Lab Objective

Learn how to create a managed Service Account(MSA).

**Lab Procedures**

**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

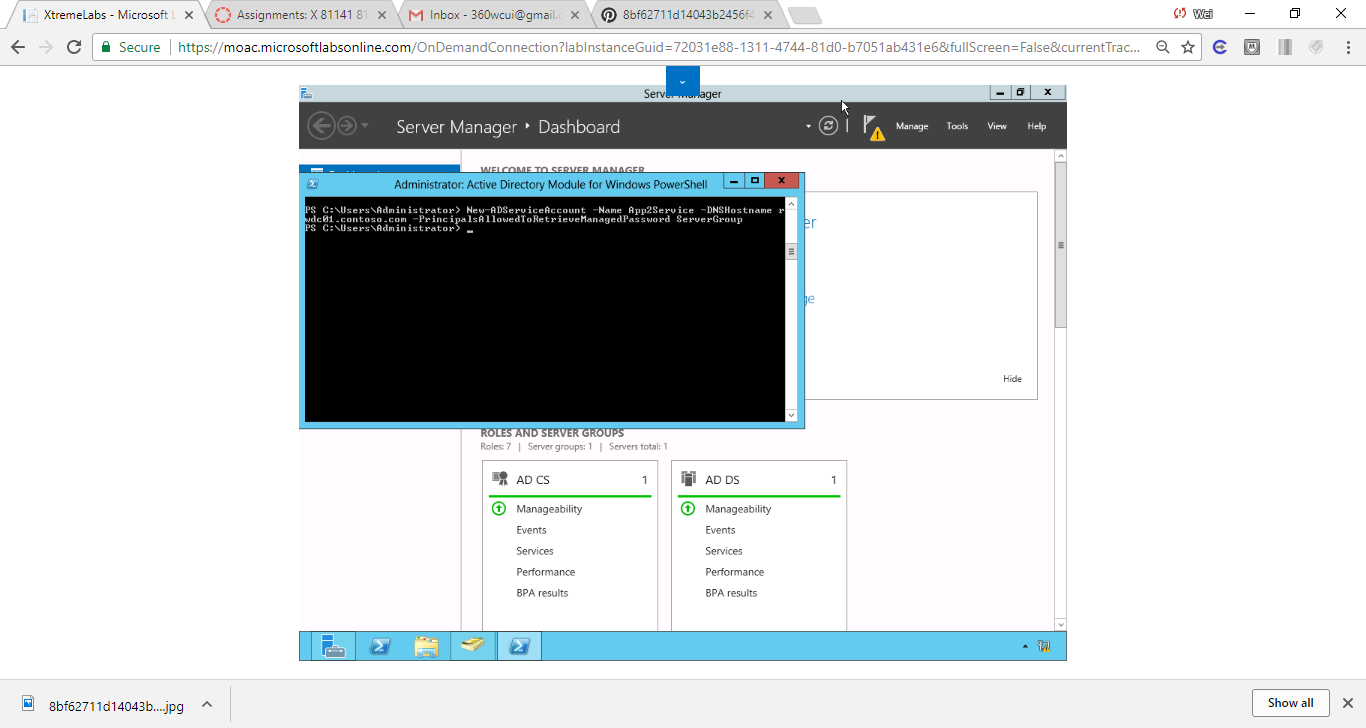


Figure Powershell Command to create an Active Directory AD service account.

