

IaaS Workshop

(Customer Lab Manual - No Prerequisites Required)

Version 2.8

Contents

[Introduction 4](#_Toc480985574)

[Purpose 4](#_Toc480985575)

[Workshop setup 4](#_Toc480985576)

[1. Creating and Managing a Resource Group 5](#_Toc480985577)

[2. Azure networking 7](#_Toc480985578)

[2.1 Creating a virtual network in Azure 7](#_Toc480985579)

[2.2 Virtual Network Peering 9](#_Toc480985580)

[3. Managing virtual machines in Azure 10](#_Toc480985581)

[3.1 Deploying virtual machines to your Azure networks 10](#_Toc480985582)

[3.2 Deploy a VM from a Quickstart template 12](#_Toc480985583)

[3.3 Connecting to a virtual machine 13](#_Toc480985584)

[3.4 Navigating virtual machine properties 16](#_Toc480985585)

[3.5 Network Security Groups 19](#_Toc480985586)

[4. Securing and Monitoring Azure Resources 20](#_Toc480985587)

[4.1 Setup and Configure Log Analytics 20](#_Toc480985588)

[4.2 Create a custom dashboard in Log analytics 23](#_Toc480985589)

[4.3 Setup and Configure Azure Security Center 24](#_Toc480985590)

[5. Configuring Azure Traffic Manager 25](#_Toc480985591)

[6. Azure Recovery Services 27](#_Toc480985592)

[6.1 Create a backup vault and backup VM 27](#_Toc480985593)

[7. Deploy a Docker container hosting solution using the Azure portal 29](#_Toc480985594)

[7.1 Prerequisites 30](#_Toc480985595)

[7.2 Create a cluster by using the Azure portal 30](#_Toc480985596)

Terms of Use & Disclaimer

© 2015 Microsoft Corporation. All rights reserved.

By using this Lab and instructions, you agree to the following terms:  The technology/functionality provided as a 'sandbox' environment and described herein is provided by Microsoft Corporation for demonstration and testing purposes of obtaining your feedback and to provide you with a learning experience. You may only use the 'sandbox' environment to evaluate such technology features and functionality and provide feedback to Microsoft.  You may not use it for any other purpose. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, or sell this 'sandbox' environment or any portion thereof.

COPYING OR REPRODUCTION OF THE MATERIALS (OR ANY PORTION OF IT) TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED UNLESS OTHERWISE AUTHORIZED.

THIS LAB PROVIDES CERTAIN SOFTWARE TECHNOLOGY/PRODUCT FEATURES AND FUNCTIONALITY, INCLUDING POTENTIAL NEW FEATURES AND CONCEPTS, IN A SIMULATED ENVIRONMENT WITHOUT COMPLEX SET-UP OR INSTALLATION FOR THE PURPOSE DESCRIBED ABOVE.  THE TECHNOLOGY/CONCEPTS REPRESENTED IN THIS LAB MAY NOT REPRESENT FULL FEATURE FUNCTIONALITY AND MAY NOT WORK THE WAY A FINAL VERSION MAY WORK.  WE ALSO MAY NOT RELEASE A FINAL VERSION OF SUCH FEATURES OR CONCEPTS. YOUR EXPERIENCE WITH USING SUCH FEATURES AND FUNCITONALITY IN A PHYSICAL ENVIRONMENT MAY ALSO BE DIFFERENT.

FEEDBACK.  If you give feedback about the technology features, functionality and/or concepts described in this Hands-on Lab to Microsoft, you give to Microsoft, without charge, the right to use, share and commercialize your feedback in any way and for any purpose.  You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the feedback.  You will not give feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your feedback in them.  These rights survive this agreement.

MICROSOFT CORPORATION HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THE LAB, INCLUDING ALL WARRANTIES AND CONDITIONS OF MERCHANTABILITY, WHETHER EXPRESS, IMPLIED OR STATUTORY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.  MICROSOFT DOES NOT MAKE ANY ASSURANCES OR REPRESENTATIONS WITH REGARD TO THE ACCURACY OF THE RESULTS, OUTPUT THAT DERIVES FROM USE OF THE LAB, OR SUITABILITY OF THE INFORMATION CONTAINED IN THE  LAB FOR ANY PURPOSE.

# Introduction

IT services have shifted dramatically over the last few years, with many organizations implementing a virtual first initiative that helps reduce the cost of hardware, HVAC, and many other cost factors to IT organizations. With the increased capability of cloud services, many IT organizations want to move more resources to the cloud. Microsoft is one of the only vendors that can provide an end-to-end solution with both public cloud services and private cloud servers.

## Purpose

The purpose of this workshop is to introduce organizations to Microsoft Azure services. This workshop is designed to expose organization to the subset of Azure services that focuses on infrastructure as a service (IAAS).

## Workshop setup

The IaaS workshop will completely utilize Microsoft Azure services, and requires only an Internet-accessible device to connect to Azure and a validate Azure subscription.

Valid options are:

1. Azure Pass
2. Precreated Azure subscription and accounts to access the subscription
3. Bring your own Azure subscription (requires owner/Admin rights)

# Creating and Managing a Resource Group

Resource Groups are ways to logically group various Azure resource. They can provide a billing boundary, delegation boundary, and can be used in various ways.

**Purpose of lab:**

In this lab you will create a Resource Group that will be utilized throughout this workshop.

**Estimated time: 10 minutes**

1. Launch Internet Explorer.
2. In the URL box, type <https://portal.azure.com/> .
3. Logon with your supplied credentials.
4. In the Azure Portal select **More Servies** from the menu on the left

*Scroll around and see the various options you can select*

1. In the context menu select **Resource Group.**
2. At the top of the **Resource Group blade** select **Add.**
3. In the **Create an empty resource group blade type** **ResStudentX** (where X is your assigned student number) in the **Resource group name** field.
4. In the **Create an empty resource group blade select** the drop down menu for **Resource Group location** and select **East US 2.**
5. At the bottom of the **Create an empty resource group blade** select **Pin to dashboard** andthen select **Create.**
6. After creation the **Resource Group properties blade** should be open on the screen.
7. In the **Resource Group Settings blade** select **Access Control (IAM).**
8. In the **Access Control (IAM) blade** select **Roles** at the top of the blade.

*Review the roles available for delegation*

1. Close the **Roles blade** by selecting the X in the top right hand corner.
2. In the **Resource Group Settings blade** select **Tags.**
3. In the **Resource Group Tags blade** type **ResstudentX** (where X is your assigned student number)in left input box (key).

In the **Resource Group Tags blade** type **SXProject1** (where X is your student number)in right input box.

