Lab 15

Configuring Server authentication

This lab contains the following exercises and activities:

|  |  |
| --- | --- |
| Exercise 15.1 | Creating a Service Account |
| Exercise 15.2 | Creating a Managed Service Account |
| Exercise 15.3 | Configuring Kerberos and Kerberos Delegation |
| Lab Challenge | Configuring Kerberos with the Setspn Command |

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 15-1.

Table 15-1

Computers Required for Lab 15

|  |  |  |
| --- | --- | --- |
| 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 15-2 to complete Lab 15.

Table 15-2

Software Required for Lab 15

|  |  |
| --- | --- |
| Software | Location |
| Lab 15 student worksheet | Lab15\_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 Lab15\_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:

* Create a service account
* Create a Group Service Account
* Configure Kerberos and Kerberos Delegation

Estimated lab time: 60 minutes

|  |  |
| --- | --- |
| Exercise 15.1 | Creating a Service Account |
| Overview | In this exercise, you create a traditional service account. |
| Completion time | 10 minutes |

**1.** Log on to RWDC01 as the **Contoso\administrator** user account with Password, **Password01**. The Server Manager console opens.

**2.** On Server Manager, click Tools > Active Directory Users and Computers.

**3.** In the console tree, expand contoso.com, if needed.

**4.** Right-click contoso.com, click New, and click Organizational Unit. The New Object – Organizational Unit dialog box opens.

**5.** In the Name text box, type **Service Accounts** and click OK.

**6.** Right-click the Service Accounts organizational unit, click New, and then click User. The New Object – User Wizard starts.

**7.** In the First name text box, type **App1**. In the Last name text box, type **Service**. In the User logon name text box, type **App1Service**. Click Next. The password options appear.

**8.** In the Password and Confirm password dialog boxes, type **Password01**. Select the Password never expires option. When a dialog box opens saying that the password should never expire and that the user will not be required to change the password at next logon, click OK.

**9.** Click Next.

**10.** Click Finish to complete creating a service account.

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

|  |  |
| --- | --- |
| Exercise 15.2 | Creating a Managed Service Account |
| Overview | During this exercise, you create and deploy a Managed Service Account (MSA). |
| Completion time | 25 minutes |

**Mindset Question: What is the advantage of using a Managed Service Account over the traditional service account that was created in Exercise 15.1?**

**1.** On RWDC01, using Server Manager, open the Tools menu and click Active Directory Users and Computers, if needed.

**2.** In Active Directory Users and Computers, right-click the Computers OU, click New, and click Group. For the Group name, type **ServerGroup** and click OK.

**3.** In the Computers OU, Right-click ServerGroup and click Properties.

**4.** When the Properties dialog box opens, click the Members tab.

**5.** Click Add. In the text box, type **Server01.**

**6.** Click Object Types, select Computers, and click OK.

**7.** Click OK to close the ServerGroup Properties.

**8.** On RWDC01, using Server Manager, open the Tools menu and select Active Directory Module for Windows PowerShell. The Active Directory Module for Windows Powershell opens.

**9.** To create a key distribution services root key for the domain, run the following command in PowerShell:

Add-KDSRootKey –EffectiveTime ((Get-Date).AddHours

(-10))

**10.** To create an Active Directory AD service account, execute the following command:

New-ADServiceAccount –Name App2Service –DNSHostname rwdc01.contoso.com

–PrincipalsAllowedToRetrieveManagedPassword ServerGroup

**11.** Take a screen shot of the Active Directory Users and Computers showing the Managed Service Account OU by pressing Alt+Prt Scr and then paste it into your Lab15\_worksheet file in the page provided by pressing Ctrl+V.

