Windows security, Active Directory and Azure AD

TD10 - Module 2 – Section 1

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](#_Toc43911519)

[Abstract and learning objectives 1](#_Toc43911520)

[Overview 2](#_Toc43911521)

[Requirements 2](#_Toc43911522)

[Before the exercise 3](#_Toc43911523)

[List of VM to start 3](#_Toc43911524)

[How to start and connect to a VM 4](#_Toc43911525)

[Exercise 1: Analyze group membership 6](#_Toc43911526)

[Task 1: Check the content of the group 6](#_Toc43911527)

[Exercise 2: User creation with AD tools and Exchange tools 7](#_Toc43911528)

[Task 1: Test Admin\_Exch permissions with Active Directory User and Computers 7](#_Toc43911529)

[Task 2: Create a mailbox and its associated user with the Exchange tools 7](#_Toc43911530)

[Exercise 3: Add All permissions to a user at the domain level 9](#_Toc43911531)

[Task 1: Check the user Test-AdPerm permissions at the domain level 9](#_Toc43911532)

[Task 2: Give to user Test-AdPerm Generic all at the domain level 9](#_Toc43911533)

[Task 3: Check the user Test-AdPerm permissions at the domain level 10](#_Toc43911534)

[Questions: 11](#_Toc43911535)

[After the Lab 12](#_Toc43911536)

[Task 1: Stop and deallocated all the VMs 12](#_Toc43911537)

# 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 see the potential security impacts of applications managing AD DS objects with a high level of privileges.

## 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

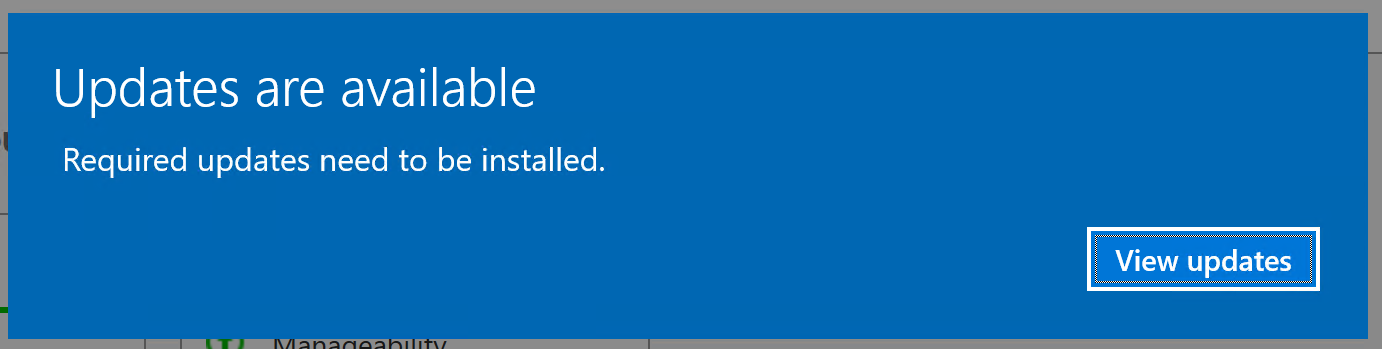
Synopsis: In this section, you will set up your environment for use in the rest of the Lab. You should have the following environment.