1. In the **Resource Group Tags blade** select **Save**

*Tags can be created for various reasons to classify assets within a Resource Group*

1. In the **Resource Group Settings blade** select **Locks**

\*Note: you cannot add a lock because of your permissions locks allow your to prevent accidental deletion of the Resource Group or its assets\*

1. Close the **Settings blade** by selecting the X in the top right hand corner

*You should see an icon on the Azure page with the name of your Resource Group, the Azure portal provides the ability to pin resources to create a custom view*

# Azure networking

With Azure, any user or organization can create a self-contained network and connect into those networks with these methods:

* Point-to-site
* Site-to-site
* Azure ExpressRoute

## Creating a virtual network in Azure

**Purpose of lab:**

In this lab you will create a virtual network that will be used to host virtual machines

**Estimated time: 10 minutes**

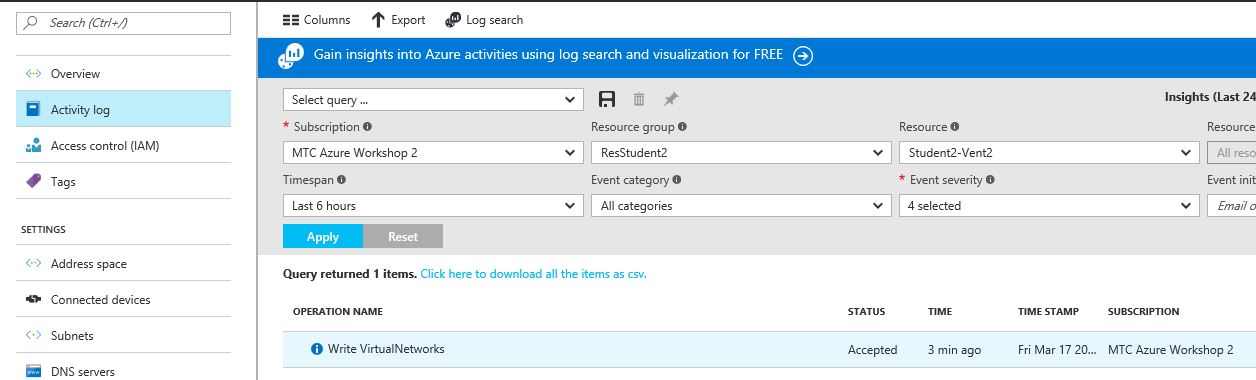
1. In the Azure portal, click **New > Networking > Virtual Network**
2. In the **Virtual network blade** validate the drop down menu under **Select a deployment model** is set to **Resource Manager**

*Resource Manager is a new set of API that is the foundation for the new Azure Portal*

1. In the **Virtual network blade** select **Create**
2. In the **Create** v**irtual network blade** type **Student***X***-Vnet1** (where *X* is your student number).
3. In the **Create** v**irtual network blade** type 10.X.0.0/16 is listed in the **Address Space** field (where *X* is your student number).
4. In the **Create** v**irtual network blade** type **Student***X***-sub1** (where *X* is your student number) in the **Subnet name** field.
5. In the **Create** v**irtual network blade** type **10.X.X.0/24** (where *X* is your student number) in the **Subnet address range** field.
6. Select the radius button **use existing** below the **Resource Group** field.
7. Select the **drop down** menu and **select** ResStudentX (where X is your student number).
8. In the **Create** v**irtual network blade** remove the check box  **Pin to dashboard** > **Create.**
9. In the Azure Dashboard select your **Resource Group** ResStudentX (where X is your assigned. student number)
10. In the **Resource Group blade** select **Add** from the top menu
11. In the Everything menu select **Virtual Network**
12. In the **Virtual network blade** select **Create**
13. In the **Create** v**irtual network blade** type **Student***X***-Vnet2** (where *X* is your student number).
14. In the **Address space** field input **172.X.0.0/16**
15. In the **Subnet Name** fieldinput **Student***X***-sub2** (where *X* is your student number).
16. In the **Subnet address range** input **172.X.X.0/24** 🡪 **Create**
17. Close any open blades
18. In the Azure Dashboard select your **Resource Group** ResStudentX (where X is your assigned. student number)
19. In the **Resource Group** from the Overview menu **select** StudentX-Vnet2 (where X is your assigned number).
20. In the **virtual network** bladeselect **DNS server**
21. In the **DNS Server blade** select **Custom DNS 🡪 Custom** radius button

\*Note if you place Domain controllers in Azure or want to use an alternate DNS server this is where the change is. Azure only uses DHCP to assign IPs you do not change the IP settings directly on a VM

1. In the **DNS Server blade** select **Discard**
2. In the **virtual network blade** select **Activity Logs**
3. In the **Activity Log** select **Write VirtualNetwork**



\*Note the Azure Activity Logs audit the service actions like creating networks, VMs, etc.

1. Select the JSON tab in the lower portion of the browser

\*Note this show the Json code that is used to perform that task

1. Close all blades

## Virtual Network Peering

Virtual network peering allows for a low latent connection between two or more virtual networks in the same Azure Region. If you wish to connect virtual network between regions you must use Exprees route or a site to site vpn.

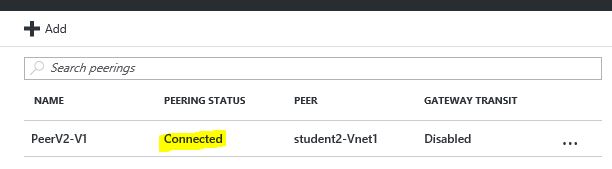
Purpose of lab

In this lab, is to connect the 2 newly created networks via peering.

Estimated time: 15 minutes

1. In the Azure Dashboard select your **Resource Group** ResStudentX (where X is your assigned. student number)
2. In the **Resource Group** blade select **Studentx-Vnet1**
3. In the **Virtual network** blade select **Peerings**
4. In the **Virtual network Peerings** blade select **Add**
5. In the **Add peering** blade input “PeerV1-V2” in the Name field
6. In the **Add peering** blade select Virtual network
7. In the **Choose virtual network** blade select **StudentX-Vnet2** (where X is your assigned student number).
8. In the **Add peering** blade check the box “Allow forwarded traffic” 🡪 Ok
9. In the **Virtual network Peerings** blade close the peering properties by select X in the top corner
10. In the **Resource Group** blade select **Studentx-Vnet2**
11. In the **Virtual network** blade select **Peerings**
12. In the **Virtual network Peerings** blade select **Add**
13. In the **Add peering** blade input “PeerV2-V1” in the Name field
14. In the **Add peering** blade select Virtual network
15. In the Choose virtual network blade Select **StudentX-Vnet1** (where X is your assigned student number).
16. In the **Add peering** blade check the box “Allow forwarded traffic” 🡪 Ok

\*Note: It might take a second but the screen should update the peering status to connected



1. Close all open blade

# Managing virtual machines in Azure

One of the services offered by Azure is Infrastructure as a Service (IaaS) this provides the ability to create and manages virtual machines. Microsoft fully supports a wide range of virtual appliances and operating systems.

## Deploying virtual machines to your Azure networks

Purpose of lab

In this lab, you will deploy two virtual machines into a Resource Group and deploy them to an Azure network.

