Windows security, Active Directory and Azure AD

TD13 – Module 2 – Section 3

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](#_Toc526182176)

[Abstract and learning objectives 1](#_Toc526182177)

[Overview 2](#_Toc526182178)

[Requirements 2](#_Toc526182179)

[Before the exercise 3](#_Toc526182180)

[List of VM to start 3](#_Toc526182181)

[How to start and connect to a VM 4](#_Toc526182182)

[Exercise 1: Event Forwarding 6](#_Toc526182183)

[Task 1: Set up the collections server 6](#_Toc526182184)

[Task 2: Create a subscription 6](#_Toc526182185)

[Task 2: Subscribe to the collection server 8](#_Toc526182186)

[Questions: 10](#_Toc526182187)

[After the Lab 11](#_Toc526182188)

[Task 1: Stop and deallocated all the VMs 11](#_Toc526182189)

# 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 implement the built-in event forwarding feature to centralize events in near real time on a collection server.

## 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 TCP port must be accessible :

* TCP/80 and TCP/443 to reach Azure Portal
* TCP from 49152 to 65535 to establish RDP remote connection to virtual machines

## Before the exercise

Duration: 10 minutes

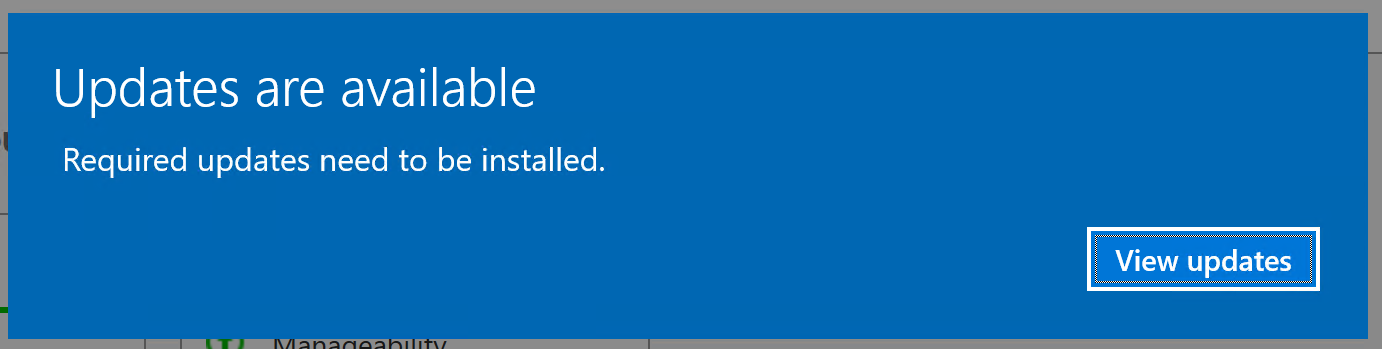
Synopsis: In this section, you will set up your environment for use in the rest of the Lab. You should have the following environment.

