Microsoft Azure Cloud Services

SummitWorks™
GLOBAL SOLUTION ARCHITECTS

Authorized & published by Summitworks Technologies Inc

Agenda

- **Azure services**
    - Compute services
        - Azure Virtual Machines (Windows)
            - Deployment of virtual machines (Portal, PowerShell, CLI)
            - Access and security for Virtual Machines

Azure Services

Compute Services

Here are some compute options currently available in Azure:

Azure
Virtual Machines

Azure
App Service

Azure
Service Fabric

Azure
Container Instances

Azure
Functions

Azure
Batch

Azure Compute Services - Virtual Machines

Azure Virtual Machines (VM)

Azure Virtual Machines (VM) is one of several types of on-demand, scalable computing resources that Azure offers. Typically, you choose a VM when you need more control over the computing environment than the other choices offer.

An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs it. However, you still need to maintain the VM by performing tasks, such as configuring, patching, and installing the software that runs on it.

Azure Virtual Machines (VM)

Azure virtual machines can be used in various ways. Some examples are:

- **Development and test** – Azure VMs offer a quick and easy way to create a computer with specific configurations required to code and test an application.
- **Applications in the cloud** – Because demand for your application can fluctuate, it might make economic sense to run it on a VM in Azure. You pay for extra VMs when you need them and shut them down when you don't.
- **Extended datacenter** – Virtual machines in an Azure virtual network can easily be connected to your organization's network.

The number of VMs that your application uses can scale up and out to whatever is required to meet your needs.

Azure Virtual Machines (VM)

What do I need to think about before creating a VM?

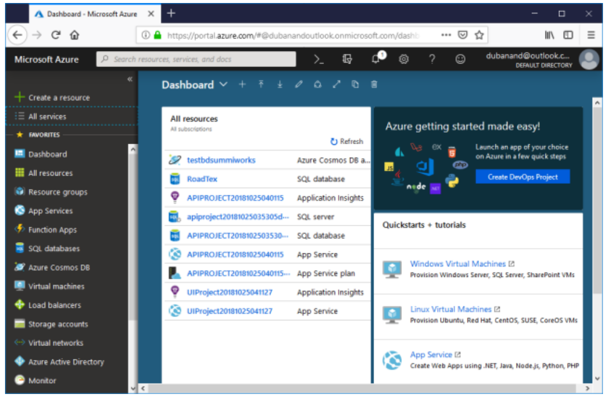
There are always a multitude of design considerations when you build out an application infrastructure in Azure. These aspects of a VM are important to think about before you start:

- The names of your application resources
- The location where the resources are stored
- The size of the VM
- The maximum number of VMs that can be created
- The operating system that the VM runs
- The configuration of the VM after it starts
- The related resources that the VM needs

Azure Virtual Machines (VM)

You have several choices for creating your VM. The choice that you make depends on the environment you are in.

- Azure portal
- Templates
- Azure PowerShell
- Client SDKs
- Azure CLI



All resources
All subscriptions

testbdsummiworks	Azure Cosmos DB a...
RoadTex	SQL database
APIPROJECT20181025040115	Application Insights
apiproject20181025035305d...	SQL server
APIPROJECT2018102503530...	SQL database
APIPROJECT20181025040115	App Service
APIPROJECT20181025040115...	App Service plan
UIProject20181025041127	Application Insights
UIProject20181025041127	App Service

Azure getting started made easy!

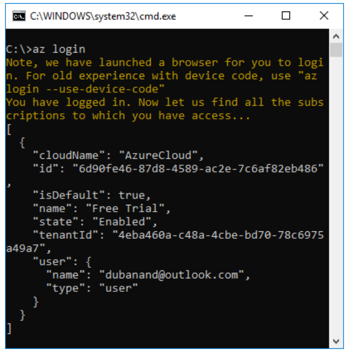
Launch an app of your choice on Azure in a few quick steps

Quickstarts + tutorials

Windows Virtual Machines
Provision Windows Server, SQL Server, SharePoint VMs

Linux Virtual Machines
Provision Ubuntu, Red Hat, CentOS, SUSE, CoreOS VMs

App Service
Create Web Apps using .NET, Java, Node.js, Python, PHP



```
C:\>az login
Note, we have launched a browser for you to logi
n. For old experience with device code, use "az
login --use-device-code"
You have logged in. Now let us find all the subs
criptions to which you have access...
[
  {
    "cloudName": "AzureCloud",
    "id": "6d90fe46-87d8-4589-ac2e-7c6af82eb486"
,
    "isDefault": true,
    "name": "Free Trial",
    "state": "Enabled",
    "tenantId": "4eba460a-c48a-4cbe-bd70-78c6975
a49a7",
    "user": {
      "name": "dubanand@outlook.com",
      "type": "user"
    }
  }
]
```