Estimated time: 15 minutes

1. In the Azure Dashboard select your **Resource Group** ResStudentX (where X is your assigned student number).
2. In the **Resource Group blade** select **Add** at the top of the blade.
3. Select the **Windows 2012 R2 datacenter** icon.
4. In the **Windows 2012 R2 datacenter** blade validate the drop down menu under **Select a deployment model** is set to **Resource Manager --> Create**
5. In the **Basics blade** in the **Name** Fieldtype **ResWebXA** (where *X* is your student number) in the **Name** field.
6. In the **Basics blade** in the Vm disk type select **HDD** from the drop down menu
7. In the **Basics blade** in the **User Name** Fieldtype **Student***X* (where *X* is your student number).
8. In the **Basics blade** in the **Password field** type **P@ssword2017** .
9. In the **Basics blade** validate the **Resource Group** field is set to ResStudentX (where X is your assigned student number).
10. In the **Basics blade** validate the Location field is set to **East US 2.**
11. In the **Basics blade** click **OK.**
12. In the **Choose a size blade** select **View all** to view various virtual machines sizes available.
13. In the **Choose a size blade** select **D2\_V2 Standard** icon.
14. In the **Choose a size blade** click the **Select** icon at the bottom of the blade.
15. In the **Settings blade** under Storage select “yes” to use managed disk
16. In the **Settings blade** select Virtual network 🡪 StudentX-Vnet1 (where X is your assigned student number).
17. In the **Settings blade** click **OK**
18. In the **Summary blade** review your selections click **OK**
19. From the **Azure Dashboard** select **New**
20. In the **New blade** select **Compute**
21. In the **Compute blade** select **Windows 2012 R2 datacenter**
22. In the **Windows 2012 R2 datacenter blade** validate the drop down menu under Select a deployment model is set to **Resource Manager** --> **Create**
23. In the **Basics blade** in the **Name** field type **ResWebXB** (where X is your student number) .
24. In the **Basics blade** in the Vm disk type select **HDD** from the drop down menu
25. In the **Basics blade** in the **User Name** fieldtype **Student***X* (where *X* is your student number) in the **User name** field.
26. In the **Basics blade** in the **Password** fieldtype **P@ssword2017** .
27. Select the Radius button **Use existing** below the **Resource Group** field.
28. Select the **drop down** menu and **selec**t **ResStudentX** (Where X is your student number).
29. In the **Basics blade** select **Ok**
30. In the **Choose a size blade** select **view all** and select **D2\_V2 Standard** icon.
31. In the **Choose a size blade** click **Select** icon at the bottom of the screen.
32. In the **Settings blade** under Storage select “**yes**” to use managed disk
33. In the **Settings blade** select Virtual network 🡪 **StudentX-Vnet2**
34. In the **Settings blade** select **OK**
35. In the **Summary blade** review your selections click **OK**

## Deploy a VM from a Quickstart template

After a virtual machine has been created on the Azure platform, an admin will need ways to manage and work with that virtual machine.

Purpose of lab

In this lab, you connect to your virtual machine via RDP and manage the virtual machine.

NOTE: You must complete the previous lab before you perform this lab.

Estimated time: 15 minutes

1. On your desktop open a new browers tab and input the url below

\* <https://azure.microsoft.com/en-us/resources/templates/anti-malware-extension-windows-vm/>

1. From your browser select the **Deploy to Azure** button
2. In the **Template blade** in the Resource group section select radius button “**Use existing**”
3. In drop down menu of the Resource group section select your resource group **ResStudentX** (where X is your student number).
4. In the **Template blade** in the “New Storage Account Name” field input **studentXres** (where X is your student number).
5. In the **Template blade** in the Public Ip Addres name input “**ResTempwkX**”) (where X is your student number).
6. In the **Template blade** in “VM Size” field input **Standard\_DS2\_v2**
7. In the **Template blade** in the “Vm name” field inpout “**ResTempX**” (where X is your student number).
8. In the **Template blade** in the “Admin Username” input “**StudentX**” (where X is your student number).
9. In the **Template blade** in the “Admin Password” field input **P@ssword2017**
10. In the **Template blade** in the “Virtual network Name” field input **RestudentX-Vnet3** (where X is your student number).
11. In the **Template blade** in “Address Prefix” field change the address to **192.X.0.0/16** (where X is your student number).
12. In the **Template blade** in “Subnet1 Prefix” field input **192.X.X.0/24** (where X is your student number).
13. In the **Template blade** in “Nic Name” field in **resstudentX-nic1** (where X is your student number).
14. In the **Template blade** in “Vm extention” field input **anti-mailware**
15. In the **Template blade** under terms and conditions **check** the box “I agree to the terms and conditions stated above” 🡪 Purchase

\*Note we pulled a template from the gallery and with a single click deployment a virtual machine and the virtual network

## Connecting to a virtual machine

After a virtual machine has been created on the Azure platform, an admin will need ways to manage and work with that virtual machine.

Purpose of lab

In this lab, you connect to your virtual machine via RDP and manage the virtual machine.

NOTE: You must complete the previous lab before you perform this lab.

Estimated time: 15 minutes

1. In the Azure Dashboard select your **Resource Group** ResStudentX (where X is your assigned student number).
2. In the **Resoure** **group** blade select the Vm object **ResWebXA** (where X is your student number).
3. In the top of the **ResWebXA** (where X is your student number) **blade** select **Connect.**
4. In the Internet Explorer open/save dialog select **Open.**
5. In the **Remote desktop connection** dialog box, selectthe **Don’t ask me again** check box, and then click **Connect**.
6. In the **Windows Security** dialog box, select the **Use other account** check box.
7. In the logon screen,type **Student***X* and the password **P@ssword2017**.
8. In the **Remote desktop connection** dialog box, selectthe **Don’t ask me again** check box, and then click **Yes**.

*You will be logged onto the virtual machine hosted in Azure.*

1. In the RDP session on the **Task** menu, click the PowerShell icon (second icon from the left).
2. In the **Powershell** windows type:

**Install-WindowsFeature -Name Web-Server -IncludeManagementTools**

*Note: wait until the install has completed before moving to the next step*

1. In the **Powershell** windows type: Ipconfig

\*write down the Ip address of the virtual machine (it should be 10.x.x.4)

1. Launch Server Manager, and then click **local server**.

In the server properties, click **IE enhanced security**.

1. On the **IE enhanced security** page, turn this feature off for both admins and users, and then click **OK**.
2. From the virtual machine, open Internet Explorer and connect to <http://aka.ms/mtcworkshop>.
3. download **Server1.html** to the C:\ Inetpub\wwwroot directory.
4. From the **Server Manager** dashboard, click **Tools** > **IIS Manager**.
5. Expand **ResWebXA**, andthenclick **No** in the window that appears.
6. Expand **Sites**, and then click **Default web site**.
7. In the middle pane, double-click **Default document**.
8. On the right menu, click **Add**.
9. In the **Name** box, type **Server1.html** (the file you downloaded in in step 13), and then click **OK**.
10. Close IIS Manager.
11. Open Internet Explorer and type [http://localhost](http://localhost/)

*You should be presented with a customer webpage from Server1*

1. Minimize the RDP session to **ResWebXA** (where X is your student number).
2. In the **Azure Dashboard** select the tile **ResWebXB** (where X is your student number).
3. In the top of the **ResWebXB** (where X is your student number) **blade** select **Connect.**
4. In the Internet Explorer open/save dialog select **Open.**
5. In the **Remote desktop connection** dialog box, selectthe **Don’t ask me again** check box, and then click **Connect**.
6. In the **Windows Security** dialog box, select the **Use other account** check box.
7. In the logon screen,type **Student***X* and the password **P@ssword2017**.
8. In the **Remote desktop connection** dialog box, selectthe **Don’t ask me again** check box, and then click **Yes**.

