Lab 6

ConfigurIng file services and Disk encryption

This lab contains the following exercises and activities:

|  |  |
| --- | --- |
| Exercise 6.1 | Encrypting Files with EFS |
| Exercise 6.2 | Configuring the EFS Recovery Agent |
| Exercise 6.3 | Backing Up and Restoring EFS Certificates |
| Exercise 6.4 | Encrypting a Volume with BitLocker |
| Lab Challenge | Configuring Network Unlock |

BEFORE YOU BEGIN

The lab environment consists of student workstations connected to a local area network, along with a server that functions as the domain controller for a domain called *contoso.com*. The computers required for this lab are listed in Table 6-1.

Table 6-1

Computers Required for Lab 6

|  |  |  |
| --- | --- | --- |
| Computer | Operating System | Computer Name |
| Server (VM 1) | Windows Server 2012 | RWDC01 |
| Server (VM 2) | Windows Server 2012 | Server01 |

In addition to the computers, you also require the software listed in Table 6-2 to complete Lab 6.

Table 6-2

Software Required for Lab 6

|  |  |
| --- | --- |
| Software | Location |
| Lab 6 student worksheet | Lab06\_worksheet.rtf (provided by instructor) |

Working with Lab Worksheets

Each lab in this manual requires that you answer questions, take screen shots, and perform other activities that you will document in a worksheet named for the lab, such as Lab06\_worksheet.rtf. You will find these worksheets on the book companion site. It is recommended that you use a USB flash drive to store your worksheets, so you can submit them to your instructor for review. As you perform the exercises in each lab, open the appropriate worksheet file using WordPad, fill in the required information, and save the file to your flash drive.

After completing this lab, you will be able to:

* Encrypt files with EFS
* Configure EFS Recovery Agent
* Back up and restore EFS certificates
* Encrypt a volume with BitLocker

Estimated lab time: 70 minutes

|  |  |
| --- | --- |
| Exercise 6.1 | Encrypting Files with EFS |
| Overview | For files that are extremely sensitive, you can use EFS to encrypt the files.During this exercise, you encrypt a file using Encrypting File System (EFS), which is a built-in feature of NTFS. |
| Completion time | 20 minutes |

**Mindset Question: You have several sales people who have sensitive material on their computer. If their laptops are stolen, the stolen information could put the company at great risk. How can you protect the important data documents?**

# Encrypting Files with EFS

**1.** Log in to Server01 as the **Contoso\administrator** user account. The Server Manager console opens.

**2.** On Server01, create a **C:\Data** folder.

**3.** Create a text file in the C:\Data folder called **test.txt** file. Type your name in the file, close the file, then click Save to save the changes.

**4.** Right-click the C:\Data folder, and then click Properties. The Properties dialog box opens.

**5.** On the General tab, click Advanced. The Advanced Attributes dialog box appears as shown in Figure 6-1.

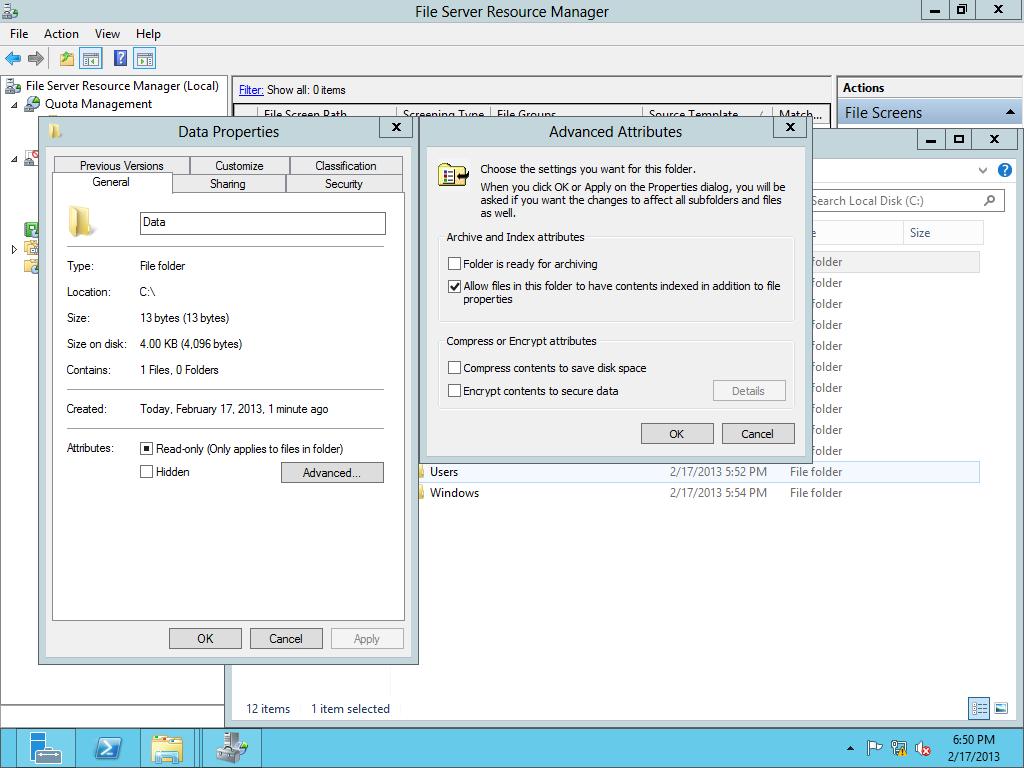


Figure 6-1

Configuring advanced attributes

**6.** Click to select *Encrypt contents to secure data*. Click OK to close the Advanced Attributes dialog box.

**7.** Click OK to close the Properties dialog box.

**8.** When Windows asks you to confirm the changes, click OK.

|  |  |
| --- | --- |
| Question 1 | What color is the C:\Data folder. |

|  |  |
| --- | --- |
| Question 2 | Is the test.txt file in the C:\Data folder also encrypted? |