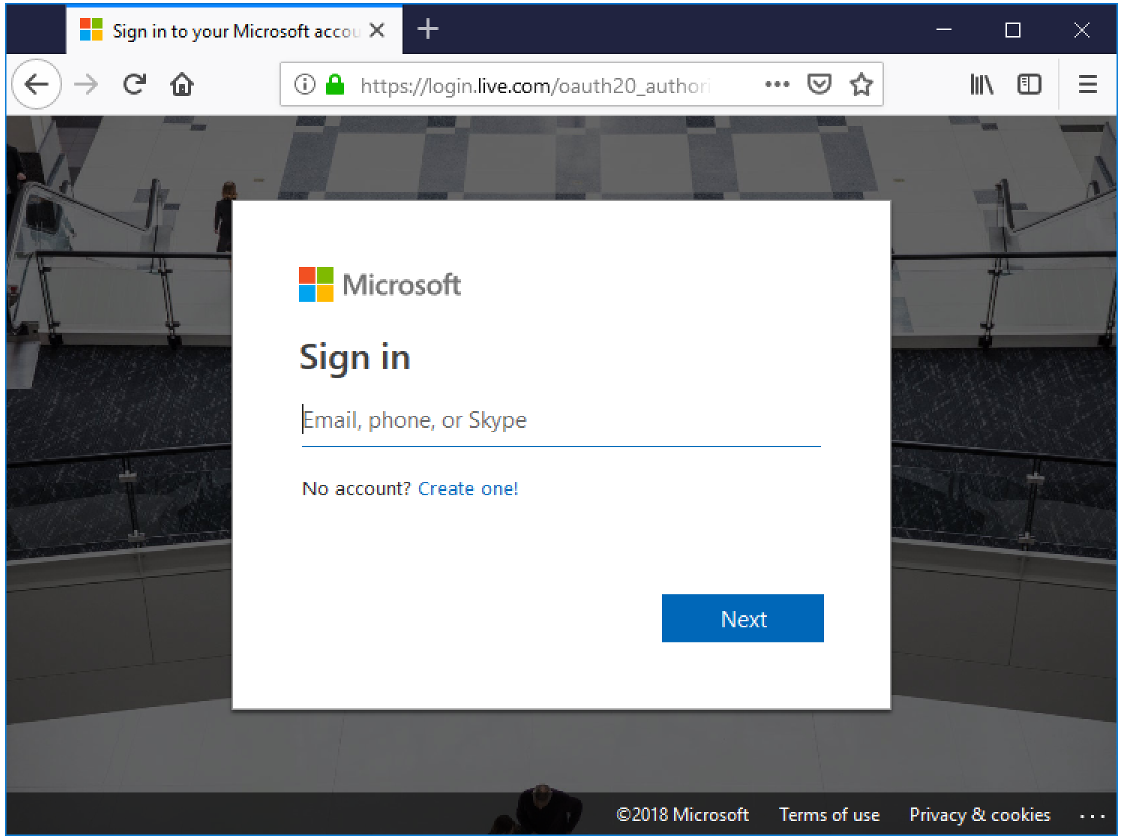
PowerShell
Microsoft Azure

Create an Azure Virtual Machine (Portal)

Azure virtual machines (VMs) can be created through the Azure portal. This method provides a browser-based user interface to create VMs and their associated resources. This quickstart shows you how to use the Azure portal to deploy a virtual machine (VM) in Azure that runs Windows Server 2016.

Sign in to the Azure portal at

https://portal.azure.com.



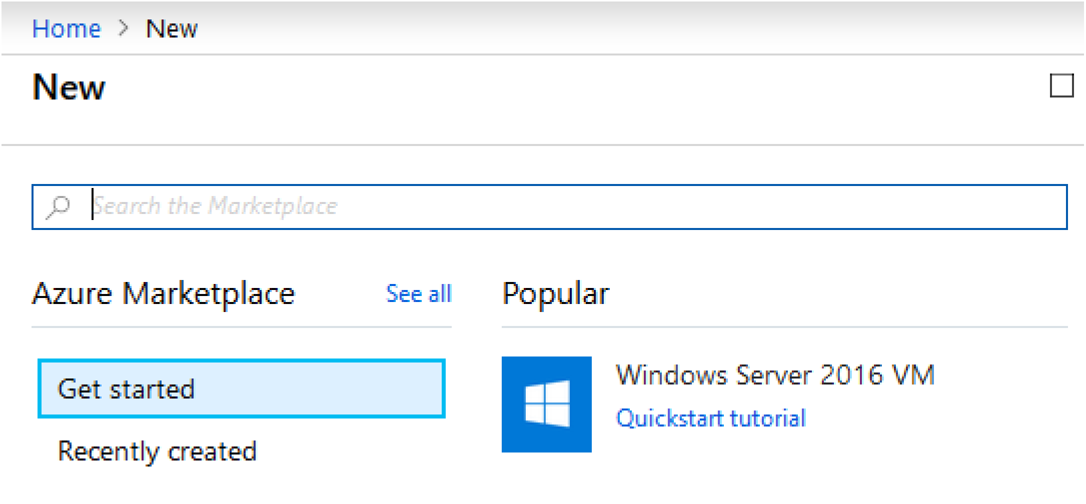
Create an Azure Virtual Machine (Portal)

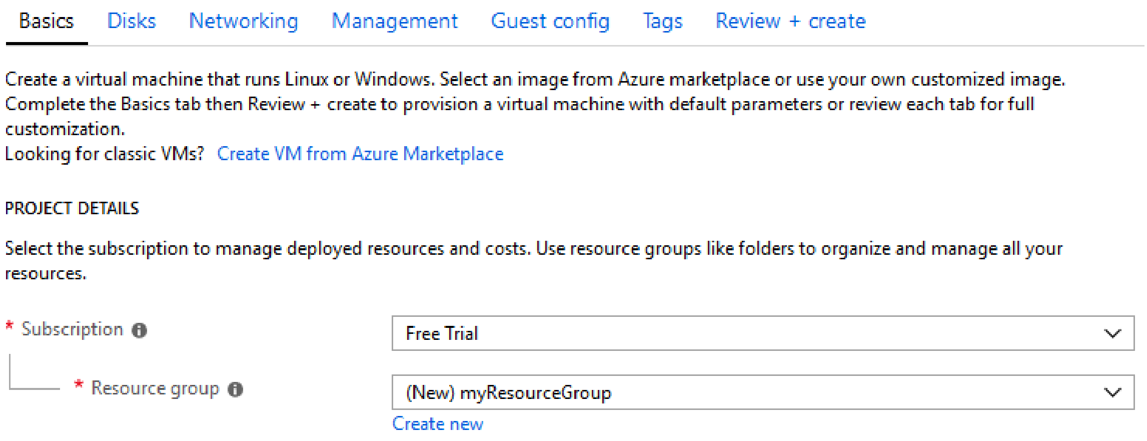
Create virtual machine

1. Choose **Create a resource** in the upper left-hand corner of the Azure portal.

2. In the search box above the list of Azure Marketplace resources, search for and select **Windows Server 2016 VM**, then choose **Create**.

3. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected and then choose to **Create new** resource group. Type the *myResourceGroup* for the name.





Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? Create VM from Azure Marketplace

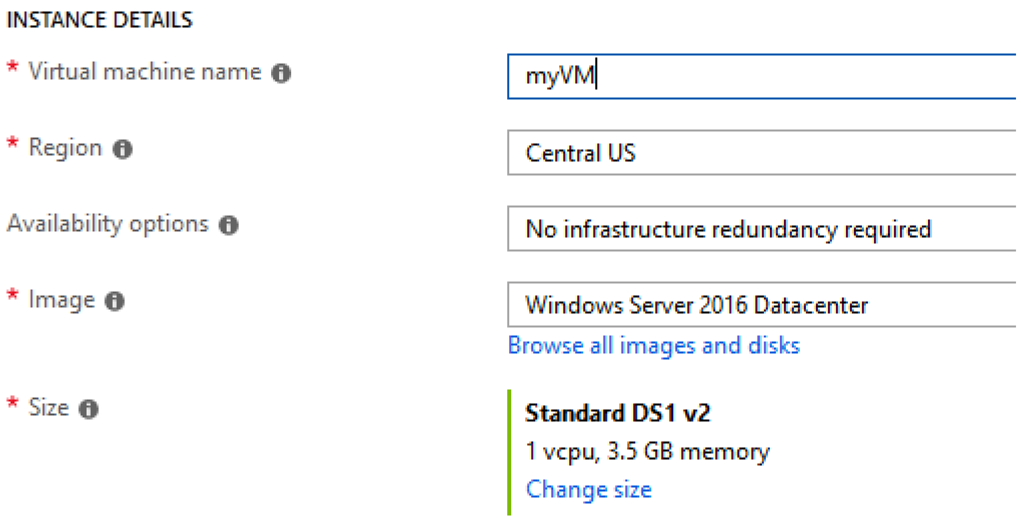
PROJECT DETAILS

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

* Subscription	Free Trial
* Resource group	(New) myResourceGroup Create new

Create an Azure Virtual Machine (Portal)

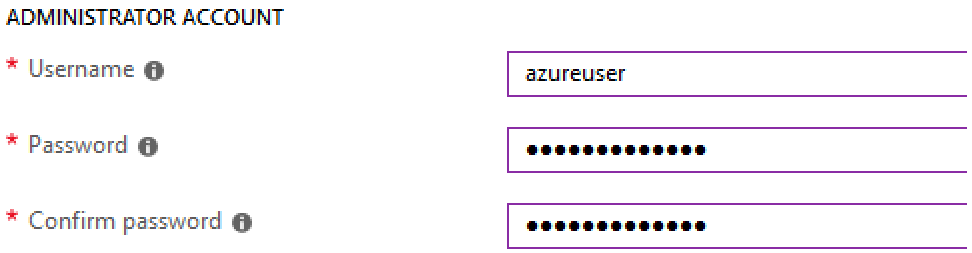
4. Under **Instance details**, type *myVM* for the **Virtual machine name** and choose *East US* for your **Location**. Leave the other defaults.



INSTANCE DETAILS

* Virtual machine name	myVM
* Region	Central US
Availability options	No infrastructure redundancy required
* Image	Windows Server 2016 Datacenter Browse all images and disks
* Size	**Standard DS1 v2** 1 vcpu, 3.5 GB memory Change size

5. Under **Administrator account**, provide a username, such as *azureuser* and a password. The password must be at least 12 characters long.

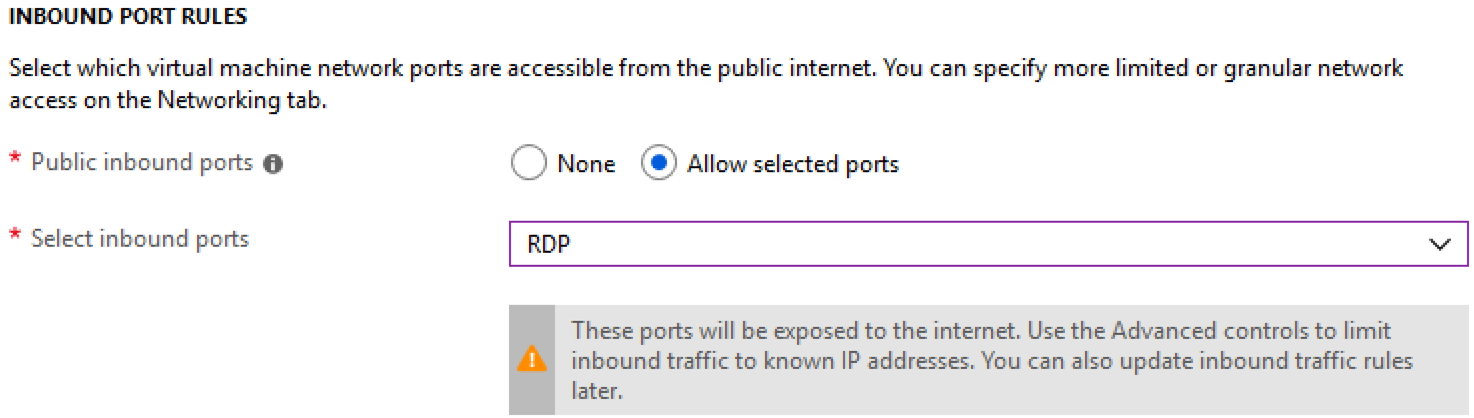


ADMINISTRATOR ACCOUNT

* Username	azureuser
* Password	••••••••••••••
* Confirm password	••••••••••••••

Create an Azure Virtual Machine (Portal)

