Windows security, Active Directory and Azure AD

TD12 – Module 2 – Section 2

July 2020  
V3.1

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only, and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third-party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

This training uses various tools and utilities downloaded from the Internet for the classroom environment.   
Downloading any tools, installing and using them should only be done at your own risk security checked the tools in a test environment.

© 2020 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx> are trademarks of the Microsoft group of companies. All other trademarks are the property of their respective owners.

Contents

[Windows security, Active Directory and Azure AD Lab step-by-step 1](#_Toc43912164)

[Abstract and learning objectives 1](#_Toc43912165)

[Overview 2](#_Toc43912166)

[Requirements 2](#_Toc43912167)

[Before the exercise 3](#_Toc43912168)

[List of VM to start 3](#_Toc43912169)

[How to start and connect to a VM 4](#_Toc43912170)

[Information 6](#_Toc43912171)

[Exercise 1: GPO for Hardening 6](#_Toc43912172)

[Task 1: Check Default user right CSI-TD-DC1 6](#_Toc43912173)

[Task 2: Create a Hardening GPO for DCs 7](#_Toc43912174)

[Task 3: Create a Hardening GPO for Exchange 8](#_Toc43912175)

[Exercise 2: Enumerate users using SAMR 10](#_Toc43912176)

[Task 1: Use NMAP to browse User in AD 10](#_Toc43912177)

[Exercise 3: LDAP connection 11](#_Toc43912178)

[Task 1: LDAP connection with Anonymous logon 11](#_Toc43912179)

[Task 2: LDAP connection without LDAP SIGN in 11](#_Toc43912180)

[Exercise 4: List group members 13](#_Toc43912181)

[Task 1: List AD group Members 13](#_Toc43912182)

[Exercise 5: LAPS 14](#_Toc43912183)

[Task 1: Install LAPS and update de schema 14](#_Toc43912184)

[Task 1: Create a GPO to deploy LAPS 14](#_Toc43912185)

[Questions: 15](#_Toc43912186)

[After the Lab 16](#_Toc43912187)

[Task 1: Stop and deallocated all the VMs 16](#_Toc43912188)

# Windows security, Active Directory and Azure AD Lab step-by-step

## Abstract and learning objectives

This training is designed to provide exposure to many of Microsoft Windows, Active Directory and Azure Active Directory security features.

## Overview

In this Lab, the attendees will deploy security group policies and manipulate various network security settings on domain controllers.

## Requirements

1. Attendee’s machine:
   1. Ideal resolution 1920 x 1080
   2. An Internet browser
   3. An RDP client
   4. Internet access without restriction on outbound connections.   
      The following outbound TCP port must be accessible :

* **TCP/80 and TCP/443** to reach Azure Portal
* **TCP/3389** to establish RDP remote connection to virtual machines exposed directly to Internet

or

* **TCP/(49152 to 65535)** to establish RDP remote connection to virtual machines exposed by a Load Balancer

## Before the exercise

Duration: 10 minutes

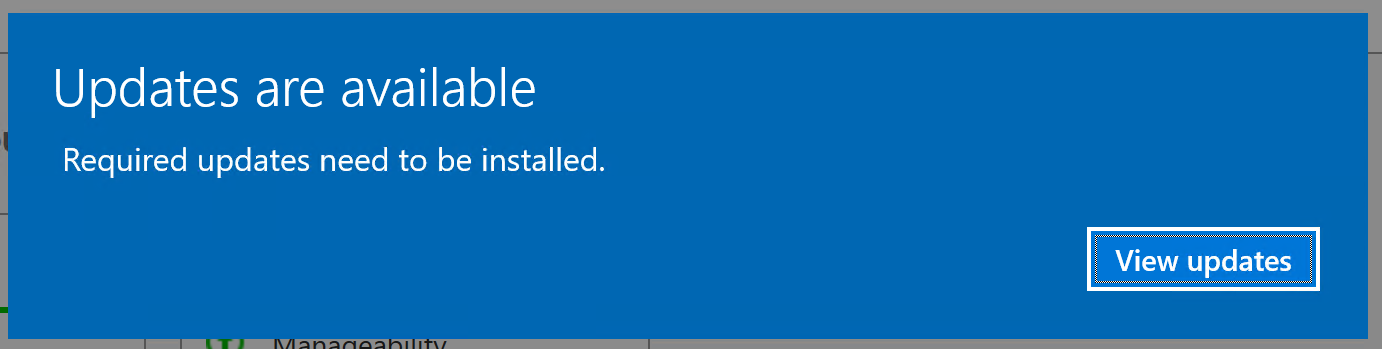
Synopsis: In this section, you will set up your environment for use in the rest of the Lab. You should have the following environment.