#### List of VM to start

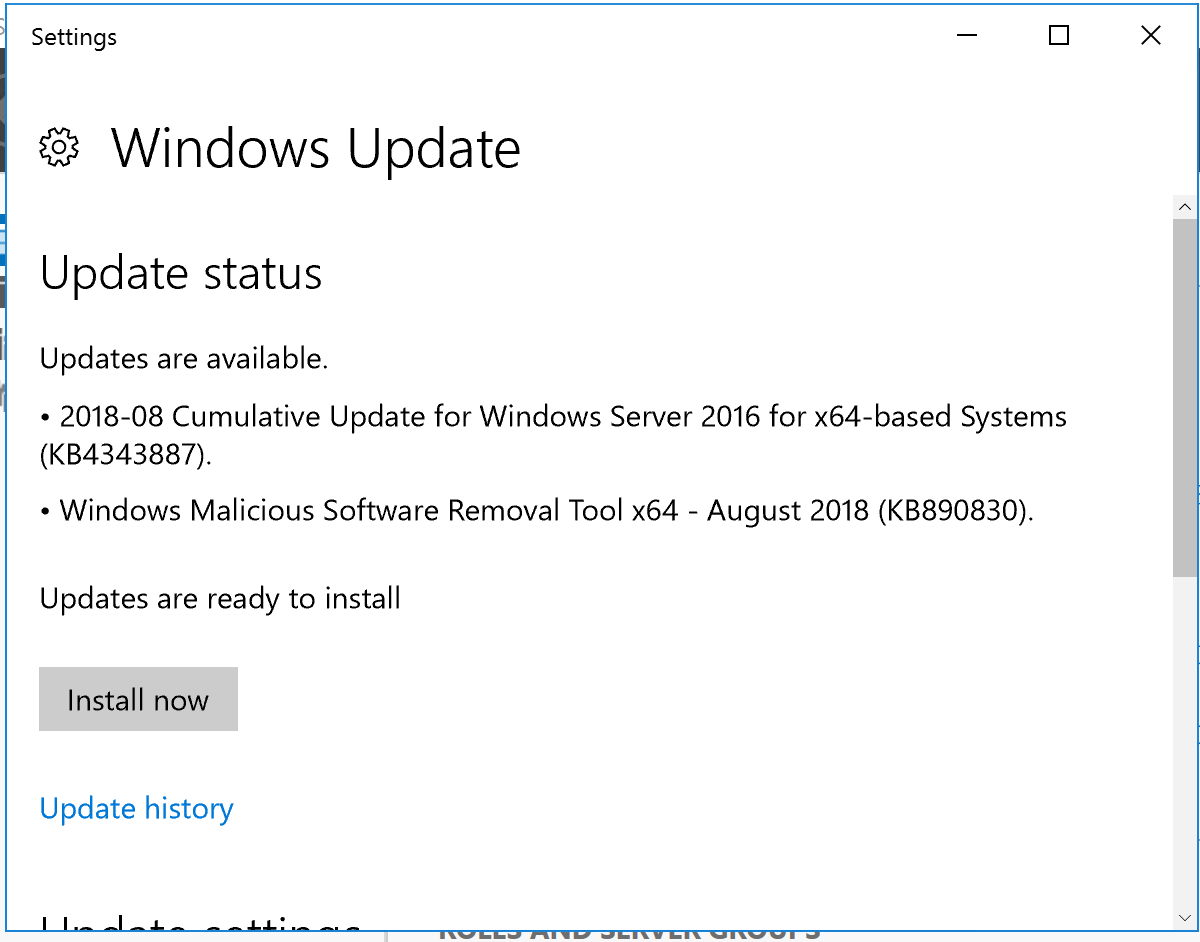
**Remember to start the DC first and to wait 1 minute before starting the other VMs.**

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



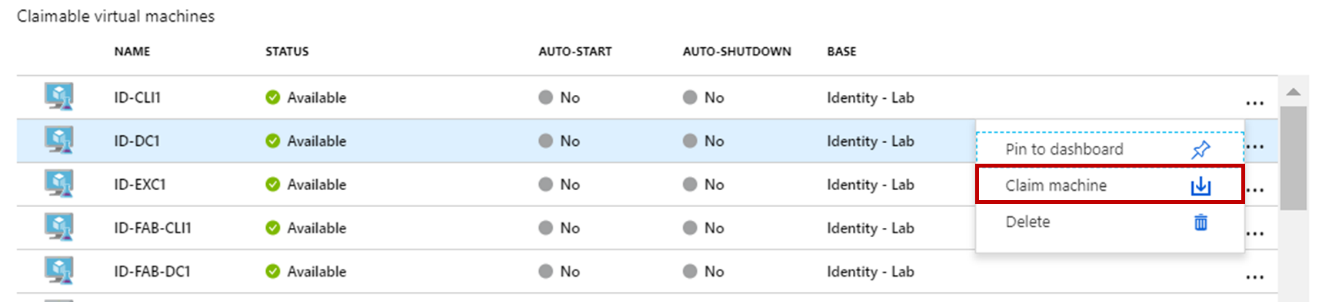
We do not need the latest updates for these labs so you can close this window.

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

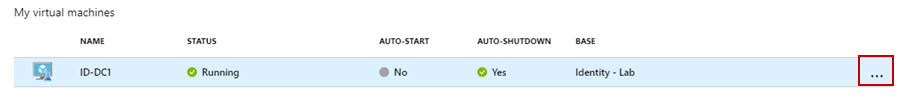
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



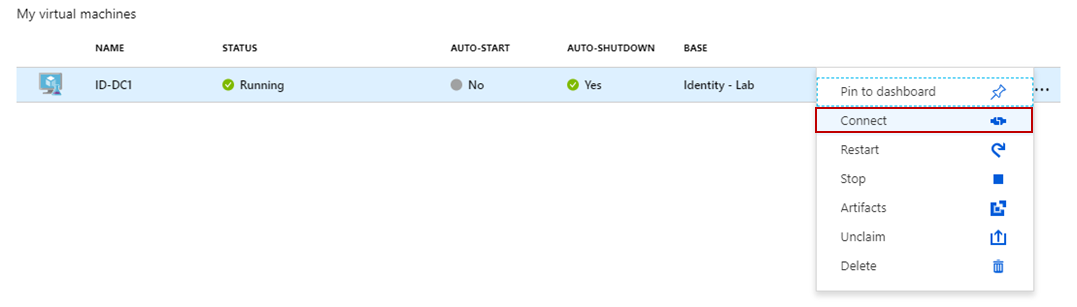
1. To start a VM, click on “Claim machine”