**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.

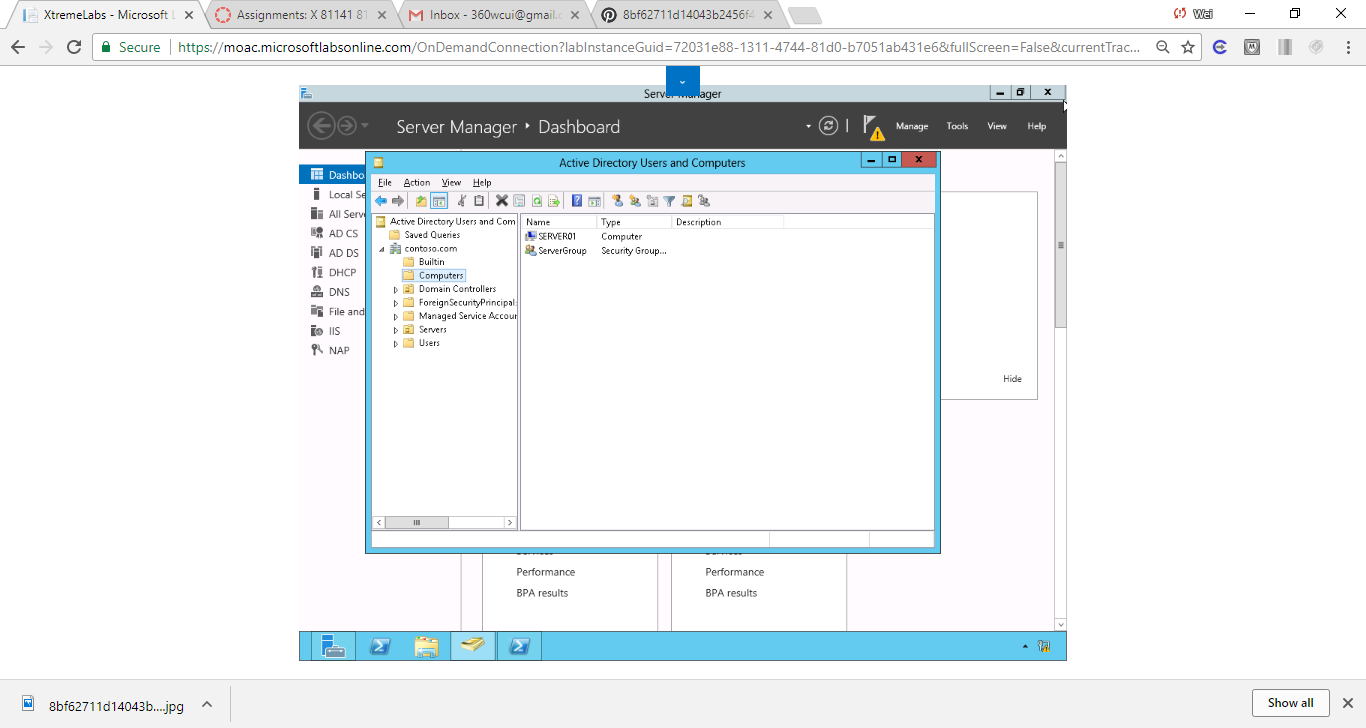


Figure ServerGroup is created in Computers OU.

