Windows security

Exercise 2 – Module 1 – Section 2

June 2020  
V1.2

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

[Analysis of a windows startup trace 1](#_Toc44075449)

[Abstract and learning objectives 1](#_Toc44075450)

[Overview 2](#_Toc44075451)

[Requirements 2](#_Toc44075452)

[Before the exercise 3](#_Toc44075453)

[List of VM to start 3](#_Toc44075454)

[How to start and connect to a VM 4](#_Toc44075455)

[Exercise 1: Analyzing the timeline of system’s boot phase 6](#_Toc44075456)

[Task 1: Prepare the lab environment 6](#_Toc44075457)

[Task 2: Examining the startup phase 8](#_Toc44075458)

[Task 3: Get insights on the early startup phase (boot phase) 8](#_Toc44075459)

[Task 4: Get insights on smss.exe operations 9](#_Toc44075460)

[Exercise 2: Analyzing the timeline of post-boot events 10](#_Toc44075461)

[Task 1: Get insights on services 10](#_Toc44075462)

[Task 2: Get insights on the logon phase 11](#_Toc44075463)

[Task 3: Monitor registry activity 11](#_Toc44075464)

[After the Lab 12](#_Toc44075465)

[Task 1: Stop and deallocated all the VMs 12](#_Toc44075466)

## Analysis of a windows startup trace

## Abstract and learning objectives

In this lab, you will train yourself in analyzing the startup and logon phase of Windows.

The lab is articulated around the Windows Performance Toolkit tool which provides detailed tracing capabilities.

## Overview

In this Lab, attendees will perform basic interpretation of a Windows Performance Toolkit trace in order to extract information about the boot and logon phase of Windows.