*You will be logged onto the virtual machine hosted in Azure.*

1. On the **Task** menu, click the PowerShell icon (second icon from the left).
2. In the **Powershell** windows type:

**Install-WindowsFeature -Name Web-Server -IncludeManagementTools**

*Note: wait until the inexit*

*stall has completed before moving to the next step*

1. Launch Server Manager, and then click **local server**.
2. In the server properties, click **IE enhanced security**.
3. On the **IE enhanced security** page, turn this feature off for both admins and users, and then click **OK**.
4. From the virtual machine, open Internet Explorer and connect to <https://aka.ms/mtcworkshop>
5. Download **Server2.html** to C:\ Inetpub\wwwroot directory.
6. From the **Server Manager** dashboard, click **Tools** > **IIS Manager**.
7. Expand **ResWebXB**, andthenclick **No** in the window that appears.
8. Expand **Sites**, and then click **Default web site**.
9. In the middle pane, double-click **Default document**.
10. On the right menu, click **Add**.
11. In the **Name** box, type **Server2.html** (the file you downloaded in step 36), and then click **OK**.
12. Close IIS Manager.
13. Open **Internet Explorer** and type [http://localhost](http://localhost/)

*You should be presented with a customer webpage from Server2*

1. In Internet Explorer type http:// < ip address you wrote down> (example <http://10.x.x.4>)

\*note this validates we are connect between 2 virtual network and our network peering is working correctly

1. Minimize the RDP session to ResWebXB (where X is your student number).

## Navigating virtual machine properties

After a virtual machine has been created, a number of additional capabilities are available to the virtual machine owner.

Purpose of lab

In this lab, you will view a number of virtual machine properties, make some configuration changes, create a CPU monitor, and navigate through various virtual machine properties.

Estimated time: 15 minutes

1. In the Azure Dashboard select your **Resource Group** ResStudentX (where X is your assigned student number).
2. In the **Resoure** **group** blade select the Vm object **ResWebXA** (where X is your student number).
3. In the **ResWebXA Settings blade** select **Activity logs.**
4. In the **Active log blade** review any audit logs that exist.
5. In the **ResWebXA Settings blade** under the **settings** section select **Properties.**

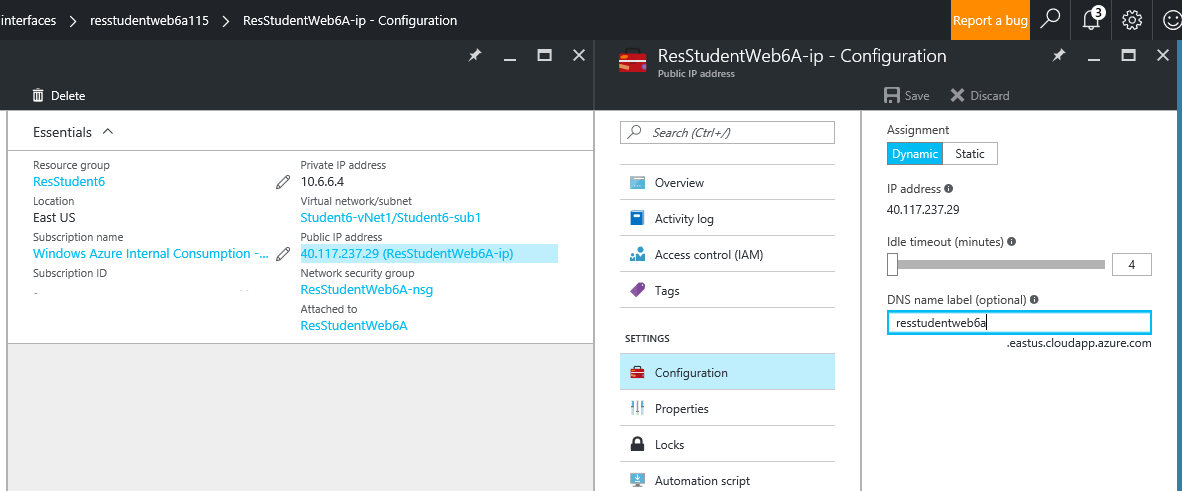
*Here you can see the IP address of your virtual machine and various other information*

1. In the **ResWebXA Settings blade** under the **MONITOR** section select **Alert rules.**
2. In the **Alert rules blade** select **Add metric alert** atthe top of the blade.
3. In the **Add rule blade** type **CPU** in the **Name** field.
4. In the **Add rule blade** type “**Monitor CPU usage**” in the **Description** field.
5. In the **Add rule blade** select the drop down menu below the **Metric** field and select **Percentage CPU**
6. In the Threshold field enter 15
7. In the period field, leave it as “Over the last 5 minutes”
8. Insert an email address to Alert in the Additional Administrator email(s) field 🡪 **OK**
9. In the **ResWebXA Settings blade** select **Tags.**
10. In the **Tags blade** select the drop down arrow in the **Key** field and select **ResstudentX** (where X is your student number).
11. In the **Tags blade** select the drop down arrow in the **Value** field **S1Project1 --> Save**

*Tags can be used for various reason like billing, categorization, etc.*

1. In the **ResWebXA Properties blade** select **Network interfaces** under the **Settings** section.
2. In the **Networks interfaces** **blade** select your network interface.
3. In the **Network Interface blade** click on the **IP address** located under **the Public IP address** section.

\*Note this is the middle section of the Network Interface blade\*

1. In the **public IP settings blade** select **Configuration**
2. In the configuration blade under the **DNS name label** input **resswebxa** (where X is your student number) --> **Save** 
3. Close the **configuration blade** by selecting the **X** in the top right
4. Close the **Network Interface blade** by selecting the **X** in the top right.
5. In the **ResWebXA Properties blade** select **Diagram** from the monitoring section

**\***Note this diagrams your virtual machine configuration showing the network information, storage information and more.

1. In the **ResWebXA Properties blade** scroll down to support & troubleshooting
2. In the **Settings blade** review the various options available

* Size, Reset Password, New support Request etc.

1. Close all blades.
2. In the Azure Dashboard select the tile **ResWebXB** (where X is your student number)
3. In the **ResXWebB** **Settings blade** select **Network interfaces**.
4. In the **Networks interfaces** **blade** select your network interface.
5. In the **Network Interface blade** click on the **IP address** located under **the Public IP address** section

\*Note this is the middle section of the Network Interface blade

1. In the **public IP settings blade** select **Configuration**
2. In the **Configuration blade** under the **DNS name label** type **reswebxb** (where X is your student number) 🡪 **Save**
3. Close all blades.

## Network Security Groups

Organizations have various methods that they use to secure IT resources, Azure provides a number of capabilities like Network Security Groups (NSGs). NSGs can be used to create firewall rules on subnets, virtual machines, and resource groups.

