WorkshopPLUS

Microsoft Azure Infrastructure as a Service (IaaS)

Introduction to Microsoft Azure Active Directory

Student Lab Manual

V1.4, May 21, 2015

Information in this document is subject to change without notice. The example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person 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, trademarked, 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.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, MS, Windows, Windows NT, MSDN, Active Directory, BizTalk, SQL Server, SharePoint, Outlook, PowerPoint, FrontPage, Visual Basic, Visual C++, Visual J++, Visual InterDev, Visual SourceSafe, Visual C#, Visual J#,  and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names herein may be the trademarks of their respective owners.

Contents

[Introduction to Microsoft Azure Active Directory 4](#_Toc414542028)

[Overview 4](#_Toc414542029)

[Objectives 4](#_Toc414542030)

[Prerequisites 4](#_Toc414542031)

[Exercises 5](#_Toc414542032)

[Exercise 1: Provisioning a Domain Controller in Azure 5](#_Toc414542033)

[Task 1 – Creating a Domain Controller in Azure 5](#_Toc414542034)

[Exercise 2: Creating a new Azure Active Directory tenant 8](#_Toc414542035)

[Task 1 - Creating a new Directory Tenant 8](#_Toc414542036)

[Task 2 - Creating a new Global Administrator Account 13](#_Toc414542037)

[Exercise 3: Configuring and Validating Directory Synchronization 17](#_Toc414542038)

[Task 1 – Installing Windows Azure Active Directory Sync 17](#_Toc414542039)

[Task 2 – Configuring Windows Azure Active Directory Sync 19](#_Toc414542040)

[Task 3 – Validating Windows Azure Active Directory Sync 23](#_Toc414542041)

[Exercise 4: Removing an Azure Active Directory Tenant 29](#_Toc414542042)

[Task 1 – Disabling Directory Synchronization 29](#_Toc414542043)

[Task 2 – Cleaning up and Removing your Azure Active Directory Tenant 30](#_Toc414542044)

[Exercise 5: Removing the Domain Controller 32](#_Toc414542045)

[Task 1 – Removing the Domain Controller 32](#_Toc414542046)

[Appendix A: Create an Azure Cloud Service 33](#_Toc414542047)

# Introduction to Microsoft Azure Active Directory

## Overview

During this lab, you will install a Domain Controller in Azure and provision an Azure Active Directory Tenant. You will then setup Directory Synchronization between Active Directory and Azure Active Directory, using Password Synchronization.

## Objectives

In this hands-on lab, you will learn how to:

* Use PowerShell to automate the creation of Virtual Machines in Azure

Setup a new Azure Active Directory Tenant

* Synchronize you on-premises Active Directory to Azure Active Directory

## Prerequisites

The following is required to complete this hands-on lab:

* [Microsoft Online Services Sign-In Assistant for IT Professionals RTW](http://go.microsoft.com/fwlink/?LinkID=286152) \*
* [Azure Active Directory Module for Windows PowerShell (64-bit version)](http://go.microsoft.com/fwlink/p/?linkid=236297) \*
* [Microsoft Azure PowerShell](http://msdn.microsoft.com/en-us/library/windowsazure/jj156055) \*
* A Microsoft Azure subscription - [sign up for a free trial](http://aka.ms/WATK-FreeTrial) with an Azure Virtual Network with at least one Subnet, an Azure Storage Account and an Azure Cloud Service
* An Azure Storage account. Make sure the storage account is in the same data center/region you intend on putting your virtual machine in. You can create this storage account via the UI or PowerShell. <http://azure.microsoft.com/en-us/documentation/articles/storage-create-storage-account/>.
* An Azure Virtual Network – this will be a standard internal Azure virtual network (not Point-to-Site or Site-to-Site). Create this virtual network in the same data center/region that the storage account is in. Please give your subnet a descriptive name (for this lab, you only need a single subnet). <http://msdn.microsoft.com/library/azure/dn631643.aspx>.
* An Azure Cloud Service – This can be an empty Cloud Service in which you intend on placing your virtual machines. If you do not know how to do this, follow the steps in Appendix A.

\* These items are already installed on the hosted lab machines.

## Exercises

This hands-on lab includes the following exercises:

* Provisioning a Domain Controller in Azure
* Creating a new Azure Active Directory Tenant
* Configuring and Validating Directory Synchronization

## Exercise 1: Provisioning a Domain Controller in Azure

In this exercise, you will learn how to create a new Domain Controller using PowerShell.

At the end of this exercise, we will execute a long-running PowerShell script. It is recommended that you continue with Exercise 2 as this script executes.

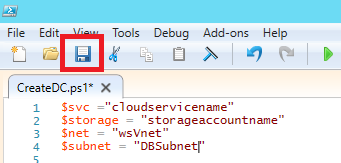
Estimated time to complete this entire lab: 90 minutes.

Estimated time to complete this exercise, until script execution: 35 minutes.

### Task 1 – Creating a Domain Controller in Azure

Make sure you have all the source files in the correct location on your machine. This will typically be in the **.\M5-Identity\Labs\IntroToMicrosoftAzureAD** directory.

1. Open **Windows PowerShell ISE** (not Microsoft Azure PowerShell) as an administrator. You can do this by typing in *powershell ise* on the Win8x tile window. Make sure your view shows the script pane and the command output window.
2. Navigate to the directory where the scripts for the hands-on labs are located: **.\M5-Identity\Labs\IntroToMicrosoftAzureAD\Source\Assets** and open **CreateDC.ps1**.
3. In the PowerShell ISE command prompt window, change the directory to **.\M5-Identity\Labs\IntroToMicrosoftAzureAD\Source\Assets.**
4. In the PowerShell ISE command prompt type in the following PowerShell command to log in to Azure:  
     
   Add-AzureAccount
5. Locate the **$svc**, **$storage**, **$net, $subscription** and **$subnet** parameters in the first four lines of the script. Change the parameters to reflect the Cloud Service that you want to use (**$svc**, e.g. “mycloudservice”), the Storage Account that you want to use (**$storage**, e.g. “mystorageaccount”), the network that you want to use (**$net**, e.g. “wsVnet”) and the subnet that you want to use (**$subnet**, e.g. “DBSubnet”). All these items have to exist in your current Azure Subscription before the script can be successfully executed. You can safely reuse any existing cloud service or storage account. Please make sure your cloud service is empty first (no deployments).  
     
   After modifying the values, click the **Save** button on the top bar to save the modifications.

  
*Change the values of required variables*

1. Start the script by pressing the **Play** button (green triangle) on the top bar. Keep track of the progress of the script. If it terminates unexpectedly, please consult your instructor. The script might take up to 60 minutes to complete.

