

# LAB01: Lab environment deployment

---

## Student Lab Manual

### Table of Contents

Exercise 1: Get familiar with your workshop environment

**Task 1 - View your workshop credentials and log into the workshop machine**

Exercise 2 - Lab pre-requisites

**Task 1 - Prepare the local development environment for lab deployment and login to Azure**

**Task 2 - Enable the Defender for Servers plan**

Exercise 3 - ArcBox deployment

**Task 1 - Deploy ArcBox using the Azure Portal**

**Task 2 - Connecting to the ArcBox Client virtual machine**

**Task 3 - Post-deployment automation**

====

## Exercise 1: Get familiar with your workshop environment

---

### Objective

This lab will guide you through the necessary steps to set up your Azure environment.

**Estimated Time to Complete This Lab**

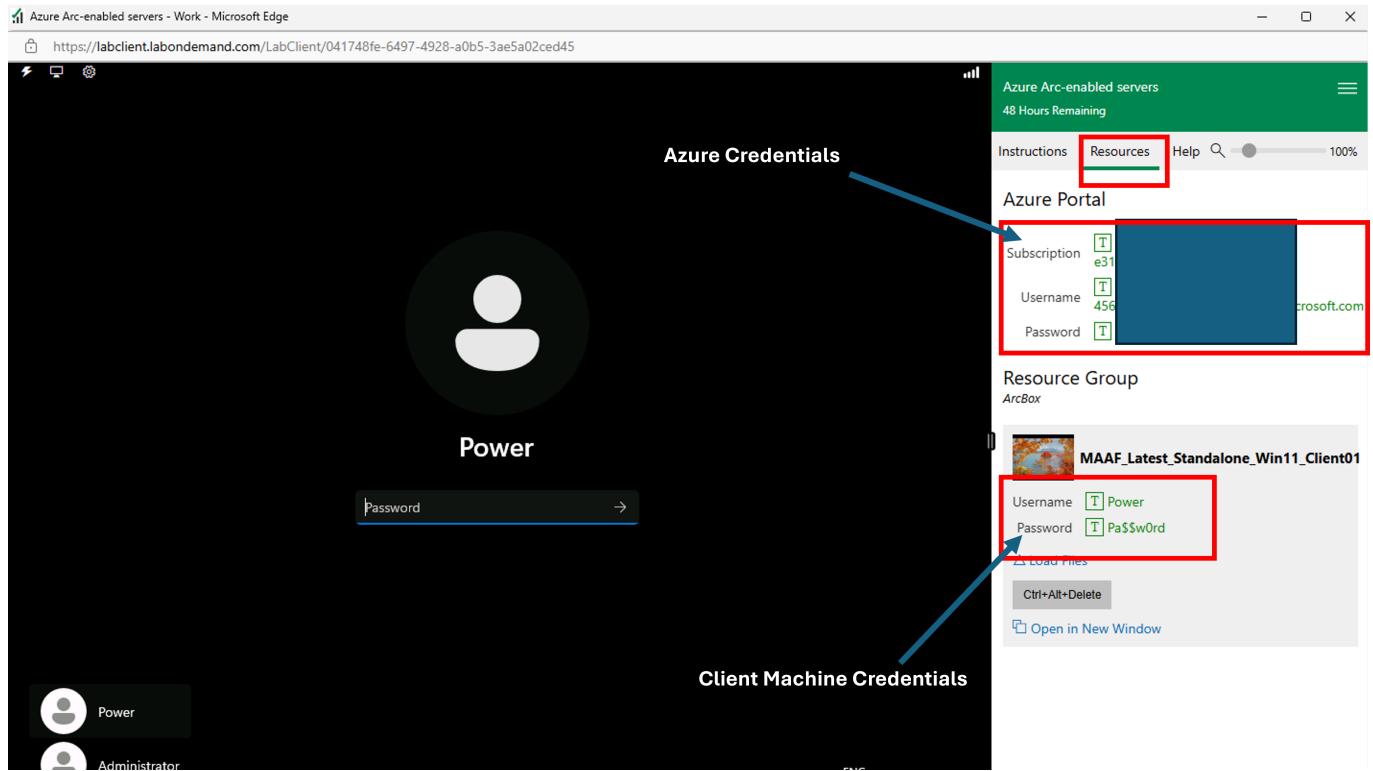
15 minutes

====

## Task 1: View your workshop credentials and log into the workshop machine

---

This lab is based on a Windows Client machine provisioned for you in the learning platform. At the top of this Instructions window, there is a menu bar with three items: **Instructions**, **Resources** and **Help** as well as a Zoom function. On the *Resources* tab you should see both the local lab machine credentials and also the Azure credentials.



[!!Important] Do not use the **END** option as it will destroy your Azure resources and end your lab. Use the **Disconnect** option when you want to take a break from the lab. Your lab timer shows how long you have left before your lab is terminated.

Azure Arc-enabled servers

95 Hr 45 Min Remaining

Instructions Resources Help

Subscription

Username

Password

Windows 11

Ctrl+Alt+Delete

Open in New Window

End

Disconnect

Split Windows

[!Important] Notice that on this tab, and throughout the instructions for this lab, you will find **squares with a capital T inside the square. This option can be used to have the lab type text for you.** If your cursor is in the password box of the login screen, and if you click on the square box with the T in it, the lab will type the password for you. This typing can be used throughout the lab and the text will appear wherever your cursor is located. **However, please note that this might not work for copying into Azure CloudShell and you will need to use Copy and Paste with the mouse right-click.**

Now log into the client machine and start with the first task of this lab. Have fun!

====

## Exercise 2 - Lab pre-requisites

---

### Objective

This exercise will walk you through preparing your local development environment to deploy the lab environment using the ArcBox sandbox.

### Estimated Time to Complete This Lab

15 minutes

### Explanation

ArcBox is a solution that deploys a complete sandbox environment with Windows and Linux machines simulating an on-premises environment. One of the Windows machines will be running a SQL Server. You will Arc-enable those machines and explore the different capabilities provided through Azure Arc. You will deploy ArcBox using the Azure Portal.

====

## Task 1: Prepare the local development environment for lab deployment and log into Azure

---

[!important] **Important:** Make sure that you carry out the steps in the Windows machine provided by the lab environment and not your local PC.

1. [] Make sure that you have the x64 version of Azure CLI version 2.66.0 or above. Start PowerShell as administrator and run the following command:

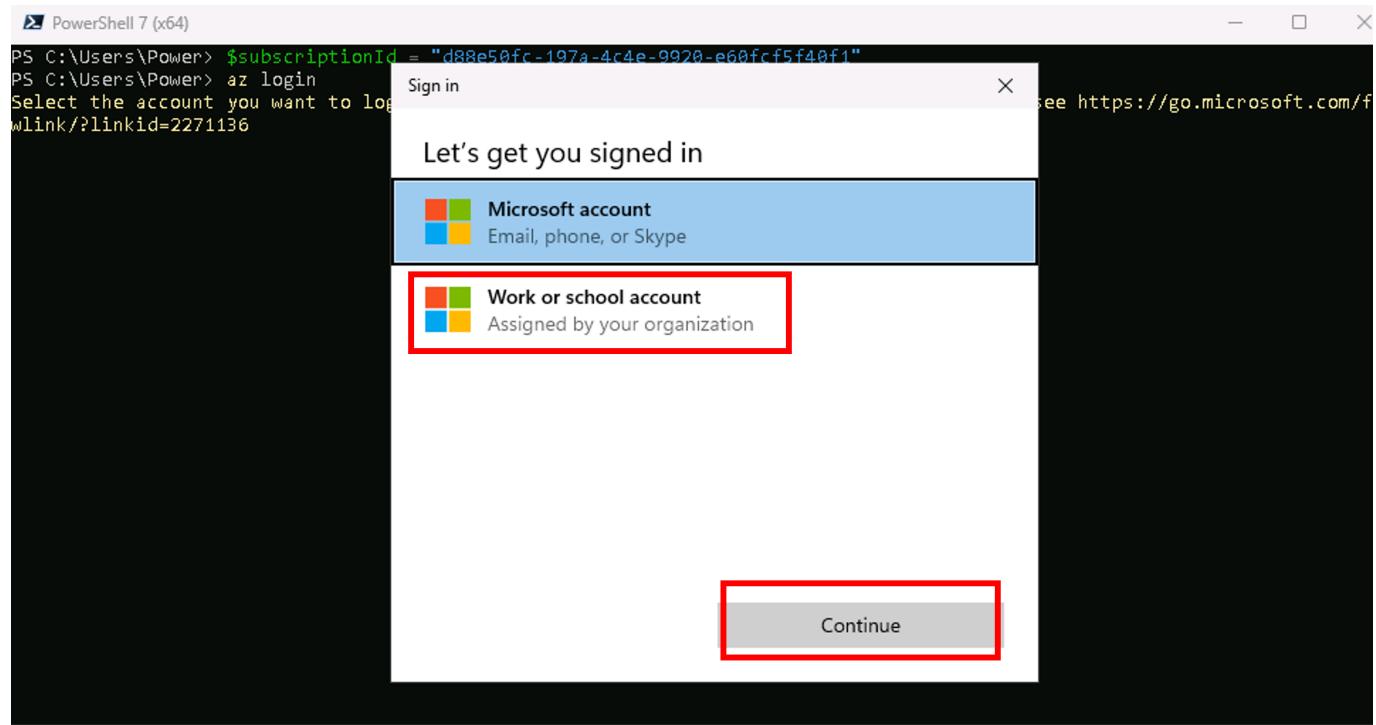
```
az --version
```

The output should confirm that you have the Azure CLI installed. If not then you can install it using the following command.

```
$ProgressPreference = 'SilentlyContinue'; Invoke-WebRequest -Uri https://aka.ms/installazurecliwindows -OutFile .\AzureCLI.msi; Start-Process msieexec.exe -Wait -ArgumentList '/I AzureCLI.msi /quiet'; Remove-Item .\AzureCLI.msi
```