**9.** Right-click the C:\Data folder and click Properties. The Properties dialog box opens.

**10.** Under the General tab, click Advanced. The Advanced Attributes dialog box opens.

**11.** Clear the *Encrypt contents to secure data* check box. Click OK to close the Advanced Attributes dialog box.

**12.** Click OK to close the Properties dialog box.

**13.** When it asks to confirm attribute changes, click OK.

**14.** From Server01, log off as administrator.

# Sharing Files Protected with EFS with Other Users

**1.** Log into RWDC01 as **contoso\administrator**, Server Manager starts. Open the Tools menu and click Active Directory Users and Computers. The Active Directory Users and Computers console opens.

**2.** Right-click the Users node, click New, then click User.

**3.** Create a new user with the following parameters:

First Name: **User1**

User logon name: **User1**

Click Next.

**4.** For the Password and Confirm password text boxes, type **Password01**. Click to select Password never expires. When an Active Directory Domain Services dialog box appears, click OK. Click Next.

**5.** When the user is ready to be created, click Finish.

**6.** Under the Users node, double-click User1. The User1 Properties dialog box opens.

**7.** Click the Member Of tab.

**8.** Click the Add button. When the Select Groups dialog box opens, type **domain admins** and click OK.

**9.** Click OK to close the User1 Properties dialog box.

**10.** On Server01, log in as **contoso\User1** with the password of **Password01**.

**11.** Open the C:\Data folder, right-click the test.txt file and click Properties.

**12.** On the General tab, click Advanced. The Advanced Attributes dialog box opens.

**13.** Click *Encrypt contents to secure data*. Click OK to close the Advanced Attributes dialog box. Click OK to close the test Properties dialog box.

**14.** When it asks if you want to encrypt the file and its parent folder, click OK.

**15.** If an Access Denied message appears, click Ignore, click Continue, click OK, and click Ignore. Click OK. If an Access Denied message appears again, click Ignore All. When you are done, the test.txt file should be green.

**16.** On Server01, log out as User1 and log in as **Contoso\Administrator**.

**17.** Open the C:\Data folder.

**18.** Double-click to open the Test.txt file.

|  |  |
| --- | --- |
| Question 3 | What error message did you get? |

**19.** Click OK to close the message, and then close Notepad.

**20.** Right-click the test.txt file and click Properties.

**21.** Click the Security tab.

|  |  |
| --- | --- |
| Question 4 | What permissions does Administrator have? |

|  |  |
| --- | --- |
| Question 5 | Why was the contoso\administrator not able to open the file? |

**22.** Go back to the General tab, click the Advanced button, clear the Encrypt check box, and then click OK.

**23.** Click OK to close the test Properties dialog box. When prompted for administrator permissions, click Continue. After the Access Denied dialog is displayed, click Cancel to close it.

|  |  |
| --- | --- |
| Question 6 | Were you able to decrypt the file? |

**24.** On Server01, log off as Administrator and log on as **User1**.

**25.** Open the C:\Data folder.

**26.** Right-click the test.txt file and click Properties. The Properties dialog box opens.

**27.** Click the Advanced button to open the Advanced Attributes dialog box.

**28.** Click to deselect the *Encrypt contents to secure data* check box, and click OK.

**29.** Click OK to close the Properties dialog box. When it asks you to provide administrator permission to change these attributes, click Continue.

**30.** Log off as User1 and log on as **contoso\administrator**.

**31.** Open the C:\Data folder.

**32.** Right-click the test.text and click Properties.

**33.** Click the Advanced button to open the Advanced Attributes dialog box.

**34.** Click to select the *Encrypt contents to secure data* check box. Click OK to close the Advanced Attributes dialog box.

**35.** Click OK to close the Properties dialog box. When it asks to apply to the folder and its contents, click OK.

**36.** Right-click the test.txt folder and click Properties. Click the Advanced button to open the Advanced Attributes dialog box.

