

## Before You Begin

Welcome! The Virtual Security Cloud Labs are your opportunity to gain valuable hands-on experience with professional-grade tools and techniques as you work through the guided lab exercises provided in the on-screen lab manual. The use of virtualization enables you to perform all of the tasks in the lab manual in a live environment without putting your personal device or institution's assets at risk.

Before you begin the guided lab exercises, please review the following preparation checklist.

1. **Run the [System Checker](#).** The System Checker will confirm that your browser and network connection are ready to support virtual labs.
2. **Review the [Common Lab Tasks document](#).** This document provides an overview of the virtual lab environment and outlines several of the recurring tasks you may need to complete your lab exercise.
3. **When you've finished, use the Disconnect button to end your session and create a StateSave.** To end your lab session and save your work, click the Disconnect button in the upper-right corner of the Lab View toolbar. When prompted, assign a name for your StateSave (we recommend using the Section, Part, and Step number where you stopped) and click Continue. Please note that a StateSave will preserve any changes written to disk in your lab session. A StateSave will not preserve any open windows or active processes, similar to restarting your computer.  
If you close your browser window without disconnecting, your lab session will automatically end after 5 minutes.
4. **[Technical Support](#) is here to help!** Our technical support team is available 24/7 to help troubleshoot common issues.  
Please note that the 24/7 support team is Level 1 only, and cannot assist with questions about lab content or the array of software used in the labs. If you believe you've identified an error in the lab guide or a problem with the lab environment, your ticket will be escalated to the Jones & Bartlett Learning product team for review. In the meantime, we recommend resetting the lab (Options > Reset) or reaching out to your instructor for assistance.

## Introduction

Every company operates within a complex combination of laws, regulations, requirements, competitors, and partners. In addition, morale, labor relations, productivity, cost, and cash flow affect how a company operates. Some organizations adhere to one or more well-known security frameworks, such as ISO 27001/270002, NIST, and CoBIT; others choose a framework based on legal requirements (e.g. PCI, for those that handle credit card information). Within this environment, management must develop and publish an overall security policy for the organization. This policy drives the creation of standards and standards drive the creation of specific procedures designed to comply with the policy. Controls ensure that all security procedures are followed, and security standards are upheld throughout the organization.

Changes in laws, regulations, and organizational priorities mean that security policies tend to change over time, and organizations “grow into” compliance organically. Each element of the security framework has a specific requirement for security professionals. They are involved with compliance monitoring, security awareness training, access control, privacy, incident response, log analysis, and more. Even with little time or financial resources allocated to the effort, it is still possible to do this successfully with the many compliance tools that are readily available for Windows and Linux systems.

In this lab, you will act as a member of the network security team. You have been given an assignment to implement two security standards that have been accepted by the organization. First, you will enforce a newly adopted corporate password policy using the Group Policy Management console. Additionally, the new policy dictates that all servers on a given subnet must be members of the Active Directory domain, but your organization has a Linux workstation that is currently a standalone system. You will join the Linux machine to the Active Directory domain using an open source tool, PowerBroker Identity Services Open.

## Learning Objectives

Upon completing this lab, you will be able to:

1. Create a domain level security policy in Windows
2. Join a Linux system to a Windows Active Directory domain
3. Explain the significance of a strict password policy

## Lab Overview

**Each section of this lab is assigned at your instructor’s discretion. Please consult your instructor to confirm which sections you are required to complete for your lab assignment.**

**SECTION 1** of this lab has three parts which should be completed in the order specified.

1. In the first part of this lab, you will implement a user password security policy on the Domain Controller.
2. In the second part of this lab, you will test that the new policy is in effect for a Windows machine.
3. In the third part of this lab, you will join a Debian Linux workstation to an Active Directory domain using a pre-installed tool, PowerBroker Identity Services Open (PBIS) and verify that the new password policy is in effect for a Linux machine.

**SECTION 2** of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods.

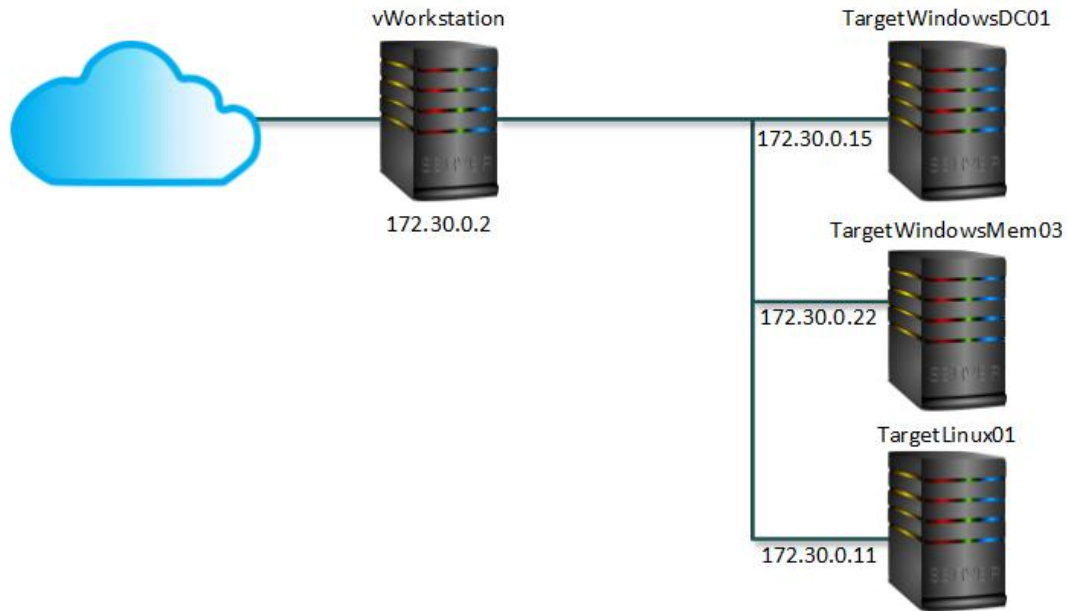
Finally, if assigned by your instructor, you will explore the virtual environment on your own in

**SECTION 3** of this lab to answer a set of questions and challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

## Topology

This lab contains the following virtual devices. Please refer to the network topology diagram below.

- vWorkstation (Windows Server 2016)
- TargetWindowsDC01 (Windows Server 2016)
- TargetWindowsMem03 (Windows Server 2016)
- TargetLinux01 (Debian Linux)



## Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- PowerBroker Identity Services Open (PBIS)
- PowerShell
- PuTTY
- Group Policy Management console
- vi Editor

## Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

### SECTION 1:

1. Lab Report file including screen captures of the following;

- newly configured Domain Password Policy;
- newly configured Account Lockout Policy;
- student user account logged on to TargetWindowsMem03;
- Administrator account logged on to TargetLinux01;

2. Files downloaded from the virtual environment:

- none;

3. Any additional information as directed by the lab:

- none;

4. Lab Assessment (worksheet or quiz - see instructor for guidance)

### SECTION 2:

1. Lab Report file including screen captures of the following:

- newly configured Domain Password Policy;
- newly configured Account Lockout Policy;
- student user account logged on to TargetWindowsMem03;
- Administrator account logged on to TargetLinux01;

2. Files downloaded from the virtual environment:

- none;

3. Any additional information as directed by the lab:

- none;

### SECTION 3:

1. Analysis and Discussion
2. Tools and Commands
3. Challenge Exercise

## Section 1: Hands-On Demonstration

**Note:** In this section of the lab, you will follow a step-by-step walk-through of the objectives for this lab to produce the expected deliverable(s).

1. On your local computer, **create** the **Lab Report file**.

Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.

2. **Proceed** with **Part 1**.

### Part 1: Configure a Domain-Level Policy

**Note:** Setting a strong password policy is one of the first steps in implementing a comprehensive security program. Weak passwords allow unauthorized access to your network, and by extension, the sensitive documents, proprietary code, and accounting files stored on it. A strong policy itself is not enough. Continuous monitoring for login success and failure is a good way to detect mischief on the network. An overabundance of failures from a particular user account can indicate a brute force attack. Equally suspicious are successful accesses at odd times or while a given resource is on vacation.

The organization you are working for has updated their password policy. You are charged with implementing that policy in the `securelabsondemand.com` domain. The new password policy must meet the following criteria.