#### List of VM to start

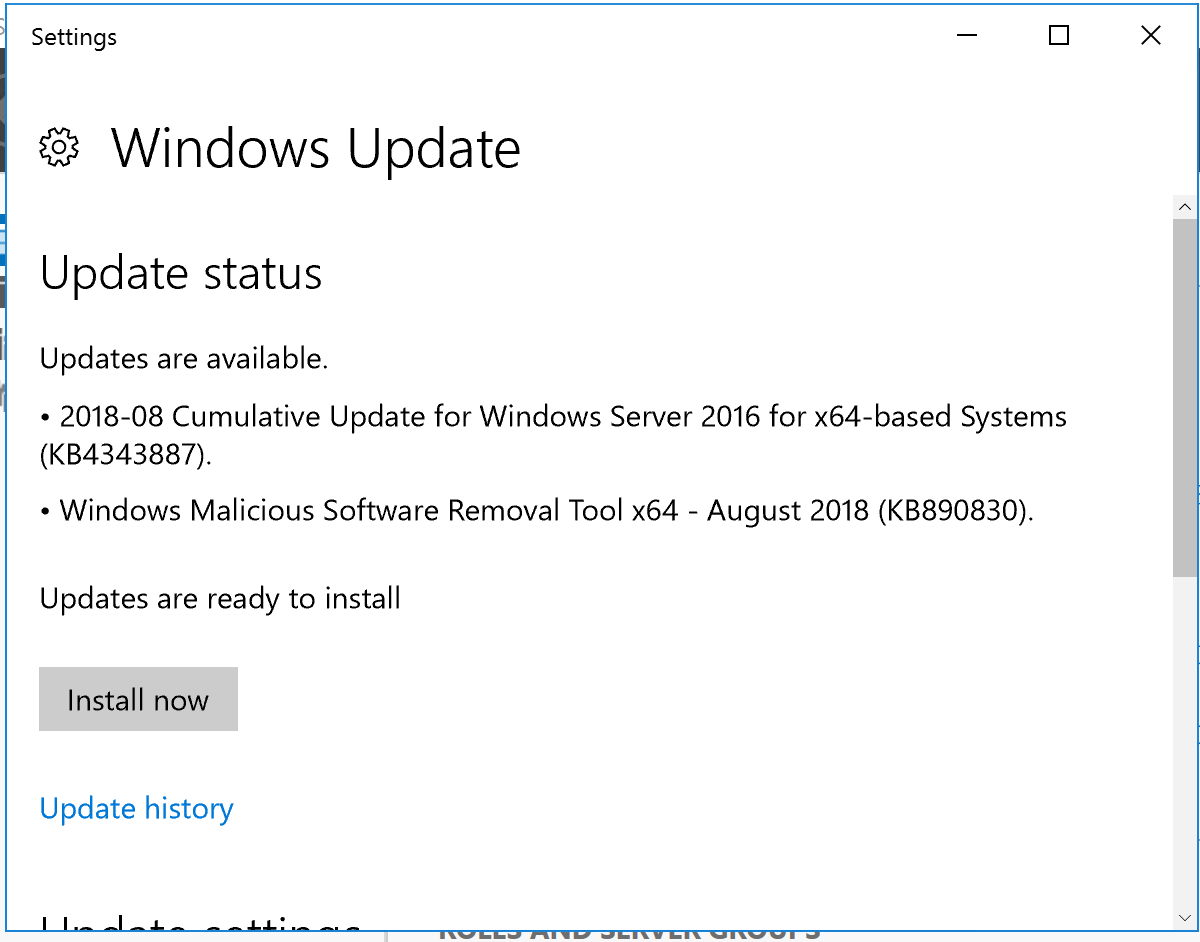
**Remember to start the DC first and to wait 1 minute before starting the other VMs.**