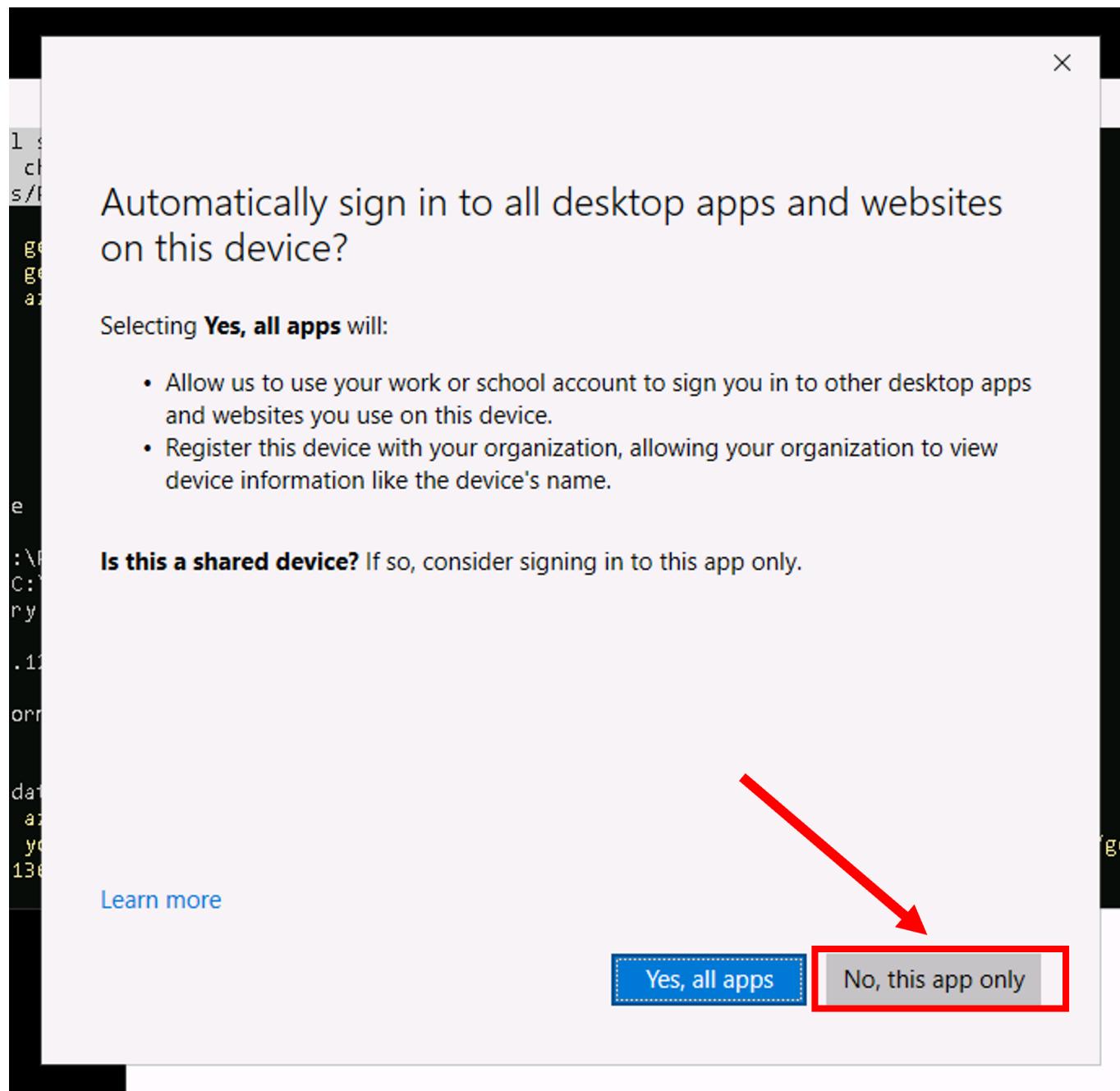
2. [] Login to AZ CLI using the `az login` command. If you are prompted to choose an account type then select *Work or school account*.

```
az login
```



[!hint] You can use Notepad or Visual Studio Code for the rest of the commands to be able to edit the needed parameters in an easier way than the PowerShell console

3. [] If you are prompted to *Automatically sign in to all desktop apps and websites on this device* select **No, this app only**



**Task 1 has been completed**

====

## Task 2: Enable Defender for Servers on your subscription

1. [] Open the EDGE browser and navigate to the Azure portal then log into Azure with lab provided credentials from the **Resources** tab

<https://portal.azure.com>

2. [] From the Azure home page, search for defender and select Microsoft Defender for Cloud.

3. [] If you already have Defender plans setup at your subscription level, you may find that Defender is already turned on for your Arc-enabled servers. However, if Defender is not enabled, select *Environment settings* from the Management section on the left blade.

4. [] Expand the Tenant Root Group, and then select **your subscription**.

5. [] Ensure that Defender CSPM is set to ON. Then enable the plan for servers, you can select either *Plan 1* or *Plan 2* for this exercise.

6. [] Click on the settings option in the *Monitoring coverage* for the Servers plan, and set the following capabilities as indicated:

- Vulnerability assessment for machines - **ON**.
- Endpoint protection - **ON**.
- Agentless Scanning for machines - **OFF**.

The screenshot shows the 'Settings & monitoring' section for the 'Servers' plan. It lists several components and their configurations:

Component	Description	Defender plans	Configuration	Status
Log Analytics agent	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. <a href="#">Learn more</a>		-	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>
Vulnerability assessment for machines	Enables vulnerability assessment on your Azure and hybrid machines. <a href="#">Learn more</a>		Selected VA tools: Microsoft Defender vulnerability management <a href="#">Edit configuration</a>	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>
Guest Configuration agent (preview)	Checks machines for security misconfigurations in the OS, applications, and environment settings. This deploys the agent to Azure virtual machines. Hybrid machines connected to Azure Arc already have this agent included in the Azure Connected Machine agent. Learn more about the Guest Configuration agent. <a href="#">Understand Azure Policy's Guest Configuration</a>		-	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>
Endpoint protection	Enables protection powered by Microsoft Defender for Endpoint, including automatic agent deployment to your servers, and security data integration with Defender for Cloud. <a href="#">Learn more</a>		-	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>
Agentless scanning for machines	Scans your machines for installed software, vulnerabilities, and secret scanning without relying on agents or impacting machine performance. <a href="#">Learn more</a>		-	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>
File Integrity Monitoring	File integrity monitoring (FIM), also known as change monitoring, examines operating system files, Windows registries, application software, Linux system files, and more, for changes that might indicate an attack.		-	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>