6. Under **Inbound port rules**, choose **Allow selected ports** and then select **RDP (3389)** and **HTTP**from the drop-down.



INBOUND PORT RULES

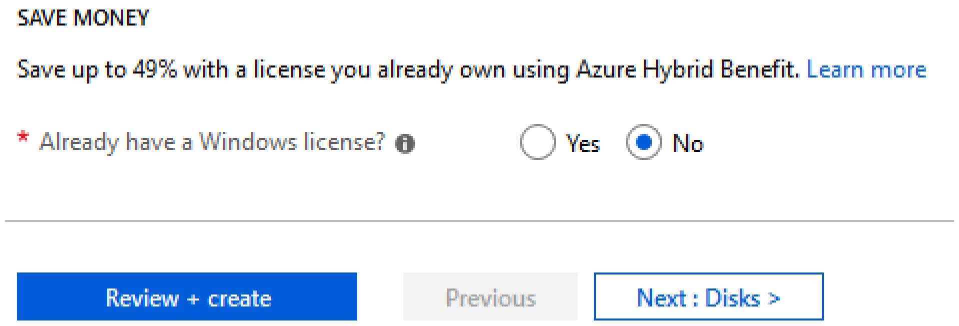
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

* Public inbound ports ○ None ● Allow selected ports

* Select inbound ports: RDP

These ports will be exposed to the internet. Use the Advanced controls to limit inbound traffic to known IP addresses. You can also update inbound traffic rules later.

7. Leave the remaining defaults and then select the **Review + create** button at the bottom of the page.



SAVE MONEY

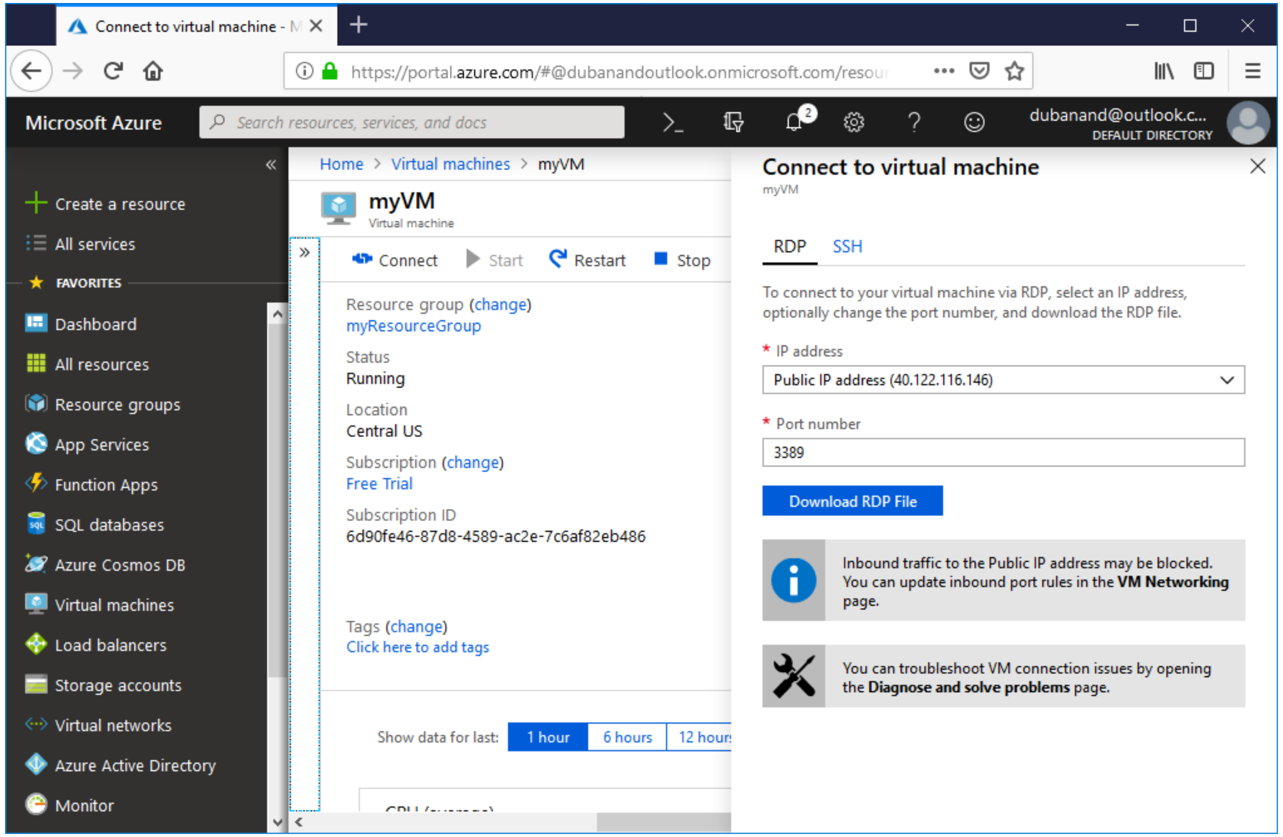
Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

* Already have a Windows license? ○ Yes ● No

Connect to Azure Virtual Machine (Portal)

Create a remote desktop connection to the virtual machine. These directions tell you how to connect to your VM from a Windows computer. On a Mac, you need an RDP client such as this Remote Desktop Client from the Mac App Store.

