Windows security, Active Directory and Azure AD

TD14 – Module 3 – 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](#_Toc44073521)

[Abstract and learning objectives 1](#_Toc44073522)

[Overview 2](#_Toc44073523)

[Requirements 2](#_Toc44073524)

[Before the exercise 3](#_Toc44073525)

[List of VM to start 3](#_Toc44073526)

[How to start and connect to a VM 4](#_Toc44073527)

[Exercise 1: Trust between Contoso and Fabrikam 6](#_Toc44073528)

[Task 1: Set a conditional forwarder in both forests 7](#_Toc44073529)

[Task 2: Set a new trust with Contoso.com 8](#_Toc44073530)

[Task 3: Enable allow to authenticate for Admin\_Lev1 on CSI-TD-SRV1 9](#_Toc44073531)

[Task 4: Share resource for Admin\_Lev1 on CSI-TD-SRV1 and CSI-TD-EXC1 9](#_Toc44073532)

[Task 5: Access Shared resource for Admin\_Lev1 on CSI-TD-SRV1 and CSI-TD-EXC1 9](#_Toc44073533)

[Task 6: Authorize Remote desktop connection for with Admin\_Lev1 on CSI-TD-CLI1 10](#_Toc44073534)

[Task 7: Logon with Admin\_Lev1 on CSI-TD-CLI1 10](#_Toc44073535)

[Questions: 11](#_Toc44073536)

[After the Lab 12](#_Toc44073537)

[Task 1: Stop and deallocated all the VMs 12](#_Toc44073538)

# 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 and manipulate Active Directory trust relationships.

## 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

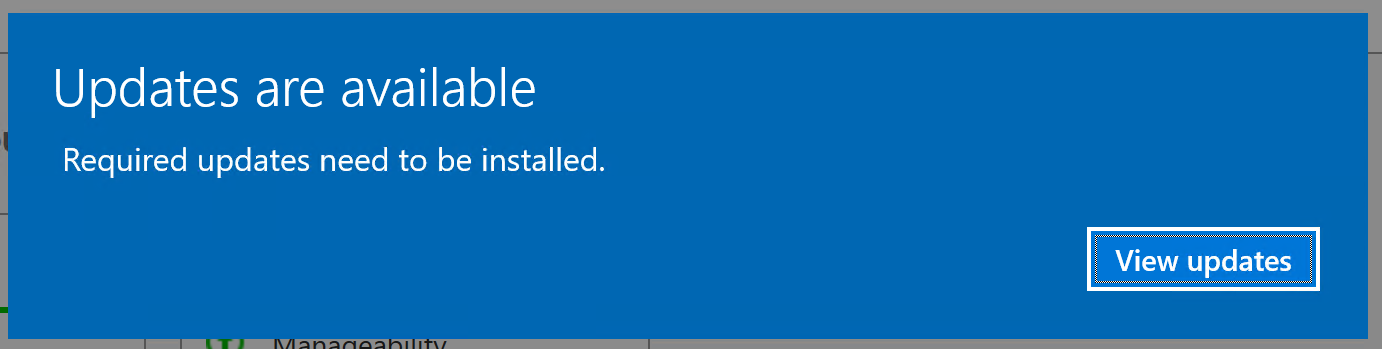
Synopsis: In this section, you will set up your environment for use in the rest of the Lab. You should have the following environment.