#### List of VM to start

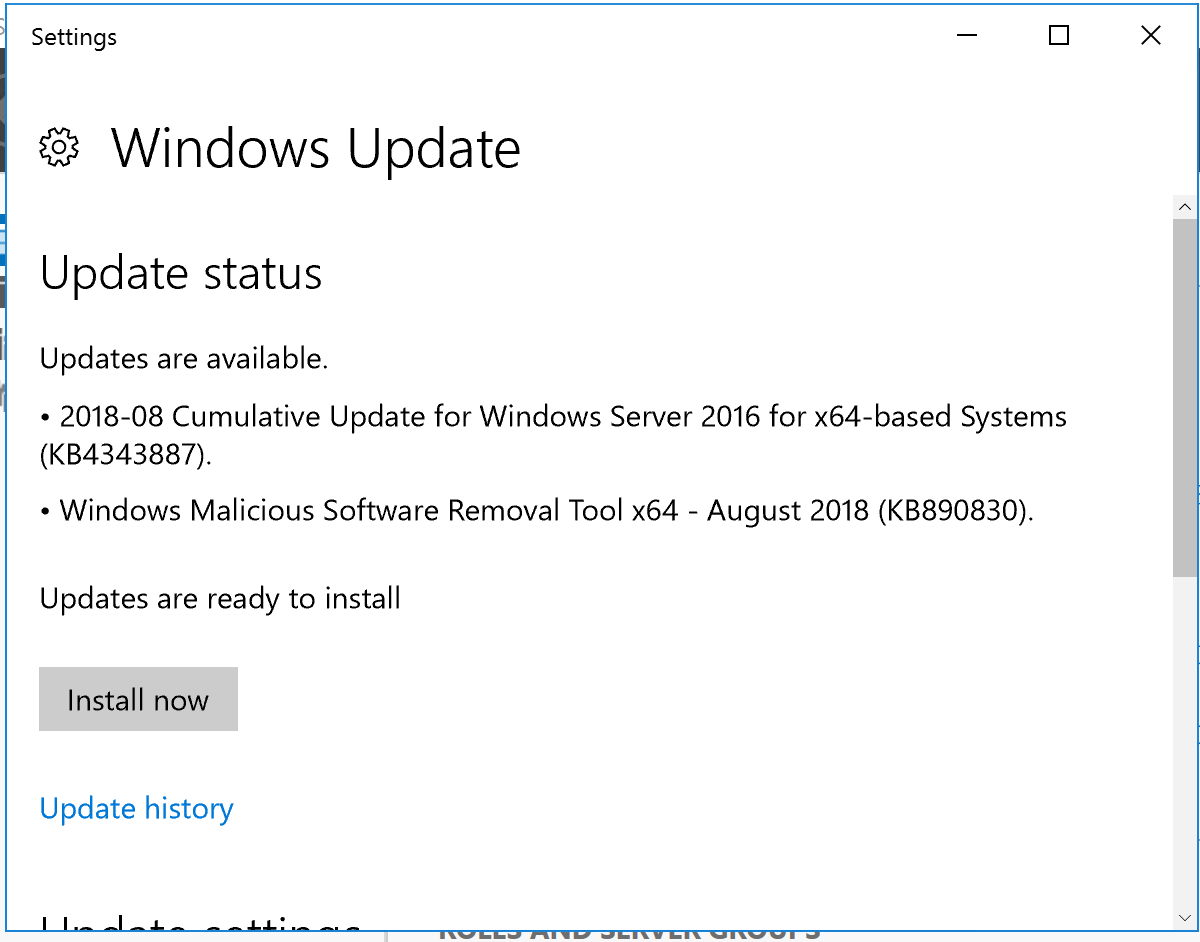
**Remember to start the DC first and to wait 1 minute before starting the other VMs.**

|  |  |  |  |
| --- | --- | --- | --- |
| Name of VM | Hostname | OS Type | Role |
| ID-DC1 | CSI-TD-DC1 | Windows Server 2016 Standard | DC |
| ID-EXC1 | CSI-TD-EXC1 | Windows Server 2016 Standard | Server |

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.



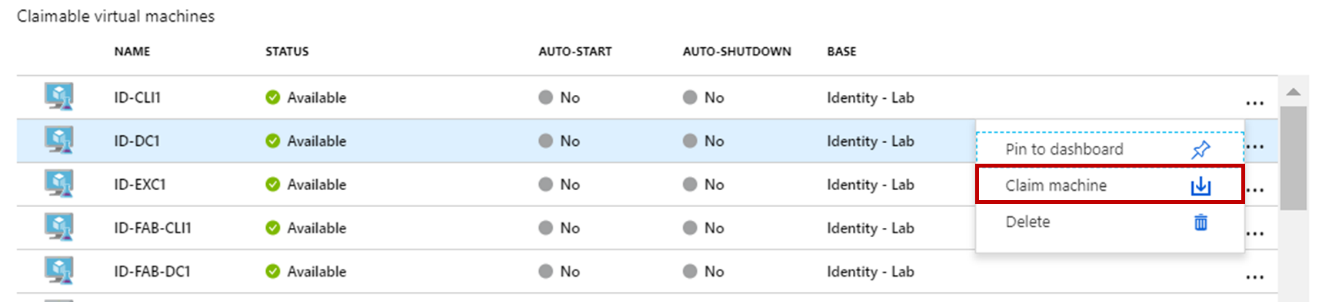
We do not need the latest updates for these labs so you can close this window.