Purpose of lab

In this lab, you will configure NSG policies to allow port 80 inbound to your virtual machines.

Estimated time: 10 minutes

1. In the Azure Portal select **More services** from the menu on the left
2. In the browse menu select Network Security Groups.
3. In the Network Security Group blade select ResWebXA-nsg (where X is your student number).
4. In the Settings blade select Inbound security rules.
5. In the Inbound security rules blade select Add from the top of the blade.
6. In the Add inbound security rules blade type AllowHTTP in the Name field.
7. In the Add inbound security rules blade use the Service drop down, and select HTTP.
8. In the Add inbound security rules blade select Allow Action section then click OK.
9. In the Inbound security rules blade validate the new rule has been created.
10. Close the Inbound security rules blade selecting the X in the top right.
11. In the Network Security Group blade select ResWebXB (where X is your student number).
12. In the Settings blade select Inbound security rules.
13. In the Inbound security rules blade select Add from the top of the blade.
14. In the Add inbound security rules blade type AllowHTTP in the Name field.
15. In the Add inbound security rules blade use the Service drop down, and select HTTP.
16. In the Add inbound security rules blade select Allow Action section then click OK.
17. In the Inbound security rules blade validate the new rule has been created.
18. close all the blades

# Securing and Monitoring Azure Resources

As assets move to the cloud organization have concerns around security and monitoring. Microsoft Azure had a number of capabilities that can provide organziations a piece of mind knowing their cloud assets are being protected and that they have full incites into those assets.

## Setup and Configure Log Analytics

Purpose of lab

In this lab, you will setup Azure Log analytics which allow you to monitor systems reguardless of there location. OMS can be use to provide a central dashboard for an organization.

Estimated time: 10 minutes

1. In the **Azure Dashboard** select **more services** from the browse menu select **Log Analytics**.
2. In the **Log Analytics blade** select Add from the top menu.
3. In the **OMS workspace blade** in the OMS Workspace field input **ResStudentXOMS** (where X is your assigned number).
4. In the **OMS workspace blade** select the radius button “Use existing” from the Resource Group section
5. In the **OMS workspace blade** from the Resource Group section user the drop down menu to select **ResstudentX** (where X is your assigned number).
6. In the **OMS workspace blade** select **OK**
7. In the **Log Analytics blade** select resstudentXoms (where X is your assigned number).
8. In the **ResstudentXoms blade** select the OMS Portal shortcut from the middle

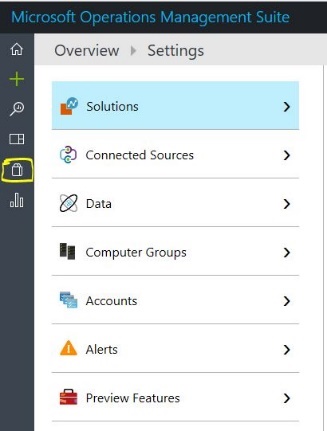
Note: this will open the OMS portal page url

1. In the **OMS Portal** select the **Settings** icon
2. In the **OMS settings** select **Data**

Note: Reivew the options available from custom logs to linux perf counters

1. In the **OMS settings Data** section select **Windows Event logs**
2. In the **Collect events from the following event logs** box input IIS select **Microsoft-IIS-Configuration/Operational**
3. Select the + button to add the log
4. In the **OMS settings** select Connected Sources 🡪 Windows Server
5. Click the link to download the Windows AgentOn
6. In the Internet Explorer save dialog select **Save As** and save the file to the **local desktop**
7. Copy the Workspace ID and Primary key information into Notepad
8. Minimize the OMS Portal (if a new tab is open go back to the Azur Portal tab)
9. In the Azure Dashboard select your **Resource Group** ResStudentX (where X is your assigned student number).
10. In the **Resoure** **group** blade select the Vm object **ResWebXA** (where X is your student number).
11. In the top of the **ResWebXA** (where X is your student number) **blade** select **Connect.**
12. In the Internet Explorer open/save dialog select **Open.**
13. In the **Remote desktop connection** dialog box, selectthe **Don’t ask me again** check box, and then click **Connect**.
14. In the **Windows Security** dialog box, select the **Use other account** check box.
15. In the logon screen,type **Student***X* and the password **P@ssword2017**.
16. In the **Remote desktop connection** dialog box, selectthe **Don’t ask me again** check box, and then click **Yes**.
17. *You will be logged onto the virtual machine hosted in Azure.*
18. Copy the OMS agent (MMASetup-AMD64.exe) from the local desktop into your virtual machine (copy and paste)
19. Double click on the OMS agent to initiate the installer
20. On the **Microsoft Monitoring Agent setup** wizard select **Next**
21. On the **Microsoft Monitoring Agent setup** Import Notice screen select **I Agree**
22. On the **Microsoft Monitoring Agent setup** Destination folder select **Next**
23. On the **Microsoft Monitoring Agent setup** Agent setup options select the check box **“Connect the agent to Azure log analytics (OMS)** 🡪 Next
24. Copy the workspace ID and primary key from the notepad file 🡪 Next
25. On the **Microsoft Monitoring Agent setup** Microsoft Update section select the radius button “Use Microsoft Windows Updates” 🡪 Next
26. On the **Microsoft Monitoring Agent setup** Ready to Install select **Install**
27. On the **Microsoft Monitoring Agent setup** select **Finish**
28. On the **Microsoft Monitoring Agent installer** select “yes” to restart the Vm
29. Open the Microsoft Operations Management Suite Portal
30. In the **OMS settings** select the icon on the left for Solutions Gallery

Note: this lists all the available monitoring solutions available today



1. In the **Solution Gallery details** select the icon on the left for **Solutions Gallery**
2. From the **Solutions Gallery** select the **Antimalware Icon**
3. From the **Solutions Gallery Details** select **Add**
4. In the **Solution Gallery details** select the icon on the left for **Solutions Gallery**
5. From the **Solutions Gallery** select the **Activity Log Analytics**
6. From the **Solutions Gallery Details** select **Add**
7. In the **Solution Gallery details** select the icon on the left for **Solutions Gallery**
8. From the **Solutions Gallery** select the **Security and Audit**
9. From the **Solutions Gallery Details** select **Add**

Note: It will take sometime for the data to report to the OMS workspace

1. From the **Solutions Gallery Details** select the **home icon** in the top left to return to the OMS dashboard

## Create a custom dashboard in Log analytics

Purpose of lab

In this lab, you will create a two custom views in OMS

Estimated time: 5 minutes

1. From the **OMS dashboard** slect the **My Dashboard** icon
2. From the **My Dashboard** page select the **Customize icon** in the top left

\*Note: OMS allow the user to create a custom view of information that is relevant to them

1. From the **Add/Edit blade** select the **+** next to“devices with “**signatures out of date**”

\*Note you will only see predefine items for the solutions gallery items installed