- Users may not reuse any of the last 15 passwords
- Users must change passwords every 30 days
- Passwords may be reset at any time
- Password must be a minimum of 9 characters
- Password must meet basic complexity
- Enforce Domain Policy over Organizational Unit Policy
- Users must be “locked out” for 10 minutes, after failing to log in 3 times in a row
- All login successes and failures must be logged

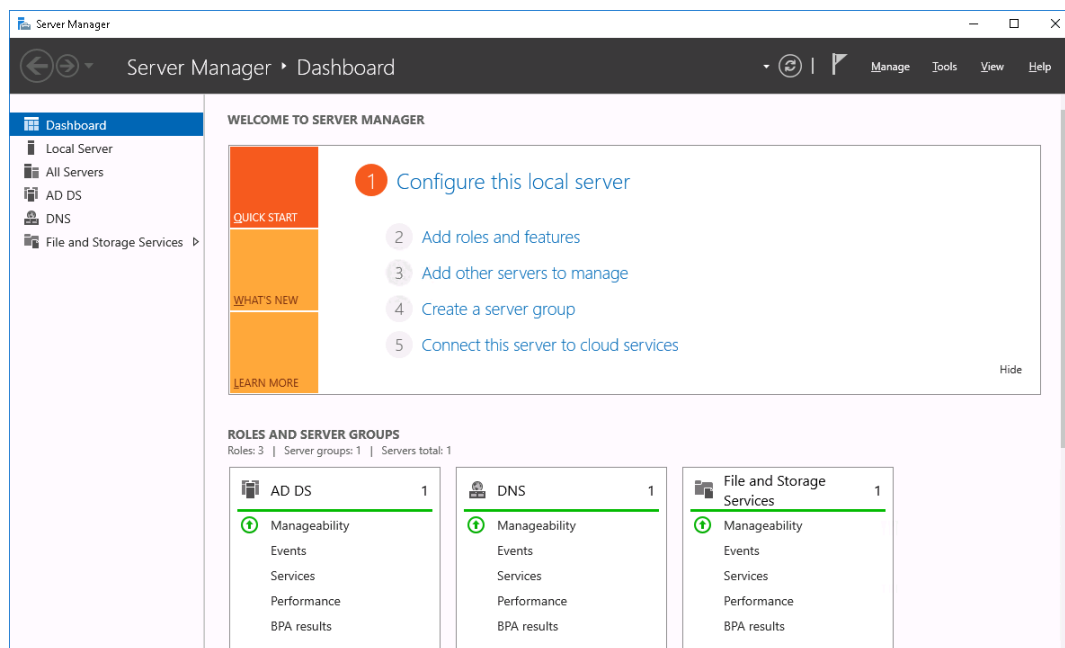
In the next steps, you will implement the organization’s password policy using Group Policy. Group Policy uses a layered approach to apply policy at the Local Server, Domain, and Sub-domain (Organizational Unit) level. Policies at the Organizational Unit level take precedence over Domain and

Local Policies. Local Policies are overridden by both Domain and Organizational Unit policies. Thus, the order of precedence is: Organizational Unit > Domain > Local.

1. On the vWorkstation desktop, **double-click** the **Connections folder**.
2. In the Connections folder, **double-click** the **TargetWindowsDC01 RDP shortcut** to open a remote connection to TargetWindowsDC01, the domain controller for the securelabsondemand.com domain.

The remote desktop will open with the IP address of TargetWindowsDC01 (172.30.0.15) in the title bar at the top of the window.

3. On the TargetWindowsDC01 taskbar, **click** the **Windows Start icon**, then **click** the **Server Manager button** to open the Server Manager application.

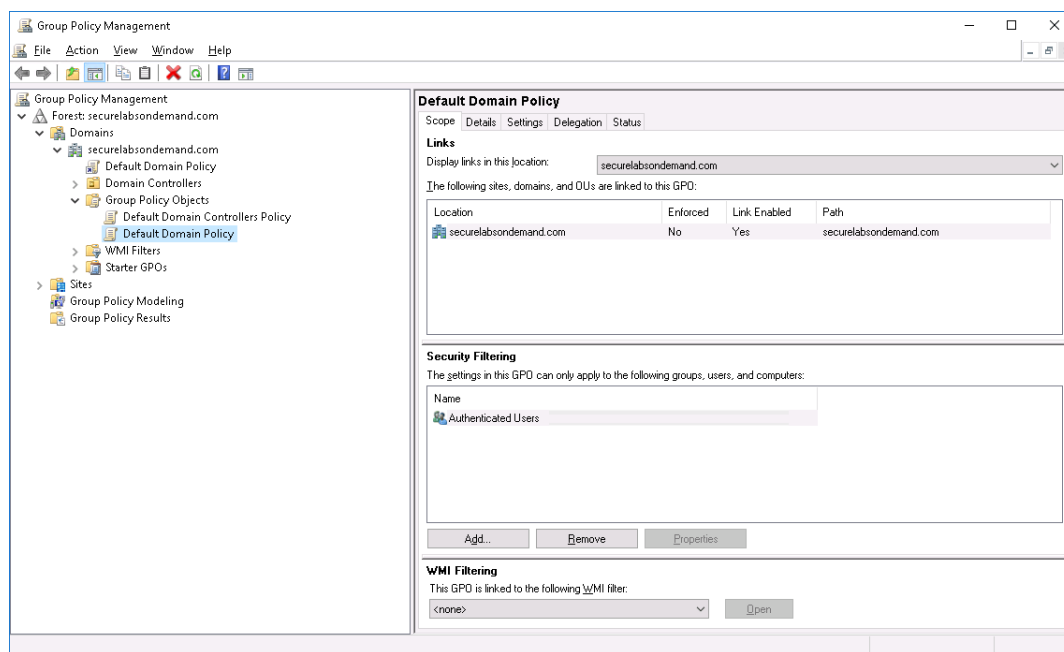


Server Manager



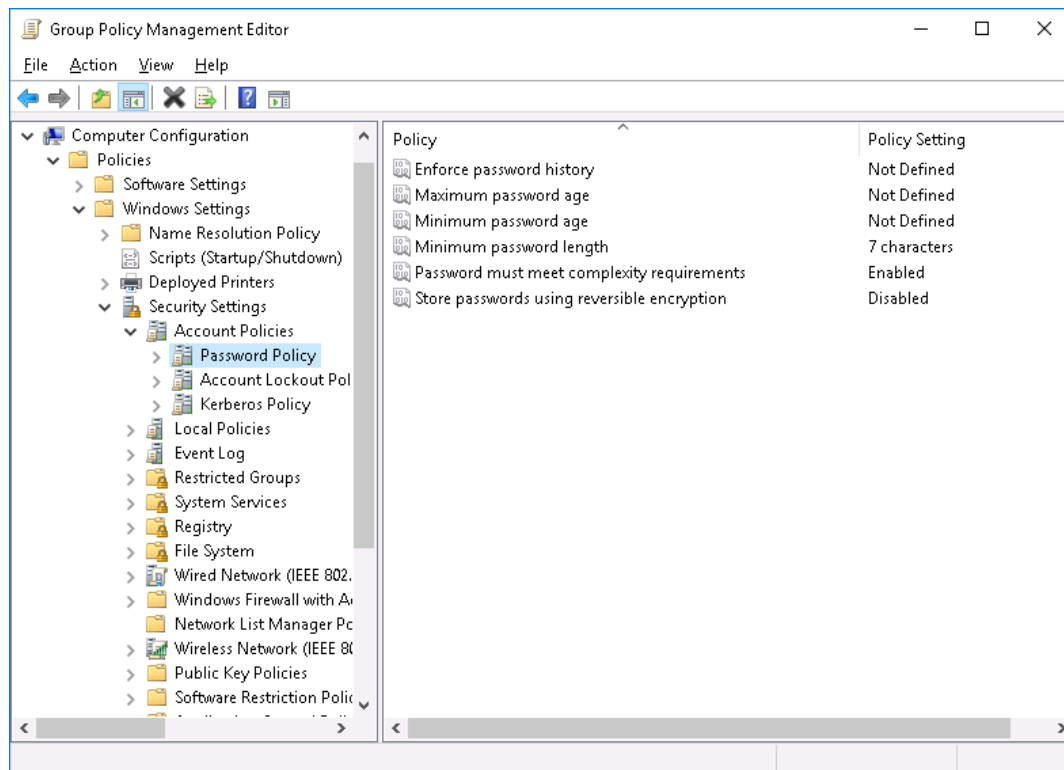
4. From the Server Manager menu bar, **select Tools > Group Policy Management** to open the Group Policy Management console.
5. In the left pane of the Group Policy Management window, **click** the Default Domain Policy link (**Forest > Domains > securelabsondemand.com > Group Policy Objects > Default Domain Policy**) if it is not already selected.

**Note:** In older versions of Microsoft Windows Domain Controllers, the Password Policies would be set to zero. This is not the case for Windows 2016 Domain Controllers; the Password Policies are now set with default values. In the next steps, you will proceed to harden the Password Policies even further.



