Windows security, Active Directory and Azure AD

TD07 – Module 1 – Section 1

June 2020  
V3.0

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](#_Toc43584032)

[Abstract and learning objectives 1](#_Toc43584033)

[Overview 2](#_Toc43584034)

[Requirements 2](#_Toc43584035)

[Before the exercise 3](#_Toc43584036)

[List of VM to start 3](#_Toc43584037)

[How to start and connect to a VM 4](#_Toc43584038)

[Exercise 1: Site Management 6](#_Toc43584039)

[Task 1: Add a new site 6](#_Toc43584040)

[Task 2: Move CSI-TD6-DC2 to the new site 6](#_Toc43584041)

[Exercise 2: OU Delegation 7](#_Toc43584042)

[Task 1: Run AD ACL Scanner on OU Paris 7](#_Toc43584043)

[Task 2: Delegate Management of an OU to a group of users 7](#_Toc43584044)

[Task 3: Compare Result of delegation with AD ACL Scanner on OU Paris 7](#_Toc43584045)

[Task 4: Install the Active Directory tools on CSI-TD6-Cli1 8](#_Toc43584046)

[Task 5 Manage OU with CSI-TD6-CLI1 8](#_Toc43584047)

[Exercise 3: LDP 9](#_Toc43584048)

[Task 1: LDP 9](#_Toc43584049)

[Exercise 4: AdminSDHolder 10](#_Toc43584050)

[Task 1: Change the Frequency for the execution of the AdminSDHolder 10](#_Toc43584051)

[Task 2: Review the AdminSDHolder’s permissions 10](#_Toc43584052)

[Task 3: Change the frequency for the execution of the AdminSDHolder 11](#_Toc43584053)

[Exercise 5: GPO management 12](#_Toc43584054)

[Task 1: Share the Public folder 12](#_Toc43584055)

[Task 2: Create a GPO to control the users’ environment 12](#_Toc43584056)

[Task 3: Review GPT and the GPO Object 13](#_Toc43584057)

[Task 4: View the Policy Execution 13](#_Toc43584058)

[Exercise 5: Fine-Grained Password Policies 14](#_Toc43584059)

[Task 1: Configure FGPP 14](#_Toc43584060)

[Task 2: Verify that the Admin-FGPP is applied to AdminCSI 14](#_Toc43584061)

[Questions: 15](#_Toc43584062)

[After the Lab 16](#_Toc43584063)

[Task 1: Stop and deallocated all the VMs 16](#_Toc43584064)

# 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 create a new forest and promote domain controllers using the graphical interfaces and PowerShell. The attendees will also use basic features of AD DS such as GPO and manipulate objects using the default administrative tools.

## 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 start up your environment for use in the rest of the Lab. You should have the following environment.