**37.** Click the Details button. The User Access to test.txt dialog box opens as shown in Figure 6-2.

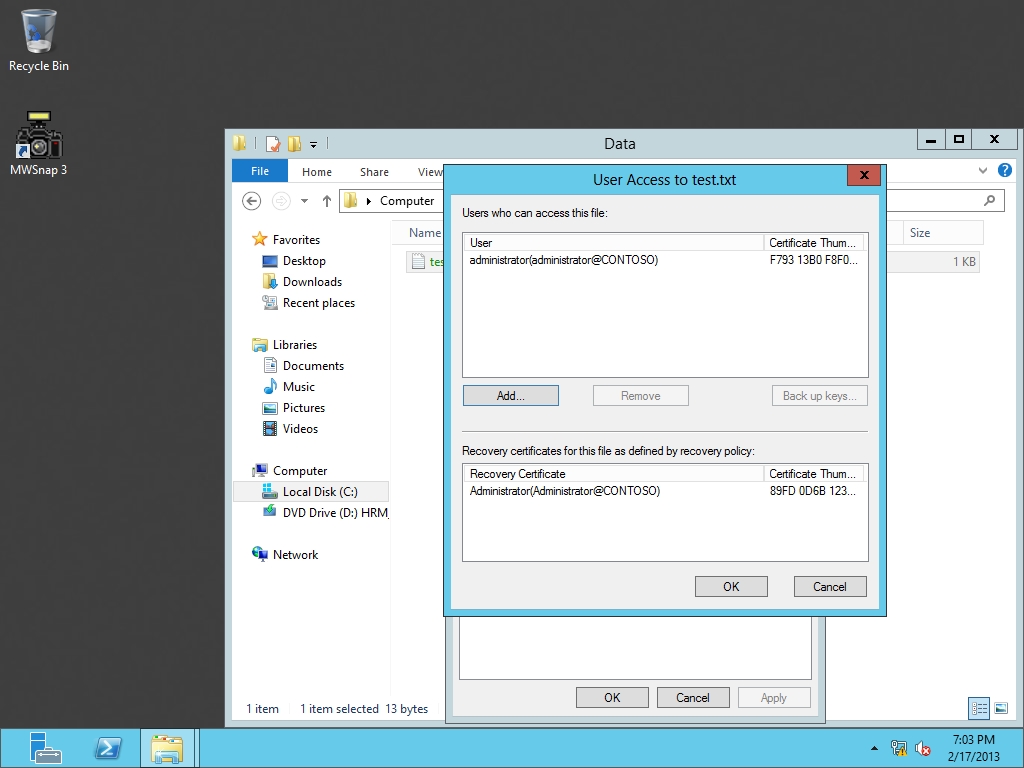


Figure 6-2

Certificate details for test.txt file

**38.** Click the Add button. When the Encrypting File System dialog box (as shown in Figure 6-3), click User1 and click View Certificate.

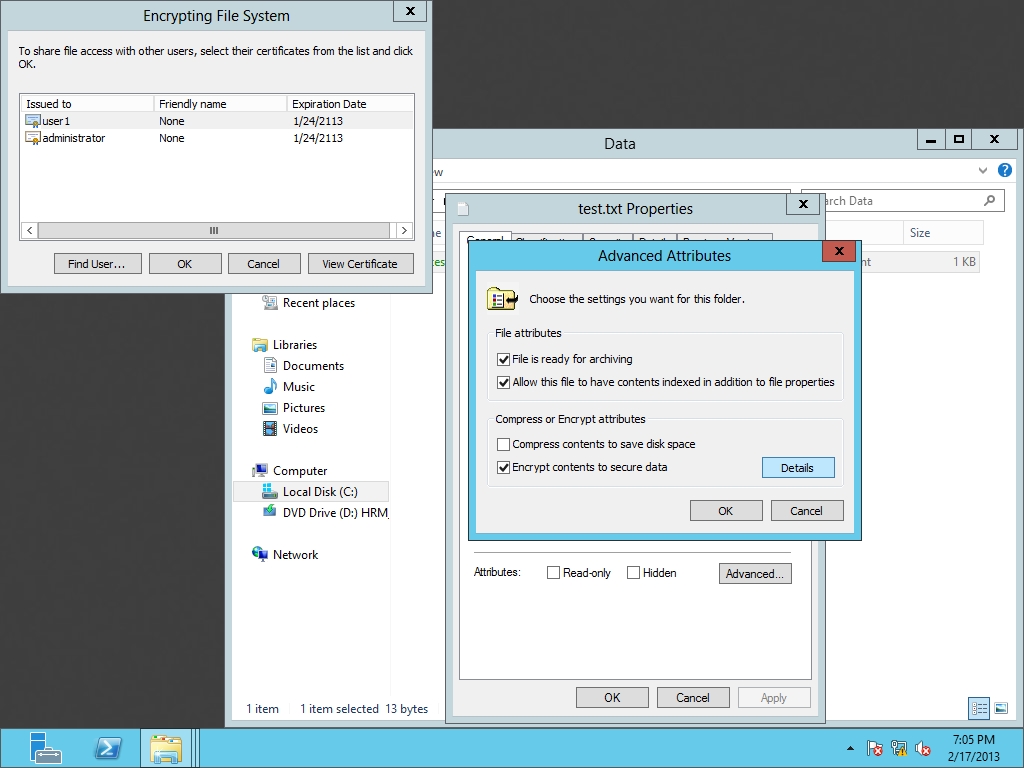


Figure 6-3

EFS certificates for test.txt

**39.** When the Certificate dialog box opens, click the Details tab.

|  |  |
| --- | --- |
| Question 7 | What is the Certificate used for? Hint: Look at the Enhanced Key Usage field**.** |

**40.** Click OK to close the Certificates dialog box.

**41.** Click OK to close the Encrypting File System dialog box.

|  |  |
| --- | --- |
| Question 8 | Looking at the User Access to test.txt dialog box, who has a Recovery Certificate? |

**42.** Take a screen shot of the User Access dialog box by pressing Alt+Prt Scr and then paste it into your Lab08\_worksheet file in the page provided by pressing Ctrl+V.

**43.** Click OK to close the User Access to test dialog box, click OK to close the Advanced Attributes dialog box, and click OK to close the test properties dialog box.

**44.** On Server01, sign out as Administrator and log in as **User1**.

**45.** Open the C:\Data folder and open the test.txt file.

|  |  |
| --- | --- |
| Question 9 | Were you able to open the file? |

**46.** Close the test.txt file.

**47.** On Server01, sign out as User1.

End of exercise. You can leave the windows open for the next exercise.

|  |  |
| --- | --- |
| Exercise 6.2 | Configuring the EFS Recovery Agent |
| Overview | During this exercise, you configure EFS Recovery Agents so that you can recover EFS encrypted files although the agent is not the owner of the file. |
| Completion time | 15 minutes |

**Mindset Question: Why do you need to have EFS Recovery Agents?**

# Installing and Configuring the Certificate Authority

**1.** On RWDC01, log on as **contoso\administrator**, if needed.

**2.** On RWDC01, on the Server Manager, open the Manage menu and click Add Roles and Features.

**3.** When the Add Roles and Features Wizard starts, click Next.

**4.** On the Select installation type page, click Next.

**5.** On the Select destination page, click Next.

**6.** On the Select server roles page, click Active Directory Certificate Services. When you are prompted to add features, click Add Features. Then when you are back to the Select server roles page, click Next.