Default Domain Policy

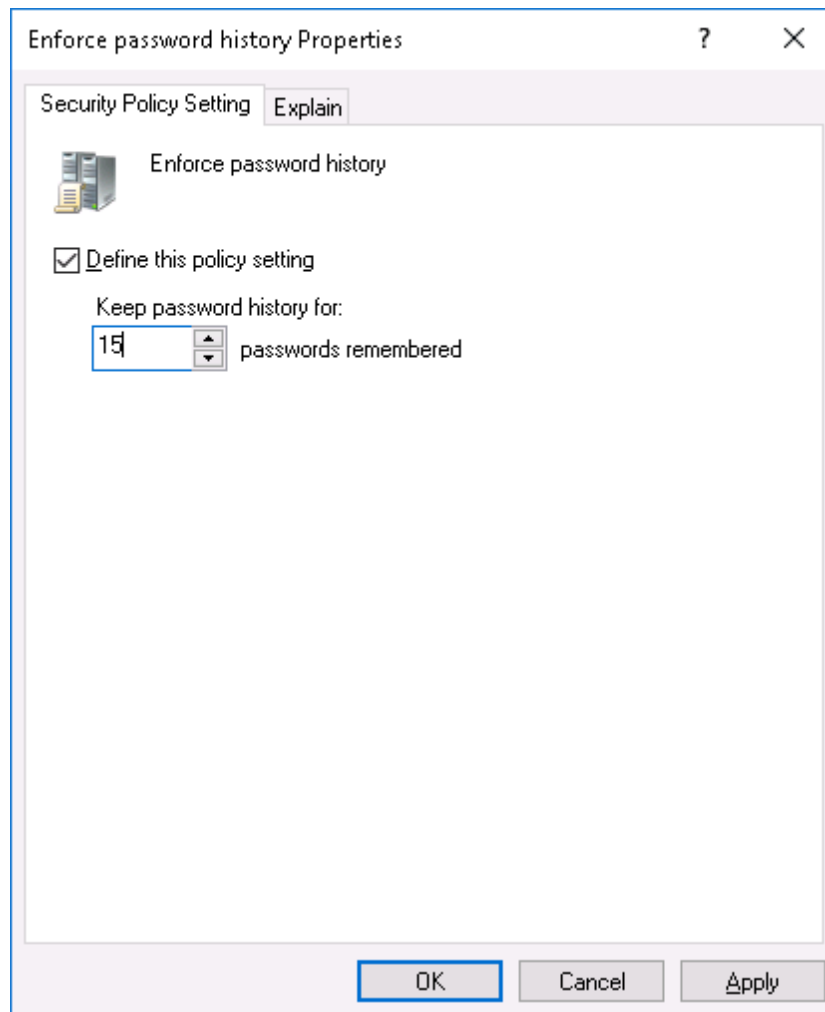
6. In the left pane of the Group Policy Management window, **right-click** the **Default Domain Policy** link and **select Edit** from the context menu to open the Group Policy Management Editor.
7. In the left pane of the Group Policy Management Editor, **click** the Password Policy link (**Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy**) to open the Password Policy settings.



### Password Policy

8. In the right pane of the Group Policy Management Editor, **double-click Enforce password history** to open the Enforce password history Properties dialog box.
9. In the Enforce password history Properties dialog box, **click the Define this policy setting checkbox**, then **type 15** in the *Keep password history for* box and **click OK** to save the change.

This policy will ensure that users cannot reuse any of their last 15 passwords.

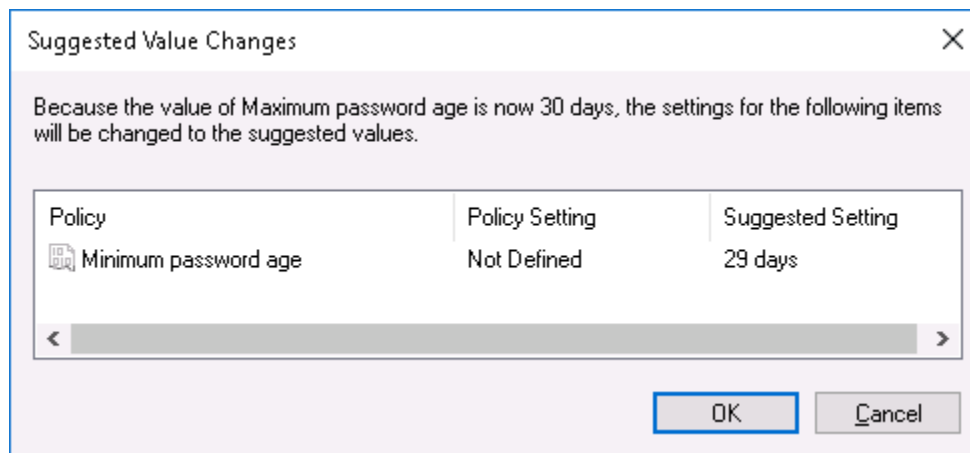


Minimum password length properties

10. In the right pane of the Group Policy Management Editor, **double-click Maximum password age** to open the Maximum password age Properties dialog box.
11. In the Maximum password age Properties dialog box, **click the Define this policy setting checkbox**, then **type 30** in the *Password will expire in* box and **click OK** to save the change.

This policy will ensure users must change passwords every 30 days.

Because the minimum password age, a related policy, is currently undefined, the Group Policy Manager will suggest a value. **Click OK** to accept the suggested change.



Suggested minimum password age

12. In the right pane of the Group Policy Management Editor, **double-click Minimum password length** to open the Minimum password length Properties dialog box.
13. In the Minimum password length Properties dialog box, **type 9** in the *Password must be at least* box, then **click OK** to save the change.

This policy will increase the default password length to 9 characters.

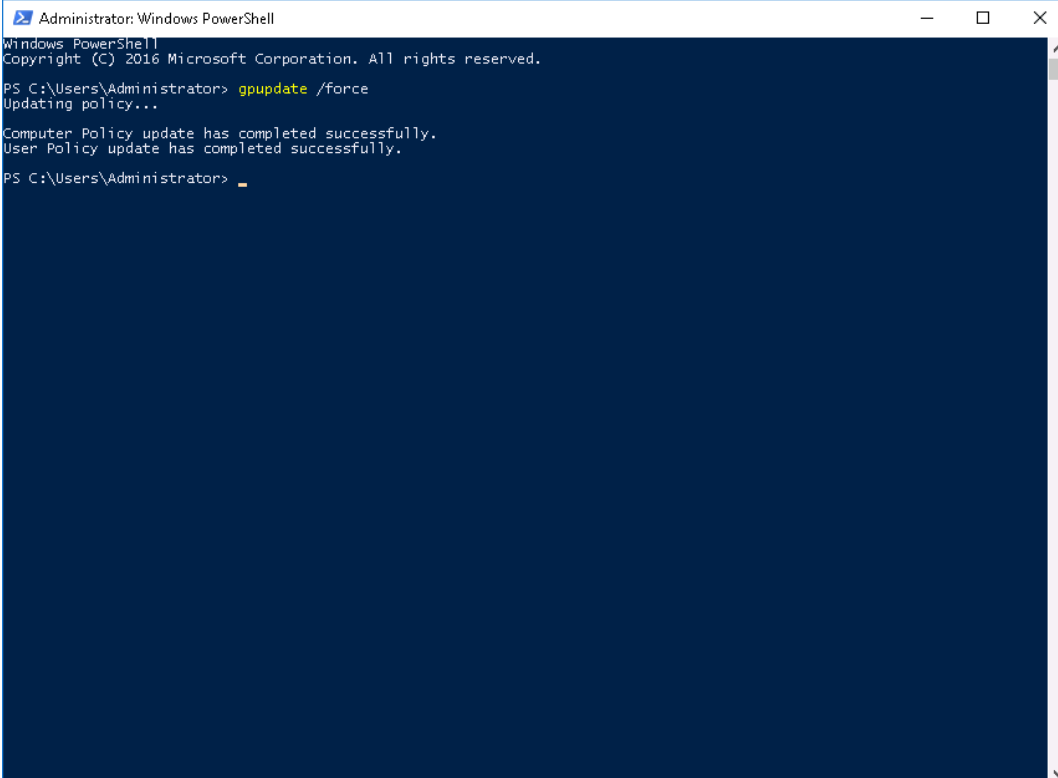
14. **Make a screen capture** showing the **newly configured Domain Password Policy settings** and **paste** it into your Lab Report file.

**Note:** In the previous steps, you made changes to the password policy. In order to see the changes take effect in the lab, you will need to force an update of all group policies, then reset the password for the student user account. You will make that change in the Active Directory Users and Computers console. Afterwards, you will return to the Group Policy Manager to implement the remaining changes to the Default Domain Policy.

15. On the TargetWindowsDC01 taskbar, **click the Windows Start icon**, then **click the Windows Powershell button** to open the Powershell application.

- At the PowerShell prompt, **type** `gpupdate /force` and **press Enter** to force an immediate update of all Group Policies on the TargetWindowsDC01 Domain Controller.