1. Select the newly created tile and **change** the tile visualization another option
2. Select the **+Add icon** at the top of the menu scroll down to “Security Warning and notable issues” and select “**Computers with insufficient protection**”
3. From the “**Security and Audit**” select “**All security activites**”
4. Select the Customize button in the top left.
5. Review the tile you just created, drill down into “All Security Activites”
6. From the **OMS dashboard** select the **home icon** on thet top left.
7. From the **OMS dashboard** select the **View Designer** icon.
8. From the View Designer select the **Donut.**
9. In the new blade input in the Name field **ResX** (where X is your assigned number).
10. In the properties blade under colors change the color options 🡪 Apply
11. In the OMS portal select Save in the top left

\*Note: In OMS you can create custom virtualizations

1. Close the OMS dashboard

## Setup and Configure Azure Security Center

Azure Security Center provides an organization the ability to review the security posture of the certain services running in Azure

Purpose of lab

In this lab, you will configure Azure Security Center and look at the various capabilities that can be enabled

Estimated time: 10 minutes

1. In the **Azure Dashboard** select **more services** from the browse menu select **security center**
2. In the **Security Center blade** select **Security Policy**
3. In the **Security Policy blade** expand the subscription and select the Resoure Group **ResstudentX** (where X is your number).
4. In the **Security Policy blade** under Inheritance select **Unique**
5. In the **Security Policy blade** under Policy Components select **Prevention Policy**
6. In the **Prevention Policy blade** enable all security policies 🡪 OK
7. In the **Security Policy blade** select **Save**
8. In the **Security Policy blade** select **Overivew**
9. In the middle paneunder **Resource security health** select **Virtual Machines**
10. Under Virtual Machine select **ReswebXa** (where X is your assigned number).
11. In the **Virtual machine health** select **Restrict access through internet facing endpoint**

\*Note: This show our virtual machine has an open access point on the internet with a medium alert

1. Selec the virtual machine in the new blade

\*Note: here you can see the network interface and the rules assigned that are allowing inbound traffic.

1. Close the ReswebXa-nsg blade by select X in the top right
2. Close the Restrict access through internet facing endpointby select X in the top right
3. Close the Virtual Machine health blade by select X in the top right
4. Close the Security Health blade by select X in the top right
5. In the **Security Center blade** select **recommendation**

\*Review all the recommendations

1. Close all open blades

# Configuring Azure Traffic Manager

Microsoft has introduced Traffic Manager, an Azure service that routes traffic between multiple locations that could be in your local datacenter or other cloud services.

Purpose of lab

In this lab, you will configure Traffic Manager to route web traffic between your two virtual machines and view the various options available for Traffic Manager.

Estimated time: 20 minutes

1. In the **Azure Dashboard** select **more services** from the browse menu select **Traffic Manager profiles.**
2. In the **Traffic Manager profiles blade** select **Add** at the top of the blade.
3. In the **Create Traffic Manager profiles blade** type **ResTmlabX** in the **name field** (where X is your student number).

\*Note this is a global name and may be in use, change the name to any available name

1. Select the drop down menu in the **Routing Method** section and select **Priority**.
2. In the **Resource Group** section select theRadius button **use existing** and from the drop down menu select **ResstudentX** (where X is your student number).
3. In the **Create Traffic Manager profiles blade** validate **East US 2** inselected for the location.
4. In the **Create Traffic Manager profiles blade** remove the check box **Pin to dashboard** then click **Create.**

**\****You may need to select the refresh button next to the Add button before the next step*

1. In the **Traffic Manager profiles blade** select **ResTMlabX** (where X is your student number).
2. In the  **Settings menu** select **Endpoints**.
3. In the **Endpoints blade** select **Add** at the top of the blade.
4. In the **Add endpoint blade select** the drop down menu under **Type** select **Azure Endpoint.**
5. In the **Name field** input **StudentXA** (where X is your student number).
6. Under the **Target resource type** select the drop down menu and choose **public IP address**
7. Click the **Target resource** field and in the **Resource blade** select **ReswebXA-ip**

\*Note If you do not see your server in the menu you missed the step to add a DNS name

1. In the **Add endpoint blade** select **OK**

*\*Note: wait until endpoint is created before moving on*

1. In the **Endpoints blade** select **Add** at the top of the blade.
2. In the **Add endpoint blade select** the drop down menu under **Type** and select **Azure Endpoint.**
3. In the **Name field** input **StudentXb** (where X is your student number).
4. Under the **Target resource type** select the drop down menu and choose **public IP address**
5. Click the **Target resource** field and in the **Resource blade** select **ReswebXb-IP 🡪 OK**

*Note: wait until endpoint is created before moving on*

1. In the **Traffic Manager Profile** **blade** select **Configuration**
2. In the **Configuration blade** type **30** in the **DNS time to live** section --> **Save.**
3. In the **ResStudentX Traffic Manager Profile blade** (where X is your student number) click **Properties**
4. Under **DNS name** click the url **restmlabX.trafficmanager.net** (where X is your student number).

\*You *should be connected to your web server 1a*

1. Minimize Internet Explorer (or changed to the Azure portal tab).
2. In the **ResStudentX Traffic Manager Profile blade** (where X is your student number) in the Settings menu, select Endpoints.
3. Select the endpoint **StudentXa** with **priority 1.**
4. In the **ResStudentX blade** (where X is your student number) select **Edit**
5. In the **ResStudentX blade** select **Disabled** under the Status field --> **Save**
6. In the **ResStudentX Traffic Manager Profile blade** (where X is your student number) click **Properties**
7. The url **restmlabX.trafficmanager.net** (where X is your student number) under **DNS name**.

*\*You should now be connected to Server 1b since we disabled the 1a endpoint. You may need to refresh your web browser or open a new in private to clear the cache.*

1. Close all open blades.

# Azure Recovery Services

With the Site Recovery service, organizations can use the cloud for a number of recovery services. Azure works with a number of backup solutions to allow you to store backups in the cloud and use the cloud for site recovery with VM replication.

## Create a backup vault and backup VM

Site Recovery is a native backup solution that can be utilized to back up content.

Purpose of lab

In this lab, we will use Site Recovery to create a backup vault that will be used for Azure backup services.