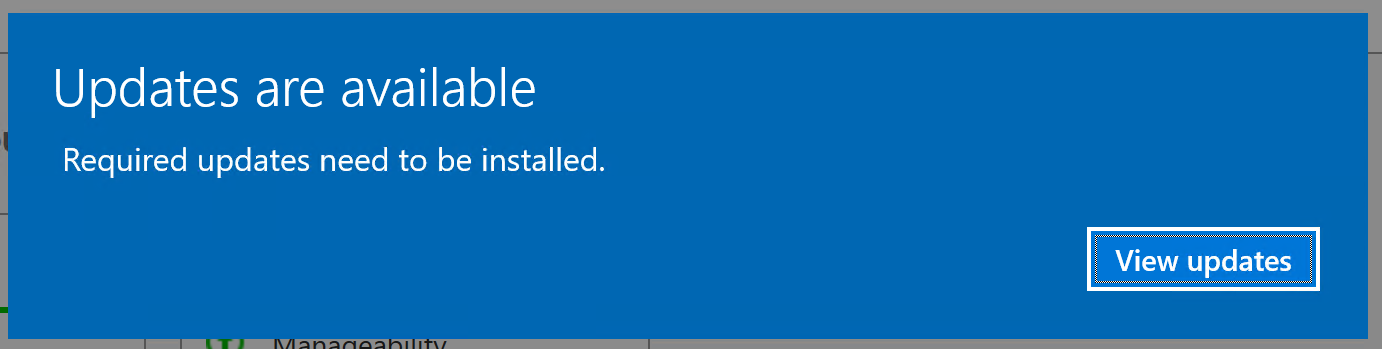
#### List of VM to start

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

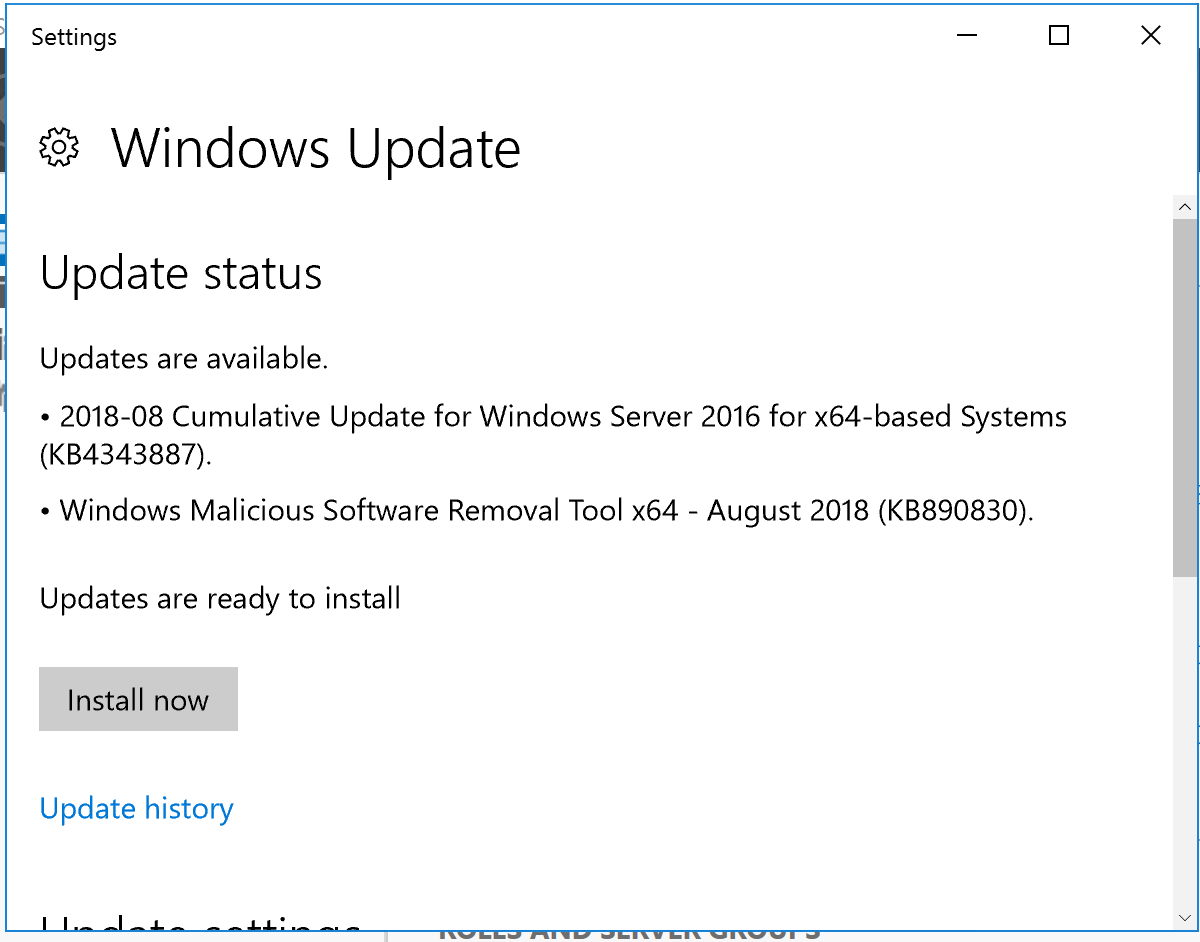
|  |  |  |  |
| --- | --- | --- | --- |
| Name of VM | Hostname | OS Type | Role |
| ID-TD6-DC1 | CSI-TD6-DC1 | Windows Server 2016 Standard | DC |
| ID-TD6-SRV1 | CSI-TD6-SRV1 | Windows Server 2016 Standard | Server |
| ID-TD6-CLI1 | CSI-TD6-CLI1 | Windows 10 Pro | Desktop |