The system will generate a confirmation message indicating that Computer and User Policy updates have been completed successfully.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

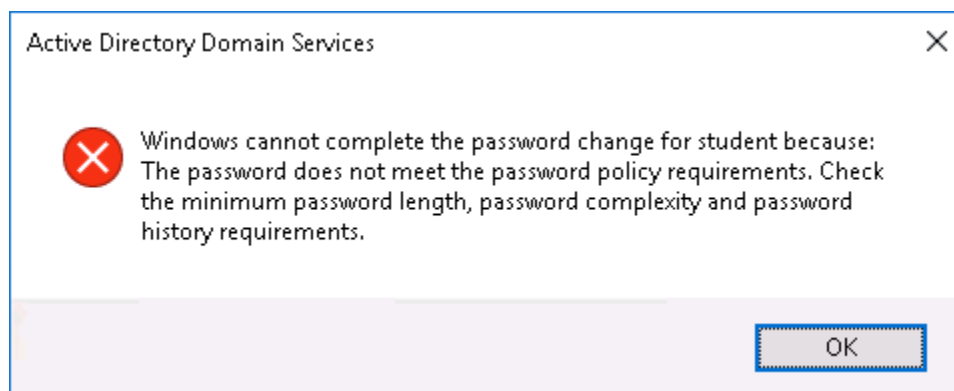
PS C:\Users\Administrator> _
```

`gpupdate`

- Minimize the PowerShell window.**
- On the TargetWindowsDC01 taskbar, **click the Server Manager icon** to restore the Server Manager window.
- On the Server Manager menu bar, **click Tools** and **select Active Directory Users and Computers** to open the Active Directory Users and Computers tool.

20. In the left pane of the Active Directory Users and Computers window, **click** the **Users organizational unit** to view users in the securelabsondemand.com domain.
21. In the right pane of the Active Directory Users and Computers window, **right-click** the **student user** and **select Reset Password** from the context menu.
22. In the Reset Password dialog box, **type P@ssw0rd**, a new password, in both the password boxes.
23. In the Reset Password dialog box, **click** the **User must change password at next logon checkbox** to remove the requirement, then **click OK** to change the password.

The system will generate an error message because this password is only 8 characters long and does not meet the new password requirements.



Active Directory error

24. **Click OK** to dismiss the error message.
25. **Repeat steps 21-23** using another new password: **P@ssw0rd!**. Be sure to remove the *User must change password at next logon* requirement.

This password meets the new requirements, so the system will generate a success message.

26. **Click OK** to dismiss the message.

27. **Close** the **Active Directory Users and Computer** window.

28. On the TargetWindowsDC01 taskbar, **click** the **Group Policy Management Editor** icon to restore the Group Policy Management Editor window.

29. In the left pane of the Group Policy Management Editor, **click** the Account Lockout Policy link (**Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy**).

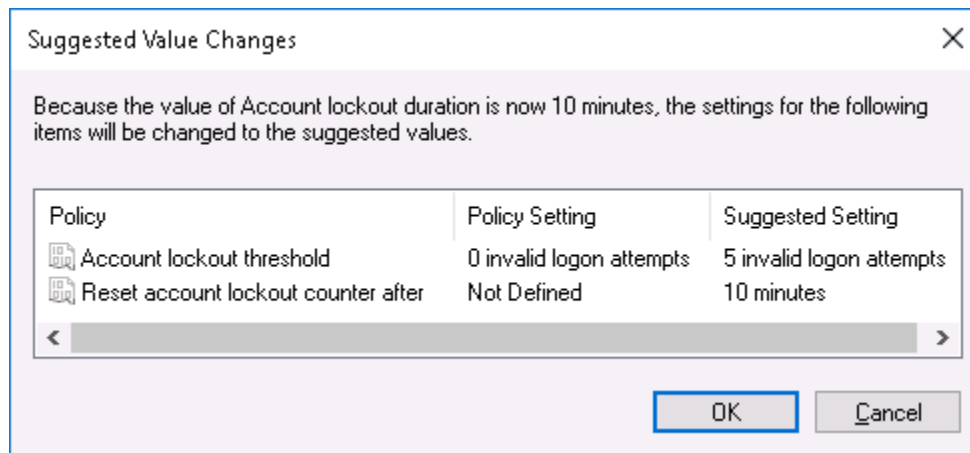
The Account Lockout policy is frequently enabled to prevent password cracking. Forcing hackers to wait any period of time in between failed login attempts may frustrate them into stopping the continued attempts, or allow you time to notice the activity.

30. In the right pane of the Group Policy Management Editor, **double-click Account lockout duration** to open the Account lockout duration Properties dialog box.

31. In the Account lockout duration Properties dialog box, **click** the **Define this policy setting checkbox**, then **type 10** in the Account is locked out for box and **click OK** to save the change.

This policy will ensure users who trigger the Account Lockout threshold will be unable to retry for 10 minutes.

**Note:** The Group Policy Manager will suggest changes to related policies. **Click OK** to accept the suggestions and close the window. The Reset account lockout counter after 10 minutes setting already meets the new password policy, which requires that users be “locked out” for 10 minutes, after failing to log in 3 times in a row. You will change the Account lockout threshold setting to meet the new password policy in the next step.



Suggested lockout policy changes

32. In the right pane of the Group Policy Management Editor, **double-click Account lockout threshold** to open the Account lockout threshold Properties dialog box.

33. In the Account lockout threshold Properties dialog box, **type 3** and **click OK** to save the change.

This policy will allow users 3 tries to correctly type their password.

34. **Make a screen capture** showing the **newly configured Account Lockout Policy settings** and **paste** it into your Lab Report file.

35. In the left pane of the Group Policy Management Editor, **click** the Audit Policy link (**Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy**).

The Audit Policy settings inform the system which items should be logged for future review. The new password policy requires that all login *successes* and *failures* must be logged.

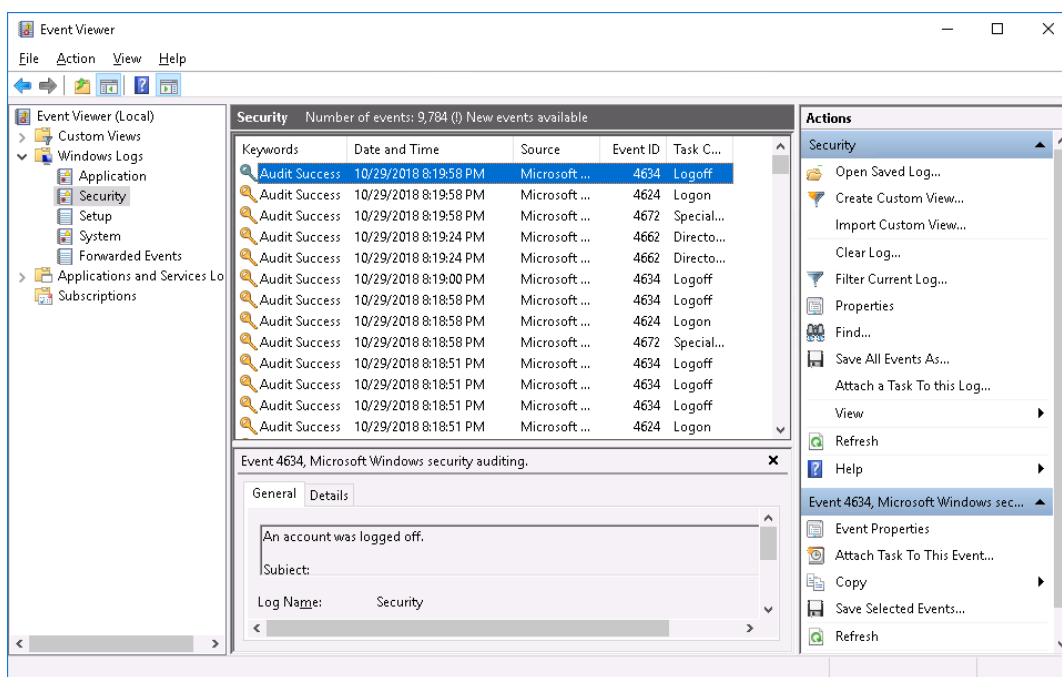
36. In the right pane of the Group Policy Management Editor, **double-click Audit account logon events** to open the Auditing account logon events Properties dialog box.



37. In the Auditing account logon events Properties dialog box, **click the Define this policy setting checkbox**, then **click the Failure checkbox** in the *Audit these attempts* section and **click OK** to save the change.

This policy will ensure that both successful logons and failed logons are logged. Notice that the Success checkbox is automatically selected when the policy is defined.