1. Click the **Connect** button on the virtual machine properties page.



Resource group (change)
myResourceGroup

Status
Running

Location
Central US

Subscription (change)
Free Trial

Subscription ID
6d90fe46-87d8-4589-ac2e-7c6af82eb486

Tags (change)
Click here to add tags

Connect to virtual machine
myVM

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

* IP address
Public IP address (40.122.116.146)

* Port number
3389

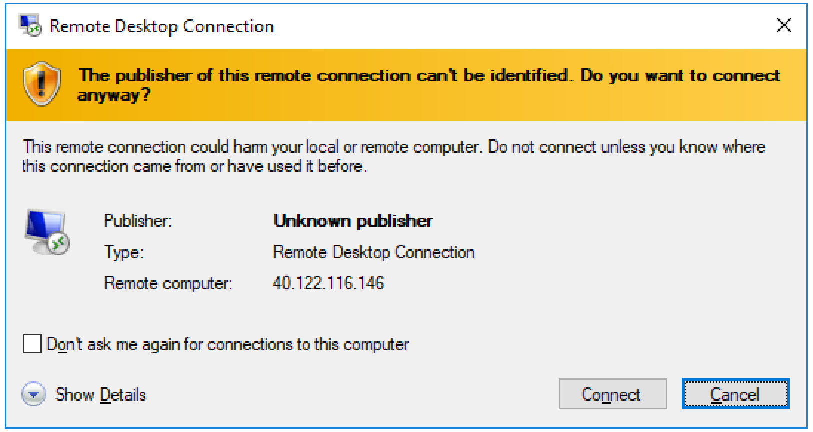
Inbound traffic to the Public IP address may be blocked. You can update inbound port rules in the **VM Networking** page.

You can troubleshoot VM connection issues by opening the **Diagnose and solve problems** page.

Connect to Azure Virtual Machine (Portal)

2. In the **Connect to virtual machine** page, keep the default options to connect by DNS name over port 3389 and click **Download RDP file**.

3. Open the downloaded RDP file and click **Connect** when prompted.



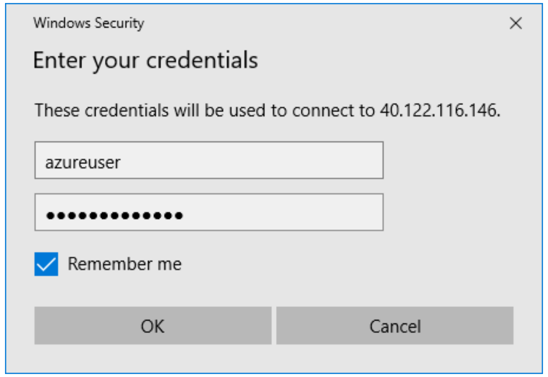
The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

Publisher: **Unknown publisher**
Type: Remote Desktop Connection
Remote computer: 40.122.116.146

□ Don't ask me again for connections to this computer

4. In the **Windows Security** window, select **More choices** and then **Use a different account**. Type the username as **localhost**\username, enter password you created for the virtual machine, and then click **OK**.



Enter your credentials

These credentials will be used to connect to 40.122.116.146.

azureuser
•••••••••••••

☑ Remember me

5. You may receive a certificate warning during the sign-in process. Click **Yes** or **Continue** to create the connection.

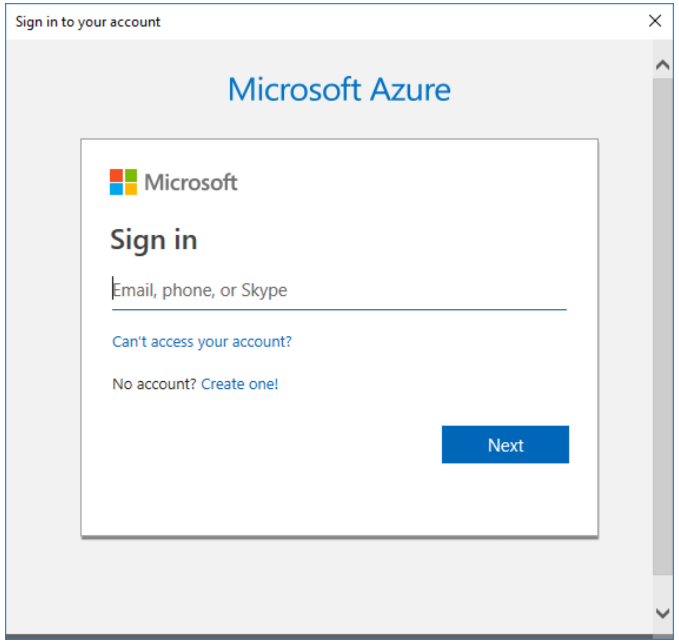
Create a Virtual Machine (PowerShell)

Connect to Your Azure Account

Enter the following cmdlet in PowerShell.