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

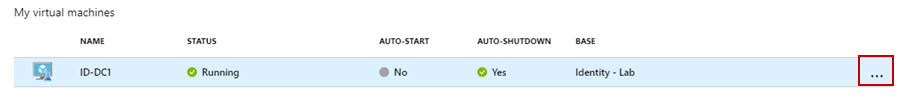
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



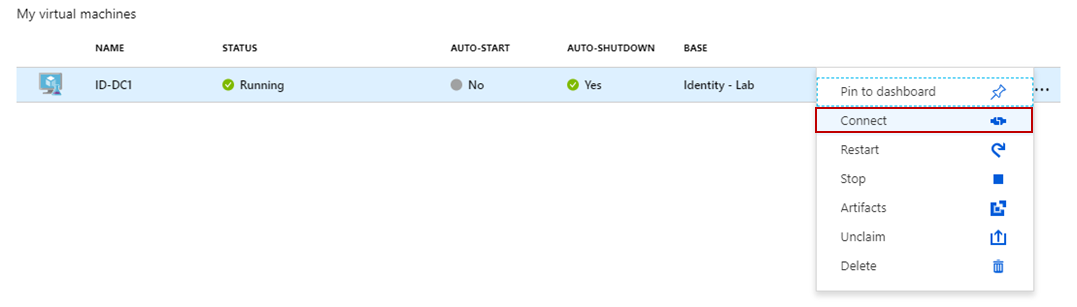
1. To start a VM, click on “Claim machine”



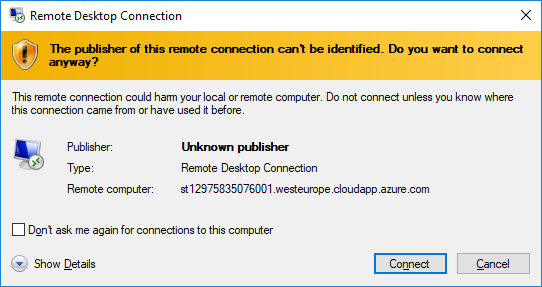
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



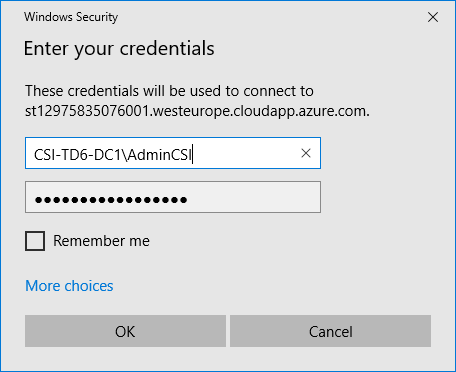
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



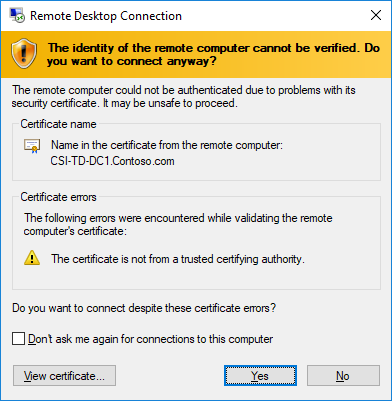
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



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.



## Exercise 1: Analyze group membership

Duration: 10 minutes

Synopsis: In this exercise, attendees will analyze the permissions associated with the user Admin\_Exch.

#### Task 1: Check the content of the group

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. Open the **Active Directory** **User and Computers** console
3. Check the content of the group **Domain Admin**
4. Is the user **Admin\_Exch** member of this group ?

………………………………………………………………………………………………

1. Check the content of the group **Enterprise Admins**
2. Is the user **Admin\_Exch** member of this group ?

………………………………………………………………………………………………

1. Check the content of the group **Organization Management**
2. Is the user **Admin\_Exch** member of this group ?

………………………………………………………………………………………………

## Exercise 2: User creation with AD tools and Exchange tools

Duration: 30 minutes

Synopsis: In this exercise, attendees will try to create a user with Admin\_Exch using AD tools and with Exchange Administration Center.

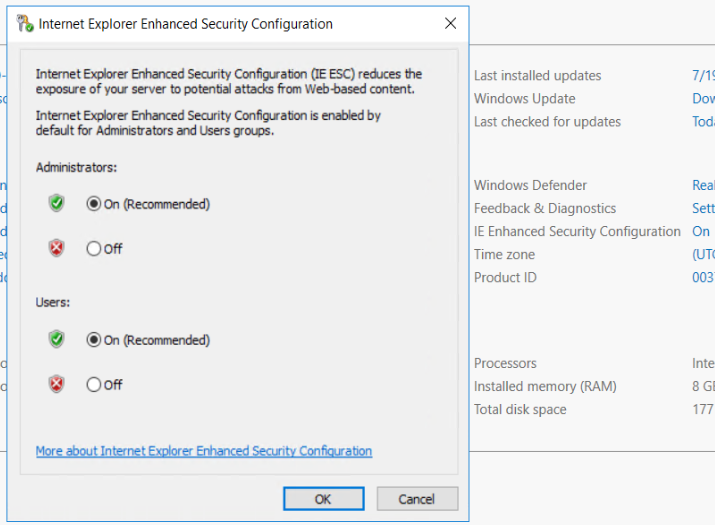
#### Task 1: Test Admin\_Exch permissions with Active Directory User and Computers