It is recommended that you now continue with Exercise 2 as the script is running.

Sample output:

PS C:\AzureIaaSWS\M5-Identity\Labs\IntroToMicrosoftAzureAD\Source\Assets> C:\AzureIaaSWS\M5-Identity\Labs\IntroToMicrosoftAzureAD\Source\Assets\CreateDC.ps1

Setting Storage Account.

Getting proper image for Virtual Machine.

Creating new Virtual Machine and waiting for boot.

OperationDescription OperationId OperationStatus

-------------------- ----------- ---------------

New-AzureVM c195dc61-217d-33c2-8eb1-386fb0b7c4a8 Succeeded

Establishing remote session to new Virtual Machine.

Promoting the Virtual Machine to Domain Controller.

Initializing and formatting raw disk.

Installing AD Domain Services.

Creating new AD Forest.

Machine will now be rebooted.

Importing CSV files for user import.

Trying to re-establish the PowerShell session to the Domain Controller.

WARNING: Unable to establish a PowerShell session. Retry in 15 seconds...

WARNING: Unable to establish a PowerShell session. Retry in 15 seconds...

Creating Users, Groups and Organizational Units. (Be patient!)

Importing Organizational Units...

Importing Users...

Importing Groups...

Adding Users to Groups...

Installing requirements for DirSync and downloading DirSync.

Installing .NET 3.5 features.

Downloading DirSync.

Done!

PS C:\AzureIaaSWS\M5-Identity\Labs\IntroToMicrosoftAzureAD\Source\Assets>

## Exercise 2: Creating a new Azure Active Directory tenant

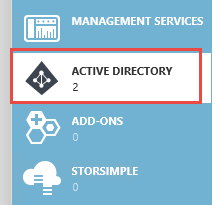
In this exercise, you will learn how to provision a new Microsoft Azure Active Directory tenant within your Microsoft Azure subscription and how to create a Global Administrator account within the Azure Active Directory.

Estimated time to complete this exercise: **10 minutes**.

### Task 1 - Creating a new Directory Tenant

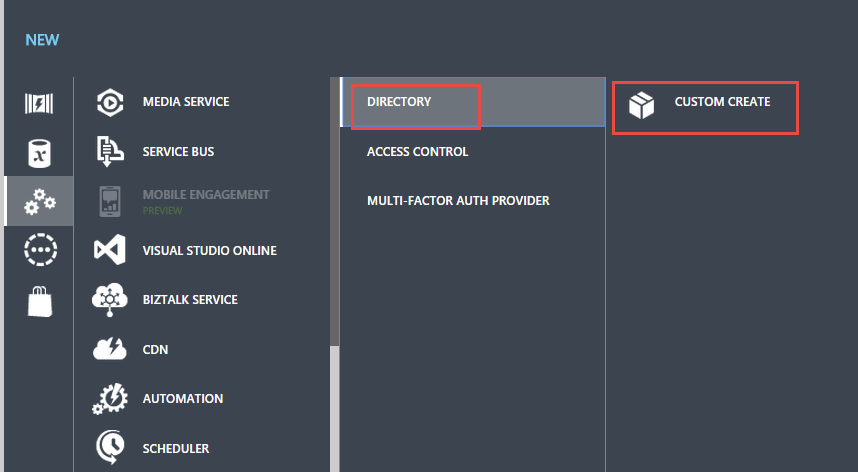
In this task, you will provision a new Microsoft Azure Active Directory Tenant from the Management Portal.

1. Sign in to the Azure Management Portal.
2. Select **Active Directory** from the left pane.



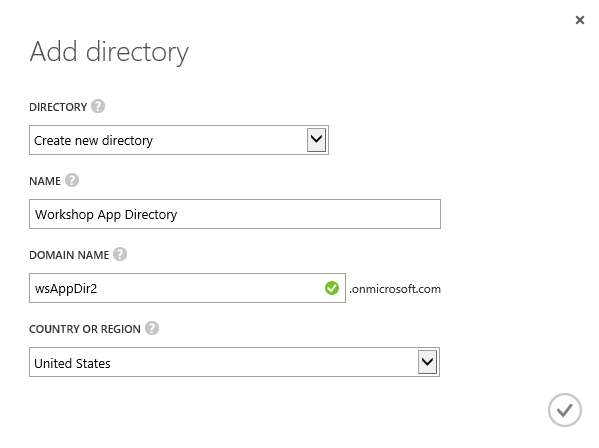
Accessing Microsoft Azure Active Directory

1. Click the **+New** button in the lower left hand corner of the portal window and then select **App Services->Active Directory->Directory->Custom Create**.



Adding a new Active Directory Tenant

1. Enter a name to describe the new domain name, the domain name and country. Click the **check** button to continue.



Filling Active Directory Information

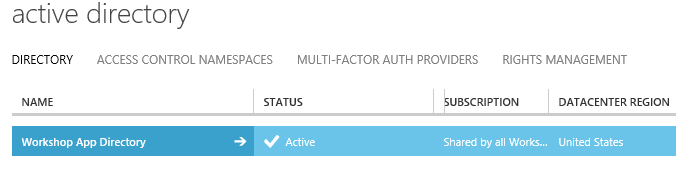
**Note:** This dialog gathers essential information needed to create a directory tenant for you.

* + **Country or Region**: The value selected in this dropdown will determine where your tenant will be created. Given that the directory will store sensitive information, please do take into account the normative about privacy of the country in which your company operates.
  + **Domain Name**: This field represents a critical piece of information: it is the part of the directory tenant domain name that is specific to your tenant, what distinguishes it from every other directory tenant.

At creation, every directory tenant is identified by a domain of the form **.onmicrosoft.com.** That domain is used in the UPN of all the directory users and in general wherever it is necessary to identify your directory tenant. After creation it is possible to register additional domains that you own. For more information, see domain management.

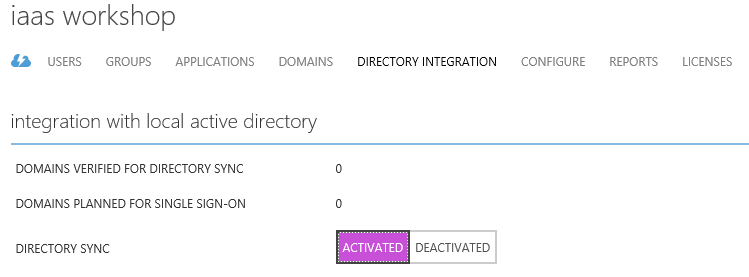
* + **The Domain Name must be unique**: the UI validation logic will help you to pick a unique value. It is recommended that you choose a handle which refers to your company, as that will help users and partners as they interact with the directory tenant.