|  |  |  |  |
| --- | --- | --- | --- |
| Name of VM | Hostname | OS Type | Role |
| ID-DC1 | CSI-TD-DC1 | Windows Server 2016 Standard | DC |
| ID-SRV1 | CSI-TD-SRV1 | Windows Server 2016 Standard | Server |
| ID-EXC1 | CSI-TD-EXC1 | Windows Server 2016 Standard | Server |
| ID-CLI1 | CSI-TD-CLI1 | Windows 10 Enterprise | Desktop |

Note that the machines have been provisioned in March 2020.   
Therefore, it is possible to see the following message while connecting for the first time to the servers:



In this case, click on View updates.



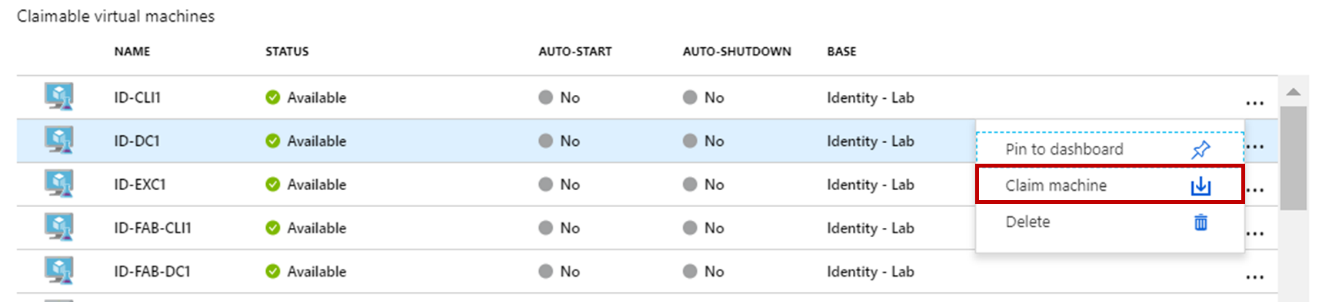
We do not need the latest updates for these labs so you can close this window.

#### How to start and connect to a VM

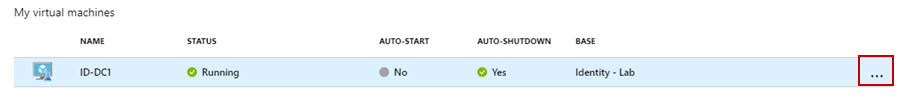
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



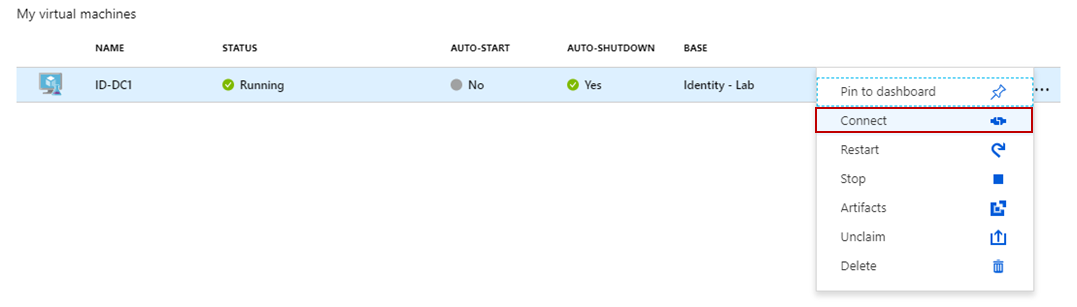
1. To start a VM, click on “Claim machine”



