Windows security, Active Directory and Azure AD

TD06 – Module 1 – Section 1

March 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.

© 2018 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](#_Toc526172121)

[Abstract and learning objectives 1](#_Toc526172122)

[Overview 2](#_Toc526172123)

[Requirements 2](#_Toc526172124)

[Before the exercise 3](#_Toc526172125)

[List of VM to start 3](#_Toc526172126)

[How to start and connect to a VM 4](#_Toc526172127)

[Exercise 1: Manage access without Active Directory 6](#_Toc526172128)

[Task 1: Create two standard users on CSI-TD6-CLI1 6](#_Toc526172129)

[Task 2: Create a standard user on CSI-TD6-SRV1 and share a folder for this user 7](#_Toc526172130)

[Task 3: Access to the share with Local\_User1 9](#_Toc526172131)

[Task 4: Access to the share with Local\_User2 9](#_Toc526172132)

[Exercise 2: New forest creation 11](#_Toc526172133)

[Task 1: Promote Domain Controller – CSI-TD6-DC1 11](#_Toc526172134)

[Task 2: Promote CSI-TD6-DC2 as a second domain controller 12](#_Toc526172135)

[Exercise 3: Add a new computer to the domain 14](#_Toc526172136)

[Task 1: Add CSI-TD6-CLI1 to the Domain Contoso.com 14](#_Toc526172137)

[Task 2: Add CSI-TD6-SRV1 to the Domain Contoso.com 14](#_Toc526172138)

[Task 3: Add Domain users to the local group Remote Desktop Users on CSI-TD6-CLI1 15](#_Toc526172139)

[Exercise 4: Discovery of the environment 16](#_Toc526172140)

[Task 1: Create a new OU 16](#_Toc526172141)

[Task 2: Create new users 17](#_Toc526172142)

[Task 3: Create a new group 17](#_Toc526172143)

[Task 4: Move CSI-TD6-CLI in the OU Paris\Computers 17](#_Toc526172144)

[Task 5 : Create a new “Account Operator” 17](#_Toc526172145)

[After the Lab 19](#_Toc526172146)

[Task 1: Stop and deallocated all the VMs 19](#_Toc526172147)

# 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 these labs, you will manipulate Windows systems in a “workgroup” environment (machines which are not domain-joined to an Active Directory domain are considered being in a “workgroup”). You will also promote your first domain controllers and discover the tools and commands used to create directory objects.

## 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

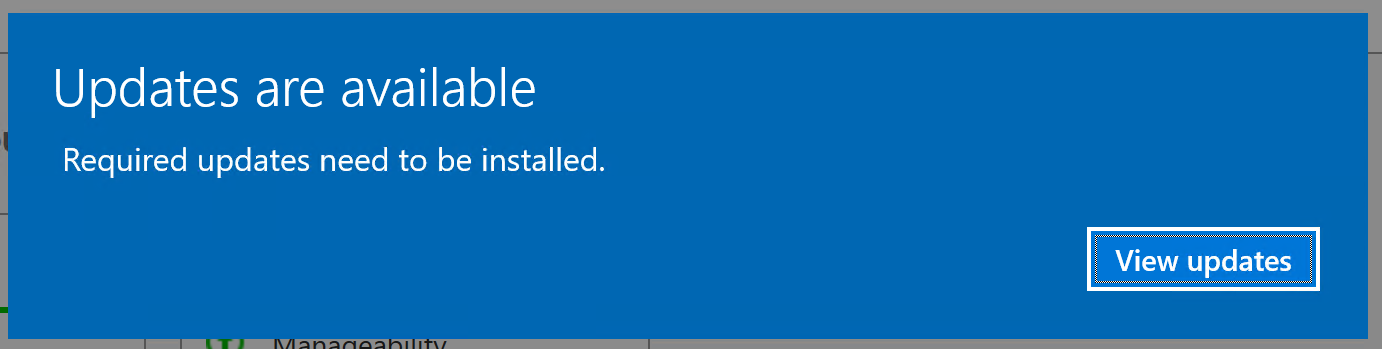
Synopsis: In this section, you will start up your environment for use in the rest of the Lab. You should have the following environment.