#### List of VM to start

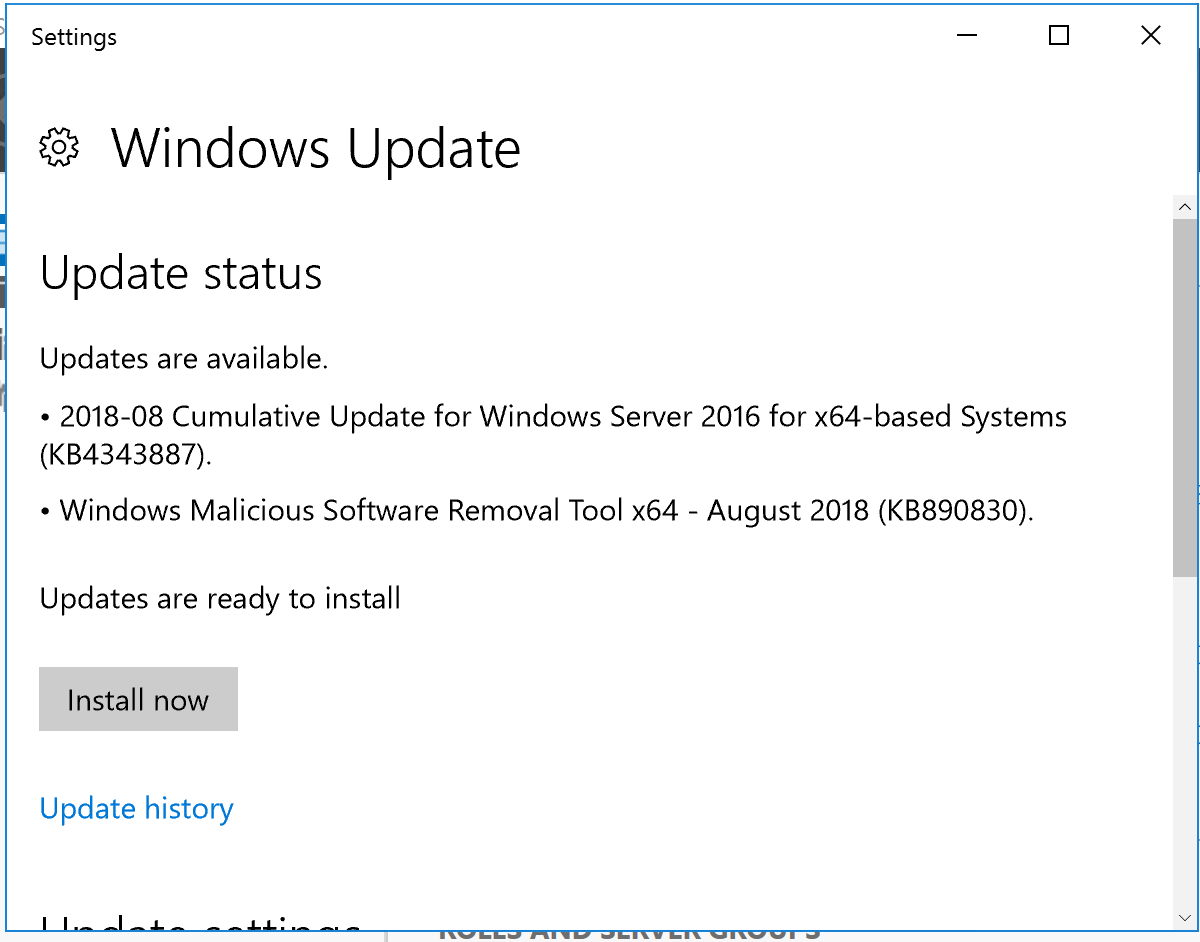
**Remember to start the in first and to wait 1 minute before starting the other VMs.**

|  |  |  |  |
| --- | --- | --- | --- |
| Name of VM | Hostname | OS Type | Role |
| ID-DC1 | CSI-TD-DC1 | Windows Server 2016 Standard | AD |
| 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 | Desktops |
| ID-FAB-DC1 | CSI-TD-FAB-DC1 | Windows Server 2016 Standard | AD |
| ID-FAB-CLI1 | CSI-TD-FAB-CLI1 | Windows 10 Enterprise | Desktops |

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.



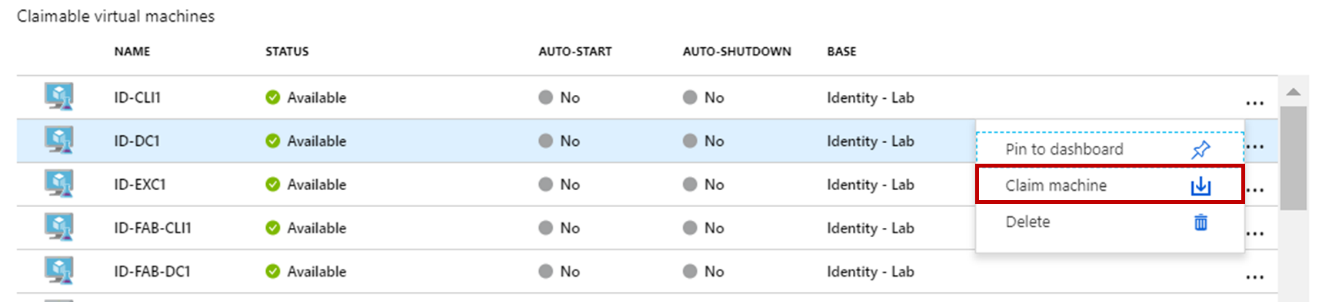
We do not need the latest updates for these labs so you can close this window.