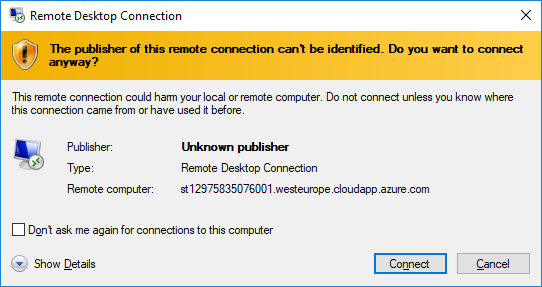
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



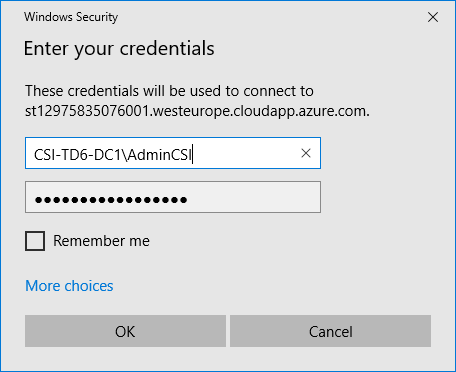
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



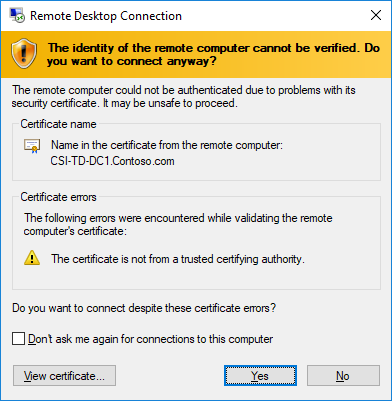
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



1. Enter the user name and password to connect to the Virtual Machine detailed in each exercise below.   
   (Do not use your student or organizational account.)



1. A warning on the self-issued certificate is displayed. You can safely ignore this warning by clicking on Yes.



## Information

If you have C drive space issue on CSI-TD-CL1

Go to the folder Tools and remove the Exchange source

## Exercise 1: GPO for Hardening

Duration: 45 minutes

Synopsis: In this exercise, attendees will create two GPOs to enforce some settings for Domain Controllers and Exchange servers.

#### Task 1: Check Default user right CSI-TD-DC1

1. Open a session on **CSI-TD-DC1**
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Launch **GPEdit.msc**
3. Check the following **User Rights Assignment**
   1. **Act Part of the Operating System**

………………………………………………………………………………………………

* 1. **Debug Programs**

………………………………………………………………………………………………

* 1. **Back up Files and directories**

………………………………………………………………………………………………

* 1. **Load and unload device drivers**

………………………………………………………………………………………………

* 1. **Force shutdown from a remote system**

………………………………………………………………………………………………

* 1. **Restore Files and directories**

………………………………………………………………………………………………

* 1. **Shutdown the system**

………………………………………………………………………………………………

1. Try to modify the User right “**Act part of the Operating System**” and to Add **Account Operators** .
2. Is it working?

………………………………………………………………………………………………

1. Do not validate the modifications
2. Try to modify the user right “**Debug Programs**” and to add **Account Operators** .
3. Is it working ?

………………………………………………………………………………………………

The setting with this icon means that the User rights has been set by GPO and can no longer be modified locally.

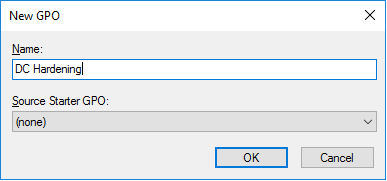
1. Close the window
2. Launch a command prompt as an **administrator**
3. Generate a GPO Result in HTML
4. Open your HTML GPO report in IE
5. Check the section **Settings/Policies/Windows Settings/Security settings/ Local Policies/User Rights Assignment**
6. Which GPO has set the User Rights “**Debug programs**”

………………………………………………………………………………………………

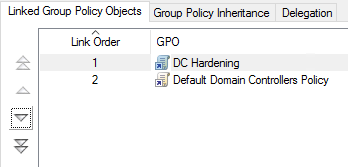
1. Close Internet Explorer

#### Task 2: Create a Hardening GPO for DCs

1. Launch **Group Policy Management**
2. Create a new **GPO** for the OU **Domain Controllers** names **DC Hardening**



1. Ensure that this GPO has a link order to 1
2. Now the link order should be
   1. **DC Hardening**: 1
   2. **Default Domain Controllers Policy**: 2