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

Add-ADComputerServiceAccount –identity server01

-ServiceAccount App2Service

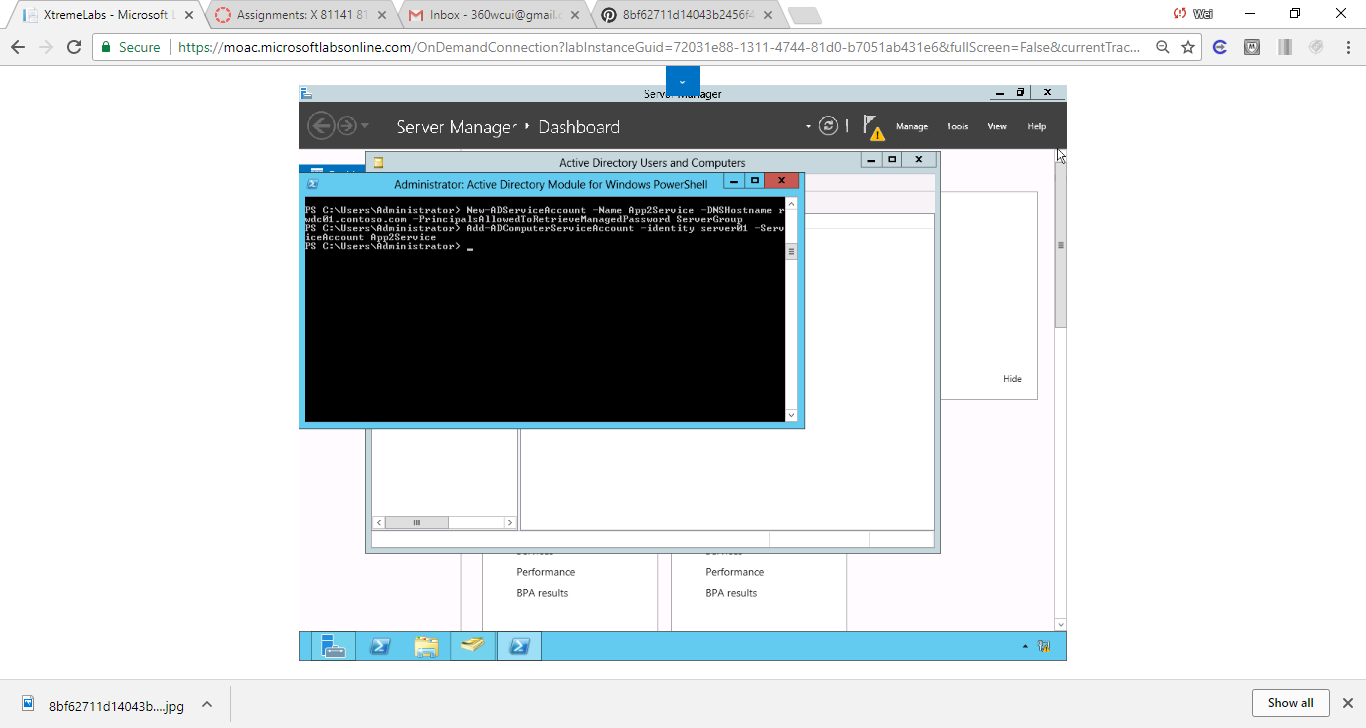


Figure . Command to associate an MSA to a computer account.