## 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

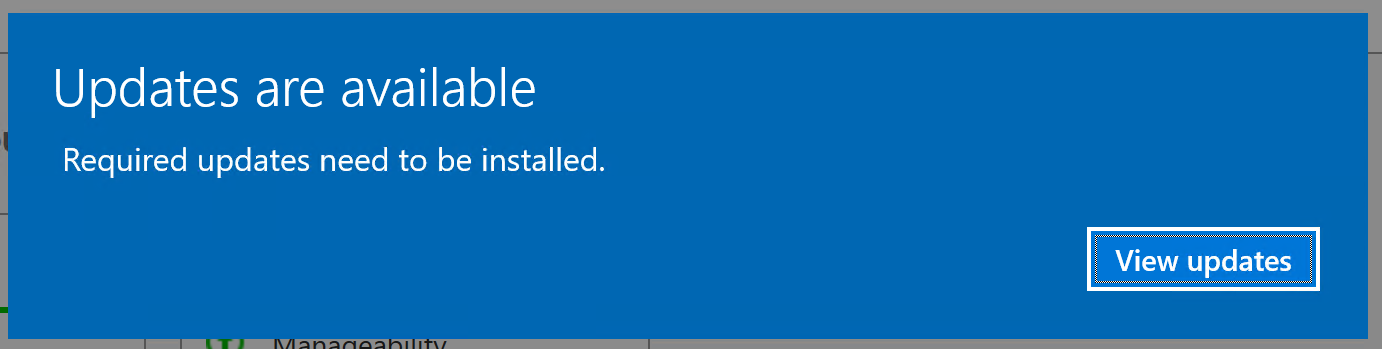
Duration: 10 minutes

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

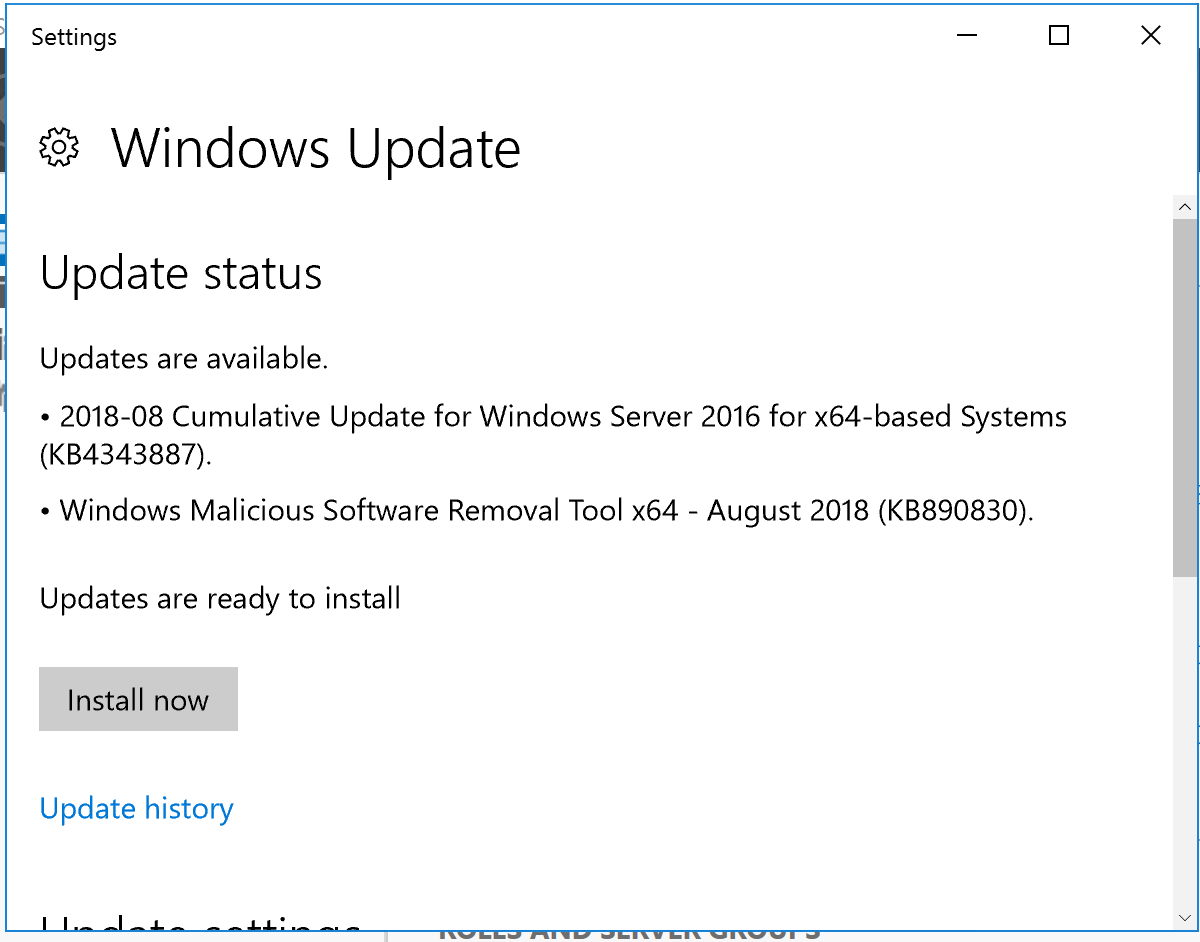
#### List of VM to start

|  |  |  |  |
| --- | --- | --- | --- |
| Name of VM | Hostname | OS Type | Role |
| CSW1-LAB | CSW1-LAB | Windows 10 Enterprise | Workstation |

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.



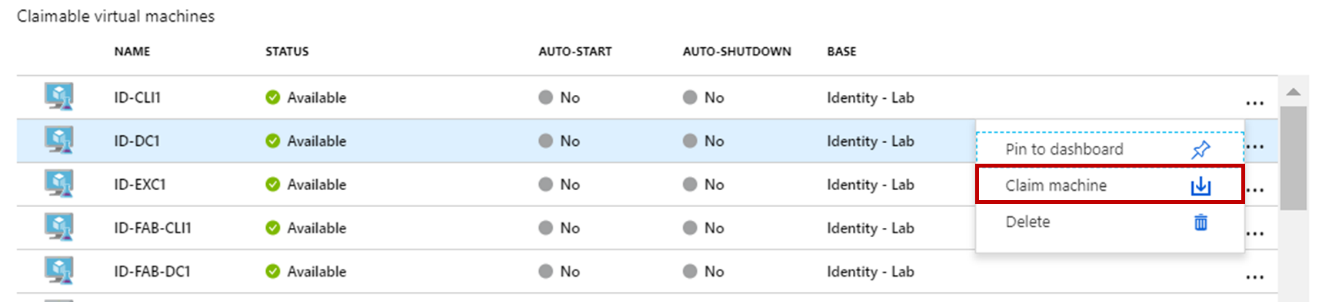
We do not need the latest updates for these labs so you can close this window.