1. Wait until the Active Directory is created (its status should display **Active**).



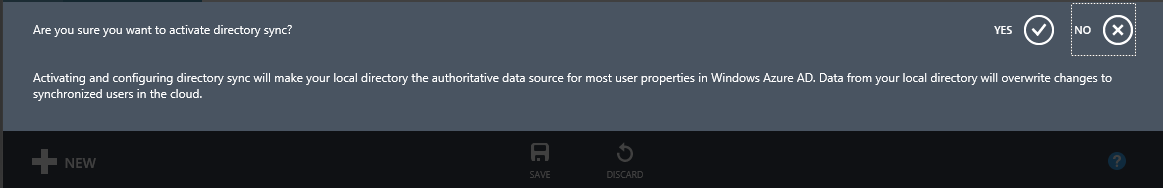
Active Directory Tenant Creation Completed

1. Now you will enable Directory Synchronization in the Azure AD tenant. Click on the newly created directory entry to display the User management UI. Click on the **Directory Integration** menu item at the top of the dashboard then then click **Activated** next to the Directory Sync option.

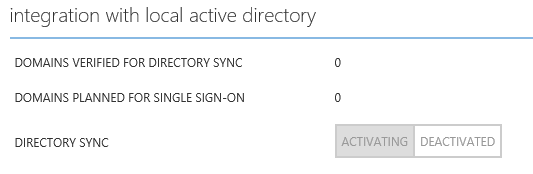


*Activating Directory Sync*

1. At the bottom of the page, click **Save**, and confirm that you want to enable Directory Sync in the tenant by clicking **Yes**.

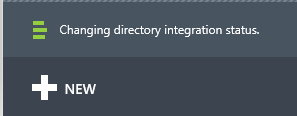


*Confirm enabling Directory Sync*

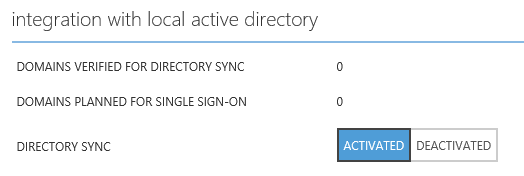


*Directory Sync status showing Activating*

Wait for this operation to complete.



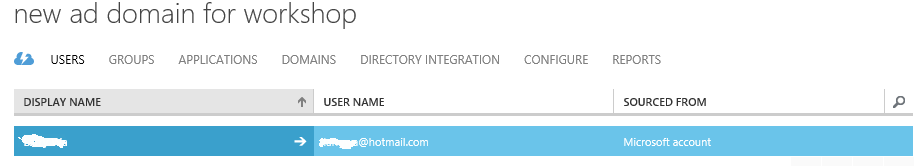
*Directory Sync is being enabled*



*Directory Sync status showing Activated*

### Task 2 - Creating a new Global Administrator Account

1. Click on the **Users** menu item at the top of the screen to display the User management UI. The directory tenant is initially empty, except for the Microsoft Account administering the Microsoft Azure subscription in which the new tenant was created.



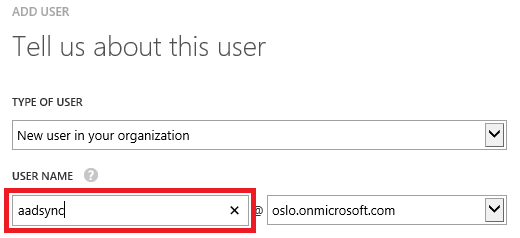
Active Directory User List

1. Now you will add a new user to the directory. Click on the **User** menu item at the top of the dashboard then then select the **Add User** button in the bottom bar.



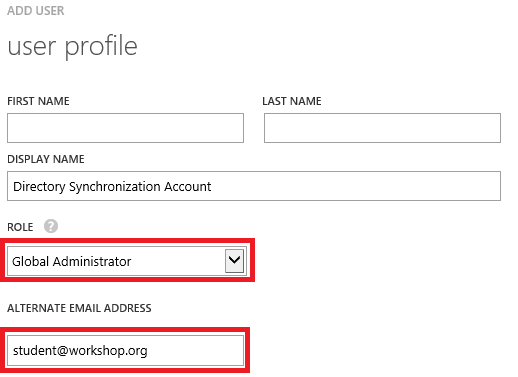
Adding a new user to Active Directory

1. In the dialog box, keep the default option of **New user in your organization** and type **aadsync** in the user name dialog. Click **Next** to continue.



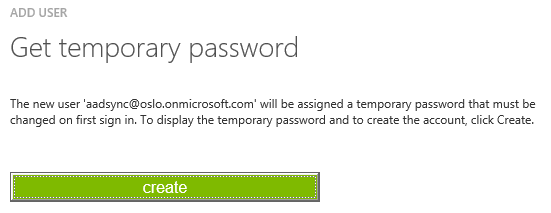
Filling out new user details

1. Enter the user profile data. Select the **Role** option of **Global Administrator** and type your email address in the **Alternate Email Address** dialog. Click **Next** to continue.



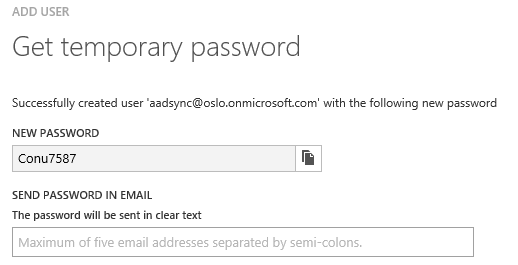
Filling out user profile information

1. The Management Portal generates a temporary password, which will have to be used at the time of the first login. At that time, the user will be forced to change password. Click the **Create** check button.



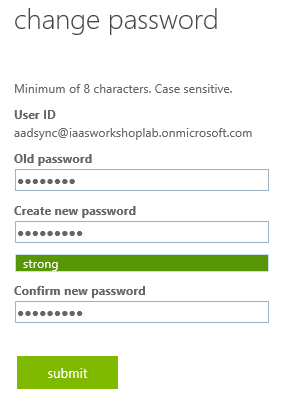
*Creating a temporary password*

Take note of the temporary password, as you will need it in the following tasks. Click the complete button to create the user.



Creating a temporary password (2)

1. Sign out of the Azure Management Portal and navigate to <https://account.activedirectory.windowsazure.com>
2. Sign in with the credentials for the Azure Active Directory Global Administrator User you have created in step 3.
3. On the page to change the password for the user, change the password by filling out the required field and clicking the **submit** button. Note the password you choose, you will need it later on.