7. [] Click *Continue* then Click *Save*.

The screenshot shows the 'Settings | Defender plans' page. It displays two sections: Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWP).

**Cloud Security Posture Management (CSPM):**

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at \$5/Billable resource/month. Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free <a href="#">Details &gt;</a>	-	Full	<input type="button" value="On"/> <input type="button" value="Off"/>
Defender CSPM	\$5/Billable resource/Month <a href="#">Details &gt;</a>	3 resources	Partial <a href="#">Settings &gt;</a>	<input type="button" value="On"/> <input type="button" value="Off"/>

**Cloud Workload Protection (CWP):**

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Servers	Plan 1 (\$5/Server/Month) <a href="#">Change plan &gt;</a>	0 servers	Full <a href="#">Settings &gt;</a>	<input type="button" value="On"/> <input type="button" value="Off"/>

## Task 2 has been completed

====

# Exercise 3 - ArcBox deployment

## Objective

In this exercise you will deploy the lab using the ArcBox solution which will deploy all the needed Azure resources to your subscription to be able to execute all the upcoming exercises.

### Estimated Time to Complete This Lab

45 minutes

### Explanation

ArcBox is a solution that deploys a complete sandbox environment with Windows and Linux machines simulating an on-premises environment. One of the Windows machines will be running a SQL Server. You will Arc-enable those machines and explore the different capabilities provided through Azure Arc. You will deploy ArcBox using the Azure Portal.

====

## Task 1: Deploy ArcBox using the Azure Portal

---

1. [] The specific setup of ArcBox used in this workshop can be deployed in any region that supports the Azure virtual machine SKU required (Standard\_E8s\_v5, v4 or v3). Occasionally, there might be restrictions on specific subscriptions that can prevent the deployment of a specific SKU even if it is available in a region. To check if there are any restrictions on your subscription you can run the following PowerShell command in **Azure Cloud Shell**. You can change the list of locations in the script if necessary by adding or removing regions. But **do not change the list of VM Skus**. If you prefer to run the command from the lab machine then make sure you login in PowerShell first using *Connect-AzAccount* command.

```
$locations = "uksouth", "northeurope", "eastus", "eastus2", "centralus"
#Do not change the VMSkus below
$VmSkus = "Standard_E8s_v5", "Standard_E8s_v4", "Standard_E8s_v3"
$locations | ForEach-Object -ThrottleLimit 10 -Parallel {
    Get-AzComputeResourceSku -Location $_ | Where-Object {$_ ResourceType -eq
    "virtualMachines" -and $_.name -in $using:VmSkus}
}
```

The output will show if there are restrictions in any of the listed regions or in specific zones in the region (for a multi-zone region). Choose a region and VM Sku combination that has no restrictions to deploy the lab VM. For example, in the following diagram we can see that *uksouth* is a very good candidate to deploy the lab. On the other hand *centralus* is not because of the full restrictions. The *northeurope* region has restrictions only in zone 3 so it should allow you to deploy.

