restart** to restart Office1 and activate TPM.
10. When the TestOut logo appears, press **Delete** to enter the BIOS.
11. Turn on and activate TPM as follows:
    a. In the left pane, expand **Security**.
    b. Select **TPM Security**.
    c. In the right pane, select **TPM Security** to turn TPM security on.
    d. Click **Apply**.
    e. Click **Activate**.
    f. Click **Apply**.
    g. Click **Exit**.
12. Turn on BitLocker as follows:
    a. After Office1 finishes rebooting, right-click **Start** and select **Control Panel**.
    b. Select **System and Security**.
    c. Select **BitLocker Drive Encryption**.
    d. Next to C:, select **Turn on BitLocker**. Now Windows is able to begin the Drive Encryption setup.
13. Save the recovery key to \\CorpServer\BU-Office1 as follows:
    a. Select **Save to a file** to back up your recovery key to a file.
    b. Browse the network to **\\CorpServer\BU-Office1** and click **Save**.
    c. After your recovery key is saved, click **Next**.

14. Select **Encrypt entire drive**; then click **Next**.
15. Leave the default setting selected when choosing the encryption mode and click **Next**.
16. Select **Run BitLocker system check**; then click **Continue**.
17. Select **Restart Now**.
18. When encryption is complete, click **Close**.
19. Open File Explorer and verify that the Local Disk (C:) drive shows the lock icon.

Lab Report: 9.8.3 Manage Certificates

Your Performance

Your Score: 4 of 4 (100%)	Pass Status: Pass
Elapsed Time: 5 minutes 5 seconds	Required Score: 100%

Task Summary

✓ Approve pending certificate requests for smart card certificates Show Details

✓ Deny the CorpSrv16 certificate request

✓ Revoke the bchan.corpnet.com certificate Show Details

✓ Unrevoke the CorpDev3 certificate

Explanation

In this lab, you perform the following:

- Approve the pending certificate requests for smart card certificates from **tsutton** and **mmallory**.
- Deny the pending web server certificate request for **CorpSrv16**.
- Revoke the certificate assigned to **bchan.CorpNet.com** using the **Key Compromise** reason code because bchan lost his smart card.
- Unrevoke the **CorpDev3** certificate.

Complete this lab as follows:

1. From Server Manager, select **Tools > Certification Authority**.
2. Expand **CorpCA-CA**.
3. Approve a pending certificate as follows:
    a. Select **Pending Requests**.
    b. Maximize the dialog so you can see who the requests are from.
    c. Right-click the **tsutton certificate request** and select **All Tasks > Issue**.
    d. Right-click the **mmallory certificate request** and select **All Tasks > Issue**.
4. Deny a pending certificate request as follows:
    a. Right-click the ***CorpSvr16 request*** and select **All Tasks > Deny**.
    b. Click **Yes** to confirm.
5. Revoke a certificate as follows:
    a. Select **Issued Certificates**.
    b. Right-click the ***bchan certificate*** and select **All Tasks > Revoke Certificate**.
    c. From the Reason code drop-down list, select the ***reason code***.
    d. Click **Yes**.
6. Unrevoke a certificate as follows:
    a. Select **Revoked Certificates**.
    b. Right-click the ***CorpDev3 certificate*** and select **All Tasks > Unrevoke Certificate**.

Lab Report: 9.10.5 Allow SSL Connections

Your Performance

Your Score: 3 of 3 (100%)
Elapsed Time: 2 minutes 18 seconds

Pass Status: Pass
Required Score: 100%

Task Summary

✓ Add a binding for HTTPS

✓ Use port 443 for HTTPS

✓ Use the www.corpnet.com certificate for SSL

Explanation

In this lab, your task is to add a binding to the CorpNet website using the following settings:

- Website: **www.corpnet.com**
- Protocol: **HTTPS**
- Port: **443**
- SSL certificate: **www.corpnet.com**

Complete this lab as follows:

1. From Server Manager, select **Tools** > **Internet Information Services (IIS) Manager**.
2. Expand **CorpWeb(CorpNet.com\Administrator)** > **Sites**.
3. Select **CorpNet.com**.
4. In the Actions pane, select **Bindings**.
5. Select **Add**.
6. Under Type, select the ***protocol*** from the drop-down list.
7. Under Port, make sure **443** is displayed.
8. Select the appropriate ***SSL certificate*** from the drop-down list; then click **OK**.
9. Click **Close**.

Lab Report: 9.12.7 Configure Fault-Tolerant Volumes

Your Performance

Your Score: 2 of 2 (100%)
Elapsed Time: 5 minutes 13 seconds

Pass Status: Pass
Required Score: 100%

Task Summary

✓ Mirror the C: drive

✓ Create a RAID 5 volume Show Details

Explanation

In this lab, you perform the following tasks:

- On Disk 1, create a mirrored volume of the System (C:) volume to add fault tolerance.
- Using Disk 2, Disk 3, and Disk 4, create a RAID 5 volume that provides both fault tolerance and improved performance using the following settings:
  - Volume size: **2 TB**
  - Drive letter: **R**
  - Format: **NTFS**
  - Volume label: **Data**

Complete this lab as follows:

1. Mirror an existing volume as follows:
   a. Right-click **Start** and select **Disk Management**.
   b. Click **OK** to initialize new disks.
   c. Maximize the Disk Management window to better view the volumes.
   d. Right-click the **System (C:)** volume and select **Add Mirror**.
   e. Select **Disk 1** that will be used for the mirrored copy.
   f. Select **Add Mirror**.
   g. Click **Yes** to convert the basic disk to a dynamic disk.
2. Create a RAID 5 volume as follows:
   a. In Disk Management, right-click a ***disk*** with free space and select **New RAID 5 Volume**.
   b. Click **Next**.
   c. Under Available, holding down the **Ctrl** key, select **Disk 3** and **Disk 4** to be part of the new volume with Disk 2.
   d. Select **Add**.
   e. Click **Next**.
   f. From the drive letter drop-down dialog, select **R**; then click **Next**.
   g. Make sure that **NTFS** is selected as the file system.
   h. In the Volume label field, enter **Data**.
   i. Select **Next**.
   j. Click **Finish** to create the volume.
   k. Click **Yes** to convert the basic disk to a dynamic disk.

Lab Report: 9.13.5 Back Up a Workstation

Your Performance

Your Score: 2 of 2 (100%) Pass Status: Pass

Elapsed Time: 5 minutes Required Score: 100%

Task Summary

✓ Create a Window 7 Compatible Backup on ITAdmin Show Details

✓ Configure Windows 10 Backups on Exec Show Details

Explanation

In this lab, you perform the following tasks:

- Configure a Windows 7-compatible backup on ITAdmin using the following settings:
  - Save the backup to the **Backup (D:)** volume.
  - Back up all of the users' data files.
  - Back up the **C:** volume.
  - Include a system image for the **C:** volume.
  - Do not set a schedule for regular backups.
  - Make a backup.
- Configure the Exec system to create Windows 10-compatible backups using the following settings:
  - Save the backup to the **Backup (E:)** volume.
  - Back up files **daily**.
  - Keep files for **6 months**.
  - Back up the entire **Data (D:)** volume.
  - Make a backup now.

Complete this lab as follows:

1. On ITAdmin, configure a Windows 7-compatible backup as follows:
   a. Right-click **Start** and select **Control Panel**.
   b. Select **System and Security**.
   c. Select **Backup and Restore (Windows 7**).
   d. Select **Set up backup** to perform a backup.
   e. Select **Backup (D:)** to save the backup and then click **Next**.
   f. Select **Let me choose** and then click **Next**.
   g. Select the ***data files*** and ***disks*** to include in the backup.
   h. Make sure that **Include a system image of drives: (C:)** is selected and then click **Next**.
   i. Select **Change schedule** to change the schedule for backups.
   j. Unmark **Run backup on a schedule**.
   k. Click **OK**.
   l. Select **Save settings and run backup**.
2. On Exec, configure Windows 10 backups as follows:
   a. From the top menu, select the **Floor 1** location tab.
   b. Select **Exec**.
   c. Select **Start**.
   d. Select **Settings**.
   e. Select **Update & security**.
   f. Select **Backup**.
   g. Select **Add a drive**.
   h. Select **Backup E:**.
   i. Verify that **Automatically back up my files** is on.

j. Select **More options**.
k. Under Back up my files, select **Daily**.
l. Under Keep my backups, select **6 months**.
m. Under Back up these folders, select **Add a folder**.
n. Select the **Data (D:)** volume and select **Choose this folder**.
o. Select **Back up now**.

Lab Report: 9.13.8 Back Up a Domain Controller

Your Performance

Your Score: 2 of 2 (100%) Pass Status: Pass

Elapsed Time: 5 minutes 18 seconds Required Score: 100%

Task Summary

✓ Create a backup schedule Show Details

✓ Perform an immediate backup of the server Show Details

Explanation

In this lab, your task is to use Windows Server Backup to complete the following tasks:

- Create a regular backup schedule for the CorpDC4 server using the following settings:
  - Backup type: **Custom**
  - Items to back up: **System State**
  - Backup frequency: **Once a day**
  - Backup time: **1:00 am**
  - Backup location: **\\CorpFiles12\Backup**
- Perform an immediate backup using the following custom settings:
  - Backup type: **Custom**
  - Items to back up: **System State** and **Local Disk (C:)**
  - Backup location: **\\CorpFiles12\Backup**

Complete this lab as follows:

1. Create a backup schedule as follows:
   a. In Server Manager, select **Tools > Windows Server Backup**.
   b. In the left pane, select **Local Backup**.
   c. In the Actions pane, select **Backup Schedule**.
   d. Click **Next** to begin the wizard.
   e. Select the ***backup type***; then click **Next**.
   f. Select **Add Items**.
   g. Select the ***items*** to be backed up; then click **OK**.
   h. Select **Next**.
2. Select the backup ***frequency***.
3. Select the backup ***time***; then click **Next**.
4. Select **Back up to a shared network folder**; then click **Next**.
5. Click **OK**.
6. Enter the ***location*** of the shared folder; then click **Next**.
7. Click **Finish**.
8. Click **Close**.
9. Perform an immediate backup as follows:
   a. In the Actions pane, select **Backup Once**.
   b. Select **Different options**; then click **Next**.
   c. Select the ***backup type***; then click **Next**.
   d. Select **Add Items**.
   e. Select the ***items*** to be backed up; then click **OK**.
   f. Select **Next**.
   g. Select **Remote shared folder**; then click **Next**.
   h. Enter the ***location*** of the shared folder; then click **Next**.
   i. Select **Backup** to start the backup.

j. Click **Close**.