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

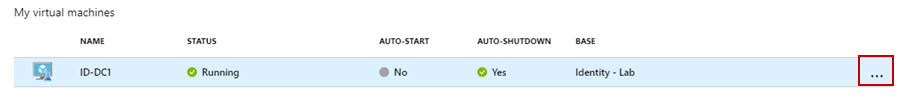
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



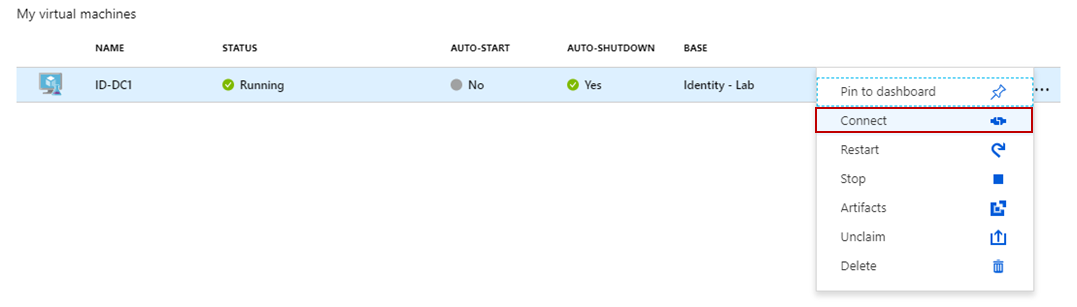
1. To start a VM, click on “Claim machine”



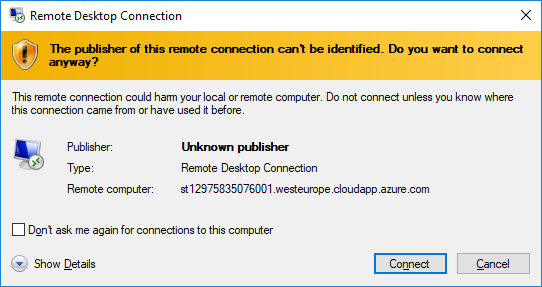
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



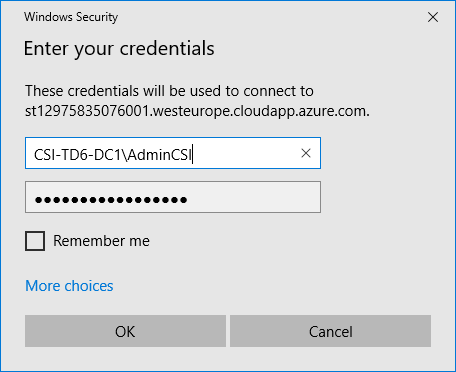
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



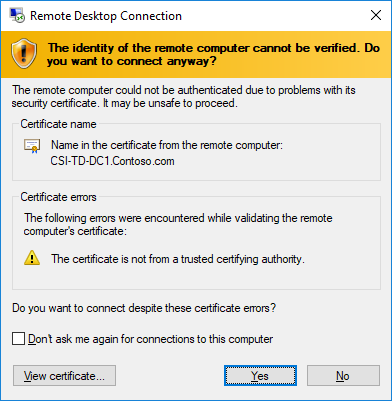
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



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: Trust between Contoso and Fabrikam

Duration: 45 minutes

Synopsis: In this exercise, the attendees will create an Active Directory trust between Contoso.com and Fabrikam.com to allow access to resources for trusted users.

#### Task 1: Set a conditional forwarder in both forests

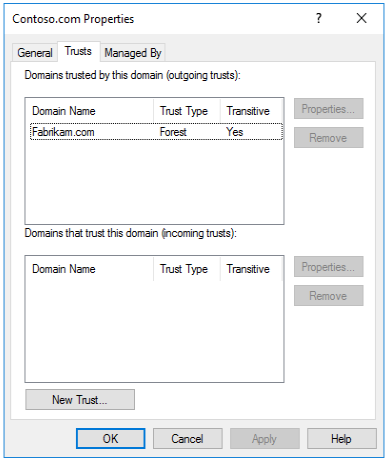
For this new trust, Fabrikam will be the Account forest and Contoso the Resource forest

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. Note the IP address for **CSI-TD-DC1**
   1. In the following section this IP address will be referenced as 10.0.0.a
3. Open a session on **CSI-TD-FAB-DC1** and **CSI-TD-FAB-CLI1**
   1. Username: **AdminCSI@fabrikam.com**
   2. Password: **FAB-PiKarAlR@AlBenMo1**
4. Note the IP address for **CSI-TD-FAB -DC1**
   1. In the following section this IP address will be referenced as 10.0.0.b
5. Launch **DNS**
   1. Set a **Conditional Forwarder**, for **Contoso.com** with the IP Address **10.0.0.a**
6. Close DNS
7. Open a session on **CSI-TD-DC1**
8. Launch **DNS**
9. Set a **Conditional Forwarder** for **Fabrikam.com** with the IP Address **10.0.0.b**