**7.** On the Select features page, click Next.

**8.** On the Active Directory Certificate Services page, click Next.

**9.** On the Select role services page, Certificate Authority is already selected. Click to select the following:

Certificate Enrollment Policy Web Service

Certificate Enrollment Web Service

Certification Authority Web Enrollment

When it asks you to add additional features for any of these features, click Add Features.

**10.** Back on the Select role services page, click Next.

**11.** On the Web Server Role (IIS) page, click Next.

**12.** On the Select role services page, click Next.

**13.** On the Confirm installation selections page, click Install.

**14.** When the Certificate Authority is installed, click Close.

**15.** On Server Manager, click the Exclamation Point in a yellow triangle and then click Configure Active Directory Certificate Services.

**16.** On the Credentials page, click Next.

**17.** On the Role Services page, click Certification Authority, as shown in Figure 6-4. Click Next.

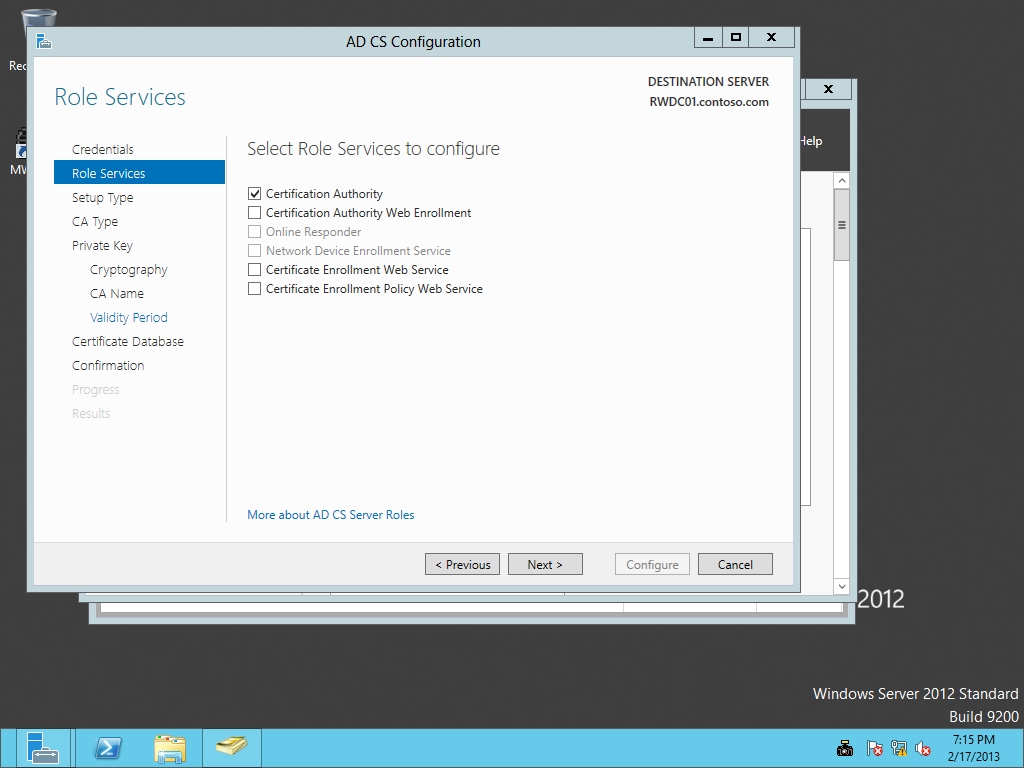


Figure 6-4

Configuring the Certification Authority

**18.** When it asks what setup type of CA you should install, click Next.

**19.** When it asks for the CA type (as shown in Figure 6-5), click Next.

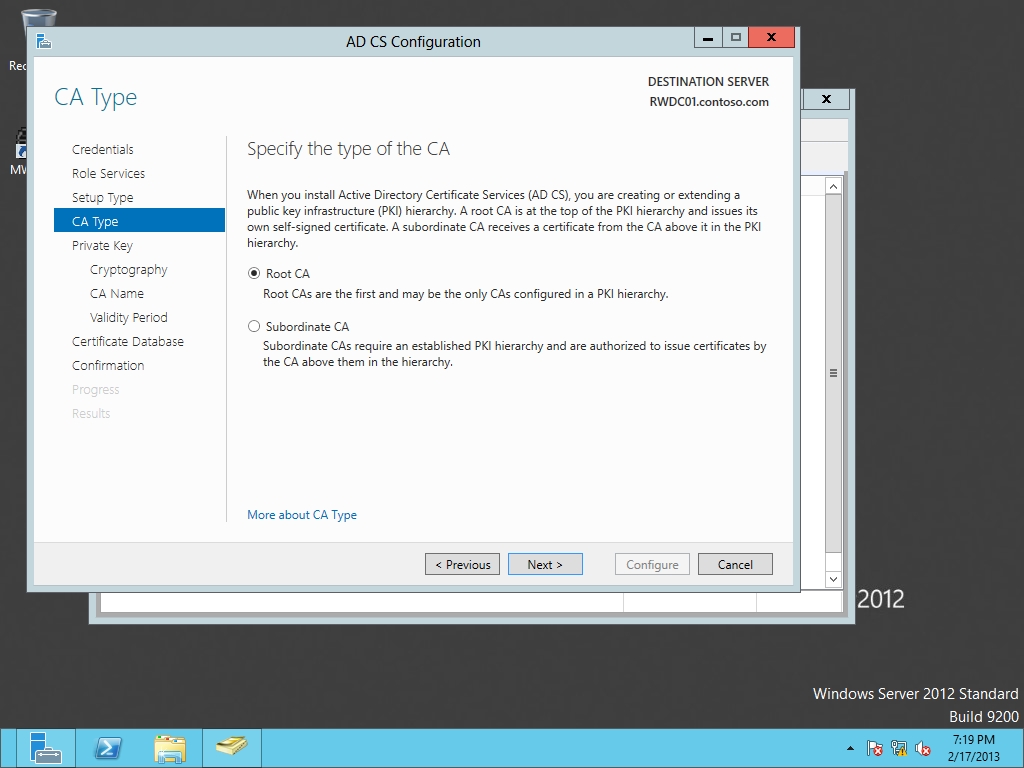


Figure 6-5

Specifying the type of CA