#### List of VM to start

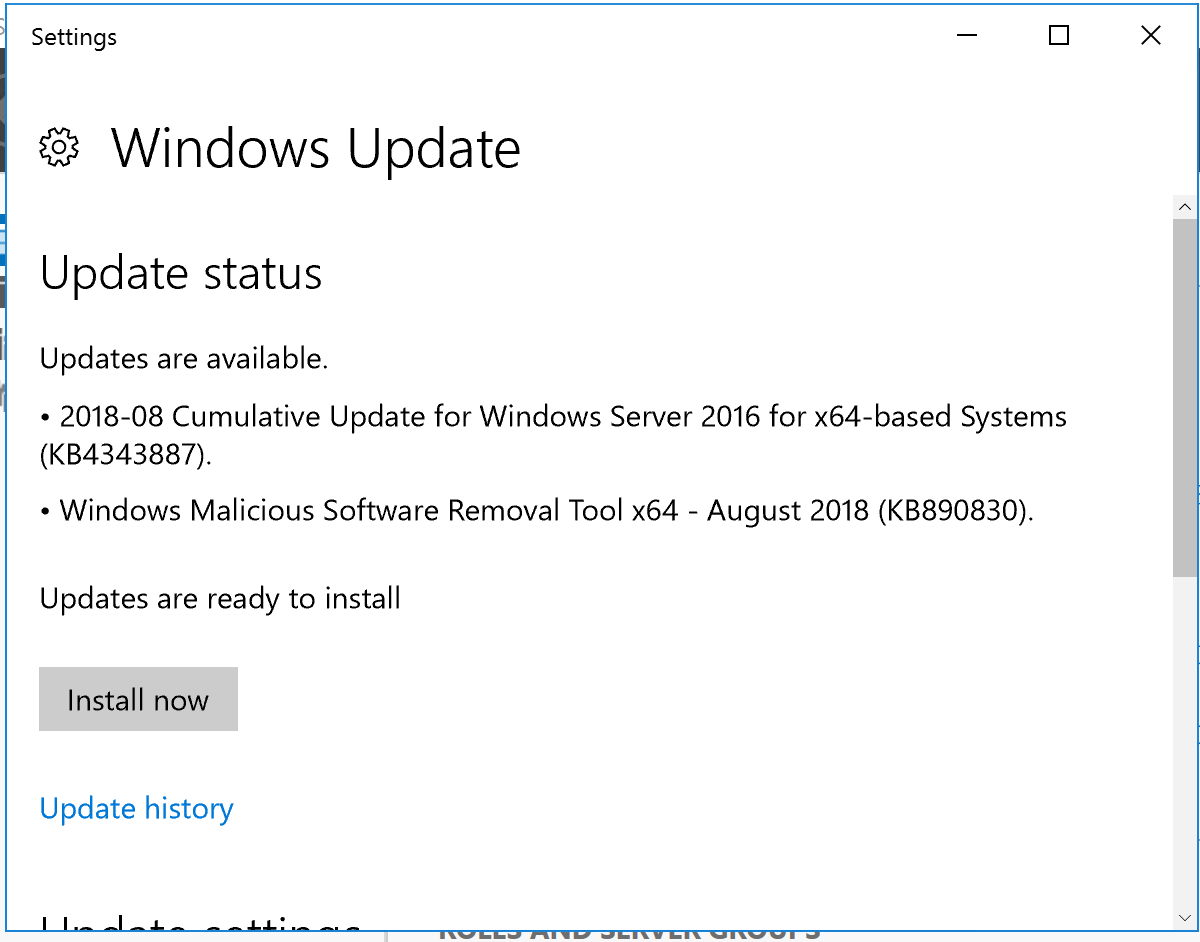
**Remember that after the domain creation, it is recommended to start the DCs first and to wait 5 minutes before starting the other VMs.**

|  |  |  |  |
| --- | --- | --- | --- |
| Name of VM | Hostname | OS Type | Role |
| ID-TD6-DC1 | CSI-TD6-DC1 | Windows Server 2016 Standard | DC |
| ID-TD6-DC2 | CSI-TD6-DC2 | Windows Server 2016 Standard | DC |
| ID-TD6-SRV1 | CSI-TD6-SRV1 | Windows Server 2016 Standard | Server |
| ID-TD6-CLI1 | CSI-TD6-CLI | Windows 10 Pro | Desktop |

Note that the machines have been provisioned in July 2018.   
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.