**Note:** The Audit policy is now set to record both successful and failed logons in the Windows Event Viewer. You can launch the Event Viewer from the Server Manager (Tools > Event Viewer). The Security Log, shown in the following figure, records those logon attempts in a format that can be filtered and exported.

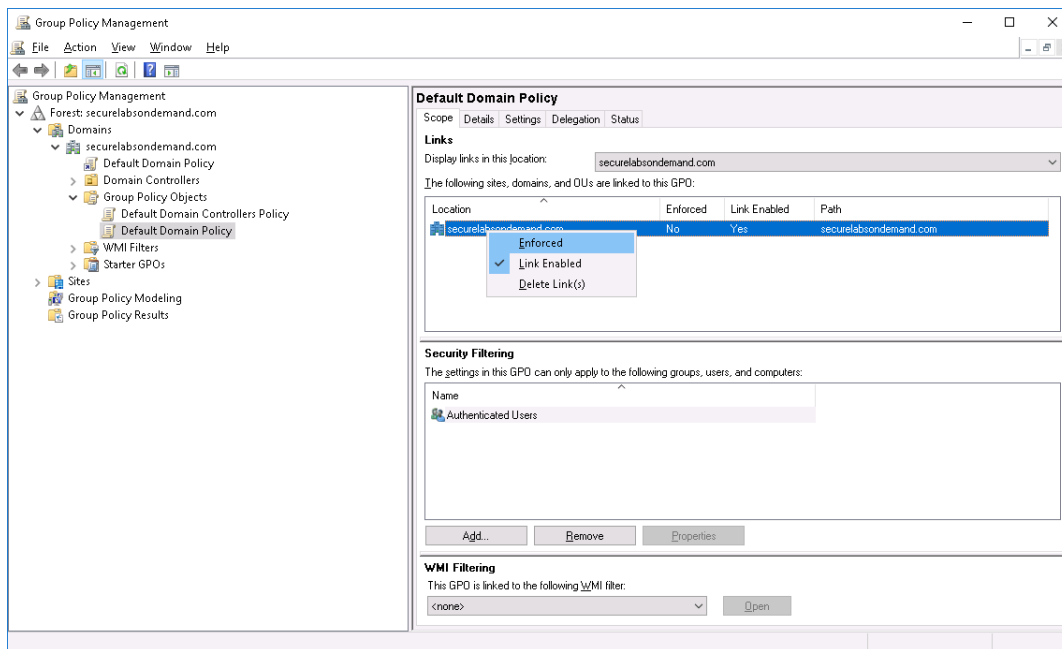


Windows Security Log

38. **Close the Group Policy Management Editor window.**
39. In the left pane of the Group Policy Management window, **click the Default Domain Policy link (Forest > Domains > securelabsondemand.com > Default Domain Policy)**, if it is not already selected.

40. In the right pane of the Group Policy Management window, in the Links section, under Location, **right-click** **securelabsondemand.com** and **select Enforced** from the context menu.

The new password policy requires that the Domain policies take precedence over Organizational Unit policies. Enforcing the Default Domain Policy option here ensures that Domain-level policies are not blocked or overridden by Organizational Unit policies even though Organizational Unit Policies have a higher precedence.



Enable Domain precedence

41. In the left pane of the Group Policy Management window, **double-click** the **Domain Controllers** link to open the Domain Controllers container in the right pane and expand the container contents in the left pane.

**Note:** The Domain Controllers “container” is a special Organizational Unit set aside for Domain Controllers only. While containers are not technically Organizational Units you can think of them as the same.

42. In the left pane of the Group Policy Management window, under Domain Controllers, **right-click Default Domain Controllers Policy** and **select Edit** from the context menu to open the Group Policy Management Editor.
43. In the left pane of the Group Policy Management Editor window, **click** the Password Policy link (**Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy**).

Notice that all of the password policies at the Domain Controller container level (which is equivalent to the Organizational Unit level) are undefined. However, because you already enforced the Domain-level policies, those policies will now apply to all Organizational Units and Domain Controller container levels. If desired, your organization could set a completely separate set of security policies for the Domain Controllers container level.

44. **Close** any **open windows**.
45. From the TargetWindowsDC01 taskbar, **restore** the **Powershell window**.
46. At the PowerShell prompt, **type** **gpupdate /force** and **press Enter** to force another update of all Group Policies on the TargetWindowsDC01 Domain Controller.
47. At the Powershell prompt, **type** **exit** and **press Enter** to close the PowerShell window.
48. **Close** the **remote TargetWindowsDC01 connection** to return to the vWorkstation desktop.

### Part 2: Verify Policy using a Member Server

**Note:** In the next steps, you will log on to the TargetWindowsMem03 machine which is a member of the securelabsondemand.com domain for which you just changed the password policies. Since the remote desktop shortcut requires a password, you will be prompted to type the new password that you set in Part 1 of this lab.

1. In the Connections folder, **double-click** the **TargetWindowsMem03 RDP shortcut** to open a remote connection to the TargetWindowsMem03 machine.

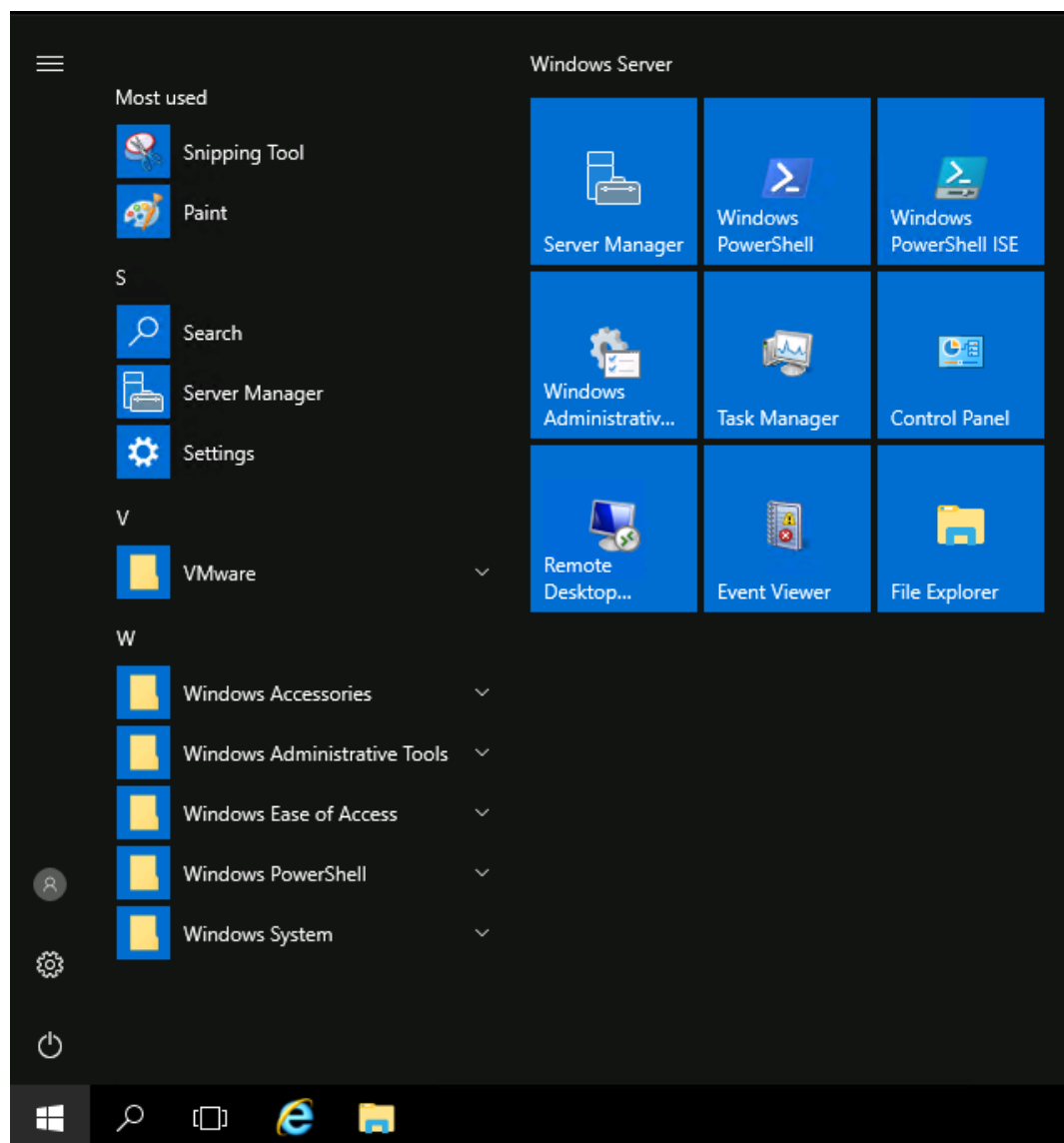
In Part 1 of this lab, you reset the password for the student account. The shortcut in the

Connections folder was created using the old password, which no longer meets the password requirements. You will need to change the credentials to match the new password you set in the Group Policy Management tool.

2. When prompted to enter the password, **type P@ssw0rd!**, the newly set TargetWindowsMem03 student password, and **press Enter** to open a remote connection to TargetWindowsMem03.

The remote desktop will open with the IP address of TargetWindowsMem03 (172.30.0.22) in the title bar at the top of the window.

3. When it opens automatically, **close** the **Server Manager window**.
4. On the TargetWindowsMem03 taskbar, **click** the **Windows Start icon** and **click** the **menu button** (?) in the top left corner of the Start menu to display the logged on user account.



Logged on user account

5. **Make a screen capture** showing the **logged on user account** and **paste** it into the Lab Report file.
6. **Close** the **remote TargetWindowsMem03 connection** to return to the vWorkstation.