1. Edit **DC Hardening**
2. Set **Act pact of the operating system** to ensure that it is empty
3. Set **Back up files and directories :** only for **Administrators**
4. Set **Debug programs** only for **Administrators**
5. Set **Force shutdown from a remote system** only for **Administrators**
6. Set **Load and unload device drivers** only for **Administrators**
7. Set **Restore files and directories** only for **Administrators**
8. Set **Shutdown the system** only for **Administrators**

*The list of User rights listed in this exercise is not the completed list of the User Rights that need to be enforced. There are here as example. You can download the recommended security settings for DCs here:* [*https://www.microsoft.com/en-us/download/details.aspx?id=55319*](https://www.microsoft.com/en-us/download/details.aspx?id=55319)

1. Close the GPO
2. Launch **GPedit.msc**
3. Check the User rights
4. Are the user rights enforced by the GPO?

………………………………………………………………………………………………

1. Close **GPEdit**
2. In command line, force the execution of the GPO
3. Launch **GPedit.msc**
4. Check the User rights
5. Are the user rights enforced by the GPO?

………………………………………………………………………………………………

1. Close **GPEdit**

#### Task 3: Create a Hardening GPO for Exchange

1. Open a session on **CSI-TD-EXC1** 
   1. Username: **Admin\_Exch@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1**
2. Add **Par\_User20** to the local **Administrators** group
3. Switch back to **CSI-TD-DC1**
4. Move **CSI-TD-EXC1** to the OU **Servers/Exchange**
5. Launch **Group Policy Management**
6. On the OU **Exchange**, create a new GPO **Exchange Hardening**
7. Edit the GPO to set the content of the Local Administrators group to :
   1. **AdminCSI**
   2. **Contoso\Domain Admins**
   3. **Contoso\Exchange Trusted SubSystem**
   4. **Contoso\Organization Management**
   5. Once done, you should have this

A screenshot of a cell phone

Description automatically generated

1. Close **Group Policy Management Editor**
2. Switch back to **CSI-TD-EXC1**
3. Force the execution of the GPO in Administrator command prompt
4. Check the content of the local **Administrators** group
5. Check the content. **Par\_User20** should have been disappeared
6. Log off from **CSI-TD-DC1** and **CSI-TD-EXC1**

*The GPO hardening for Exchange servers should contain other settings. But all the settings need to be validated with the Exchange team to be sure to not break Exchange servers.*

## Exercise 2: Enumerate users using SAMR

Duration: 20 minutes

Synopsis: In this exercise, attendees will use NMAP to retrieve users’ information from a domain controller without using LDAP.

#### Task 1: Use NMAP to browse User in AD

1. Open a session on **CSI-TD-DC1**
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Launch **Command Prompt**
3. Note the IP address for **CSI-TD-DC1**
   1. In the following section this IP address will be referenced as 10.0.0.a
4. Logon to **CSI-TD-CLI1**
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
5. Add the local user **Local\_User1** to the local **Administrators** group
6. Close the session
7. Open a session on **CSI-TD-CLI1**
   1. Username: **.\Local\_User1**
   2. Password: **Ilovesecu\*!**
8. Launch **Zenmap** as Administrator: C:\Program Files (x86)\Nmap
9. Scan using **Zenmap** for 445 **smb-enum-users** for the DC IP
10. Review the result. As a local user with no AD right, you can browse the list of AD users

The default configuration for a Windows Server 2016 forest do not allow SAM-R enumeration in anonymous.