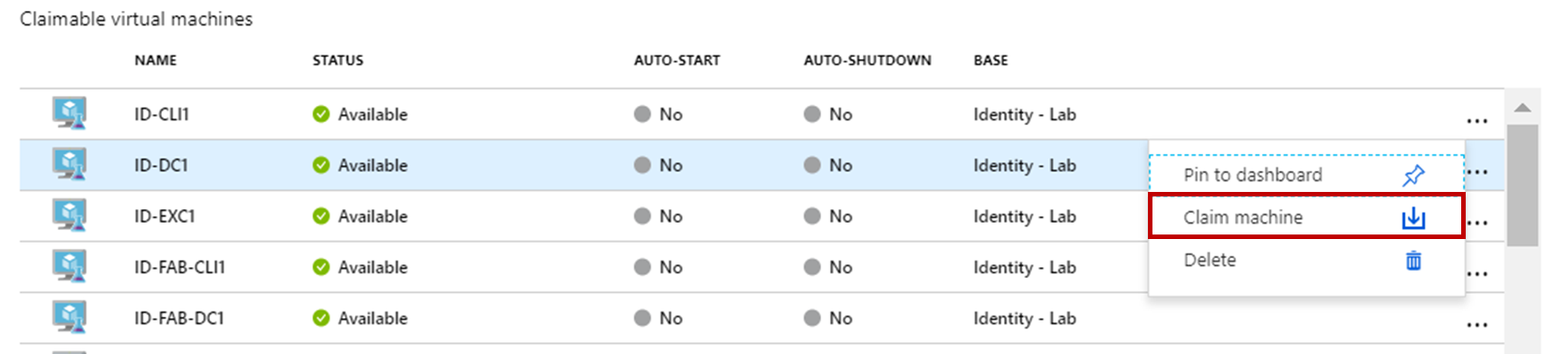
We do not need the latest updates for these labs so you can close this window.

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

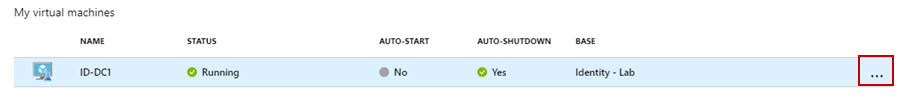
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



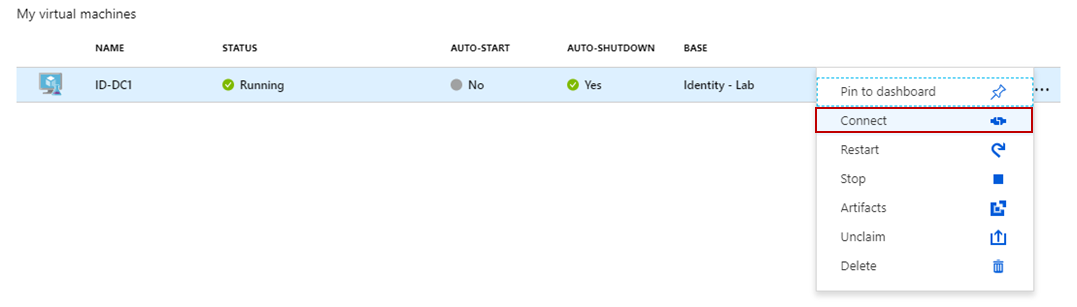
1. To start a VM, click on “Claim machine”



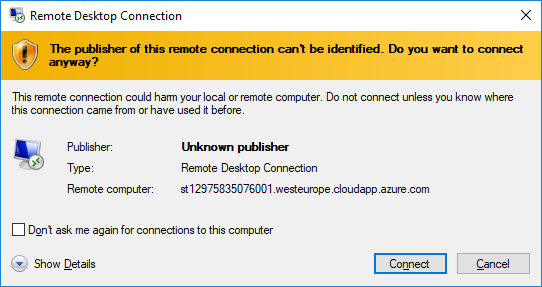
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