1. Sign out of the page by clicking on the username at the right top of the page and clicking **Sign out**.

## Exercise 3: Configuring and Validating Directory Synchronization

In this exercise, we will configure Directory Synchronization, synchronize our Active Directory to Azure Active Directory and validate that synchronization is working properly.

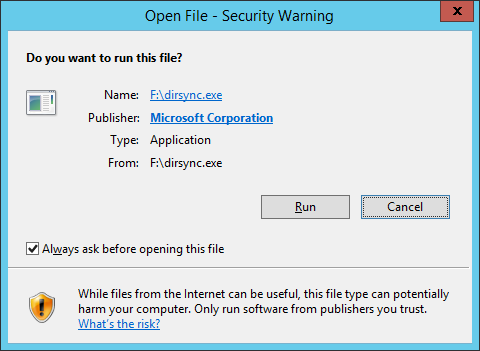
Before starting this exercise, make sure that the script from Exercise 1 has finished successfully. If not, consult your instructor.

Estimated time to complete this exercise: **25 minutes**.

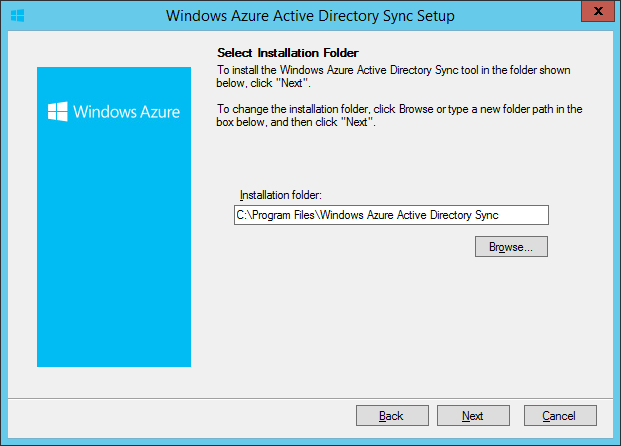
### Task 1 – Installing Windows Azure Active Directory Sync

In this task, you will configure Directory Synchronization from your Active Directory to the Azure Active Directory.

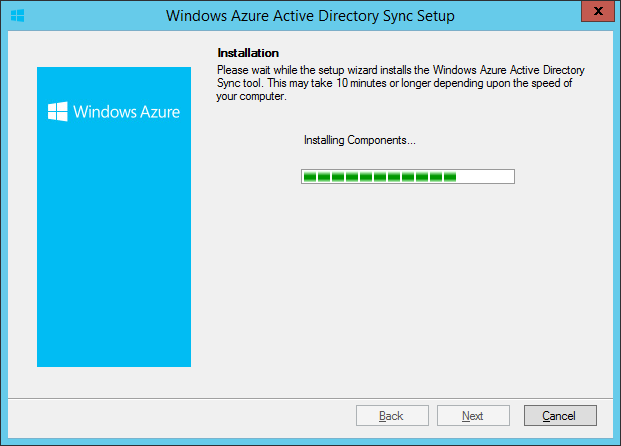
1. Remote Desktop connection into the newly created Domain Controller using the credentials specified in the script (**$adm**, **$pwd**). After the remote session has been established, double-click the **dirsync.exe** file located in the root of the **F:** drive of the machine (**F:\dirsync.exe**). If you get a security warning, as shown in the following image, please click **Run** to continue,



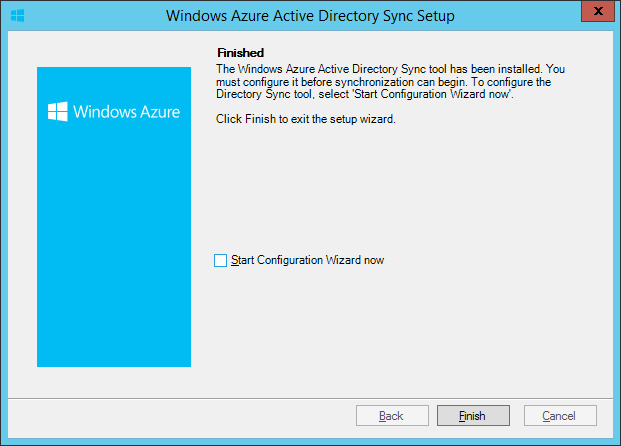
1. After all the files have been extracted, the Windows Azure Active Directory Sync Setup wizard starts. Click **Next** to continue. Select **I accept** and click **Next** to continue.



1. Accept the default location and click **Next** to continue.

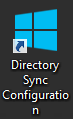


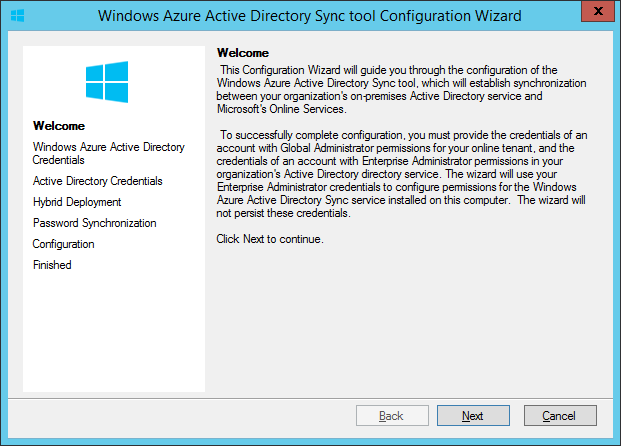
1. Wait for the installation to complete. Once completed, click **Next** to continue.
2. Since we installed the Windows Azure Active Directory Sync tool on a Domain Controller, we need to log off from the server before we can start to configure the tool.  
   **Clear** the checkbox for **Start Configuration Wizard now** and click **Finish** to close the setup wizard.



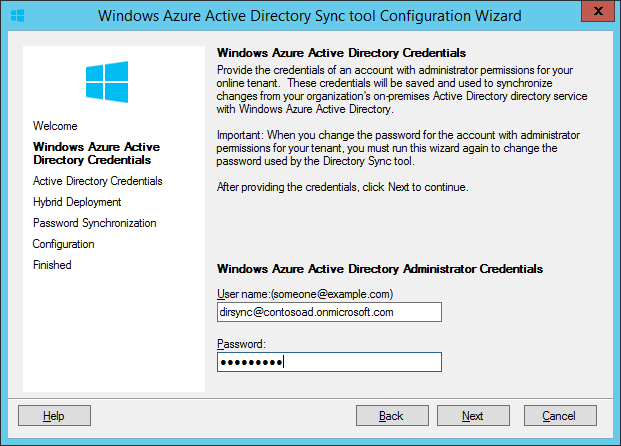
1. Log off from the domain controller.