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

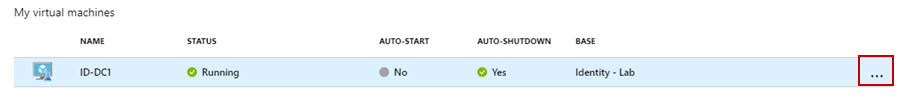
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



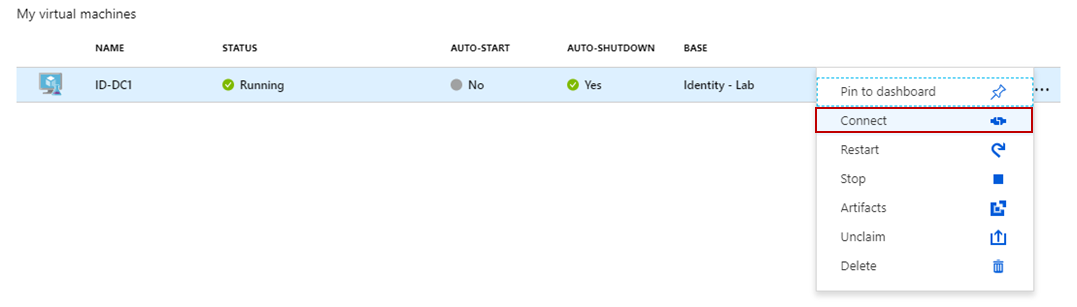
1. To start a VM, click on “Claim machine”



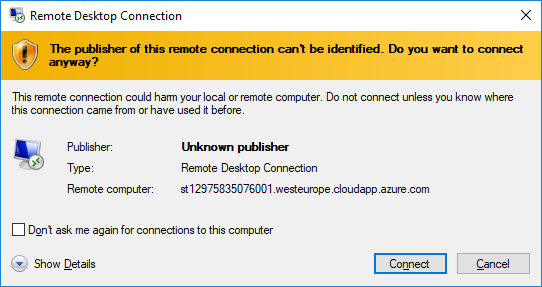
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



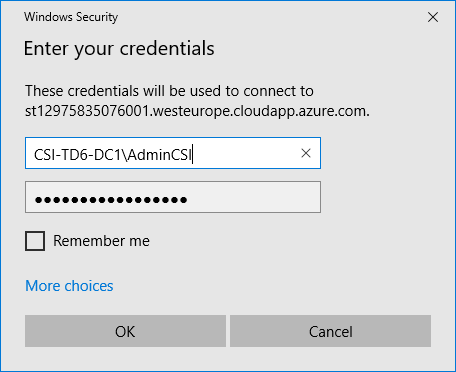
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



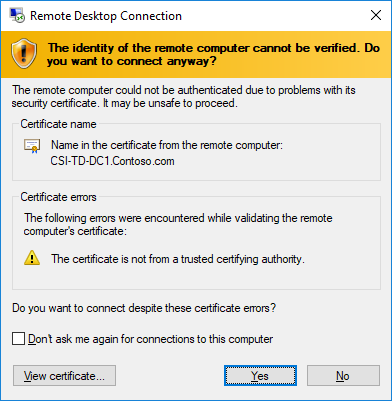
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



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: Analyzing the timeline of system’s boot phase

Duration: 45 minutes

Synopsis: In this exercise, you will learn how to use the Windows Performance Analyzer tool to extract information about the boot phase of a Windows system.

For all the assignments in this exercise, you will work on the machine named **CSW1-LAB** using the following credentials:  
 Username: CSW1-LAB\local\_student  
 Password: 08Fc720C!0eK2

#### Task 1: Prepare the lab environment

1. Start **wpa.exe**  
   Note: Windbg.exe is located in the **C:\LabContent\Tools\Windows Performance Toolkit** folder
2. Select **File** \ **Open**
3. Select the **boot.etl** file from **C:\LabContent\Material\XBootTrace**

Before moving on with this lab exercise, there are some basic concepts of Windows Performance Analyzer that you need to understand.