ResourceType	Name	Location	Zones	RestrictionInfo
virtualMachines	Standard_E8s_v3	uksouth	{2, 1, 3}	
virtualMachines	Standard_E8s_v4	uksouth	{2, 1, 3}	
virtualMachines	Standard_E8s_v5	uksouth	{2, 1, 3}	
virtualMachines	Standard_E8s_v3	centralus	{2, 1, 3}	{type: Location, locations: centralus, type: Zone, locations: centralus, zones: 1, 2, 3}
virtualMachines	Standard_E8s_v4	centralus	{2, 1, 3}	{type: Location, locations: centralus, type: Zone, locations: centralus, zones: 1, 2, 3}
virtualMachines	Standard_E8s_v5	centralus	{2, 3, 1}	{type: Location, locations: centralus, type: Zone, locations: centralus, zones: 1, 2, 3}
virtualMachines	Standard_E8s_v3	eastus2	{2, 1, 3}	{type: Zone, locations: eastus2, zones: 1}
virtualMachines	Standard_E8s_v4	eastus2	{2, 1, 3}	{type: Zone, locations: eastus2, zones: 1}
virtualMachines	Standard_E8s_v5	eastus2	{2, 1, 3}	{type: Zone, locations: eastus2, zones: 1}
virtualMachines	Standard_E8s_v3	eastus	{1, 3, 2}	{type: Location, locations: eastus, type: Zone, locations: eastus, zones: 1, 2, 3}
virtualMachines	Standard_E8s_v4	eastus	{1, 2, 3}	{type: Location, locations: eastus, type: Zone, locations: eastus, zones: 1, 2, 3}
virtualMachines	Standard_E8s_v5	eastus	{1, 3, 2}	{type: Location, locations: eastus, type: Zone, locations: eastus, zones: 1, 2, 3}
virtualMachines	Standard_E8s_v3	...theurope	{1, 3, 2}	{type: Zone, locations: northeurope, zones: 3}
virtualMachines	Standard_E8s_v4	...theurope	{2, 1, 3}	{type: Zone, locations: northeurope, zones: 3}
virtualMachines	Standard_E8s_v5	...theurope	{2, 3, 1}	{type: Zone, locations: northeurope, zones: 3}

[!alert] Make sure that you have selected a region with no restrictions on the required virtual machine sku (as explained above). Failure to do so might cause your deployment to fail. You will need to enter the name of the selected region and VM SKU in the deployment template in the next step.

2. [] Open the Microsoft Edge browser and paste the following URL.

```
++++https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2FAzure%2Farc_jumpstart_levelup%2Fmain%2Fazure_arc_servers_jumpstart%2FARM%2Fazuredetect.json+++
++
```

3. [] Enter values for the the template parameters then click *Review + create*.

[!alert] The only acceptable resource group name is **ArcBox**. If you choose any other name then your deployment will fail.

[!hint] Make sure to note the Windows admin username and password as you will use them in later exercises. In order to avoid using a username and password combination that does not meet the complexity requirements which would lead to the failure of the deployment, we recommend using the username **arcdemo** and the password **Arcboxlabs@12345**.

[!hint] Review the [complexity requirements](#) for the Windows virtual machine's password

# Custom deployment

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

 Customized template v1  
6 resources

 Edit template  Edit parameters  Visualize

## Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Resource group \* ⓘ  Create new

Instance details

Region \* ⓘ

Spn Tenant Id ⓘ

Client Vm Sku \* ⓘ

Windows Admin Username \* ⓘ

Windows Admin Password \* ⓘ

Log Analytics Workspace Name \* ⓘ

Github Account ⓘ

Github Branch ⓘ

Rdp Port ⓘ

Ssh Port ⓘ

Email Address \* ⓘ

Location

[Previous](#) [Next](#) [Review + create](#)

[!hint] The deployment takes around 20 minutes to complete.

[!hint] If you see any failure in the deployment, please check that you have selected a region with no restrictions on the virtual machine sku and consult your workshop instructor. In some cases a transient issue might cause a deployment error. The best action in these cases is to redeploy the template. **Make sure that you delete the whole resource group (not only the resources inside it) and once the deletion is completed you can redeploy the template.**

## Task 1 has been completed

====

## Task 2: Connecting to the ArcBox Client virtual machine

Various options are available to connect to *ArcBox-Client* VM on Azure. However, for this lab you will use the direct RDP method - available after configuring access to port 3389 on the *ArcBox-NSG* Network Security Group.