### Task 2 – Configuring Windows Azure Active Directory Sync

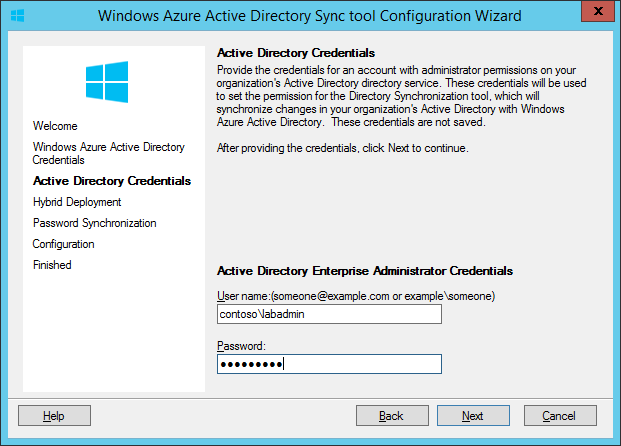
1. Remote Desktop back into the domain controller. The installation of the Microsoft Azure Active Directory Sync tool has created an icon on the desktop to configure Directory Synchronization.  
   Locate the icon and double-click it to start the Microsoft Azure Active Directory Synchronization tool Configuration Wizard.
2. On the Welcome page of the Microsoft Azure Active Directory Sync tool Configuration Wizard, click **Next** to continue.



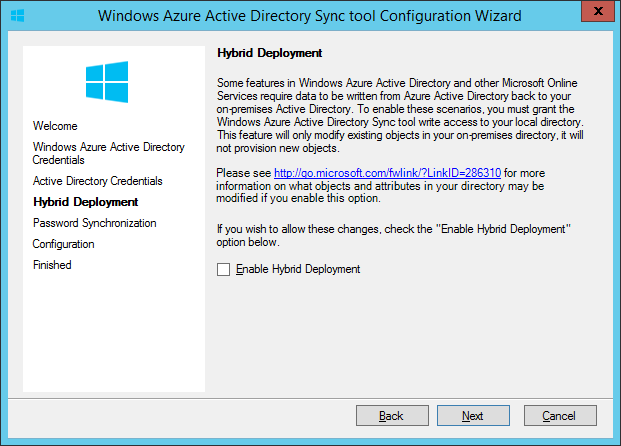
1. On the Microsoft Azure Active Directory Credentials page of the Microsoft Azure Active Directory Sync tool Configuration Wizard, enter the username for the Global Administrator user that we have created in Exercise 1. (e.g. [aadsync@contoso.onmicrosoft.com](mailto:aadsync@contoso.onmicrosoft.com)) Click **Next** to continue.



1. On the Active Directory Credentials page of the Microsoft Azure Directory Sync tool Configuration Wizard, enter the credentials of the domain administrator. (e.g. contoso\labadmin) Click **Next** to continue.



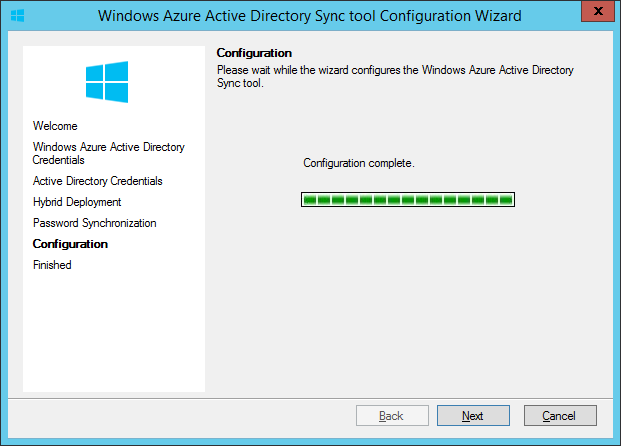
1. On the Hybrid Deployment page of the Microsoft Azure Active Directory Sync tool Configuration Wizard, make sure that Enable Hybrid Deployment is not checked and click **Next** to continue.



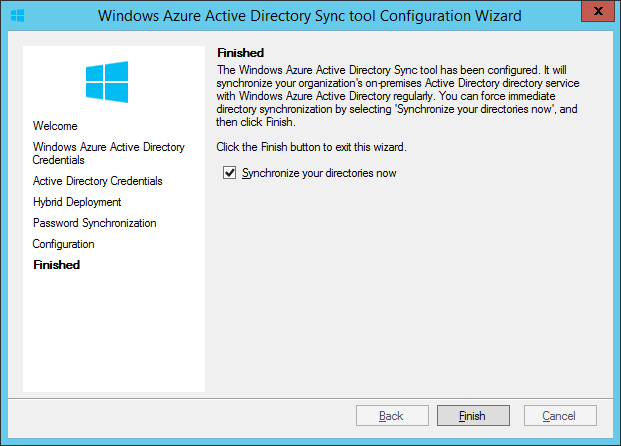
1. On the Password Synchronization page of the Microsoft Azure Active Directory Sync tool Configuration Wizard, **check** the checkbox for Enable Password Sync and click **Next** to start the Directory Synchronization Configuration.

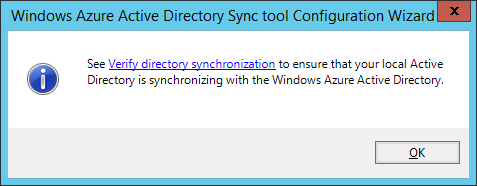


1. On the Configuration page of the Microsoft Azure Active Directory Sync tool Configuration Wizard, wait for the configuration to complete. After configuration has completed, click **Next** to continue.



1. On the Finished page of the Microsoft Azure Active Directory Sync tool Configuration Wizard, make sure the Synchronize your directories now is checked and click **Finish** to continue.



1. Dismiss the final notification from the Microsoft Azure Active Directory Sync tool Configuration Wizard by clicking **OK**. The wizard will now close, and the initial, full synchronization of the Windows Active Directory to Microsoft Azure Active Directory will commence. It will take a considerable amount of time for the replication to complete.   
   

In the lab, it will take approximately 45 minutes to replicate the Active Directory to Azure Active Directory. The password synchronization following the initial Directory Synchronization will take an additional 30 minutes.

### Task 3 – Validating Windows Azure Active Directory Sync

In this task, we will confirm that Directory Synchronization has been setup correctly and that objects from Active Directory are properly replicating to Azure Active Directory.

1. From the domain controller, open the Event Viewer on the machine.
2. Check to see if you have an event with **ID 611** (Level: Information, Source: Directory Synchronization) in the Application log. This events signals the start of a full directory synchronization.