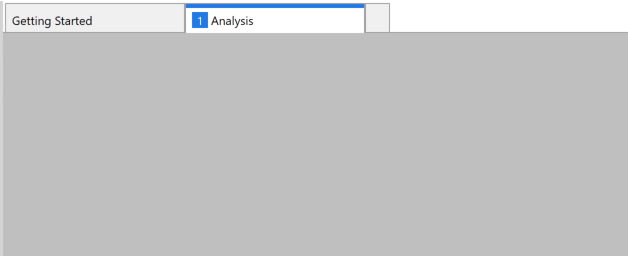
WPA is a graphical tool. Its main window is divided into 2 parts:

* **The graph explorer**. This is basically the data available. All the providers which were enabled during the tracing session (ie: when the trace was collected) are displayed as available graphs and grouped logically.

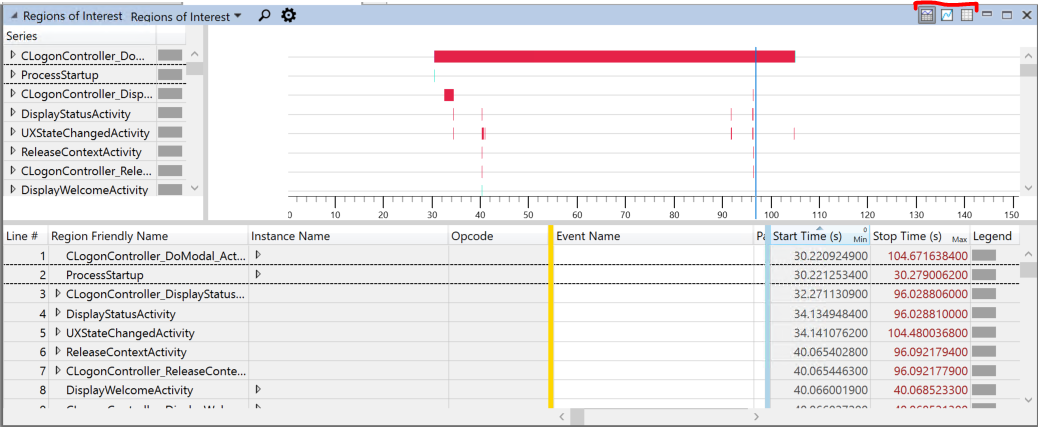


* **The analysis window** It is basically where the graphs are displayed. Multiple graphs can be opened. The x axis is the time. All graphs are synced regarding selected time meaning that any time selection in a graph is reflected in other graphs. A graph can be opened by double-clicking on it or by dragging it from the graph window to the analysis window

Empty Analysis window:



For any particular graph, you can switch between graphical representation only, data tables only or a mixed view (graph + data):



In the table view, there are mainly 3 kind of columns:

* Key area – at the left of the gold bar. Columns in the key area are used to group or index events of the data table.
* Data area – between the gold and the blue bar. It contains data for the specific event row which are not part of the key(s). The data for columns that appear in the data area is neither grouped nor graphed.
* Graphing area – at the right of the blue bar. The data in that columns generates lines or bars on the graph.

At any time, you can consult the documentation of any command by hitting the **F1** key or opening the **Help** \ **Help Topics F1** menu item.

#### Task 2: Examining the startup phase

In this Task, you will display the timeline of driver loading during the startup sequence which was recorded.

1. Open the System Activity\Images\Lifetime By Process, Image graph
2. Organize the columns so that it matches the following pattern:
   1. Line #, Image Name
   2. <Gold Bar>
   3. Session ID, ImageSize, Checksum, TimeDateStamp, File Description, File Version, Binary File version, Product Name
   4. <Blue Bar>
   5. Start Time, Legend

*Hint: Columns can be selected by right clicking on any existing column or by click on the gear  icon.*

Additional Questions:

1. Using only this image data table, how can you spot the moment when the kernel has ended its initialization and is ready to launch use mode applications?
2. When did the kernel end its initialization phase (seconds count since start of trace, rounded to the nearest ms)?
3. What are the first 2 processes launched in the Session 0?  
   First process:   
   Second process:
4. When did the winlogon.exe process start (seconds count since start of trace, rounded to the nearest ms)?