|  |  |
| --- | --- |
| Question 1 | In which OU was the account created? |

**12.** To associate an MSA to a computer account, execute the following command in PowerShell:

Add-ADComputerServiceAccount –identity server01

-ServiceAccount App2Service

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

**14.** Open the Manage menu and click Add Roles and Features.

**15.** When the Add Roles and Features Wizard opens, click Next.

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

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

**18.** Click Active Directory Domain Services. When it asks to add features, click Add Features. Then click Next.

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

**20.** On the Active Directory Domain Services page, click Next.

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

**22.** When the installation is complete, click Close.

**23.** On Server01, with Server Manager, open the Toolsmenu and click *Active Directory Module for Windows PowerShell*.

**24.** When PowerShell starts, execute the following command to add the computer account to Server01:

Add-ADComputerserviceaccount –Identity Server01

–ServiceAccount App2Service

**25.** On Server01, with Server Manager, open the Tools menu and click Services. The Services console opens.

**26.** Double-click the SNMP Trapservice. The SNMP Trap Properties dialog box opens.

**27.** Click the Log On tab.

**28.** Select This account option and type **contoso\app2service$**.

|  |  |
| --- | --- |
| Question 2 | Why is the $ used? |

**29.** Clear the password in the Password and Confirm password text boxes.

**30.** Click OK.

**31.** When it says that the account has been granted the Log On As A Service, click OK.

**32.** If it states that the new logon name will not take effect until you stop and restart the service, click OK.

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

|  |  |
| --- | --- |
| Exercise 15.3 | Configuring Kerberos and Kerberos Delegation |
| Overview | In this exercise, you create a Service Principal Name (SPN) for an account and configure Kerberos Delegation. |
| Completion time | 10 minutes |

**Mindset Question: When you want to use Kerberos, what names are used to represent users and what format does it follow?**

**1.** On RWDC01, with Server Manager, click Tools > ADSI Edit. The ADSI Edit console opens.

**2.** Right-click ADSI Edit in the console tree, and then click Connect To. When the Connection Settings dialog displays, click OK.

**3.** Double-click Default Naming Context in the console tree, expand the DC=contoso,DC=com, and then click OU=Service Accounts.

**4.** In the Details pane, right-click the App1 Service and then click Properties. The CN=App1 Service Properties dialog box opens as shown in Figure 15-1.