[!alert] Once you have logged on to the *ArcBox-Client* VM you might see some Powershell scripts in the process of being executed. DO NOT close any windows or stop any scripts. The set-up automation will close the completed windows automatically

# Connecting directly with RDP

By design, ArcBox does not open port 3389 on the network security group. Therefore, you must create an NSG rule to allow inbound 3389.

- Open the *Network settings* for the *ArcBox-Client* machine in the Azure portal and click *Create port rule* to add a new inbound rule.

The screenshot shows the Azure portal interface for a virtual machine named 'ArcBox-Client'. In the left sidebar, under the 'Networking' section, the 'Network settings' link is highlighted with a red circle containing the number '1'. In the main content area, under the 'Network interface / IP configuration' section, there is a 'Network security group' entry for 'ArcBox-NSG'. Below it, the 'Create port rule' button is highlighted with a red circle containing the number '2'.

The screenshot shows the same Azure portal interface as the previous one, but now with an additional inbound port rule listed in the NSG rules table. The 'Create port rule' button has a dropdown menu open, and the 'Inbound port rule' option is highlighted with a red box.

Priority ↑	Name	Port	Protocol	Source	Destination	Action
65000	AllowVhnetinBound	Any	Any	VirtualNetwork	VirtualNetwork	<span>Allow</span>
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	<span>Allow</span>
65500	DenyAllInBound	Any	Any	Any	Any	<span>Deny</span>

- Specify the IP address that you will be connecting from (or use *My IP address*) and select RDP as the service. If you need to retrieve your public IP address (not required if you use the *My IP address* setting) then you can do so by accessing <https://icanhazip.com> or <https://whatismyip.com>.

ArcBox-Client | Network settings

Network interface / IP configuration  
ArcBox-Client-NIC (primary) / ipconfig1 (primary)

Source: My IP address

Source IP addresses/CIDR ranges: [redacted]

Source port ranges: \*

Destination: Any

Service: RDP

Destination port ranges: 3389

Protocol: TCP (selected)

Add Cancel Give feedback

3. [] Now you can run the Remote Desktop Connection App and connect to the *ArcBox-Client* machine using the user name and password that you have set on the deployment template.

Settings - Microsoft Azure

Microsoft Azure

Search results for 'rdp':

- Remote Desktop Connection (App)
- Search the web:
  - rdp - See more search results
  - rdp port
  - rdp settings
  - rdp wrapper
  - rdp manager
  - rdp server
  - rdpwrap
  - rdpguard
  - rdp client
  - rdp hosting

Remote Desktop Connection (App)