Note: If you see events with ID 6313 (Level: Error, Source: FIMSynchronizationService) in the Application log, you can safely ignore these. If you want to fix the problem, please open a command prompt and run:

lodctr.exe "C:\Program Files\Windows Azure Active Directory Sync\SYNCBUS\Synchronization Service\Bin\mmsperf.ini"

1. During synchronization, you might see numerous events with **ID 104** (Level: Information, Source: Directory Synchronization) in the Application log. This indicates that objects are being exported to Azure Active Directory. Each event represents a single batch of 30 objects being replicated to Azure Active Directory.  
     
   Wait until you see an event with **ID 114** (Level: Information, Source: Directory Synchronization) in the Application log. This event signals the end of the export to Microsoft Azure Active Directory. The event is followed by an event with ID 0 (Level: Information, Source: Directory Synchronization) in the Application log. It should read:

MA: Windows Azure Active Directory Connector Profile: Export Result: success

1. After the initial Directory Synchronization has completed, check the Application log for an event with **ID 601** (Level: Information, Source: Directory Synchronization). This event indicates that Password Synchronization has started and the event text should read:

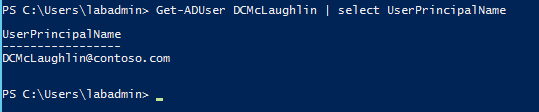
Password Synchronization Manager has started.

This event is followed by numerous 650, 656, 651 and 657 events that indicate that passwords have been synchronized to Azure Active Directory. Each set of events represents a single batch of 50 accounts.

The last events for Password Synchronization are the events with ID 653 and 654. Wait for the password synchronization to complete.

1. Check the Event Log for any errors you might see. If you see unexpected error messages, please consult <http://support.microsoft.com/kb/2684395> or your trainer for further troubleshooting.
2. On the **domain controller** machine, start Windows PowerShell and view the User Principal Name of user DCMcLaughlin by using this command:

Get-ADUser DCMcLaughlin | select UserPrincipalName



1. On the hosted lab machine (or on your own machine), start **Windows Azure Active Directory Module for Windows PowerShell**.
2. Connect to Azure Active Directory using the Global Administrator account you created in Exercise 1, Task 2. Use the following command to connect to Azure Active Directory:

Connect-MsolService

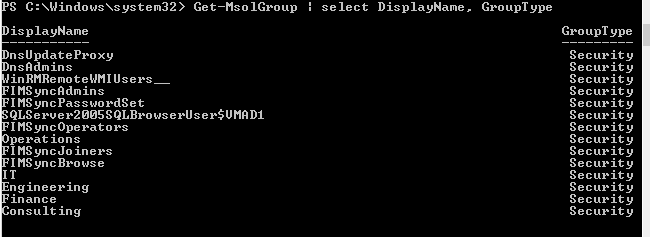
1. In order to see if our user accounts were properly synchronized to Microsoft Azure Active Directory, we can get a few user accounts from Microsoft Azure Active Directory using this PowerShell command:

Get-MsolUser -MaxResults 10



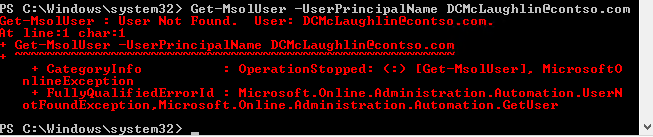
1. In order to see if our groups were properly synchronized to Microsoft Azure Active Directory, we can get a few user accounts from Microsoft Azure Active Directory using this PowerShell command:

Get-MsolGroup | select DisplayName, GroupType



1. Try to find the same user **DCMcLaughlin** in Azure Active Directory by issuing this command:

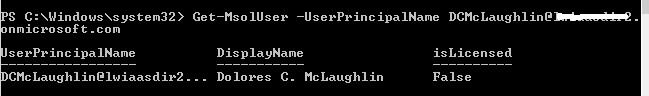
Get-MsolUser -UserPrincipalName DCMcLaughlin@contoso.com



Question: Why can the user not be found?

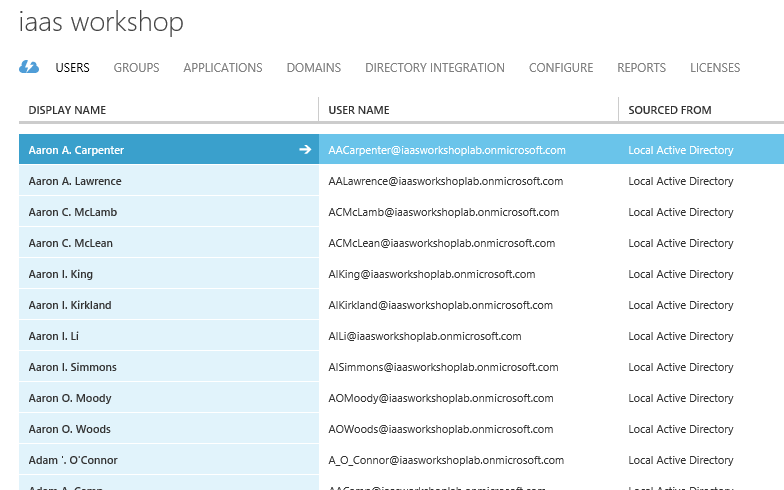
1. Try to find the same user **DCMcLaughlin** in Azure Active Directory by issuing this command: NOTE: Change the ‘contoso’ domain name to the name of the AD directory you created.