Estimated time: 10 minutes

1. In the **Azure Dashboard** select **More services** -> Select **Recovery Services Valuts**
2. In the **Recovery Services Vaults** blade select **Add**
3. In the **Recovery Services Vaults** blade input **ResStudent***X***-Vault (**where *X* is your student number) in the Name field.
4. In the **Recovery Services Vaults** under the **Resource Group** field select the radius button **Use existing**
5. In the **Recovery Services Vaults** under the **Resource Group** select from the drop down menu **ResStudentX** (Where X is your student number)
6. In the **Recovery Services Vaults** select **Pin to dashboard** -> **Create**
7. In the **Azure Dashboard** select **ResStudent***X***-Vault (**where *X* is your student number)
8. In the **Recovery Services Vault blade** select **Backup** from the top menu
9. In the **Backup Goal blade** in the Where is your workload running select **Azure**
10. In the **Backup Goal blade** in the What do you want to backup select **Virtual Machine -> OK**
11. In the **Backup Policy blade** under choose backup policy select the drop down menu 🡪 **Create new**

Note: review all the backup options that are available to configure for your Vm

1. Under policy name input **ResXPolicy** (where X is your assigned number). 🡪 **OK**
2. On the **Select Virtual machines blade** select ReswebXa (where X is your assigned number) 🡪 **Ok**
3. In the **Backup blade** select **Enable backup**
4. In the **Recovery Services Vault blade** under Protected items select **Backup items**
5. In the **Backup Items blade** select **Azure Virtual machine**
6. Select the virtual machine **ReswebXa** (where X is your assigned number).
7. In the **Backup Items blade** select **Backup now** from the top menu
8. In the **Backup now blade** select **Backup**
9. In the **Recovery Services Vault blade** select **Jobs** (this will be a few blade back)
10. In the **Recovery Services Vault blade** select **Backup Jobs**

\*Note: this will show the history of all backup jobs

1. Close all blades

# Deploy a Docker container hosting solution using the Azure portal

**OPTIONAL - Lab Seven: Setup Azure Container Service**

In this lab we'll look at Microsoft Azure's Container as a Service solution called: Azure Container Service (ACS). Aka.ms/containercamp

* [Deploy Azure Container Service](https://github.com/tripdubroot/ContainerCamp/blob/master/labfive/deploy-acs.md)
* [Connect and Use ACS](https://github.com/tripdubroot/ContainerCamp/blob/master/labfive/connect-acs.md)

1. [Prerequisites](https://docs.microsoft.com/en-us/azure/container-service/container-service-deployment#prerequisites)
2. [Create a cluster by using the Azure portal](https://docs.microsoft.com/en-us/azure/container-service/container-service-deployment#create-a-cluster-by-using-the-azure-portal)
3. [Create a cluster by using a quickstart template](https://docs.microsoft.com/en-us/azure/container-service/container-service-deployment#create-a-cluster-by-using-a-quickstart-template)
4. [Next steps](https://docs.microsoft.com/en-us/azure/container-service/container-service-deployment#next-steps)

**Deploy a Docker container hosting solution using the Azure portal**

Azure Container Service provides rapid deployment of popular open-source container clustering and orchestration solutions. This document walks you through deploying an Azure Container Service cluster by using the Azure portal or an Azure Resource Manager quickstart template. +

You can also deploy an Azure Container Service cluster by using the [Azure CLI 2.0](https://docs.microsoft.com/en-us/azure/container-service/container-service-create-acs-cluster-cli) or the Azure Container Service APIs.+

For background, see [Azure Container Service introduction](https://docs.microsoft.com/en-us/azure/container-service/container-service-intro).+

## Prerequisites

* **Azure subscription**: If you don't have one, sign up for a [free trial](http://azure.microsoft.com/pricing/free-trial/?WT.mc_id=AA4C1C935). For a larger cluster, consider a pay-as-you go subscription or other purchase options.

##### Note

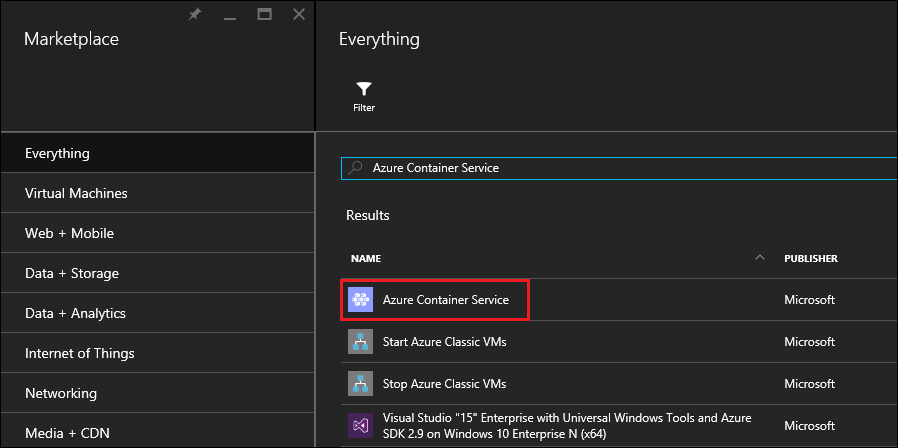
Your Azure subscription usage and [resource quotas](https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits), such as cores quotas, can limit the size of the cluster you deploy. To request a quota increase, open an [online customer support request](https://docs.microsoft.com/en-us/azure/azure-supportability/how-to-create-azure-support-request) at no charge.

* **SSH RSA public key**: When deploying through the portal or one of the Azure quickstart templates, you need to provide the public key for authentication against Azure Container Service virtual machines. To create Secure Shell (SSH) RSA keys, see the [OS X and Linux](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/mac-create-ssh-keys) or [Windows](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows) guidance.
* **Service principal client ID and secret** (Kubernetes only): For more information and guidance to create an Azure Active Directory service principal, see [About the service principal for a Kubernetes cluster](https://docs.microsoft.com/en-us/azure/container-service/container-service-kubernetes-service-principal).