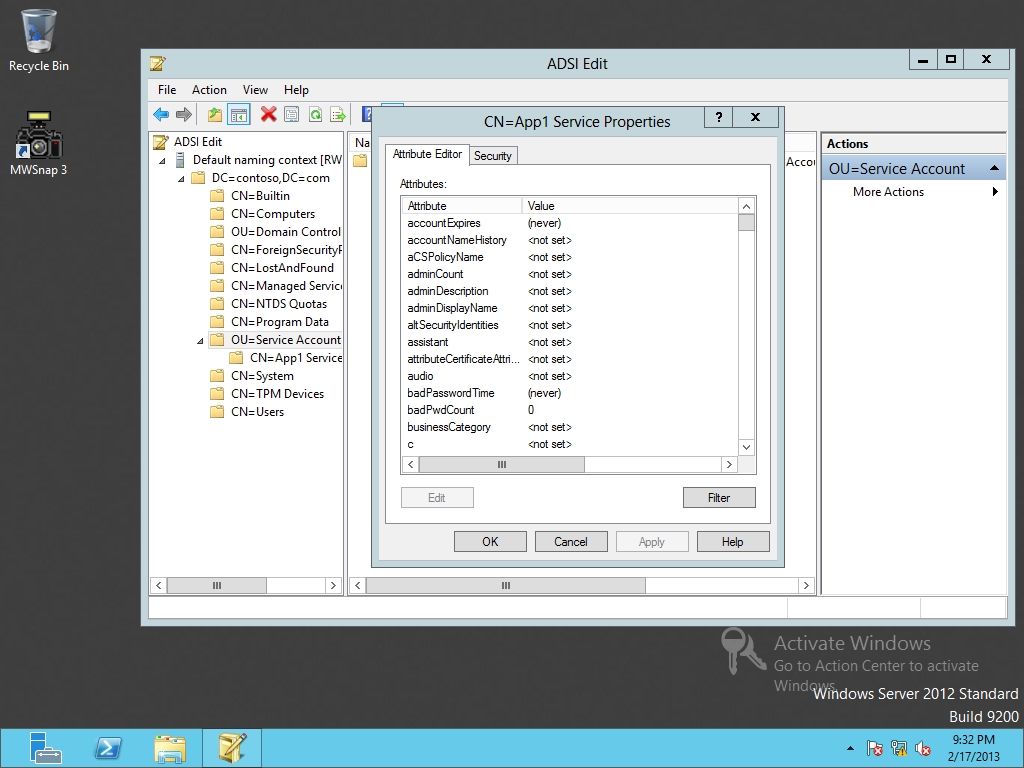


Figure 15-1

Editing the properties of a user

**5.** In the Attributes list, double-click servicePrincipalName to display the Multi-valued String Editor dialog box as shown in Figure 15-2.

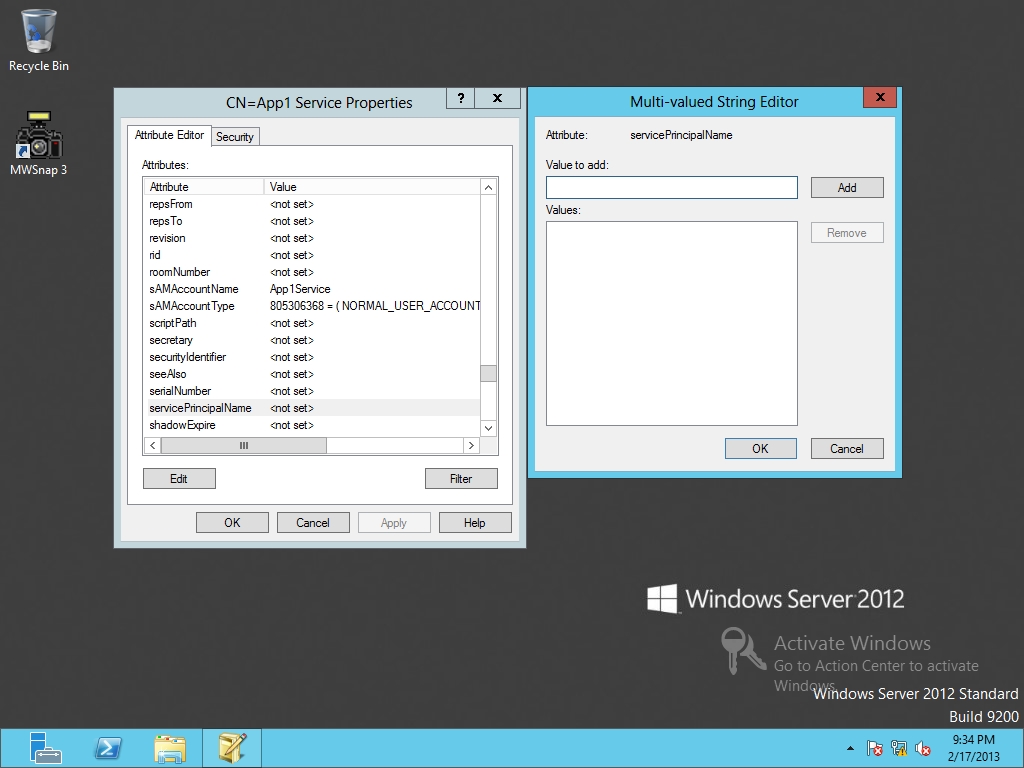


Figure 15-2

Modifying the servicePrincipalName

**6.** In the Value to add field, type **http/portal.contoso.com:443** and then click Add.

**7.** Click OK twice.

**8.** Using Server Manager, open the Tools menu, and click *Active Directory Users and Computers*.

**9.** Navigate to and click the Service Accounts organizational unit.

**10.** Right-click App1 Service and click Properties. The Properties dialog box opens.

**11.** Click the Delegation tab.

**12.** To allow this account to be delegated for a service, click *Trust this user for delegation to any service (Kerberos only)*, as shown in Figure 15-3.