Get-MsolUser -UserPrincipalName **DCMcLaughlin**@contoso.onmicrosoft.com

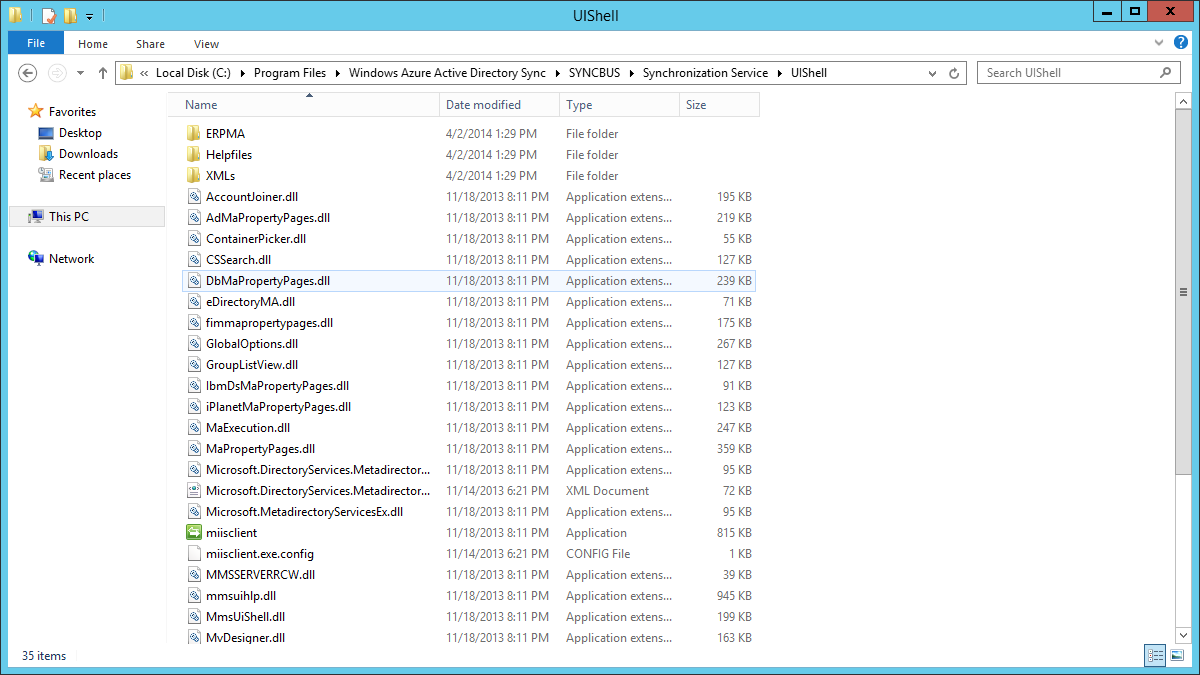


Question: Why is the User Principal Name of the user in Active Directory different from the one in Azure Active Directory? How can we prevent this from happening?

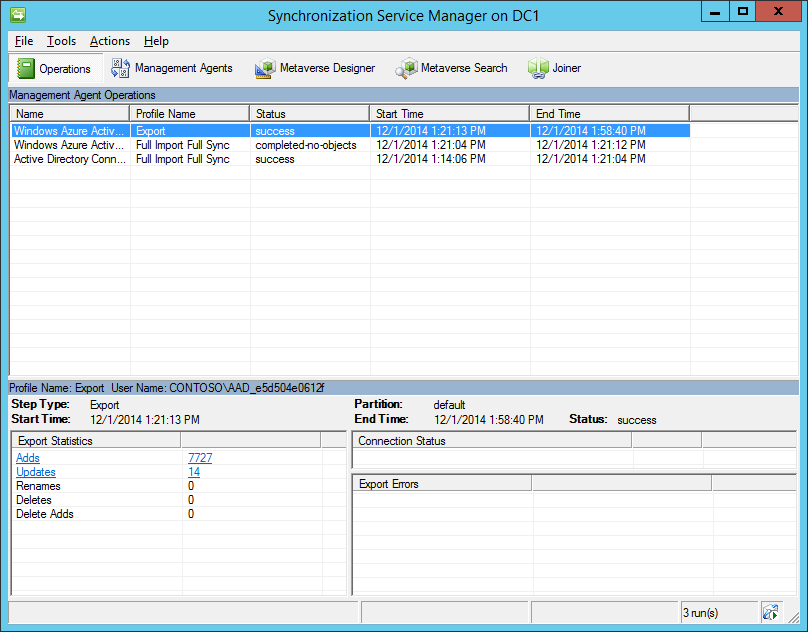
1. Start Internet Explorer and navigate to <https://account.activedirectory.windowsazure.com> Sign in with **DCMcLaughlin@contoso.onmicrosoft.com** and password **Pa$$w0rd!** Validate that you successfully logon with the credentials provided, indicating that Directory Synchronization and Password Synchronization have completed successfully. Sign out of the page by clicking on the username at the right top of the page and clicking **Sign out**.
2. Log on to the [Microsoft Azure Management Portal](http://manage.windowsazure.com/). Navigate to the **Microsoft Azure Active Directory** that you created and click the **Users**tab. Validate that you see the Active Directory users here. Check the ***Sourced From***column and see that these users are sourced from your Active Directory. Your directory user names and domain will appear slightly different.

  
Also check the *Groups* tab to see if all the groups have been properly synchronized.

1. On the domain controller, browse to the **C:\Program Files\Windows Azure Active Directory Sync\SYNCBUS\Synchronization Service\UIShell** folder, and start the **miisclient.exe** application by double-clicking it.



1. In the Synchronization Service Manager, validate that you do not see any errors in the **Status** column in the **Management Agent Operations** window.  
   In the screenshot provided, the Microsoft Azure Active Directory Synchronization tool is in the process of exporting changes in the Active Directory to Microsoft Azure Active Directory.



*The Directory Synchronization Tool User Interface*

1. Close the tool when you are finished.

## Exercise 4: Removing an Azure Active Directory Tenant

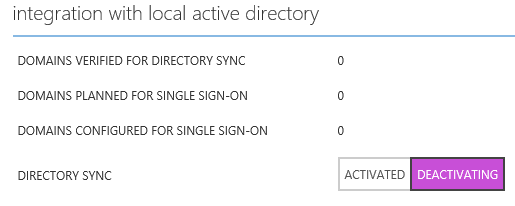
In this exercise, we will remove the previously created Azure Active Directory Tenant

Estimated time to complete this exercise: 10 minutes.

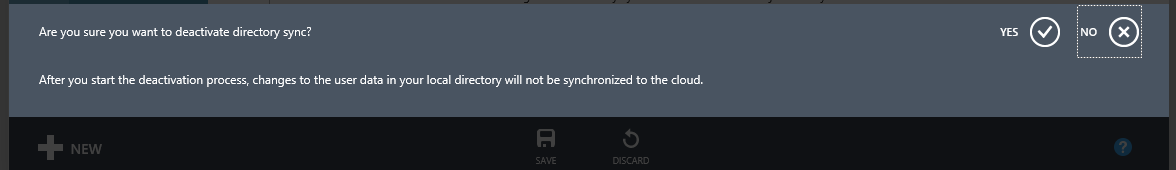
### Task 1 – Disabling Directory Synchronization

In this task, you will disable Directory Synchronization from your Active Directory to the Azure Active Directory.

1. Sign in to the Azure Management Portal.
2. Select **Active Directory** from the left pane.
3. Select the Azure Active Directory you created in Exercise 2 and select the **Directory Integration** tab.
4. Click **DEACTIVING** next to Directory Sync.



1. At the bottom of the page, click **Save** and click **Yes** to confirm the action.



We will not wait for this process to complete, since this process can take up to 72 hours.