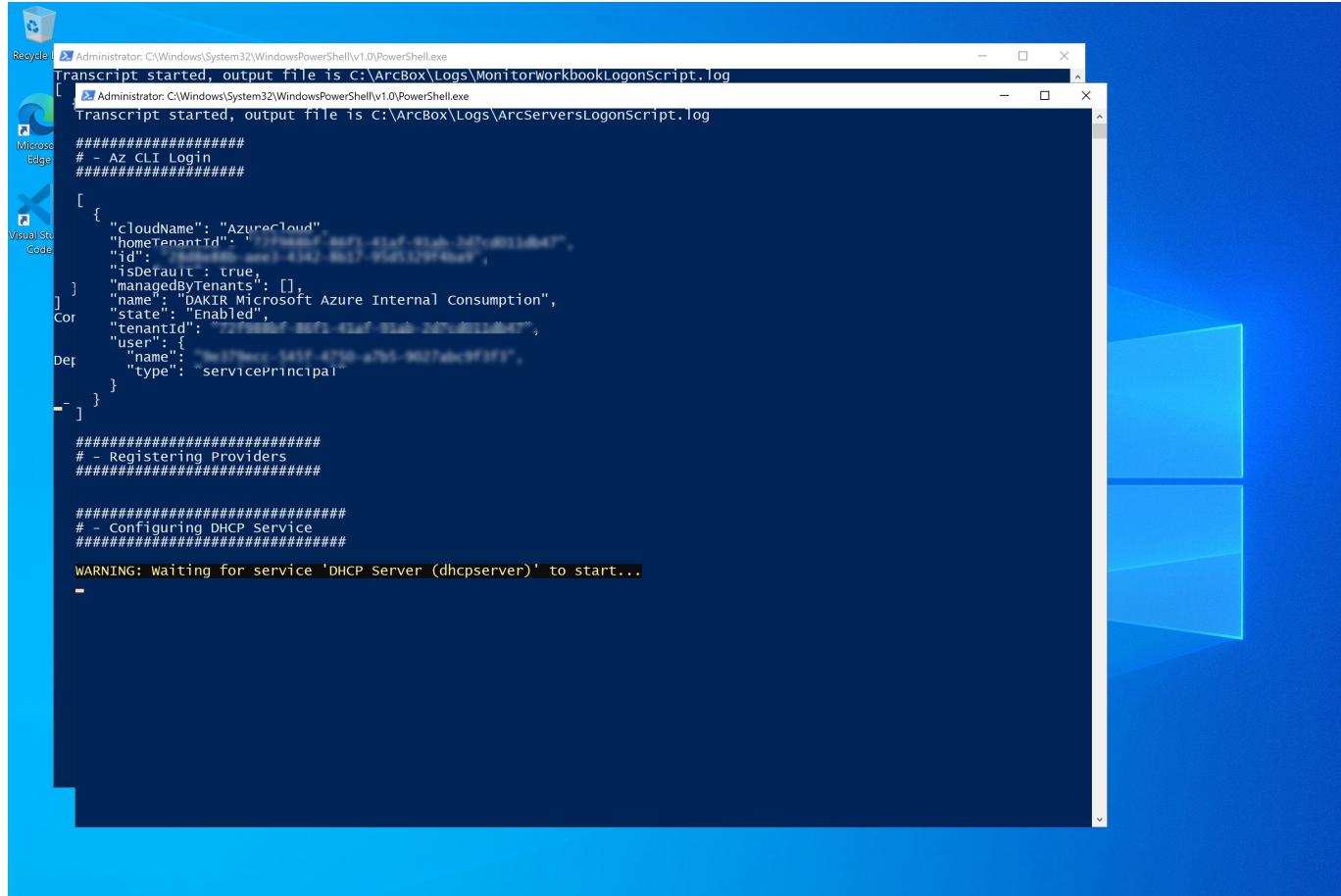
- Open
- Run as administrator
- Open file location
- Pin to Start
- Pin to taskbar
- Uninstall

**Task 2 has been completed**

====

## Task 3: Post-deployment automation

1. [] Once you log into the *ArcBox-Client* VM, multiple automated scripts might be open and running. These scripts usually take 10-20 minutes to finish (**Do not close any windows and do not stop any running scripts!**), and once completed, the script windows will close automatically. At this point, the deployment is complete.



```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\PowerShell.exe
Transcript started, output file is C:\ArcBox\Logs\MonitorworkbookLogonScript.log
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\PowerShell.exe
Transcript started, output file is C:\ArcBox\Logs\ArcServersLogonScript.log

#####
# - AZ CLI Login
#####

[ {
  "cloudname": "AzureCloud",
  "homeTenantId": "93f9eaa7-46f1-43af-91ab-2d7c4013d847",
  "id": "00000000-0000-0000-0000-000000000000",
  "isDefault": true,
  "managedByTenants": [],
  "name": "DAKIR Microsoft Azure Internal Consumption",
  "state": "Enabled",
  "tenantId": "72f98bf-8c72-43a7-91a0-2d7c4013d847",
  "user": {
    "name": "b61579eccc-545f-4750-a765-9627abc9f3f3",
    "type": "servicePrincipal"
  }
}

#####
# Registering Providers
#####

#####
# Configuring DHCP Service
#####

WARNING: Waiting for service 'DHCP Server (dhcpserver)' to start...
```

2. [] Deployment is complete when you see the following screen background! Let's begin exploring the features of Azure Arc-enabled servers with the other labs in this workshop.



**Task 3 has been completed**

====

**Congratulations, you have completed all tasks in this lab**

Click **Next** for the next lab or **Go back to the main table of content**