**Please ensure that ID-TD6-DC2 has been turned off**

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.



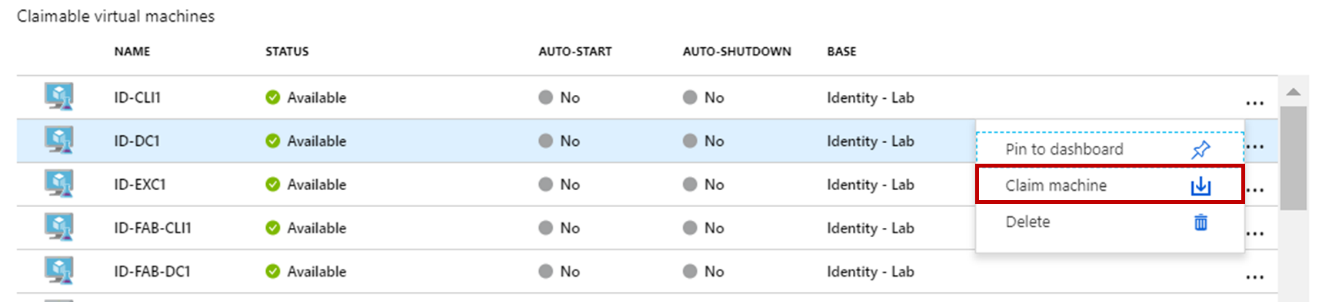
We do not need the latest updates for these labs so you can close this window.

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

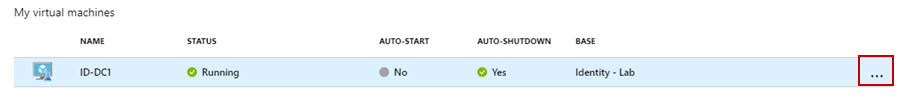
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



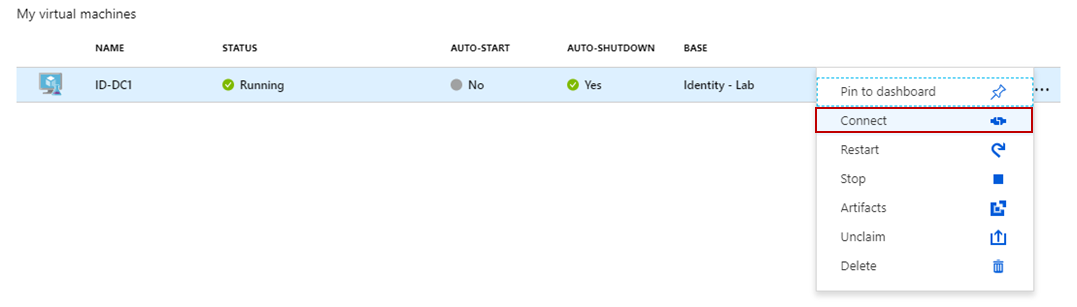
1. To start a VM, click on “Claim machine”



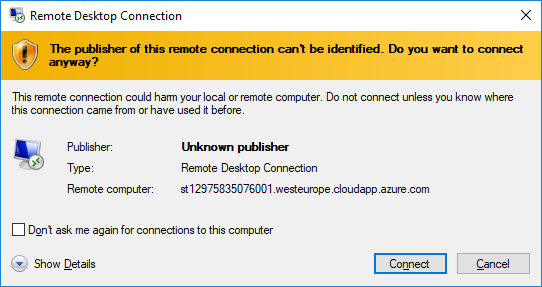
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