1. Open a session on **CSI-TD-DC1**
2. Using registry, **Enable SAM-R logging**
   1. **RestrictRemoteSamAuditOnlyMode**
   2. **RestrictRemoteSam**
3. Switch back to **CSI-TD-CLI1**
4. Scan using **Zenmap** for 445 **smb-enum-users** for the DC IP
5. Switch batch to the **CSI-TD-DC1**
6. Open the **Event Viewer**
7. Go the **System** Journal
8. Check for the event between **16962** to **16969**
9. Close **Event Viewer**
10. Remove **RestrictRemoteSamAuditOnlyMode** in the registry
11. Switch back to **CSI-TD-CLI1**
12. Scan using **Zenmap** for 445 **smb-enum-users** for the DC IP
13. The test failed because Anonymous logon is no longer authorized
14. Close **Zenmap**
15. Log off
16. Switch batch to the **CSI-TD-DC1**

SAM-R enumerations is common a technic in the attacker’s reconnaissance phase.

## Exercise 3: LDAP connection

Duration: 30 minutes

Synopsis: In this exercise the attendees will test different ways to authenticate through LDAP and visualize the security implications of using simple binds.

#### Task 1: LDAP connection with Anonymous logon

1. Open a session on **CSI-TD-DC1**
2. Create a user named **Test\_LDAP** with password **Ilovesecu\*! i**n the OU **Test**
3. Open a session on **CSI-TD-CLI1**
   1. Username: **.\Local\_User1**
   2. Password: **Ilovesecu\*!**
4. Launch **LDP**
5. If **LDP** is not available
   1. Launch Explorer
   2. Launch **PowerShell** in **Administrator** mode
   3. **Cd \Tools**
   4. .\**WindowsTH-RSAT\_WS\_1803-x64.msu**
6. Launch **LDP**
7. Choose **Connect/Bind** using **Simple bind**
8. Click **View** and select **Tree** for **: OU=Test,DC=Contoso,DC=Com**
9. Check the information for **Test\_LDAP**
10. As Anonymous access is authorized on this OU, you are authorizing to check the content of the OU using anonymous connection
11. Close **LDP**

#### Task 2: LDAP connection without LDAP SIGN in

1. Open a session on **CSI-TD-DC1**
2. Using Registry : Enable LDAP logging
3. Open a session on **CSI-TD-CLI1**
   1. Username: .\Local\_User1
   2. Password: **Ilovesecu\*!**
4. Launch **Network Monitor** as **Administrator**
5. Start a new **Capture** by clicking on **Start** button
6. Launch **LDP**
7. Choose **Connect**/**Bind** using **Simple bind** and the following user
   1. User: **contoso\par\_User05**
   2. Password: **Ilovesecu\*!**
8. **Stop** the capture
9. Save the Capture and named it **LDAPSignIn**
10. Capture Analysis
    1. Find **LDAPMessage:Bind Request**,
    2. On the **Frame Details,** expand **LDAPmessage** and **Bind Request.** The name and password of the user are displayed in clear
       1. BindRequest: Version:3, Name:**contoso\par\_User05**, UserName: **Ilovesecu\*!,** Authentication type = simple
11. Close **Netmon**
12. Close **LDP**
13. Switch to **CSI-TD-DC1**
14. Open Event Viewer
15. Expand **Applications and Services Logs\Directory Services**
16. Filter for the event **2889**
17. This event allows you to track LDAP simple bind over a clear text.
18. Launch **Group Policy Management**
19. Edit **DC Hardening**
20. Set **Domain controller: LDAP server signing requirements** to **Require signing**
21. Close **Group Policy Management Editor**
22. Close **Group Policy Management**
23. Force the execution of the GPO in Administrator command prompt
24. Switch back to **CSI-TD-CLI1**
25. Right click on the Windows button
26. Launch **LDP**
27. Choose **Connect/Bind** using **Simple bind** for
    1. User: **contoso\par\_User05**
    2. Password: **Ilovesecu\*!**
28. The connection should fail with the following error message :
    1. Server error: 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839 Error 0x2028 **A more secure authentication method is required for this server.**
29. Now to connect using LDAP, you won’t be able to use Simple bind
30. Close your session on **CSI-TD-CLI1**
31. Close your session on **CSI-TD-DC1**

## Exercise 4: List group members

Duration: 20 minutes

Synopsis: In this exercise, attendees will

#### Task 1: List AD group Members

1. Open a session on CSI-TD-DC1
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Using **Active Directory Administrative Center**, check the content of the groups :
   1. **Enterprise Admins**
   2. **Schema Admins**
3. What should be the content of the group **Schema Admins** ?