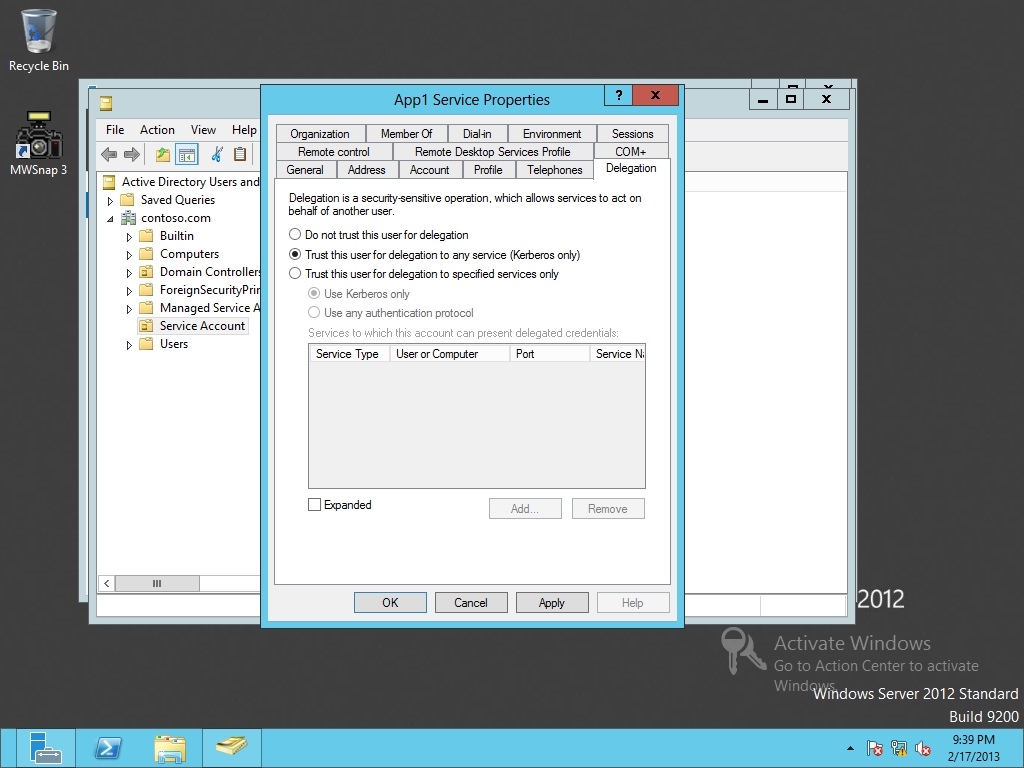


Figure 15-3

Configuring Kerberos delegation

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

Lab REview Questions

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

**1.** In Exercise 15.2, what are the minimum requirements for Managed Service Accounts?

**2.** In Exercise 15.2, when using the PrincipalsAllowedToRetrieveManagedPassword option, what kind of objects can you specify?

**3.** In Exercise 15.2, what do you use to create a Managed Service Account?

**4.** In Exercise 15.3, what was used to define an SPN for an account?

|  |  |
| --- | --- |
| Lab Challenge | Configuring Kerberos with the SetSPN Command |
| Overview | To complete this challenge, you will demonstrate how to configure Kerberos with the SetSPN command writing the step to complete the tasks described in the scenerio. |
| Completion time | 5 minutes |

You need to configure an SPN for an account. You decide that you want to create the SPN using the command prompt. What command would you use to configure the SPN in the same way that you did in Exercise 15-3.

Take a screen shot of the netsh command prompt window by pressing Alt+Prt Scr and then paste it into your Lab15\_worksheet file in the page provided by pressing Ctrl+V.

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.