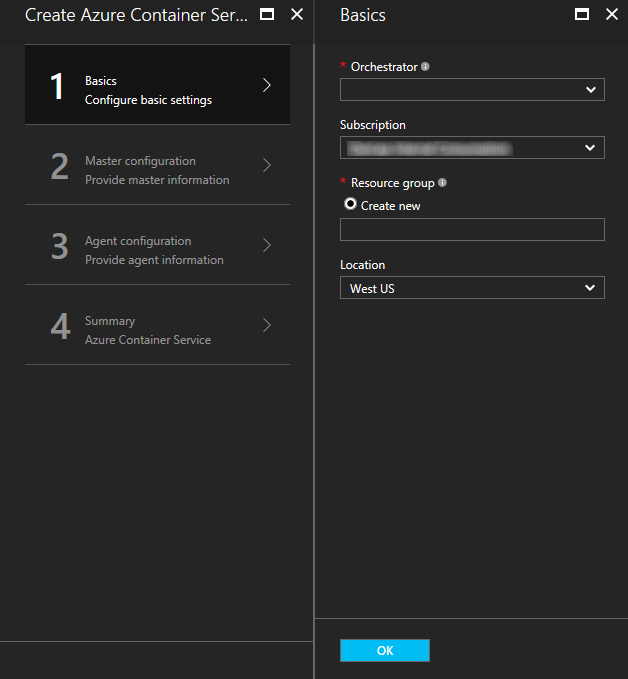
+

## Create a cluster by using the Azure portal

1. Sign in to the Azure portal, select **New**, and search the Azure Marketplace for **Azure Container Service**.

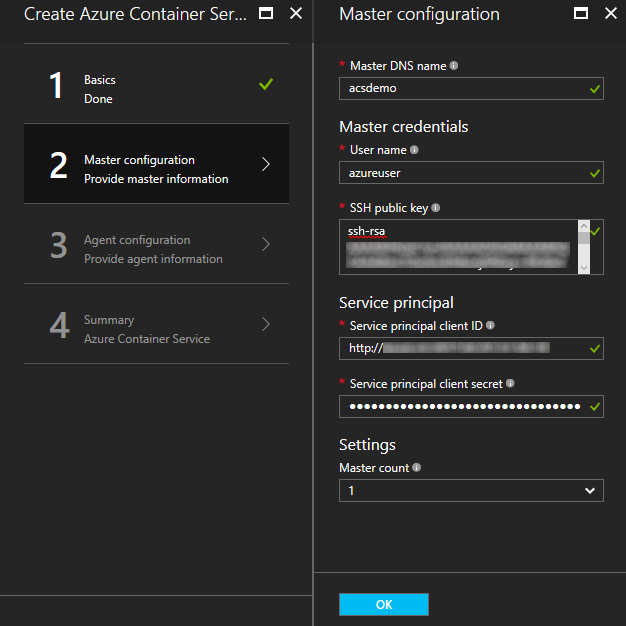


1. Click **Azure Container Service**, and click **Create**.
2. On the **Basics** blade, enter the following information:
   * **Orchestrator**: Select one of the container orchestrators to deploy on the cluster.
     + **DC/OS**: Deploys a DC/OS cluster.
     + **Swarm**: Deploys a Docker Swarm cluster.
     + **Kubernetes**: Deploys a Kubernetes cluster.
   * **Subscription**: Select an Azure subscription.
   * **Resource group**: Enter the name of a new resource group for the deployment.
   * **Location**: Select an Azure region for the Azure Container Service deployment. For availability, check [Products available by region](https://azure.microsoft.com/regions/services/).



Click **OK** when you're ready to proceed.

1. On the **Master configuration** blade, enter the following settings for the Linux master node or nodes in the cluster (some settings are specific to each orchestrator):
   * **Master DNS name**: The prefix used to create a unique fully qualified domain name (FQDN) for the master. The master FQDN is of the form prefixmgmt.location.cloudapp.azure.com.
   * **User name**: The user name for an account on each of the Linux virtual machines in the cluster.
   * **SSH RSA public key**: Add the public key to be used for authentication against the Linux virtual machines. It is important that this key contains no line breaks, and it includes the ssh-rsa prefix. The username@domain postfix is optional. The key should look something like the following: **ssh-rsa AAAAB3Nz...<...>...UcyupgH azureuser@linuxvm**.
   * **Service principal**: If you selected the Kubernetes orchestrator, enter an Azure Active Directory **Service principal client ID** (also called the appId) and **Service principal client secret** (password). For more information, see [About the service principal for a Kubernetes cluster](https://docs.microsoft.com/en-us/azure/container-service/container-service-kubernetes-service-principal).
   * **Master count**: The number of masters in the cluster.
   * **VM diagnostics**: For some orchestrators, you can enable VM diagnostics on the masters.



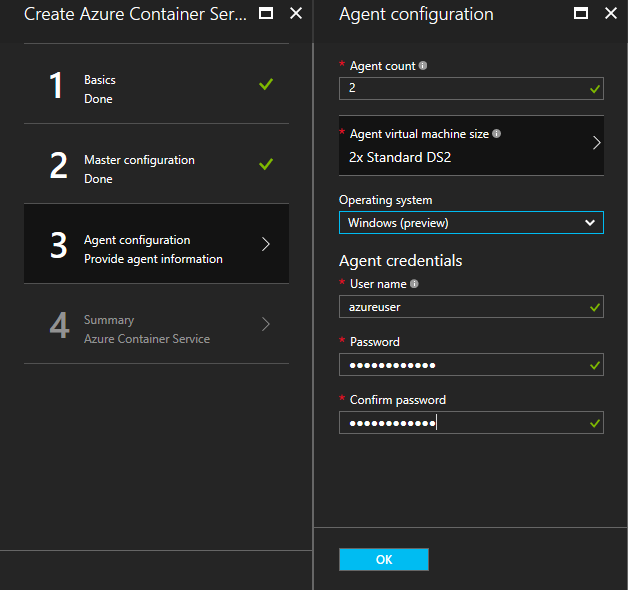
Click **OK** when you're ready to proceed.

1. On the **Agent configuration** blade, enter the following information:
   * **Agent count**: For Docker Swarm and Kubernetes, this value is the initial number of agents in the agent scale set. For DC/OS, it is the initial number of agents in a private scale set. Additionally, a public scale set is created for DC/OS, which contains a predetermined number of agents. The number of agents in this public scale set is determined by the number of masters in the cluster: one public agent for one master, and two public agents for three or five masters.
   * **Agent virtual machine size**: The size of the agent virtual machines.
   * **Operating system**: This setting is currently available only if you selected the Kubernetes orchestrator. Choose either a Linux distribution or a Windows Server operating system to run on the agents. This setting determines whether your cluster can run Linux or Windows container apps.

##### Note

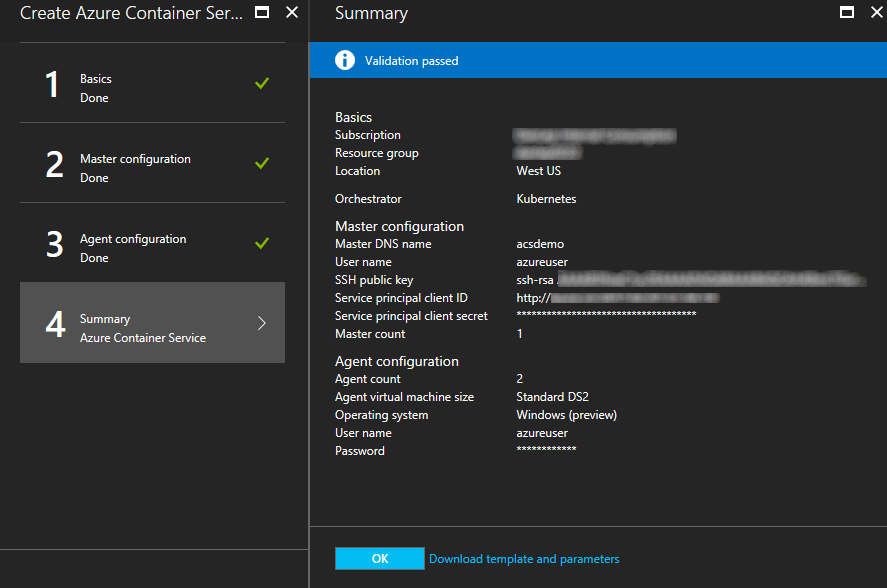
Windows container support is in preview for Kubernetes clusters. On DC/OS and Swarm clusters, only Linux agents are currently supported in Azure Container Service.

* + **Agent credentials**: If you selected the Windows operating system, enter an administrator **User name** and **Password** for the agent VMs.



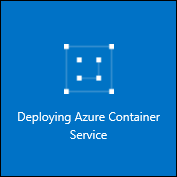
Click **OK** when you're ready to proceed.

1. After service validation finishes, click **OK**.



1. Review the terms. To start the deployment process, click **Create**.

If you've elected to pin the deployment to the Azure portal, you can see the deployment status.



1

The deployment takes several minutes to complete. Then, the Azure Container Service cluster is ready for use.

This document is for informational purposes only.  MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.