Connect-AzureRmAccount

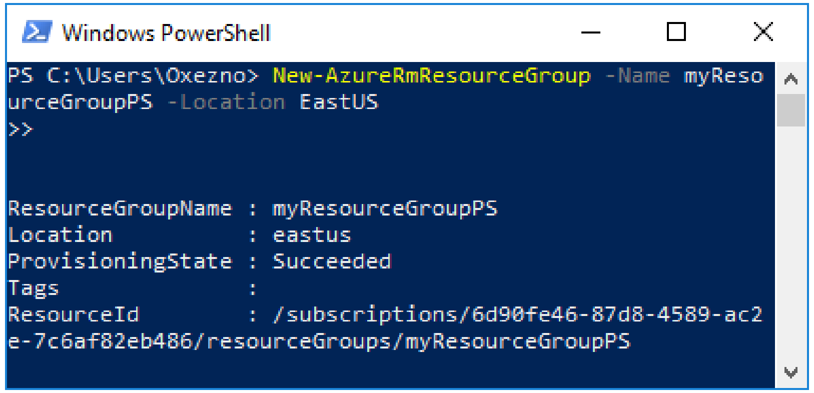
The screen will pop up and ask for credentials of your account. Enter the credentials and sign in.



Create resource group

Create an Azure resource group with New-AzureRmResourceGroup. A resource group is a logical container into which Azure resources are deployed and managed.

New-AzureRmResourceGroup -Name myResourceGroup -Location EastUS



```
PS C:\Users\Oxezno> New-AzureRmResourceGroup -Name myReso
urceGroupPS -Location EastUS
>>


ResourceGroupName : myResourceGroupPS
Location          : eastus
ProvisioningState : Succeeded
Tags              :
ResourceId        : /subscriptions/6d90fe46-87d8-4589-ac2
e-7c6af82eb486/resourceGroups/myResourceGroupPS
```

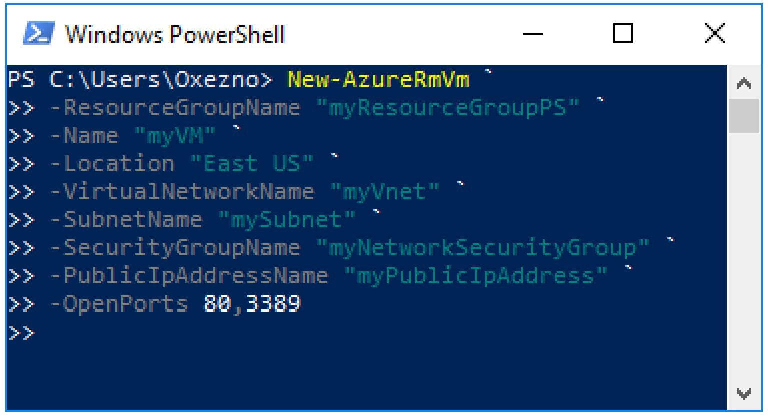
Create a Virtual Machine (PowerShell)

Create virtual machine

Create a VM with New-AzureRmVM. Provide names for each of the resources and the New-AzureRmVM cmdlet creates if they don't already exist.

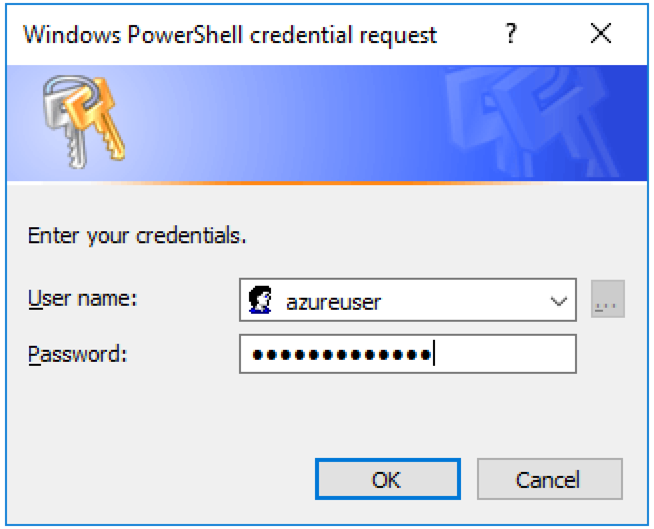
When prompted, provide a username and password to be used as the logon credentials for the VM:

```
New-AzureRmVm `
    -ResourceGroupName "myResourceGroup" `
    -Name "myVM" `
    -Location "East US" `
    -VirtualNetworkName "myVnet" `
    -SubnetName "mySubnet" `
    -SecurityGroupName "myNetworkSecurityGroup" `
    -PublicIpAddressName "myPublicIpAddress" `
    -OpenPorts 80,3389
```



Windows PowerShell

```
PS C:\Users\Oxezno> New-AzureRmVm `
>> -ResourceGroupName "myResourceGroupPS" `
>> -Name "myVM" `
>> -Location "East US" `
>> -VirtualNetworkName "myVnet" `
>> -SubnetName "mySubnet" `
>> -SecurityGroupName "myNetworkSecurityGroup" `
>> -PublicIpAddressName "myPublicIpAddress" `
>> -OpenPorts 80,3389
>>
```



Windows PowerShell credential request

Enter your credentials.