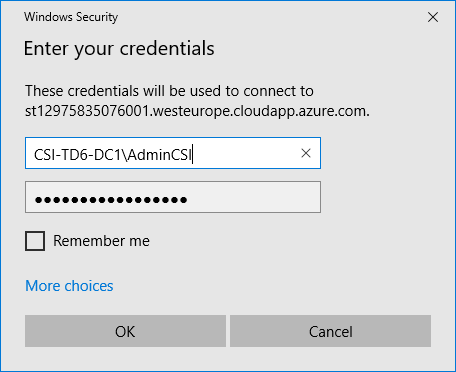
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



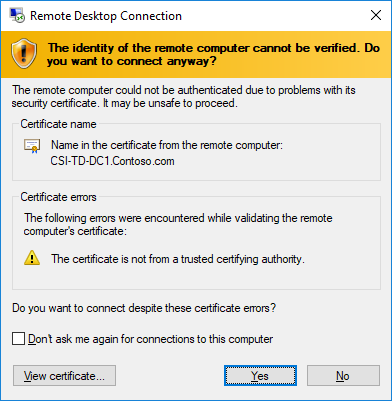
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



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: Manage access without Active Directory

Duration: 30 minutes

Synopsis: In this exercise, attendees will demonstrate how resources’ access works without Active Directory, and the need to duplicate account to allow access for several users to the same resources.

#### Task 1: Create two standard users on CSI-TD6-CLI1

1. Log on to the client:
   1. Username: **.\AdminCSI**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Create two standards users named :
   1. User name: **Local\_User1**
   2. User name: **Local\_User2**
   3. Password: **Ilovesecu\*!**
   4. If necessary, don’t forget to uncheck **User Must change password at Next logon**
3. Add the group “**Authenticated Users”** to the group **Remote Desktop Users**. This step is necessary to allow standard users to connect to this machine via the RDP protocol
4. Click on **Groups**
5. Double click on **Remote Desktop Users**
6. **Add Local\_User1** and **Local\_User2 to the group Remote Desktop Users**
7. Log off from the machine

#### Task 2: Create a standard user on CSI-TD6-SRV1 and share a folder for this user

In a “workgroup” environment, when a user wants to access protected data from another Windows computer on the network, the same account with the same password and both systems have to exist on the source and the target.

1. Log on to CSI-TD6-SRV1:
   1. Username: **.\AdminCSI**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Create two standards users named :
   1. User name: **Local\_User1**
   2. User name: **Local\_User2**
   3. Password: **Ilovesecu\*!**
   4. If necessary, don’t forget to uncheck **User Must change password at Next logon**
3. Under C:\, create a folder named **Prod**
4. Share this folder
5. Permissions :
   1. Remove Everyone
   2. Add **Full Control** for **Local\_User1**
   3. Right click on the folder and select **Properties**
6. Add NTFS permissions **Full control** permission for **Local\_User1**

#### Task 3: Access to the share with Local\_User1

1. Log on to CSI-TD6-CLI1:
   1. Username: **.\Local\_User1**
   2. Password: **Ilovesecu\*!**
2. Access to [**\\10.0.0.15\Prod**](file://10.0.0.15/Prod)
3. Create a file in the folder
4. The operation should succeed (without any authentication prompts)
5. Log out

#### Task 4: Access to the share with Local\_User2

1. Log on to CSI-TD6-CLI1:
   1. Username: **.\Local\_User2**
   2. Password: **Ilovesecu\*!**
2. Access to [**\\10.0.0.15\Prod**](file://10.0.0.15/Prod)
3. Try to create a file and a folder
4. Local\_User2 should not be able to access to the folder because
   1. His account does not exist on the target server
   2. He has no permissions on the folder
5. Log off

## Exercise 2: New forest creation

Duration: 45 minutes

Synopsis: In this exercise, attendees will create a new forest and add a second domain controllers to the forest. The second domain controller will be added without using the GUI interface.