………………………………………………………………………………………………

1. Launch **Windows** **Powershell**
2. Check the content of the Administrators group
3. Check the content of the Administrators group using Recursive
4. Check the content of the **“Servers Operators”** group
5. Check the content of the **"System Administrators" group**
6. Is there anything suspicious about one of these groups?  
   ………………………………………………………………………………………………
7. List the members of the following groups
   1. **Account Operators**
   2. **Print Operators**
   3. **Backup Operators**
8. Which security principals should be removed from these groups?  
   ………………………………………………………………………………………………
9. Close session on **CSI-TD-CLI1** and **CSI-TD-DC1**

## Exercise 5: LAPS

Duration: 45 minutes

Synopsis: In this exercise, attendees will implement LAPS.

#### Task 1: Install LAPS and update de schema

The source of LAPS is located on [\\Csi-td-dc1\laps](file://Csi-td-dc1/laps).

In this lab, we will install LAPS on the DC. It should be already installed on the management computer.

1. Open a session on CSI-TD-DC1
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. In the folder **C:\LAPS,** run **LAPS.x64.msi**
3. Ensure to select **Entire feature will installed on the local hard drive** and click **Next**
4. Launch **PowerShell** to update the schema for LAPS
5. In **PowerShell**, Import the LAPS module
6. In **PowerShell**, Update the schema for LAPS
   1. This command only works because **AdminCSI** is member of the **Schema Admins** group
7. In PowerShell, Grant computers the ability to change their own password on the OU **File SRV**
8. In PowerShell, Grant Admin\_Paris and AdminCSI the permission to retrieve password

#### Task 1: Create a GPO to deploy LAPS

The source of LAPS is located on [\\Csi-td-dc1\laps](file://Csi-td-dc1/laps)

Note that we will use GPOs to deploy LAPS because we do not have deployment tools such as SSCM installed in our labs. GPOs are rarely used in production environment to deploy msi packages.

1. Open a session on **CSI-TD-DC1**
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Launch **Group Policy Management**
3. Create a new GPO named **\\** for the OU **File SRV**
4. Assigned LAPS (LAPS.x64) as a New Package with the path [\\Csi-td-dc1\laps](file://Csi-td-dc1/laps)
5. On **Password Settings,** for **LAPS**
   1. Select **Enabled**
   2. Set **Password length** to **25**
6. **Enable Local admin password management**
7. Close the GPO
8. Close **Group Policy Management Editor**
9. Using **Active Directory Users and Computers**,move **CSI-TD-SRV1** to the OU **Servers/File SRV**
10. Open a session on **CSI-TD-DC1**
    1. Username: **AdminCSI@contoso.com**
    2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
11. Reboot the server
12. Logon to **CSI-TD-SRV1**
13. Verify that **LAPS** application has been deployed
14. Log off
15. Switch back to **CSI-TD-DC1**
16. In the **Powershell**, display the password for the local **Administrator** for **CSI-TD-SRV1**
    1. Note the password
    2. If no password is showed up, reboot **CSI-TD-SRV1**
17. Log off form **CSI-TD-DC1**
18. Switch to **CSI-TD-SRV1**
19. Logon with
    1. Username: .\**AdmonCSI** Be careful of the name it is Adm**o**nCSI and not AdminCSI
    2. Password: **Enter the password showed with the** Get-AdmPwdPassword command
20. Log off form **CSI-TD-SRV1**

## Questions:

1. Why do we enforce User rights with GPO?

………………………………………………………………………………………………

1. What is the risk of using an LDAP connection that is not signed?

………………………………………………………………………………………………

1. Why is it recommended to deploy LAPS?

………………………………………………………………………………………………

## After the Lab

Duration: 10 minutes

In this exercise, attendees will deallocate any Azure resources that were started in support of the lab.

#### Task 1: Stop and deallocated all the VMs

1. Properly shutdown all the VMs
2. Deallocate the VM in the Azure Portal
3. To Stop a VM, simply click on Unclaim.