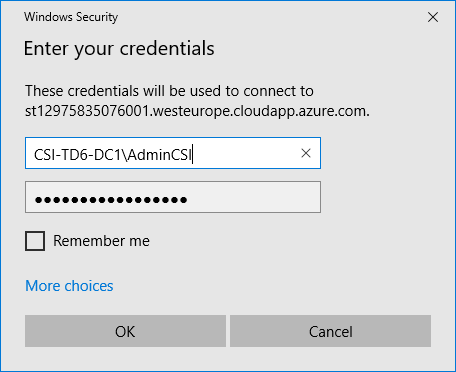
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



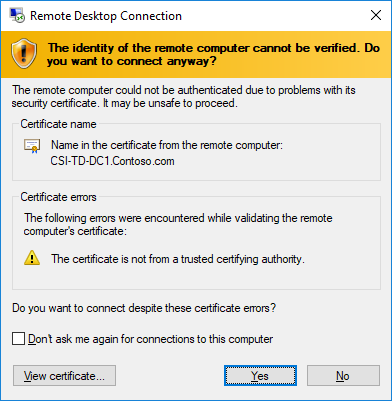
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



1. Enter the username 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.



## Exercise 1: Site Management

Duration: 45 minutes

Synopsis: In this exercise, attendees will add a new AD site and move a DC into the newly created site.

#### Task 1: Add a new site

1. Logon to **CSI-TD6-DC1**
   1. Username:  [**YourAdmAccount@contoso.com**](mailto:%20AdminCSI@contoso.com)
   2. Password: **Your password**
2. Add a new site named : **New-York**Note that an AD site names are used in DNS queries. As a result, they cannot contain spaces.
3. Choose link : **DefaultIPSiteLink**
4. Rename **DefaultFirstSite** with the name **Paris**

#### Task 2: Move CSI-TD6-DC2 to the new site

1. Move CSI-TD6-DC2 to the site **New-York**

## Exercise 2: OU Delegation

Duration: 45 minutes

Synopsis: In this exercise, attendees will set the OU’s permissions to an administrator and test the delegation. The permissions on the OU before and after the delegation will also be compared.

#### Task 1: Run AD ACL Scanner on OU Paris

1. Check if **ADACLScanner** is present in the folder Tools
   1. If not Download it on Internet et unzip it in cd \ADACLScanner
2. In **PowerShell,** run **ADACLScan.ps1** 
   1. **Connect** and Select OU **Paris**
   2. **Output Options** section, select **CSV File**
3. Click **Run Scan**
4. Close **AD ACL Scanner**

#### Task 2: Delegate Management of an OU to a group of users

1. Open **Active Directory Users and Computers**
2. On OU **IT\users**
3. Create a user
   1. Username: **Admin\_Par**
   2. Password : **IloveSec\*!**
4. Go to OU **IT\Groups**
   1. Create a global group named **Paris-Admin**
   2. Add **Admin\_Par** to the new created group
5. Right click on **Paris** OU and select **Delegate Control** to the group **Paris-Admin**
   1. **Create, delete and manager User accounts**
   2. **Create, delete and manager groups**

#### Task 3: Compare Result of delegation with AD ACL Scanner on OU Paris

1. In **PowerShell,** run **ADACLScan.ps1** 
   1. Select OU **Paris**
2. In **Compare** tab, click on **Enable compare**
3. Click on **Select Template**
4. Select the **CSV file generate during the first run**
5. In **Output Options**, ensure that **HTML** is selected
6. Click **Run Scan**
7. Compare the results in the html file
8. Close **AD ACL Scanner**

#### Task 4: Install the Active Directory tools on CSI-TD6-Cli1

We first need to enable internet name resolution in order to download the administrative toolset that we are going to install on CSI-TD6-CL1.