### Task 2 – Cleaning up and Removing your Azure Active Directory Tenant

In this task, you will remove all users and groups from the Azure Active Directory in order to be able to remove the directory. After all objects have been removed, you will remove the directory itself.

1. On the hosted lab machine, Windows Azure Active Directory Module for Windows PowerShell,
2. Connect to Azure Active Directory using the Global Administrator account you created in Exercise 1, Task 2. Use the following command to connect to Azure Active Directory:

Connect-MsolService

1. In order to remove all synchronized Groups from Azure Active Directory, issue this command:

Get-MsolGroup | Remove-MsolGroup -Force

PS C:\> Get-MsolGroup | Remove-MsolGroup -Force

PS C:\>

1. In order to remove all synchronized Groups from Azure Active Directory, issue this command:

Get-MsolUser –All | where {$\_.UserPrincipalName –notlike “\*#EXT#\*”} | Remove-MsolUser -Force

It is expected that you get one error message; you cannot remove your own account. You can prevent this error if you add another *where* clause to the PowerShell command. This command will run for approximately 2 hours, so please continue without waiting for full completion. After the command has ran, and all users except your own user have been deleted from the Azure Active Directory, so continue to the next step.

PS C:\> Get-MsolUser –All | where {$\_.UserPrincipalName –notlike “\*#EXT#\*”} | Remove-MsolUser -Force

Remove-MsolUser : You cannot remove yourself as a user. Use another administrator account or have another administrator remove your user account.

At line:1 char:21

+ Get-MsolUser -All | Remove-MsolUser -Force

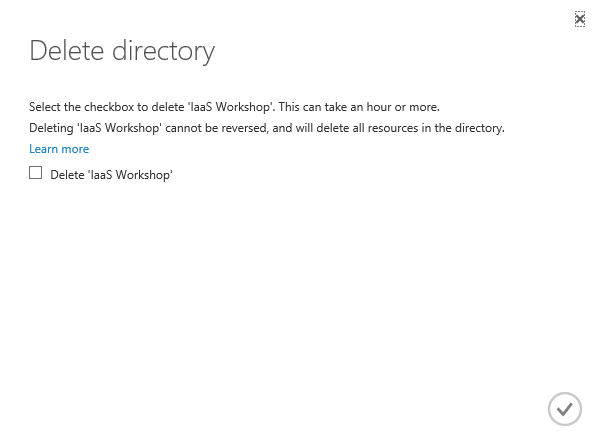
+ ~~~~~~~~~~~~~~~~~~~~~~

+ CategoryInfo : OperationStopped: (:) [Remove-MsolUser], MicrosoftOnlineException

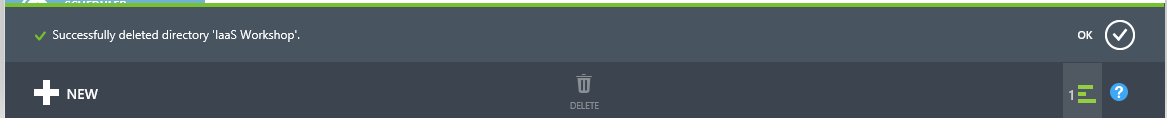
+ FullyQualifiedErrorId : Microsoft.Online.Administration.Automation.UserRemoveSelfException,Microsoft.Online.Administration.Automation.RemoveUser

PS C:\>

1. After all the users, except your administrative account and the Global Administrator account created for directory synchronization have been deleted, log on to the Azure Management Portal and delete the account created for directory synchronization. Go to Active Directory, select the Azure Active Directory you created, select the synchronization user and click **DELETE** at the bottom of the screen. Confirm that you want to delete the user by clicking **YES** at the right hand side of the bottom banner.
2. In the Azure Management Portal, navigate back one level, to Active Directory, highlight the Azure Active Directory you created and click **DELETE** at the bottom of the screen. Confirm that you want to delete this Azure Active Directory by selecting the box in front of *“Delete ‘MyAzureActiveDirectory’”* and clicking the **Okay** button at the bottom of the dialog.



Wait for the operation to complete and dismiss the message at the bottom of the screen by clicking **OK**.



## Exercise 5: Removing the Domain Controller

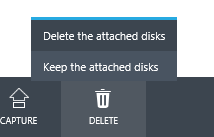
In this exercise, we will remove the previously created Domain Controller.

Estimated time to complete this exercise: 5 minutes.

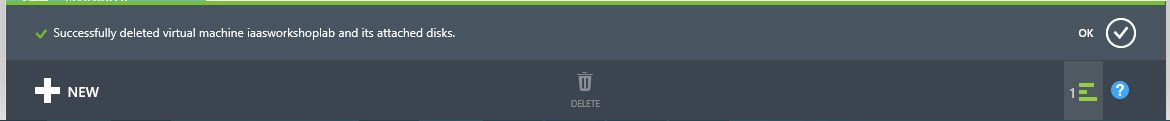
### Task 1 – Removing the Domain Controller

In this task, you remove the domain controller previously created.

1. Sign in to the Azure Management Portal.
2. Select **Virtual Machines** from the left pane.
3. Select the Domain Controller you created in Exercise 1 and click **DELETE** at the bottom of the screen. On the popup menu, click **Delete the attached disks**.

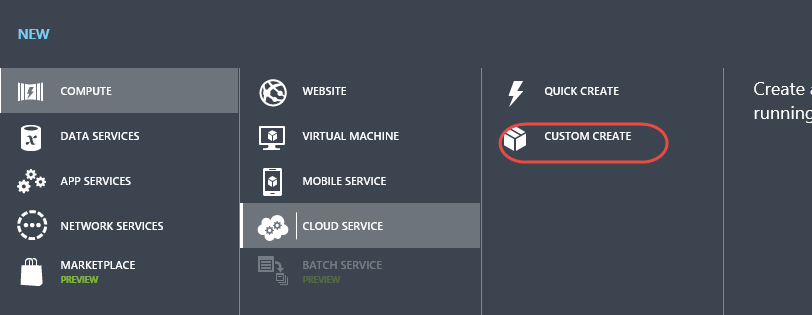


1. Confirm that you want to delete the Virtual Machine, as well as the disks, by clicking **YES** in the bottom banner. Wait for the operation to finish, and dismiss the message at the bottom of the screen by clicking **OK**.



# Appendix A: Create an Azure Cloud Service

1. Log in to your Azure Subscription.
2. Select **New->Compute->Cloud Service->Custom Create**.



1. Give your Cloud Service a unique name and then select the data center/region to place the Cloud Service in. The select the check button.