**20.** On the Specify the type of the private key page, click Next.

**21.** On the Specify the Cryptography for CA page, click Next.

**22.** On the Specify the name of the CA page, click Next.

**23.** For the Validity Period, click Next.

**24.** On the CA database page, click Next.

**25.** On the Confirmation page, click Configure.

**26.** When the CA is configured, take a screen shot of the CA is configured by pressing Alt+Prt Scr and then paste it into your Lab08\_worksheet file in the page provided by pressing Ctrl+V.

**27.** Click Close.

**28.** If it asks to configure additional role services, click No.

# Configuring the EFS Recovery Agent

**1.** On RWDC01, log off as Contoso\Administrator and log in as **Contoso\User1**.

**2.** On RWDC01, using Server Manager, open the Tools menu and click Group Policy Management. The Group Policy Management console opens.

**3.** Expand Forest, Domains, and contoso.com.

**4.** Right-click the Default Domain Policy and click Edit.

**5.** When Group Policy Management Editor opens, expand Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\ as shown in Figure 6-6.

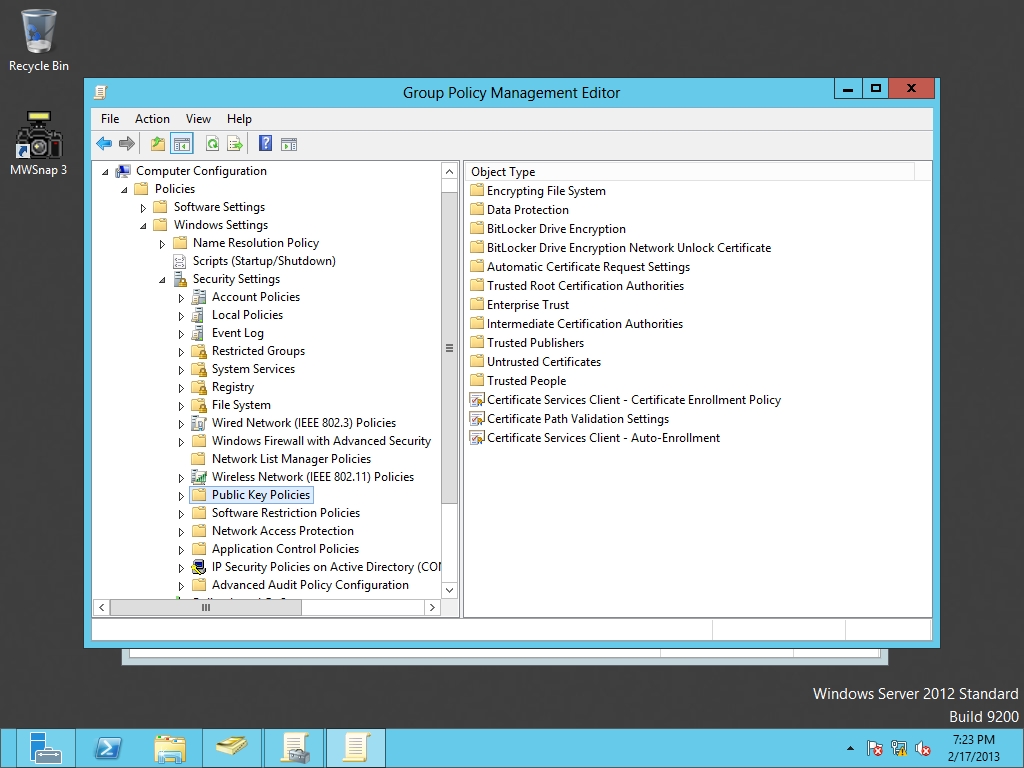


Figure 6-6

Opening the GPO public key policies

**6.** Right-click Encrypting File System, and select Create Data Recovery Agent. If you double-click Encrypting File System, you will see the Administrator listed in the right pane as shown in Figure 6-7.