User name: azureuser

Password: •••••••••••••

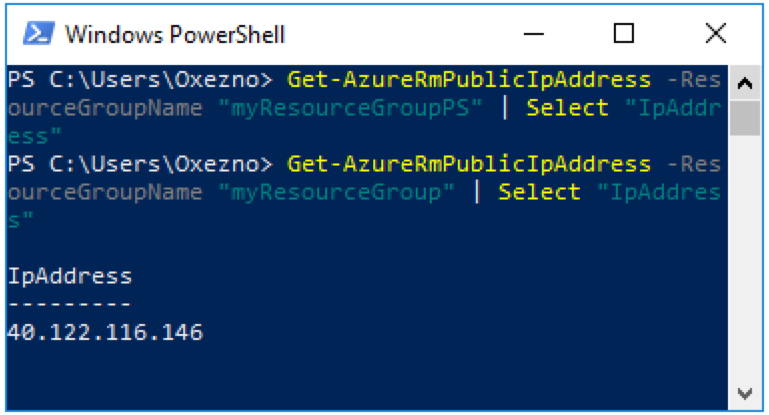
Create a Virtual Machine (PowerShell)

Connect to virtual machine

After the deployment has completed, RDP to the VM. To see your VM in action, the IIS web server is then installed.

To see the public IP address of the VM, use the [Get-AzureRmPublicIpAddress]() cmdlet:

Get-AzureRmPublicIpAddress -ResourceGroupName "myResourceGroup" | Select "IpAddress“



```
PS C:\Users\Oxezno> Get-AzureRmPublicIpAddress -Res
ourceGroupName "myResourceGroupPS" | Select "IpAddr
ess"
PS C:\Users\Oxezno> Get-AzureRmPublicIpAddress -Res
ourceGroupName "myResourceGroup" | Select "IpAddres
s"

IpAddress
---------
40.122.116.146
```

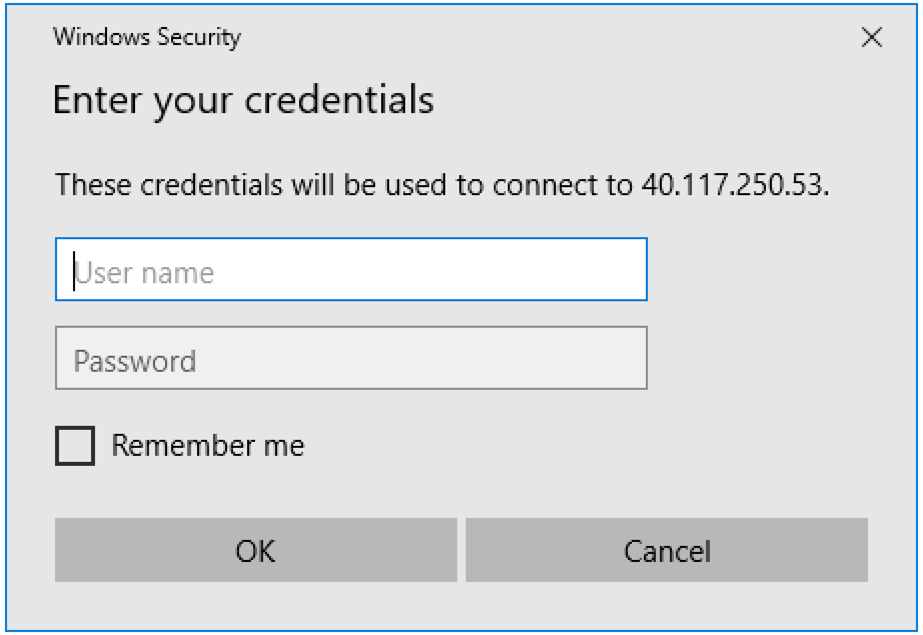
Use the following command to create a remote desktop session from your local computer. Replace the IP address with the public IP address of your VM.

mstsc /v:publicIpAddress

Create a Virtual Machine (PowerShell)

In the **Windows Security** window, select **More choices**, and then select **Use a different account**. Type the username as **localhost***username*, enter password you created for the virtual machine, and then click **OK**.

You may receive a certificate warning during the sign-in process. Click **Yes** or **Continue** to create the connection



Windows Security

Enter your credentials

These credentials will be used to connect to 40.117.250.53.

Create a Virtual Machine (CLI)

Connect to Your Azure Account

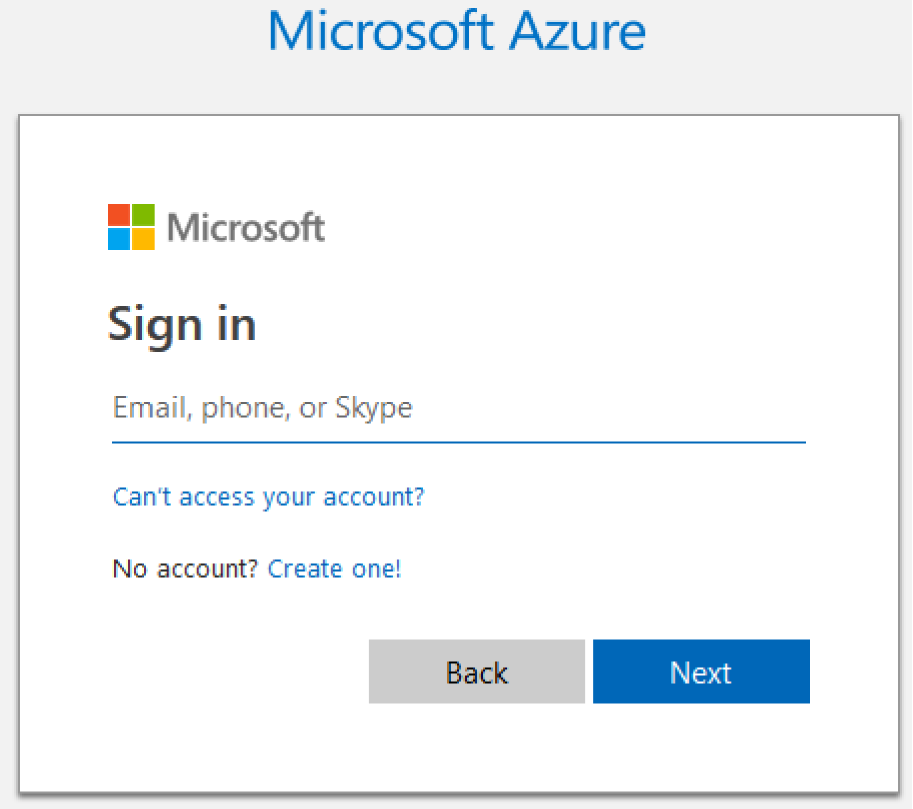
You can now run the Azure CLI with the az command from either Windows Command Prompt or PowerShell. PowerShell offers some tab completion features not available from Windows Command Prompt. To sign in, run the command:

```
az login
```

If the CLI can open your default browser, it will do so and load a sign-in page.