1. Logon to **CSI-TD6-DC1**
   1. Username:  [**YourAdmAccount@contoso.com**](mailto:%20AdminCSI@contoso.com)
   2. Password: **Your password**
2. Add a forwarder in DNS to allow Internet resolution
   1. Enter **168.63.129.16**
3. Logon to **CSI-TD6-CLI1**
   1. Username:  [**YourAdmAccount@contoso.com**](mailto:%20AdminCSI@contoso.com)
   2. Password: **Your password**
4. Launch **Edge**
5. Go to this link: <https://www.microsoft.com/en-ca/download/details.aspx?id=45520> and download **Remote Server Administration Tools for Windows 10**
6. Select **WindowsTH-RSAT\_WS\_1803-x64.msu**
7. Install the **RSAT tools for Windows 10** and click **Yes** to install the **KB2693643**
8. Log Off

#### Task 5 Manage OU with CSI-TD6-CLI1

1. Logon to **CSI-TD6-CLI1**
   1. Username:  [**Admin\_Par@contoso.com**](mailto:%20Admin01@contoso.com)
   2. Password: **IloveSec\*!**
   3. Click on **Other password options**
2. Click on the Windows button  on the taskbar, click on **Windows Administrative Tools** and choose **Active Directory Administrative Center**
3. Go to **IT\Users**
4. Create a new user
   1. Username: **User10**
   2. Password : **IloveSec\*!**
   3. Were you able to create the user? Why?

………………………………………………………………………………………………

………………………………………………………………………………………………

1. Go to **Paris/Users**
2. Create a new user
   1. Username: **Par\_User10**
   2. Password : **IloveSec\*!**
   3. Click on **Other password options**
   4. Were you able to create the user? Why?

………………………………………………………………………………………………

………………………………………………………………………………………………

1. Log off

## Exercise 3: LDP

Duration: 30 minutes

Synopsis: In this exercise, attendees will use LDP.EXE to query the directory.

#### Task 1: LDP

1. Logon to **CSI-TD6-DC1**
   1. Username:  [**YourAdmAccount@contoso.com**](mailto:%20AdminCSI@contoso.com)
   2. Password: **Your password**
2. Right click on the Windows button  on the taskbar and choose **Run**
3. Enter **LDP.EXE** and click **OK**
4. Click **Connection/Bind**
5. Click **View**, and then click **Tree**. Leave **BaseDN** blank and click **OK**
6. Expand the domain and navigate to OU **Paris/Users**
7. Double-click on **PAR\_User1**
8. All the User’s attributes will be displayed
9. View the **NT Security Descriptor** of **Par\_User1**
10. Search for **Par\_User1** in the domain using its **samaccountname**.
    1. Select attributes :
       1. : **objectClass;name;description;canonicalName;ObjectSID**
11. Review the **Results** on the right section
12. Some other searches that can be performed:
    1. All Users: **(&(objectCategory=person)(objectClass=user))**
    2. Specific User based on its logon name: **(&(sAMAccountName=User10)(objectClass=user))**
    3. Specific users based on the lastname: **(&(sn=John)(objectClass=user))**
    4. Specific Users based on the first name: **(&(givenName=Smith)(objectClass=user))**
13. View the configuration partition and its content
14. Close **LDP**

## Exercise 4: AdminSDHolder

Duration: 30 minutes

Synopsis: In this exercise, attendees will see how the AdminSDHolder works and the steps to perform when a user is not more depending of the AdminSDHolder.