**Note:** While passwords such as *P@ssw0rd!* or *!dr0wss@P* meet all of the new password requirements, they also demonstrate that it is still possible to make a new password that is very similar to an old one by simply reversing the order or appending characters to the end of a base password,

such as *P@ssw0rd*. Retaining a base password may be easy for users to remember, but it also makes it easier for a hacker to crack once they've determined the base password. User security education and user policy adoption are critical in any organization because the best security control is a willing and educated end user.

### Part 3: Add a Linux Workstation as a member of a Windows Domain

**Note:** In a corporate network, it is quite common for the IT department to have more than one operating system, or different platforms. In this scenario, your organization has a standalone Linux machine in a network governed by Windows Active Directory. The new corporate policy includes a requirement that all standalone systems must be brought into the Active Directory domain to help with good password management practices and help prevent unauthorized access to network resources.

Integrating Linux with Active Directory is not always a simple task. In the next steps, you will join a Linux server to a Windows 2016 domain using a pre-installed tool, PowerBroker Identity Services Open (PBIS).

1. In the Connections folder, **double-click** the **putty icon** to open a PuTTY session.
2. When prompted to run the application, **click Run** to continue.
3. In the PuTTY Configuration window, **type** **172.30.0.11** (the TargetLinux01 server) in the Host Name box and **click Open** to open a SSH session.

If prompted with a PuTTY Security Alert pop-up, **click Yes** to continue.

4. At the login prompt, **type** the following credentials and **press Enter** to log in with escalated privileges.
  - Login as: **root**
  - Password: **toor**

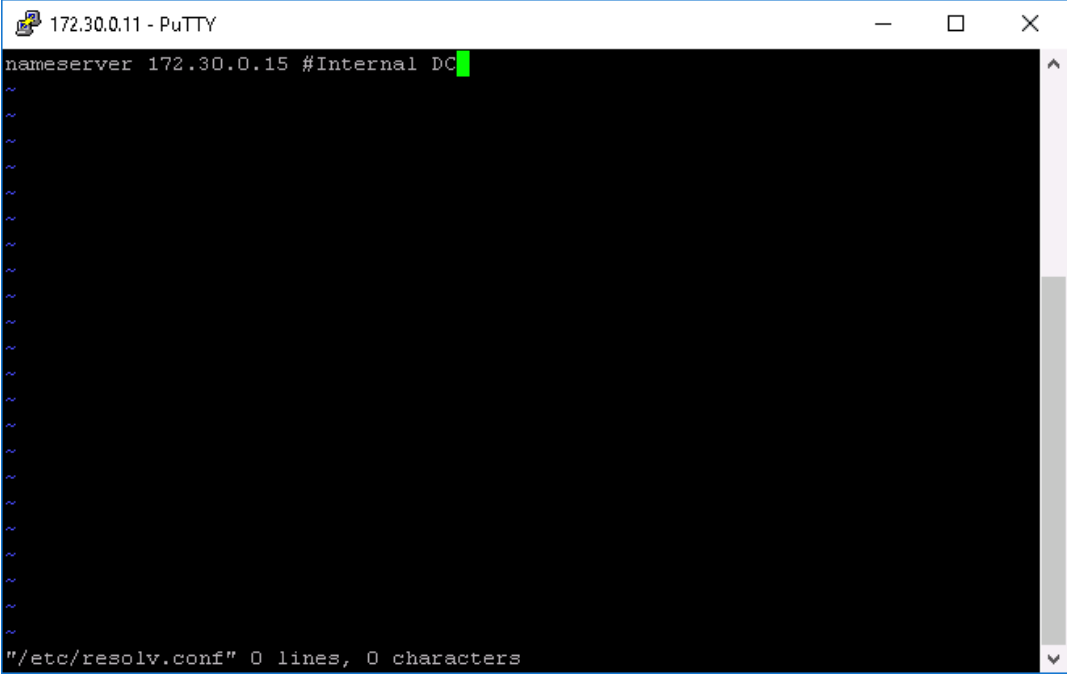
For security purposes, your password input will not appear on-screen.

5. At the root prompt, **type** **vi /etc/hosts** and **press Enter** to open the hosts file in the vi editor.









The screenshot shows a PuTTY terminal window titled "172.30.0.11 - PuTTY". The terminal displays the command `nameserver 172.30.0.15 #Internal DC` being entered. Below the command, there are several tilde (~) characters, indicating that the file is being edited in a text editor. At the bottom of the terminal, it says `"/etc/resolv.conf" 0 lines, 0 characters`.

Edited resolv.conf

13. In the vi Editor, **press ESC** to exit edit mode.
14. In the vi Editor, **type `:wq!`** and **press Enter** to save the file, close the vi Editor, and return to the root prompt.
15. At the root prompt, **type `exit`** and **press Enter** to close the PuTTY session and return to the vWorkstation.
16. In the Connections folder, **double-click** the **TargetLinux01 RDP shortcut** to open a remote connection to the TargetLinux01 machine.

The remote desktop will open with the IP address of TargetLinux01 (172.30.0.11) in the title bar at the top of the window.

17. When prompted to enter the student password, **type `student`**, the current password for this machine, and **press Enter** to continue.

**Note:** This RDP connection uses *local* credentials to log in to the machine. In the next steps, you will join the Linux system to the *securelabsondemand.com* Domain using the PowerBroker Identity Services Open (PBIS) tool. This change will apply the Domain settings you configured in Part 1 of this lab.

18. From the TargetLinux01 menu bar, **click Applications** and **select Accessories > Terminal** to open a terminal window.
19. At the command prompt, **type `su`** and **press Enter** to execute the switch user / super user (su) command and elevate your current privileges.

Notice that the command prompt changes from *student* to *root*.

20. When prompted for a password, **type `toor`** and **press Enter** to log in.

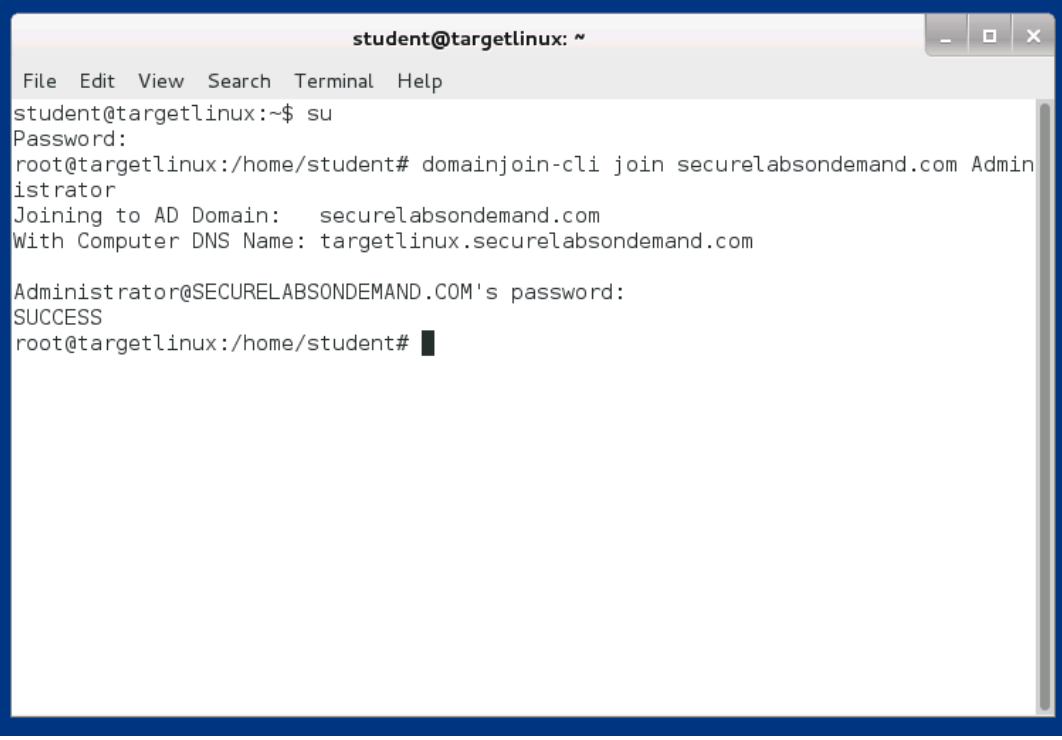
For security purposes, your password input will not appear on-screen.

21. At the command prompt, **type `domainjoin-cli join securelabsondemand.com Administrator`** and **press Enter** to join the Linux server to the *securelabsondemand.com* domain.

22. When prompted for the domain administrator's password, **type `P@ssw0rd`** and **press Enter**.

For security purposes, your password input will not appear on-screen.

The system will generate a success message when the Linux machine has successfully joined the Active Directory domain.

A terminal window titled 'student@targetlinux: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
student@targetlinux:~$ su
Password:
root@targetlinux:/home/student# domainjoin-cli join securelabsondemand.com Administrator
Joining to AD Domain: securelabsondemand.com
With Computer DNS Name: targetlinux.securelabsondemand.com

Administrator@SECURELABSONDEMAND.COM's password:
SUCCESS
root@targetlinux:/home/student#
```