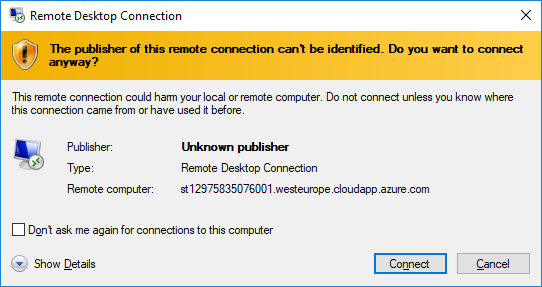
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



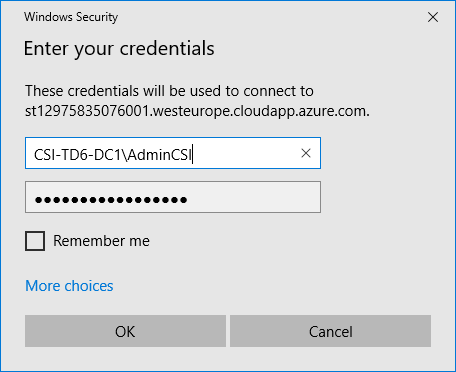
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



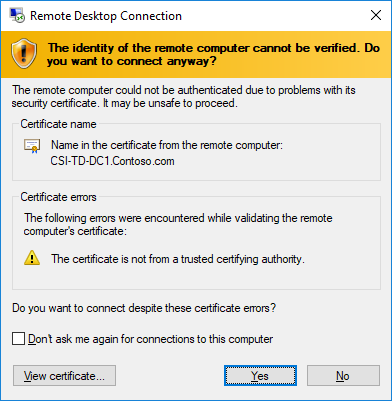
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



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.



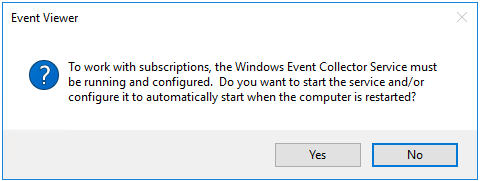
## Exercise 1: Event Forwarding

Duration: 45 minutes

Synopsis: In this exercise, attendees will learn how to configure event forwarding.

#### Task 1: Set up the collection server

1. Open a session on **CSI-SRV-DC1**
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Open a **Command Prompt as Administrator**
3. Check with the program **winrm if the service is started**:
   1. WinRM service is already running on this machine
   2. WinRM is already set up for remote management on this computer
4. In the **Event Viewer** , Click **Subscription and click Yes**



#### Task 2: Create a subscription

1. **Create a Subscription**
   1. **Test Subscription**
   2. Description : This is a test
   3. Leave Destination log with **Forwarded Events**
2. Click on **Source computer initiated**
   * 1. **CSI-TD-SRV1**
     2. **CSI-TD-EXC1**
     3. **CSI-TD-DC1**
3. Collect Event **Information** **, ID 101** in the **Application** log

#### Task 2: Subscribe to the collection server

1. On **CSI-TD-SRV1**
2. Launch **GPEdit.msc**
3. Find **Configure Target Subscription Manager and configure as follow**
   1. Click on **Enabled**
   2. Click **Show**
   3. Enter **Server=http://CSI-TD-SRV1.contoso.com:5985/wsman/SubscriptionManager/WEC,Refresh=20**
      1. The refresh interval is set to 20 for the lab
4. Repeat this configuration on **CSI-TD-EXC1** and **CSI-TD-DC1**
   1. In real life, we will use a GPO to configure event forwarding on each server
5. Switch to **CSI-TD-SRV1**
6. At the **command prompt** in **Administrator** mode, enter
   1. **eventcreate /T INFORMATION /L Application /ID 101 /D "Test subscription 101"**
7. Switch to **CSI-TD-SRV1**
8. At the command prompt, enter
   1. **eventcreate /T INFORMATION /L Application /ID 101 /D "Test subscription 101"**
9. Switch to the **Event Viewer** on **CSI-TD-SRV1**
10. Select **Windows Log\Forwarded Events**
11. You should see 2 events
    1. **111** indicates that a source computer connects
    2. **101** which is the forwarded event
       1. The event may take some time to show up

## Questions:

1. Why is the purpose of configuring Event Forwarding?

………………………………………………………………………………………………

1. What is the easiest way to deploy Event Forwarding?

………………………………………………………………………………………………

## 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.