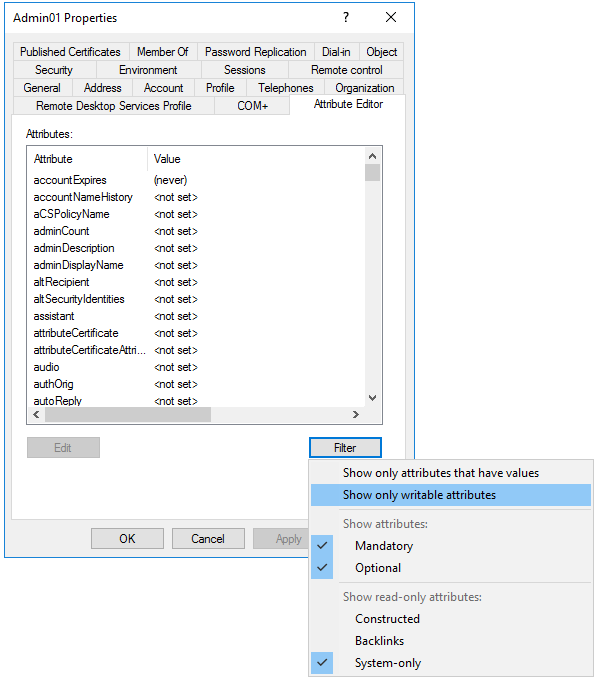
#### Task 1: Change the Frequency for the execution of the AdminSDHolder

1. Logon to **CSI-TD6-DC1**
   1. Username:  [**YourAdmAccount@contoso.com**](mailto:%20AdminCSI@contoso.com)
   2. Password: **Your password**
2. Using the registry, change the frequency of the execution of the AdminSDHolder to 2 minutes (120)
3. Restart the machine and wait until it goes back online before continuing the labs

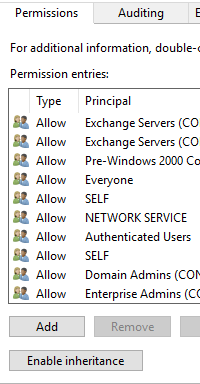
Note that changing this value is not particularly recommended. We are changing the default value from 1 hour to 2 minutes to avoid waiting too long to see the results in our labs.

#### Task 2: Review the AdminSDHolder’s permissions

1. Using “Active Directory User and Computers” review the permissions of the **AdminSDHolder** containerlocated on **in System**
2. Expand the OU **IT\Users**
3. Review the permission of the account for **Admin\_Account** and choose **Properties**
4. Select the tab **Attribute Editor**
5. Click on **Filter** and choose **Show only attributes that have values**



1. Check the value of **AdminCount**
2. As the user is member of the group **Account Operators,** it depends on the **AdminSDHolder**, so its **adminCount** value is **1**
3. Remove **Admin\_Account** from the group **Account Operators**
4. Wait 2 minutes
5. Right click on **Admin\_Account** and choose **Properties**
6. Select the tab **Attribute Editor**
7. Review the **adminCount**
   1. The value should still be set to 1  
      The protection mechanism does not unprotect accounts. This has to be done manually.
8. Click on the **Security** tab
9. Click **Advanced**
10. The Inheritance is still disabled



1. Click on **Enable Inheritance**
2. Click **OK**
3. Click **Yes** on the warning
4. Select the tab **Attribute Editor**
5. Set the **adminCount** to **0**

Note that simply setting the adminCount attribute to 0 does nothing as the attribute is just written by the process and not read. And the opposite is also true. If you set the adminCount attribute of an account to 1 whereas this account is not in the scope of the adminSDHolder, the account does not become protected.

#### Task 3: Change the frequency for the execution of the AdminSDHolder

1. Right click on the Windows button  on the taskbar and choose **Run**
2. Enter **Regedit** and click **OK**
3. Go to **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters**
4. Remove the value **AdminSDProtectFrequency**

## Exercise 5: GPO management

Duration: 45 minutes

Synopsis: In this exercise, attendees will create a GPO to impose some settings to the computers and users located in an OU.