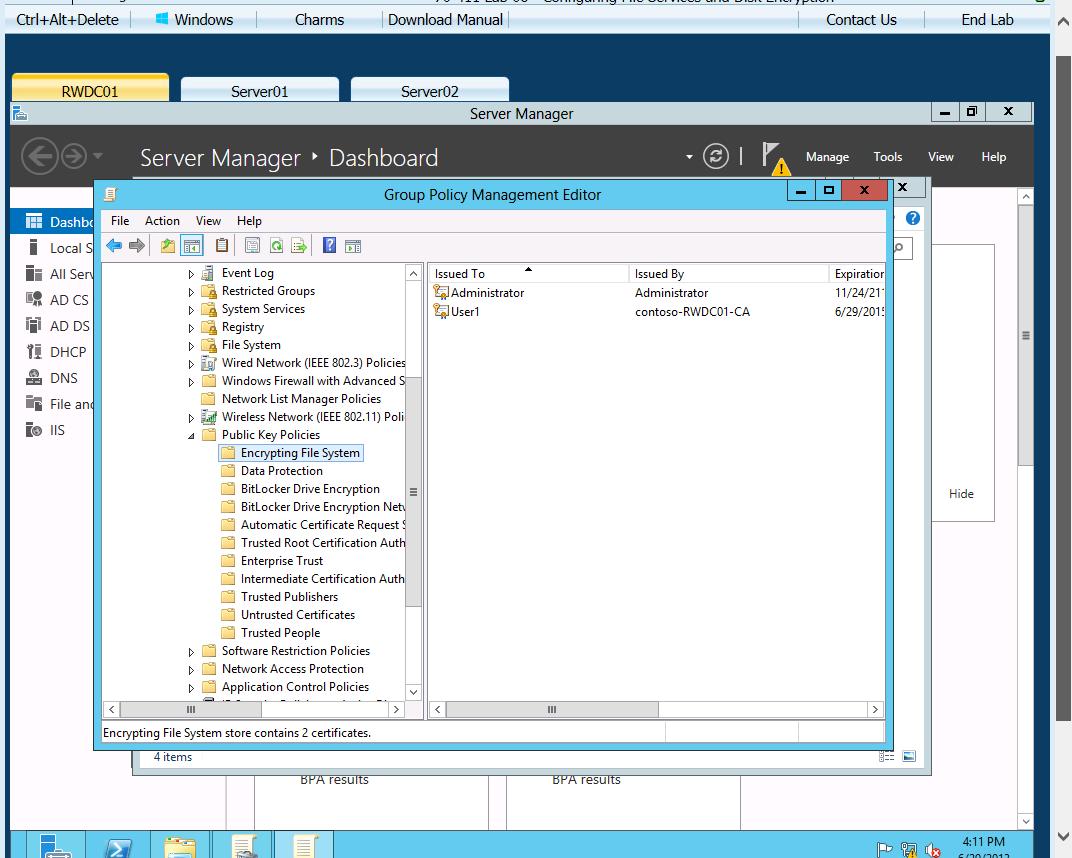


Figure 6-7

Viewing the current EFS recovery agents

**7.** On RWDC01, log off as Contoso\User1 and log in as **Contoso\Administrator**.

|  |  |
| --- | --- |
| Question 10 | What is needed for a user to become a data recovery agent? |

End of exercise. You can leave the windows open for the next exercise.

|  |  |
| --- | --- |
| Exercise 6.3 | Backing Up and Restoring EFS Certificates |
| Overview | During this exercise, you back up an EFS certificate and later restore after you delete the certificate. |
| Completion time | 10 minutes |

**Mindset Question: You had a standalone computer that failed and had to be rebuilt. On the computer, you had some files that were encrypted with EFS. Fortunately, you backed up the files from time to time to a removable drive. After you rebuilt the computer, you decide to copy the files from the removable drive. Although you are using the same username and password that you used before, you cannot open the files because they are encrypted. What can you do?**

# Backing Up the EFS Certificates

**1.** Log on to Server01 as **contoso\administrator**. The Server Manager console opens.

**2.** Right-click the Start button and click Command Prompt (Admin).

**3.** From the command prompt, execute the **certmgr.msc** command. The certmgr console opens.

**4.** In the left pane, double-click Personal, and then click Certificates.

**5.** In the main pane, right-click the certificate that lists Encrypting File System under Intended Purposes. Select All Tasks, and then click Export as shown in Figure 6-8.