PBIS confirmation message

23. At the command prompt, **type exit** and **press Enter** to remove elevated privileges.
24. At the command prompt, **type exit** and **press Enter** to close the terminal window.
25. In the top right corner of the TargetLinux01 menu bar, **click student**, the logged on user's name, and **select Log Out** to close your remote connection and return to the vWorkstation.
26. When prompted, **click Log Out** again to confirm.

**Note:** In the next steps, you will use the Active Directory Users and Computers Console to reset the password for the Administrator user account to meet the requirements of the new password policy. Afterwards, you will use that new password to log on to the TargetLinux server.

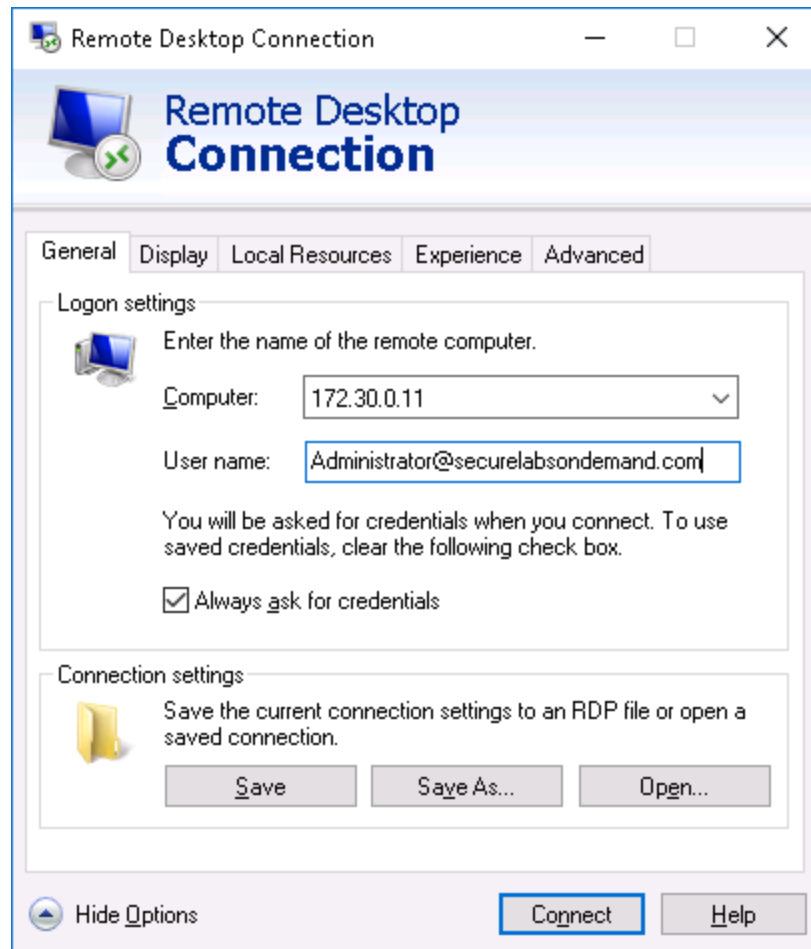
27. In the Connections folder, **double-click** the **TargetWindowsDC01 RDP shortcut** to open a remote connection to the TargetWindowsDC01 machine.
28. On the TargetWindowsDC01 taskbar, **click** the **Windows Start icon**, then **click** the **Server Manager button** to open the Server Manager application.
29. From the Server Manager menu, **click Tools** and **select Active Directory Users and Computers** to open the Active Directory Users and Computers tool.
30. In the left pane of the Active Directory Users and Computers window, **click** the **Users Organizational Unit** to view users in the securelabsondemand.com domain, if necessary.
31. In the right pane of the Active Directory Users and Computers window, **right-click** the **Administrator user** and **select Reset Password** from the context menu.
32. In the Reset Password dialog box, **type P@ssw0rd!**, a new password, in both password boxes, then **click OK**.

Because the Administrator account is currently logged on to the TargetWindowsDC01 server, you cannot edit the *User must change password at next logon* option. The account will automatically be prompted for a password the next time it is used.

33. **Click OK** to dismiss the success message.
34. **Close** the **Active Directory Users and Computer window**.
35. **Close** the **Server Manager window**.
36. **Close** the **remote TargetWindowsDC01 connection** to return to the vWorkstation.
37. In the Connections folder, **right-click** the **TargetLinux01 RDP shortcut** and **select Edit** from the context menu.

The original RDP shortcut uses the student account credentials to log on to the machine. You will need to edit the settings for this connection to use the Administrator account instead.

38. In the User name box, **type Administrator@securelabsondemand.com**, overwriting the student account name.  
Notice the capitalization on the account name. You must use a capital A.



Remote desktop credentials

39. **Click Connect** to complete the connection.
40. When prompted for the Administrator's password, **type P@ssw0rd!**, the new password for this account.  
The Linux GNOME desktop will open and the logged on user's account name will appear in the upper right corner of the screen.

**Note:** If you receive an error stating that the GNOME desktop did not start correctly, dismiss it. This is normal and part of the Security policy blocking some features of the Debian Linux desktop. **Click OK** to dismiss the message.

41. **Make a screen capture** showing the **Linux desktop with the logged on user's account name** and **paste** it into your Lab Report file.

42. **Close** the **remote TargetLinux01 connection** to return to the vWorkstation.

**Note:** This completes Section 1 of this lab. There are no deliverable files for this section.

## Section 2: Applied Learning

**Note:** **SECTION 2** of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods.

**Please confirm with your instructor that you have been assigned Section 2 before proceeding.**

1. On your local computer, **create** the **Lab Report file**.  
Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.
2. If you already completed Section 1 of this lab, you will need to reset the virtual environment before beginning Section 2. To reset the virtual environment, complete one of the following options.
  - a. **Click Options > Reset Lab** to restore all virtual machines to their base state. This will take several minutes to complete. If you do not see the vWorkstation desktop after five minutes, **click Options > Reload Lab** to reload your lab connection.
  - b. **Click Disconnect**, then **select Discard Changes** to end your lab session without creating a StateSave. If you previously created a StateSave, delete the StateSave at the launch page, then start a new lab session.
3. **Proceed** with **Part 1**.

### Part 1: Configure a Domain-Level Policy

**Note:** Setting a strong password policy is one of the first steps in implementing a comprehensive security program. Weak passwords allow unauthorized access to your network, and by extension, the sensitive documents, proprietary code, and accounting files stored on it. A strong policy itself is not enough. Continuous monitoring for login success and failure is a good way to detect mischief on the network. An overabundance of failures from a particular user account can indicate a brute force attack. Equally suspicious are successful accesses at odd times or while a given resource is on vacation.

The organization you are working for has updated their password policy. You are charged with implementing that policy in the `securelabsondemand.com` domain. The new password policy must meet the following criteria.

- Users may not reuse any of the last 10 passwords
- Users must change passwords every 25 days
- Passwords may be reset at any time
- Password must be a minimum of 10 characters
- Password must meet basic complexity
- Enforce Domain Policy over Organizational Unit Policy
- Users must be “locked out” for 5 minutes, after failing to log in 3 times in a row
- All login successes and failures must be logged

In the next steps, you will implement the organization’s password policy using Group Policy. Group Policy uses a layered approach to apply policy at the Local Server, Domain, and Sub-domain (Organizational Unit) level. Policies at the Organizational Unit level take precedence over Domain and Local Policies. Local Policies are overridden by both Domain and Organizational Unit policies. Thus, the order of precedence is: Organizational Unit > Domain > Local.

1. **Open a remote connection** to the **TargetWindowsDC01** machine.
2. **Launch** the **Server Manager** and **open** the **Group Policy Management** tool.
3. **Navigate** to the Default Domain Policy (**Forest > Domains > securelabsondemand.com > Group Policy Objects > Default Domain Policy**).

**Note:** In older versions of Microsoft Windows Domain Controllers, the Password Policies would be set to zero. This is not the case for Windows 2016 Domain Controllers; the Password Policies are now set with default values. You will proceed to harden the policies even further.

4. **Open** the **Group Policy Management Editor** for Default Domain Policy.
5. **Navigate** to Password Policies (**Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policies**), and update the following password policies as noted.



- Enforce password history: **Keep last 10 passwords**
  - Maximum password age: **Change passwords every 25 days**
  - Minimum password length: **Change the default to 10 characters**
6. **Make a screen capture** showing the **newly configured Domain password policies** and **paste** it into your Lab Report file.

**Note:** In the previous steps, you made changes to the password policy. In order to see the changes take effect in the lab, you will need to reset the password for the student user account. You will make that change in the Active Directory Users and Computers Console. Afterwards, you will return to the Group Policy Manager to implement the remaining changes to the Default Domain Policy.

7. **Restore** the **Server Manager window** and **launch** the **Active Directory Users and Computers tool**.
8. In the Users organizational unit, **reset** the **password** for the student account.
9. In the Reset Password dialog box, **change** the password to **!!dr0wss@P**, then **deselect** the **User must change password at next logon checkbox** and **click OK** to change the password.