**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

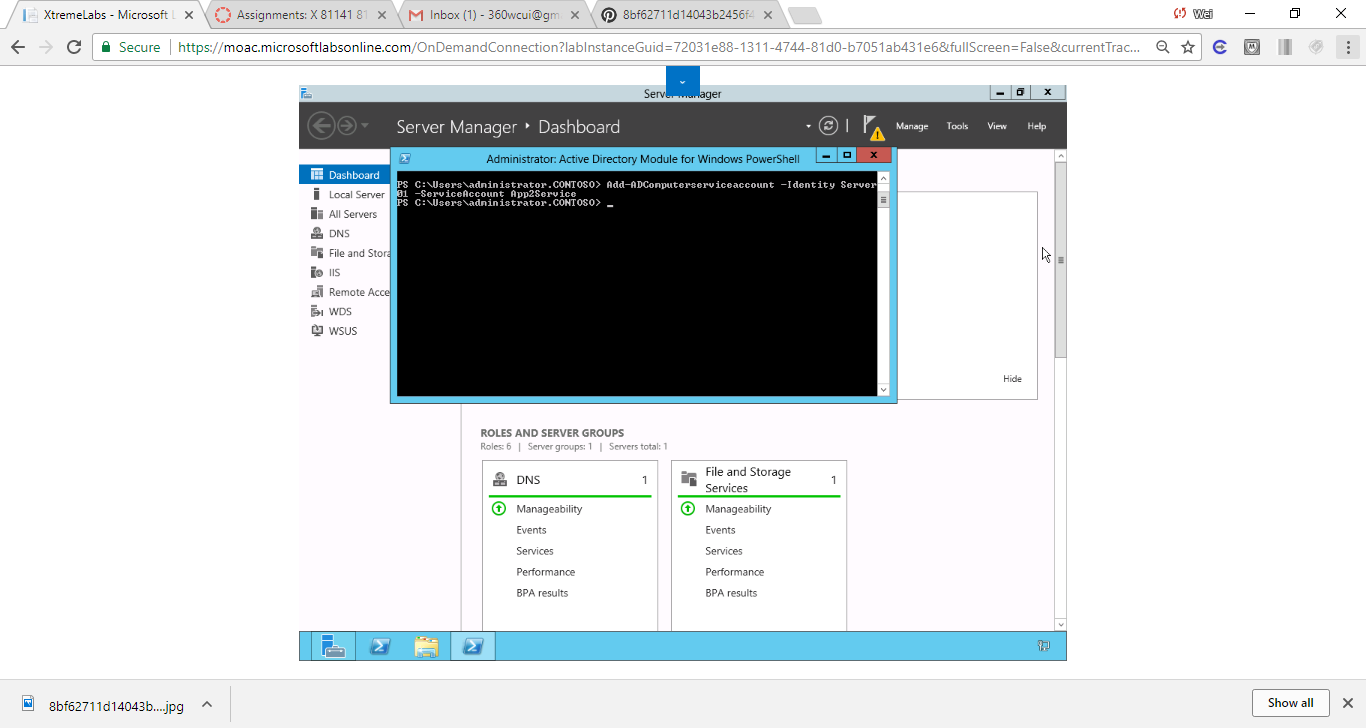


Figure . Command to add the computer account to Server01.

**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$**.

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

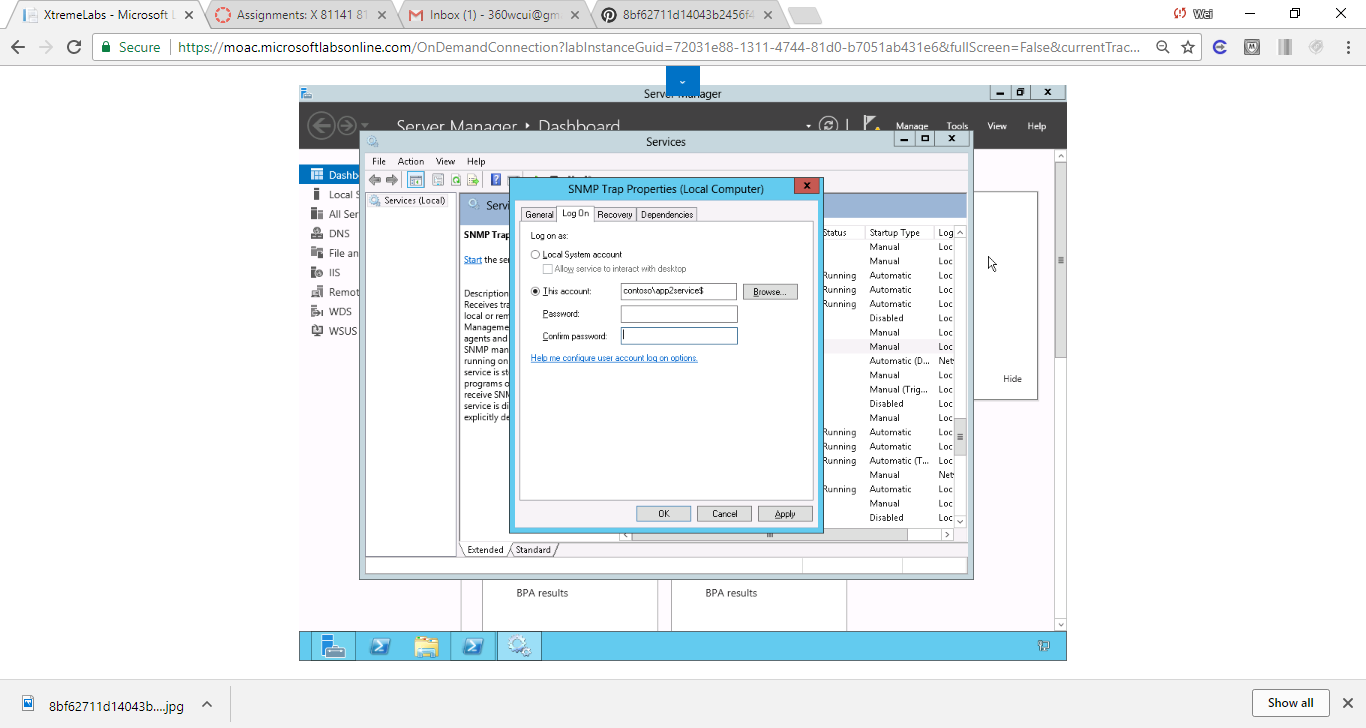


Figure . Clear the password in the Password and Confirm password text boxes.