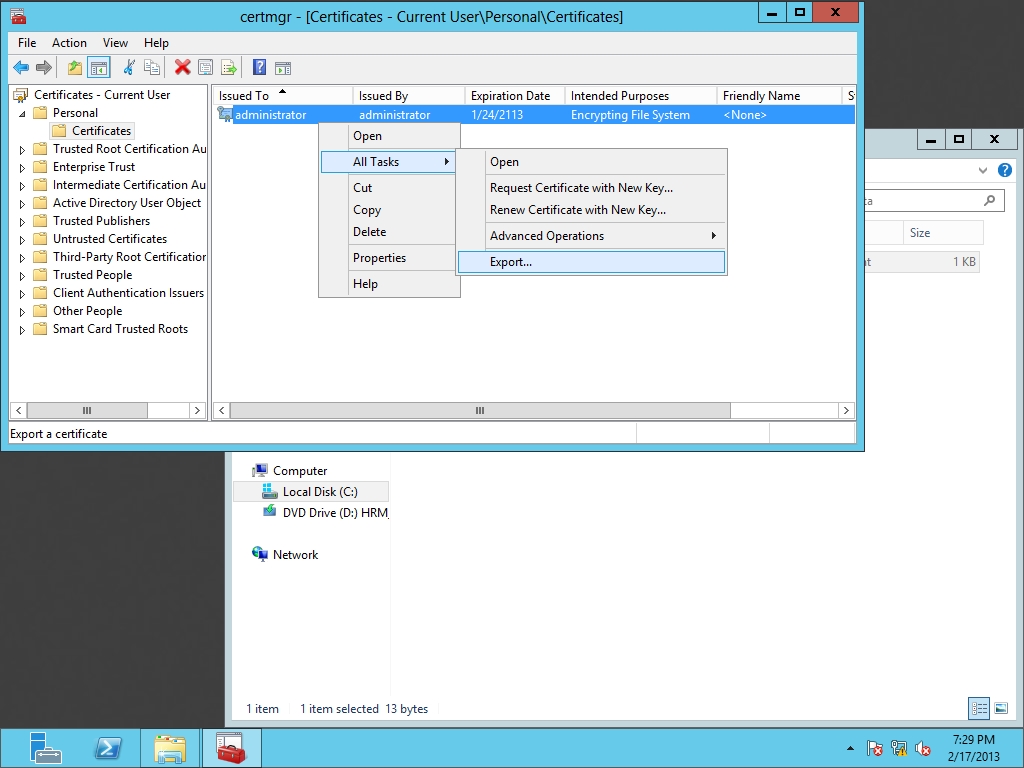


Figure 6-8

Exporting a certificate

**6.** When the Certificate Export Wizard starts, click Next.

**7.** On the Export Private Key page, click Yes, export the private key, and then click Next.

**8.** On the Export File Format page (as shown in Figure 6-9), click Next.

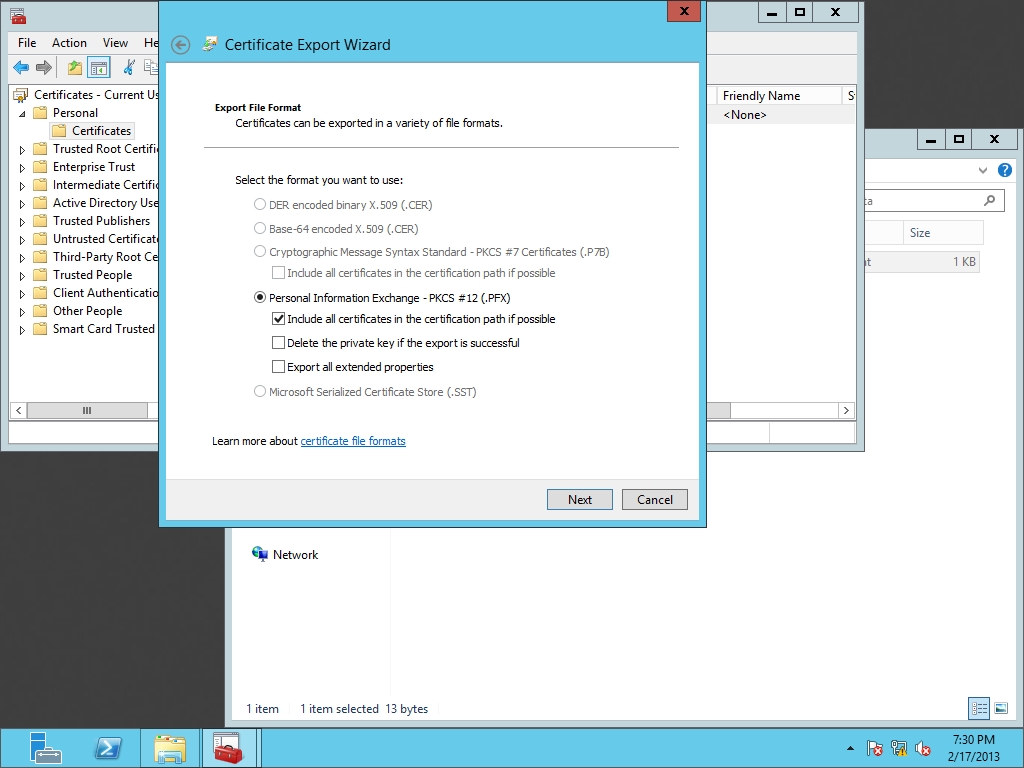


Figure 6-9

Specifying the exported format

**9.** On the Security page, select the Password check box, and type in the password of **Password01** in the Password and Confirm password text boxes. Click Next.

|  |  |
| --- | --- |
| Question 11 | What is the difference between the cer and the pfx format when backing up digital certificates? |

**10.** On the File to Export page, type **C:\Cert.bak** in the File name text box, Click Next.

**11.** Take a screen shot of the Certificate Export wizard by pressing Alt+Prt Scr and then paste it into your Lab08\_worksheet file in the page provided by pressing Ctrl+V.

**12.** When the wizard is complete, click Finish.

**13.** When the export is successful, click OK.

# Restoring the EFS Certificate

**1.** Right-click the Administrator certificate and click Delete. When it asks if you want to delete the certificate, read the warning and click Yes.

**2.** Right-click Certificates, select All Tasks, and then select Import.

**3.** When the Certificate Import Wizard starts, click Next.

**4.** On the File to Import page, type **c:\cert.bak.pfx**, and click then Next.

**5.** If it asks for a password, type **Password01** in the Password text box and click Next.

**6.** On the Certificate Store page, click Next.

**7.** On the Completing the Certificate Import Wizard page, click Finish.

**8.** When the import is successful, click OK.

**9.** Take a screen shot of the Certificates console by pressing Alt+Prt Scr and then paste it into your Lab06\_worksheet file in the page provided by pressing Ctrl+V.

**10.** Close Certificate Manager and close the Command Prompt.

End of exercise. You can leave the windows open for the next exercise.

|  |  |
| --- | --- |
| Exercise 6.4 | Encrypting a Volume with BitLocker |
| Overview | In this exercise, you create a new volume and then use BitLocker to encrypt the entire volume. |
| Completion time | 10 minutes |

**Mindset Question: How does EFS and BitLocker differ?**

**1.** Log in to Server02 as the **Contoso\Administrator** user account. The Server Manager console opens.

**2.** On Server02, on Server Manager, click Manage and click Add Roles and Features. The Add Roles and Feature Wizard opens.