#### Task 1: Promote Domain Controller – CSI-TD6-DC1

1. Log on to the server CSI-TD6-DC1:
   1. Username: **.\AdminCSI**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Add Roles **Active Directory Domain Services**
3. Promote server to Domain Controller for a new forest : named **Contoso.com**
   1. Password for directory restoration operations (this password will be necessary if we need to restore a domain controller):
      1. **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
4. Once rebooted (the reboot may take few minutes), you will sign into with new domain **AdminCSI** account
   1. Username: **CONTOSO\AdminCSI** or [**AdminCSI@contoso.com**](mailto:administrator@contoso.com)
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
      1. **If a changed password is required enter : the same password.**
      2. **If the keyboard is in English, here the password : PiKqrQlR2QlBen?o&**
      3. **Note that l is a L in lower case**
5. Set the password for **AdminCSI** to PasswordNeverExplired

#### Task 2: Promote CSI-TD6-DC2 as a second domain controller

1. Log on to the server CSI-TD6-DC2:
   1. Username: **AdminCSI**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Add Roles **Active Directory Domain Services using Powershell**
3. Promote server to Domain Controller for the named Contoso.com using Powershell
   1. Password for directory restoration operations (this password will be necessary if we need to restore a domain controller):
      1. **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**

## Exercise 3: Add a new computer to the domain

Duration: 30 minutes

Synopsis: In this exercise, attendees will join new computers to the domain.

#### Task 1: Add CSI-TD6-CLI1 to the Domain Contoso.com

1. Log on to the CSI-TD6-CLI1:
   1. Username: **.\AdminCSI**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Join CSI-TD6-CLI1 to the domain Contoso.com

#### Task 2: Add CSI-TD6-SRV1 to the Domain Contoso.com

1. Switch to Log on to the CSI-TD6-SRV1:
   1. Username: .**\AdminCSI**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Join CSI-TD6-SRV1 to the domain Contoso.com

#### Task 3: Add Domain users to the local group Remote Desktop Users on CSI-TD6-CLI1

These steps are necessary to allow standard users to connect via the RDP protocol

1. Log on to the CSI-TD6-CLI1:
   1. Username: **.\AdminCSI**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Add Domain the domain group “**Domain users** “ to the local group Remote Desktop Users on **CSI-TD6-CLI1**

In a real deployment, the clients are physical machines on the front of the end users. This does not require to add the Domain Users into the Remote Desktop groups. This operation is performed in our case because we use the RDP protocol to access the virtual machines in Azure.

## Exercise 4: Discovery of the environment

Duration: 30 minutes

Synopsis: In this exercise, attendees will discover the basic management of Active Directory by creating organizational unit, users, groups.

#### Task 1: Create a new OU

1. Log on to CSI-TD6-DC1:
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Click on Windows button  on the taskbar, click on **Windows Administrative Tools** and choose **Active Directory Administrative Center**
3. Create the followingOrganizational Unit structure
4. **Paris**
   1. **Users**
   2. **Groups**
   3. **Computers**
5. **IT**
   1. **Users**
   2. **Groups**
   3. **Computers**

#### Task 2: Create new users

1. Under the container **Users**, create a new user with **FirstName-Adm** and add it to the **“Domain Admins”** group
2. Close the session and open the session with the new Domain Admins account
3. Under the OU **Paris/Users**, create 5 users : **PAR\_User1, PAR\_User2, PAR\_User3, PAR\_User4 and PAR\_User5**
   1. Password: **Ilovesecu\*!**

Disable change password at next log on

Note that you can technically create an account without setting a password. But the account will have to be disabled and you will need to set a password to enable the account. We will learn later that it is also possible to enable a user without setting a password under certain conditions.

#### Task 3: Create a new group

* 1. Under the OU **Paris/Group**,create a group named : **Paris Prod**

1. Click **OK**

All actions performed with the console can be done with PowerShell. In order to see the PowerShell equivalent of what has been done in the GUI, you can expand the Windows PowerShell history section at the bottom of the console:

#### Task 4: Move CSI-TD6-CLI in the OU Paris\Computers

1. Click on the **Contoso (local)** and click **Computers**
2. Move Computer account from **CSI-TD6-CLI1 to the OU Paris/Computer**

#### Task 5 : Create a new “Account Operators”

1. In the OU IT/Users, create a new account named
   1. **Admin\_account**
   2. Password: **Ilovesecu\*!**
   3. Disable change password at next log on
2. Add the new user to the group “**Account Operators”**

We will learn later what are the default permissions given to the group Account Operators.

## 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.