#### Task 1: Share the Public folder

1. Logon to **CSI-TD6-SRV1**
   1. Username:  [**YourAdmAccount@contoso.com**](mailto:%20AdminCSI@contoso.com)
   2. Password: **Your password**
2. Launch **Explorer**
3. Create a folder named **Public**
4. Share the folder without changing the share permissions
5. In the Security Tab, add this permission **Domain Users\Read**
6. Close the **Public** **Properties** windows

#### Task 2: Create a GPO to control the users’ environment

1. Logon to **CSI-TD6-DC1**
   1. Username:  [**YourAdmAccount@contoso.com**](mailto:%20AdminCSI@contoso.com)
   2. Password: **Your password**
2. Launch **Group Policy Management**
3. Go to the **Paris OU**
4. Create and link a new GPO named **Paris\_GPO**
5. Edit **Paris\_GPO**
6. In the **Group Policy Management Editor**
7. Under **User Configuration/Preferences,** find the setting tocreate a new shortcut **Shortcuts :** 
   1. Action **Create**
   2. Name : **Public-CSI-TD6-SRV1**
   3. Target Type: **File System Object**
   4. Location: **Desktop**
   5. Target Path: [**\\CSI-TD6-SRV1\public**](file://CSI-TD6-SRV1/public)
8. Under **User Configuration\Policies** , find the setting to change the wallpaper to **: Windows\Web\Wallpaper\Contoso.jpg**
9. Under **Computer Configuration\Policies,** find the setting to add :
   1. **Interactive logon: Message text for users attempting to log on**
   2. Type: **This computer is the property of Contoso. Unauthorize access are prohibited**
   3. **Interactive logon: Message title for users attempting to log on**
   4. Check **Define this policy setting**
   5. Type: **Contoso Disclaimer**

#### Task 3: Review GPT and the GPO Object

1. Still on **CSI-TD6-DC1**, locate the folder **C:\Windows\SYSVOL\sysvol\Contoso.com\Policies**
2. This folder contains a folder per GPO
3. Each GPO is identified by its GUID
4. To determine the **GUID** of the GPO **Paris\_GPO**
5. Switch to **Group Policy Management**
6. Find the GUID for the GPO : **Paris\_GPO**
7. Switch back to **Explorer**
8. Check if a folder is named after the **Unique ID** you noted
   1. This folder is the GPT of the GPO

You can also navigate into the file structure to visualize some of the setting you have set with the GUI. Those are the configuration files which actually store the settings.

#### Task 4: View the Policy Execution

1. Restart CSI-TD6-CLI1
2. Logon with
   1. Username: **Par\_**[**user1@contoso.Com**](mailto:user1@contoso.Com)
   2. Password: **Ilovesecu\*!**
3. If necessary, reboot twice
4. Did you see the disclaimer ?

………………………………………………………………………………………………

1. Which wallpaper do you see ? Contoso’s wallpaper?

………………………………………………………………………………………………

1. Do you see the shortcut for Public-CSI-TD6-SRV1 ?

………………………………………………………………………………………………

1. Log off from CSI-TD6-CLI1

## Exercise 5: Fine-Grained Password Policies

Duration: 20 minutes

Synopsis: In this exercise, attendees will learn how to create Fine-Grained Password Policies and how to attach it to a group.

Although the FGPPs are called policies, they are not group policies! Therefore, they do not apply to the domain or to an OU but to a user or the member of a group.

#### Task 1: Configure FGPP

1. Logon to **CSI-TD6-DC1**
   1. Username:  [**YourAdmAccount@contoso.com**](mailto:%20AdminCSI@contoso.com)
   2. Password: **Your password**
2. Launch **Active Directory Administrative Center**
3. Go to **System/Password Settings Container**
4. Create a new **Password Settings**
5. Name : **Admin-FGPP**
6. Precedence : **1**
7. Enforce minimum password length : **15**
8. Add it to **Domain Admins** Group

#### Task 2: Verify that the Admin-FGPP is applied to AdminCSI

1. Click **Global Search**
2. In the **Search Zone**, Enter **AdminCSI**
3. Click **Search**
4. Right click on the **AdminCSI** and Select **View resultant password setting**
5. The **Admin-FGPP** should be displayed

## Questions:

1. Why moving DC2 to the New York Site and what are the purposes of AD sites?

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

1. What should you do after removing a user account from a privileged group?

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

## 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.