#### Task 3: Get insights on the early startup phase (boot phase)

In this task, you will learn how to display the events from the boot loader.

1. Open the **System Activity \ Generic Events** graph
2. Order the columns at the left of the gold bar so that events are only grouped by Provider Name.
3. Sort the data table by Time (Ascending)
4. Unfold the Microsoft-Windows-Kernel-Boot provider

Additional Questions:

1. What is the first file loaded by the bootloader?
2. Is VSM enabled?
3. What are the load options (*hint: have a look at BootType events*)?
4. When does the Winload.efi application gets loaded?

#### Task 4: Get insights on smss.exe operations

In this task, you will display more details about the various operations performed by smss.exe

1. Open the **System Activity \ Generic Events** graph
2. As explained in the main course, smss.exe can exist in multiple instance. In order to distinguish the various instances, find a way to add the Process name in the data table (between gold and blue bars).
3. Order the columns at the left of the gold bar so that events are only grouped by Provider Name.
4. Sort the data table by Time (Ascending)
5. Unfold the Microsoft-Windows-Subsys-SMSS provider

Additional Questions:

1. What is the first task performed by smss.exe?
2. What is the first application launched by the session-agnostic smss.exe?
3. What is the purpose of this application?
4. Regarding session #1, when does smss.exe start csrss.exe?

## Exercise 2: Analyzing the timeline of post-boot events

Duration: 45 minutes

Synopsis: In this exercise, you will learn how to use the Windows Performance Toolkit to get detailed timeline of post boot events including Service startup and main logon events

For all the assignments in this exercise, you will work on the machine named **CSW1-LAB** using the following credentials:  
 Username: CSW1-LAB\local\_student  
 Password: 08Fc720C!0eK2

#### Task 1: Get insights on services

In this task, you will discover how to get information about services startup.

1. Open the **System Activity \ Services** graph
2. Arrange the column layout so that you can display the services ordered only by their start time. We don’t need grouping for this exercise.

Additional Questions:

1. Capture a screenshot of the view editor for the Services graph. The view editor window can be opened by clicking the gear icon **
2. What is the first service group to start?
3. Which group the ProfSvc service belongs to?
4. When does the ProfSvc service gets started (seconds count since start of trace, rounded to the nearest ms)?
5. What is the name of the process hosting the VSS service? What is its PID?
6. What is the start type of service SstpSvc?

#### Task 2: Get insights on the logon phase

In this task, you will discover how to get information about services startup.

1. Open **System Activity \ Generic events**
2. Order the columns at the left of the gold bar so that events are only grouped by Provider Name.
3. Sort the data table by Time (Ascending)
4. Unfold the Microsoft-Windows-Winlogon provider

Additional Questions:

1. What is the first operation of Winlogon.exe?
2. How much time did it take to start LogonUI.exe (round the result to the nearest ms)?
3. Which is the first provider being notified by Winlogon?
4. How long does the logon phase last (round the result to the nearest ms)?
5. What is the shell command run by winlogon?
6. Use the Windows Logon graph to count the number of providers which are notified of the Logon event.

#### Task 3: Monitor registry activity

In this task, you will learn how to use the Windows Performance Toolkit to monitor registry activity.

1. Open the **Storage \ Registry \ Count by Operation, Process, Key** graph
2. Organize the column set so that registry I/Os are grouped first by Key name then, by operation. Ensure that the keys appear as a tree (so that we can fold and unfold the keys).

Additional Questions:

1. Which process tries to access the \Registry\MACHINE\SECURITY\Policy\Secrets\$MACHINE.ACC key?
2. How much times does this process access the key?
3. Does the key exist?
4. What is the purpose of the $MACHINE.ACC key?
5. What can you conclude about the machine?

## After the Lab

Duration: 10 minutes

In this exercise, attendees will deprovision any Azure resources that were created 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.