1. Open a session on **CSI-TD-EXC1**
   1. Username: **Admin\_Exch@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1**
2. Check if all the Exchange service are started
   1. Right click on the Windows button et chose **Run**
   2. Enter **Services.msc** and click **Ok**
   3. Ensure that all the services starting with Microsoft Exchange and with a startup type set to **Automatic** have a status **Running** (except for the service **Microsoft Exchange Notifications Broker**, this service is set to **Automatic** but its status is not running and it is normal)
   4. During this lab, if you have issue with connection to the Exchange server, try to reboot CSI-TD-EXC1 and check then if all the Exchange services are running
3. Launch **Active Directory Users and Computers**
4. In the OU **Paris\Users,** create a new user called **Par\_User03** with the information you want
5. Are you able to create a user in this OU?

………………………………………………………………………………………………

#### Task 2: Create a mailbox and its associated user with the Exchange tools

1. Launch the Server Manager (if the application is not already launched)
2. In **Local Server**, click on **IE Enhanced Security Configuration : On**



1. On the **Administrators** section, select **Off**
   1. Remember that this configuration is not recommended.
2. Launch **Internet Explorer**
   1. If necessary, click **Ok** to accept the recommended settings
3. Enter [**https://CSI-TD-EXC1.contoso.com/ecp**](https://CSI-TD-EXC1.contoso.com/ecpi) in the address bar
   1. Ignore the certificate error and click on **Continue** with this website
4. Authenticate using the following credentials:
   1. Username: **Admin\_Exch@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
5. Click on **Recipients**
6. Create a new user with a mailbox : Alias : **Par\_User03** in the OU **Paris\Users**
7. Launch **Active Directory Administrative Center**
8. Check the content of the OU **Paris\Users**
9. Is **Par\_User03** exist in the OU ?

………………………………………………………………………………………………

1. Why **Admin\_Exch** was able to create a user in the OU Paris using Exchange tools and not using the AD tools ?

………………………………………………………………………………………………

………………………………………………………………………………………………

1. Using the **Active Directory Administrative Center**, check the owner for the user **Par\_User03**
2. Who is the owner of the user ?

………………………………………………………………………………………………

1. Close the session on **CSI-TD-EXC1**

## Exercise 3: Add All permissions to a user at the domain level

Duration: 30 minutes

Synopsis: In this exercise, attendees will add permissions to a standard user at the domain using Exchange Management shell.

#### Task 1: Check the user Test-AdPerm permissions at the domain level

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 **Active Directory User and Computer**
3. Click on **View** and choose **Advanced Features**
4. Select OU **Admin**
5. Display the Properties for the user **Test-ADPerm**
6. Which group the user is member of ?

………………………………………………………………………………………………

1. Close the dialog box
2. Check the permissions at the domain level and ensure that **Test-ADPerm** is not listed
3. Close the dialog box

#### Task 2: Give to user Test-AdPerm Generic all at the domain level

1. Open a session on **CSI-TD-EXC1**
2. Launch **Exchange Management Shell**
3. In the Exchange Power Shell Windows, enter the following command:
   1. **Add-ADPermission "DC=contoso,DC=com" -User Test-ADPerm -AccessRights GenericAll**

#### Task 3: Check the user Test-AdPerm permissions at the domain level

1. Switch to **CSI-TD-DC1**
2. Go to **Active Directory Users and Computers**
3. Right click on the domain **Contoso.com**
4. Click on the **Security** tab
5. Scroll down and check if the user **Test-ADPerm** is listed and if yes check its permissions
6. If Yes , what are the permissions associated with this account ?

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

**This security issue has been fixed by the Exchange product group since February 2019. However, Exchange servers contain very sensitive data and still have a lot of permissions in AD. They should be considered as very sensitive servers**

Note This has been corrected by the Exchange CU12

## Questions:

1. Why are the permissions Add-ADPermission potentially dangerous for a security stand point?

………………………………………………………………………………………………

1. Why was the **Admin\_Exch** user able to create an account in the OU Paris using Exchange tools and was not using the AD tools?

………………………………………………………………………………………………

1. Why should Exchange servers be considered as very sensitive severs?

………………………………………………………………………………………………

## 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.