#### Task 2: Set a new trust with Contoso.com

For this new trust, Fabrikam will be the Account forest and Contoso the Resource forest

1. Open a session on **CSI-TD-FAB-DC1** and **CSI-TD-FAB-CLI1**
   1. Username: **AdminCSI@fabrikam.com**
   2. Password: **FAB-PiKarAlR@AlBenMo1**
2. Click on Windows button  on the taskbar, click on **Windows Administrative Tools** and choose **Active Directory Domains and Trusts**
3. Create a **New Trust** for the domain name : **Contoso.com**
   1. **Forest Trust**
   2. Select **One-way:incoming**
   3. Select **Both this domain and the specified domain**
   4. Enter the credential for the **Contoso** domain
   5. Select **Selective Authentication**, click **Next**
4. **Confirm Incoming Trust, select Yes, confirm the incoming trust**
5. Switch to **CSI-TD-DC1**
6. In **Active Directory Domains and Trusts**



1. Click **OK**

#### Task 3: Enable allow to authenticate for Admin\_Lev1 on CSI-TD-SRV1

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 Users and Computers**
3. Expand **Server\File SRV**
4. For **CSI-TD-SRV1** in the **Security** tab **Add**
   1. **Admin\_lev1** from the domain fabrikam.com
   2. Credential for the domain Fabrikam
      1. Username: [**AdminCSI@fabrikam.com**](mailto:AdminCSI@fabrikam.com)
      2. Password: **FAB-PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
5. Select for Admin\_Lev1 **Allowed to authenticate**

#### Task 4: Share resource for Admin\_Lev1 on CSI-TD-SRV1 and CSI-TD-EXC1

1. Open a session on **CSI-TD-SRV1**
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Launch **Explorer**
3. Create a folder named **Admin\_Lev1** and share it
   1. Remove **Everyone**
   2. Add **Full Control** for **Fabrikam\Admin\_lev1**
4. On the **Security** tab, Add **Full Control** for Fabrikam\Admin\_lev1
5. Repeat all this task on **CSI-TD-EXC1**

#### Task 5: Access Shared resource for Admin\_Lev1 on CSI-TD-SRV1 and CSI-TD-EXC1

1. Open a session on **CSI-TD-FAB-CL1**
   1. Username: **AdminCSI@fabrikam.com**
   2. Password: **FAB-PiKarAlR@AlBenMo1**
2. Add **Admin\_lev1** to the group **Remote Desktop Users**
3. Close the session
4. Open a session on **CSI-TD-FAB-CLI1**
   1. Username: **Admin\_Lev1@Fabrikam.com**
   2. Password: **FAB-PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
5. Go to [\\CSI-TD-SRV1.contoso.com\admin\_lev1](file://CSI-TD-SRV1.contoso.com/admin_lev1)
6. Are you able to access to the share folder? Why?

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

1. Are you able to create a file?

………………………………………………………………………………………………

1. Go to [\\CSI-TD-EXC1.contoso.com\admin\_lev1](file://CSI-TD-EXC1.contoso.com/admin_lev1)
2. Are you able to access to the share folder? Why?

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

1. Are you able to create a file?

………………………………………………………………………………………………

#### Task 6: Authorize Remote desktop connection for with Admin\_Lev1 on CSI-TD-CLI1

This step is necessary to allow Admin\_Lev1 user to connect via RDP

1. Log on to the **CSI-TD-CLI1**
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Right click on Windows button  on the taskbar and choose **Computer Management**
3. Add **Fabrikam\Admin\_lev1** to the group **Remote Desktop Users**
4. Log Off

#### Task 7: Logon with Admin\_Lev1 on CSI-TD-CLI1

1. Log on to the **CSI-TD-CLI1**:
   1. Username: **Admin\_Lev1@fabrikam.com**
   2. Password: **FAB-PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Are you able to open a session? Why?

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

1. **Repeat Task 3 for CSI-TD-CLI1**
2. Are you able to open a session? Why?

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

## Questions:

1. How can you avoid a UPN suffix to cross the trust?

………………………………………………………………………………………………

………………………………………………………………………………………………

1. What imply using **Selective authentication?**

………………………………………………………………………………………………

………………………………………………………………………………………………

## 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.