This password meets the new requirements so the system will generate a success message.

10. **Dismiss** the **success message**.
11. **Close** the **Active Directory Users and Computers window** and **restore** the **Group Policy Management Editor window**, then complete the remaining policy changes.
12. **Navigate** to the Account Lockout Policy (**Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy**) and update the following account lockout policies as noted.

The Account Lockout policy is frequently enabled to prevent password cracking. Forcing hackers to wait any period of time in between failed login attempts may frustrate them into stopping the continued attempts, or allow you time to notice the activity.

- Account lockout duration: **Change the lockout time to 5 minutes**
- Account lockout threshold: **Change the lockout attempts to 3 tries**

**Note:** The system will generate a pop-up window with suggestions for related policy options. **Click OK** to accept the suggestions and dismiss the window.

13. **Make a screen capture** showing the **configured Account Lockout Policies** and **paste** it into your Lab Report file.
14. **Navigate** to the Audit Policy (**Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy**) and update the following account lockout policies as noted.

The Audit Policy settings inform the system which items should be logged for future review. The new password policy requires that all login *successes* and *failures* must be logged. A potential draw back in enabling auditing is that if the system is under load and a brute force attack occurs, this will generate more disk, network, and CPU spikes, which can cripple a system.

- Audit account logon events: **Both successful logons and failed logons are logged**
15. **Close** the **Group Policy Manager Editor** window.
  16. **Enforce** the **default domain policy** for securelabsondemand.com.

The new password policy requires that the Domain policies take precedence over Organizational Unit policies. Enforcing the Default Domain Policy option here ensures that Domain-level policies are not blocked or overridden by Organizational Unit policies even though Organizational Unit Policies have a higher precedence.

17. **Close** any **open windows** and **open PowerShell**.
18. At the PowerShell prompt, **execute the command** to force an immediate update of all Group Policies on the Domain Controller, then **close** the **PowerShell window**.

The system will generate a confirmation message indicating that the Computer and User

Policy update has been updated successfully.

19. **Close the remote TargetWindowsDC01 connection.**

## **Part 2: Verify Policy using a Member Server**

**Note:** In the next steps, you will log on to the TargetWindowsMem03 machine which is a member of the securelabsondemand.com domain for which you just changed the password policies. Since the new policy requires a 10-character password, you will be prompted to use the administrator password.

1. **Open a remote connection** to the **TargetWindowsMem03** machine.
2. When prompted, **enter** **!!dr0wss@P**, the new student account password.
3. **Open the Windows Start menu** and **click the menu button** (?) to reveal the logged on user account.
4. **Make a screen capture** showing the **logged on user account** and **paste** it into the Lab Report file.
5. **Close the remote TargetWindowsMem03 connection.**

**Note:** While *P@ssw0rd!2* or *!!dr0wss@P* meet all of the new password requirements, they also demonstrate that it is still possible to make a new password that is very similar to an old one by simply reversing the order or appending characters to the end of a base password, such as *P@ssw0rd!*. Retaining a base password may be easy for users to remember, but it also makes it easier for a hacker to crack once they've determined the base password. User security education and user policy adoption are critical in any organization because the best security control is a willing and educated end user.

## **Part 3: Add a Linux Workstation as a member of a Windows Domain**

**Note:** In a corporate network, it is quite common for the IT department to have more than one operating system, or different platforms. In this scenario, your organization has a standalone Linux machine in a network governed by Windows Active Directory. The new corporate policy includes a requirement that all standalone systems must be brought into the Active Directory domain to help with

good password management practices and help prevent unauthorized access to network resources.

Integrating Linux with Active Directory is not always a simple task. In the next steps, you will join a Linux server to a Windows 2016 domain using a pre-installed tool, PowerBroker Identity Services Open (PBIS).

1. **Open the PuTTY application.**
2. **Open an SSH session to 172.30.0.11.**
3. At the PuTTY login prompt, **enter** the following credentials to log in with escalated privileges.

- Login as: **root**
- Password: **toor**

4. At the root prompt, **execute the command** to open the /etc/hosts file in the vi editor.

The hosts file maps IP addresses to hostnames.

5. In the line below 172.30.0.11 targetlinux.securelabsondemand.com targetlinux, **insert** **172.30.0.15 TargetWindowsDC01.securelabsondemand.com TargetWindowsDC01** to allow the Linux system to reach the Domain Controller (DC) on the Windows 2016 server by name, then **save the hosts file**.

6. **Execute the command** to open the /etc/resolv.conf file in the vi editor.

The resolv.conf file is used to configure the Domain Name Server (DNS).

7. At the cursor, **insert** **nameserver 172.30.0.15 #Internal DC** to direct the Linux system to use the Windows Domain Controller as the DNS server, then **save the file**.

8. **Close the PuTTY session.**

9. **Open a remote connection** to the **TargetLinux01** machine.
10. When prompted to enter the student password, **type student** and **press Enter** to continue.

**Note:** This RDP connection uses *local* credentials to log in to the machine. In the next steps, you will join the Linux system to the securelabsondemand.com Domain using the PowerBroker Identity Services Open (PBIS) tool. This change will apply the Domain settings you configured in Part 1 of this lab.

11. Open a terminal window and **execute the command** to elevate your current privileges,  
  
When prompted, **enter** the password **toor**.
12. At the command prompt, **execute domainjoin-cli join securelabsondemand.com Administrator** to join the Linux server to the securelabsondemand.com domain.
13. When prompted for the domain administrator password, **type P@ssw0rd**, then **press Enter**.

The system will generate a success message when the Linux machine has successfully joined the Active Directory domain.

14. At the command prompt, **execute the command** to remove elevated privileges, then **close the terminal window**.
15. **Log Out** of the **Student account** to close the remote TargetLinux01 connection.

**Note:** In the next steps, you will use the Active Directory Users and Computers Console to reset the password for the Administrator user account to meet the requirements of the new password policy. Afterwards, you will use that new password to log on to the TargetLinux server.

16. **Open a remote connection** to the **TargetWindowsDC01** machine.

17. **Launch** the **Server Manager** and open **Active Directory Users and Computers**.
18. In the Users OU, **select** the **Administrator account**, and **reset** the password to **!!dr0wss@P**.  
  
Because the Administrator account is currently logged on to the TargetWindowsDC01 server, you cannot click the User must change password at next logon option. The account will automatically be prompted for a password the next time it is used.
19. **Click OK** to dismiss the message.
20. **Close** any **open windows**.
21. **Close** the **remote TargetWindowsDC01 connection**.
22. **Open a remote connection** to the **TargetLinux01** machine using the **Administrator@securelabsondemand.com** account.

The original RDP shortcut uses the studentaccount credentials to log in to the machine. You will need to edit the settings for this connection to use the Administrator account. Notice the capitalization on the account name. You must use a capital A.

23. When prompted for the Administrator's password, **enter !!dr0wss@P**, the new password for this account.

The Linux GNOME desktop will open and the logged on user's account name will appear in the upper right corner of the screen.

**Note:** If you receive an error stating that the GNOME desktop did not start correctly, dismiss it. This is normal and part of the Security policy blocking some features of the Debian Linux desktop. **Click OK** to dismiss the message.

24. **Make a screen capture** showing the **Linux desktop with the logged on user's account name** and **paste** it into your Lab Report file.

25. **Close** the **remote TargetLinux01 connection**.

**Note:** This completes Section 2 of this lab. There are no deliverable files for this section.

## Section 3: Lab Challenge and Analysis

**Note:** The following challenge questions are provided to allow independent, unguided work, similar to what you will encounter in a real situation. You should aim to improve your skills by getting the correct answer in as few steps as possible. Use screen captures in your lab document where possible to illustrate your answers.

### Part 1: Analysis and Discussion

In Part 1 of this lab, you changed the Audit Policy to record both successful and unsuccessful login attempts. What drawbacks do you foresee when Auditing is enabled for both success and failure?

### Part 2: Tools and Commands

In Part 1 of this lab, you changed the Audit Policy to record both successful and unsuccessful login attempts. You also changed the Account Lockout duration. Using the TargetWindowsMem03 shortcut in the Connections folder, attempt to open a remote connection to that machine using the wrong password 3 times in order to trigger an account lockout. Once the lockout period has expired, open a remote connection to the TargetWindowsMem03 machine and open the Event Viewer in the Server Manager (Tools > Event Viewer) and make a screen capture showing the failed logins.

### Part 3: Challenge Exercise

On the TargetWindowsDC01 machine, use the Active Directory Users and Computers tool to create a new domain user account for yourself, using your own name and password. Use the domain email address when prompted. Open a remote connection to TargetWindowsMem03 and attempt to connect using your own credentials by editing the shortcut in the Connections folder. Make screen captures to document your process and record the results of your log in attempt. Briefly describe why your attempt succeeded or failed.

*Hint: You may need to grant permission to your account to use Remote Desktop Protocol on the TargetWindowsMem03 machine.*