**3.** On the Before you begin page, click Next.

**4.** Select Role-based or feature-based installation and then click Next.

**5.** On the Select destination server page, click Next.

**6.** On the Select server roles page, click Next.

**7.** On the Select features page, select BitLocker Drive Encryption.

**8.** When the Add Roles and Features Wizard dialog box displays, click Add Features.

**9.** On the Select Features page, click Next.

**10.** On the Confirm installation selections page, click Install.

**11.** When BitLocker is installed, click Close.

**12.** Reboot the Server02.

**13.** Log in to Server02 as the **Contoso\Administrator**. The Server Manager console opens.

**14.** Using Server Manager, open the Tools menu and click Computer Management. The Computer Management console opens.

**15.** Expand the Storage node and click Disk Management.

**16.** Right-click the C drive and click Shrink Volume.

**17.** In the *Enter the amount of space to shrink in MB* text box, type **3000** and click Shrink.

**18.** Under Disk 0, right-click the unused space and click New Simple Volume.

**19.** When the Welcome to the New Simple Volume Wizard starts, click Next.

**20.** On the Specify Volume Size page, click Next.

**21.** On the Assign Drive Letter or Path page, click Next.

**22.** On the Format Partition page, click Next.

**23.** When the wizard is complete, click Finish.

**24.** Close Computer Management.

**25.** Click the Start button, and then click the Control Panel.

**26.** Click BitLocker Drive Encryption. The BitLocker Drive Encryption window opens as shown in Figure 6-10.

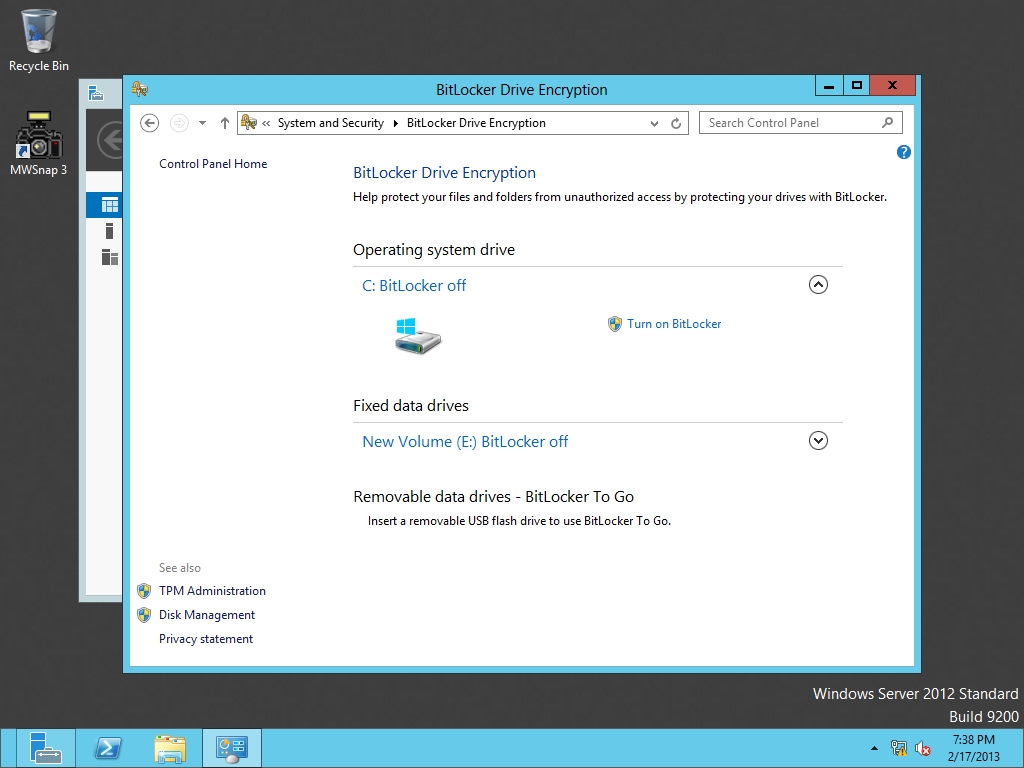


Figure 6-10

Opening the BitLocker settings

**27.** Click the down arrow next to the E drive. Then click Turn on BitLocker. A BitLocker Drive Encryption (E:) window opens.

**28.** On the *Choose how you want to unlock this drive* page, click to select the *Use a password to unlock the drive*. Type a password of **Password01** in the *Enter your password and Reenter your password* text boxes, and then click Next.

**29.** On the *How do you want to back up your recovery key?* page, click Save to a file option.

**30.** When the *Save BitLocker recovery key as dialog box* opens, type **\\rwdc01\Software\** before BitLocker Recovery Key <GUID>.txt and click Save. Click Next.

**31.** On the BitLocker Drive Encryption (E:) page, select Encrypt entire drive radio button, and click Next.

**32.** On the *Are you ready to encrypt this drive?* page, click Start encrypting.

**33.** When the drive is encrypted, take a screen shot of the BitLocker window by pressing Alt+Prt Scr and then paste it into your Lab06\_worksheet file in the page provided by pressing Ctrl+V

**34.** Close the BitLocker Drive Encryption window.

Lab REview Questions

|  |  |
| --- | --- |
| **Completion time** | **10 minutes** |

**1.** In Exercise 6.1, how do you enable EFS?

**2.** In Exercise 6.1, how do you allow other users to view an EFS file that you encrypted?

**3.** In Exercise 6.2, how does a user get to be an EFS Recovery Agent?

**4.** In Exercise 6.3, what format did you use when backing up the certificates, so that it can also store the private and public keys?

**5.** In Exercise 6.4, what did you use to encrypt an entire volume?

**6.** In Exercise 6.4, from where do you control BitLocker?

|  |  |
| --- | --- |
| Lab Challenge | Configuring Network Unlock |
| Overview | To complete this challenge, you will demonstrate how to enable Network Unlock. |
| Completion time | 10 minutes |

Starting with Windows Server 2012, Windows supports a Network Unlock feature, whereas when a computer connects to an organization domain, volumes that are encrypted with BitLocker will automatically be decrypted. What are the hardware and software components for Network Unlock and where is the Unlock key stored?

End of lab. You can log off or start a different lab. If you want to restart this lab, you’ll need to click the End Lab button in order for the lab to be reset.