**30.** Click OK.

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

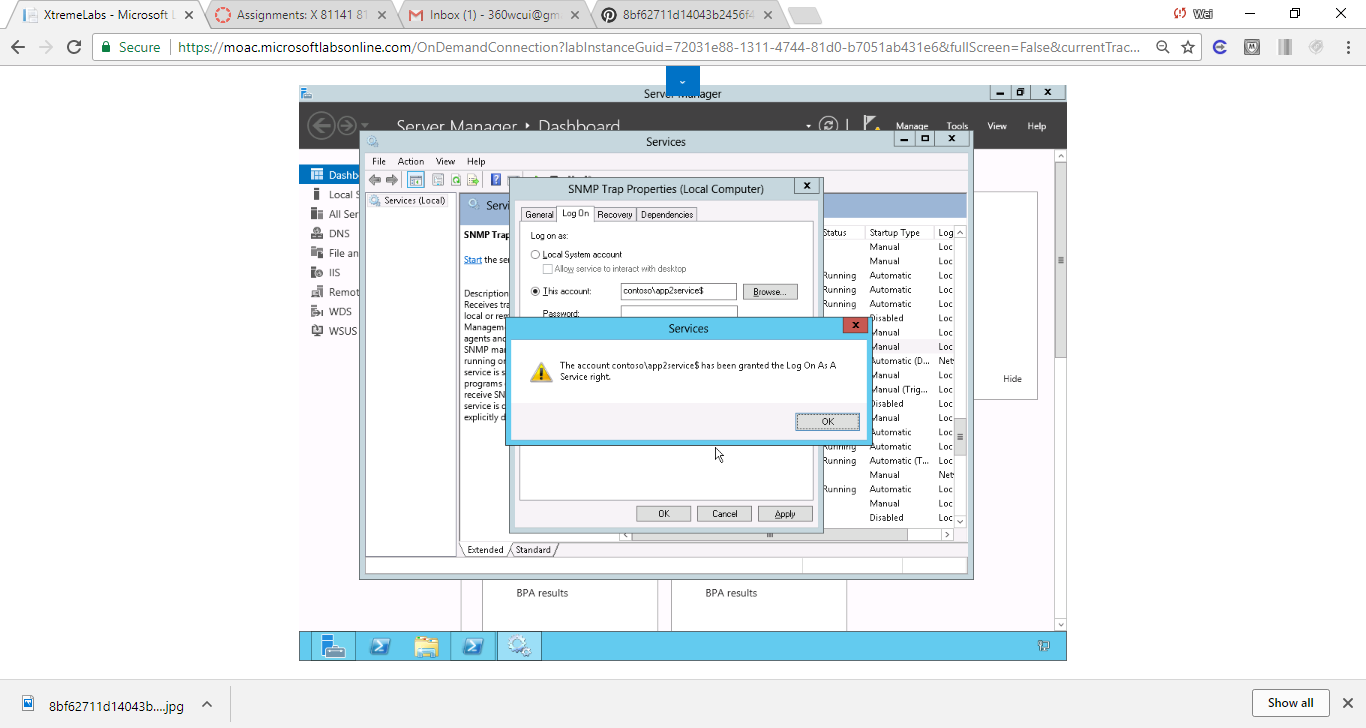


Figure . Alert message that the account has been granted the Log On As A Service.

**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.

**Lab Summary**

During this exercise, I created and deployed a Managed Service Account (MSA). The advantage of using a Managed Service Account over the traditional service account is that the password will automatically change on a regular basis. $ in the account option is a wide card that applies to any service matches the prefix. The Active Directory Module for Windows PowerShell has been extensively used in this exercise. To create a Managed Service Account. *The Add-ADComputerserviceaccount* command is used to create the account.