Otherwise, you need to open a browser page and follow the instructions on the command line to enter an authorization code after navigating to https://aka.ms/devicelogin in your browser.

Sign in with your account credentials in the browser.



Microsoft Azure

Microsoft

Sign in

Email, phone, or Skype

Can't access your account?

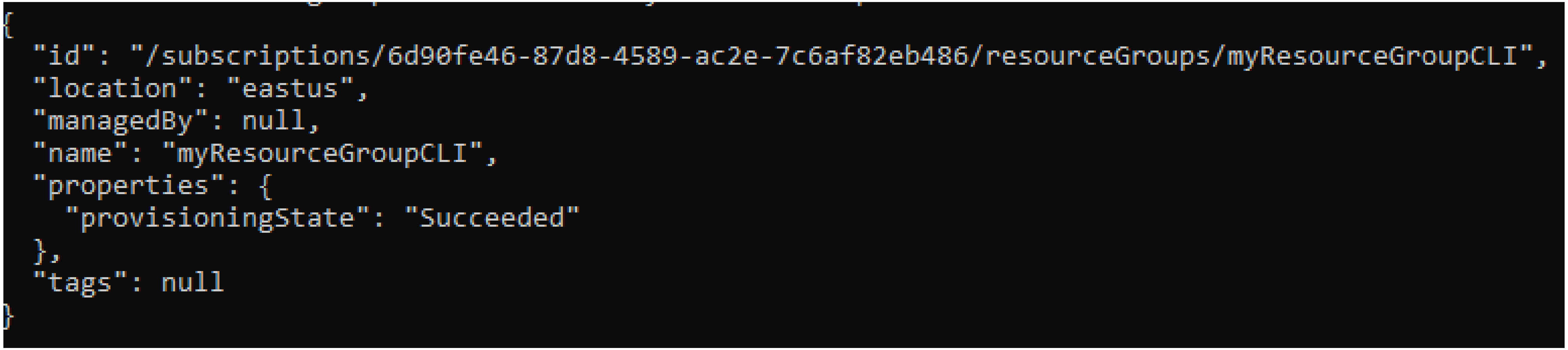
No account? Create one!

Create a Virtual Machine (CLI)

Create a resource group

Create a resource group with the az group create command. An Azure resource group is a logical container into which Azure resources are deployed and managed. The following example creates a resource group named *myResourceGroup* in the *eastus* location:

```
az group create --name myResourceGroupCLI --location eastus
```



```
{
  "id": "/subscriptions/6d90fe46-87d8-4589-ac2e-7c6af82eb486/resourceGroups/myResourceGroupCLI",
  "location": "eastus",
  "managedBy": null,
  "name": "myResourceGroupCLI",
  "properties": {
    "provisioningState": "Succeeded"
  },
  "tags": null
}
```

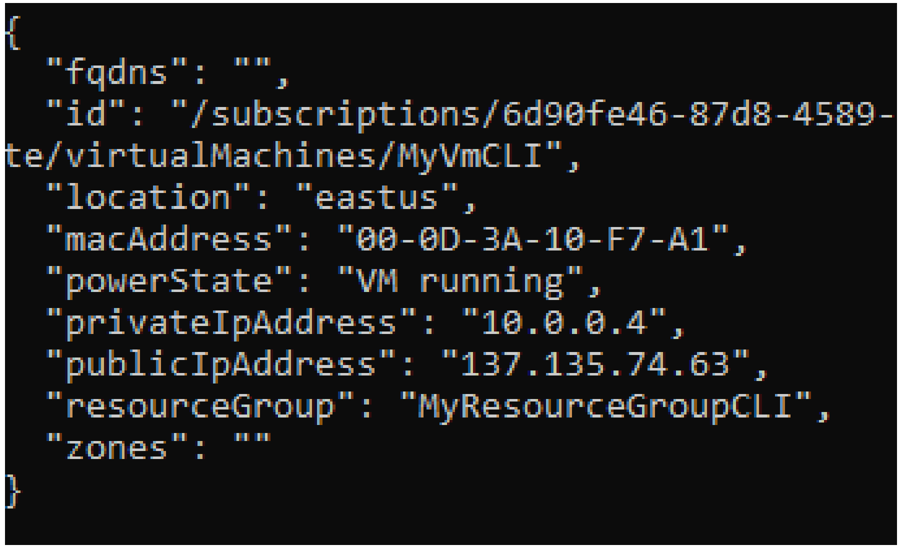
Create a Virtual Machine (CLI)

Create virtual machine

Create a VM with az vm create. The following example creates a VM named *myVM*. This example uses *azureuser* for an administrative user name and *myPassword12* as the password. Update these values to something appropriate to your environment. These values are needed when you connect to the VM.

az vm create -n MyVmCLI -g MyResourceGroupCLI --image Win2012R2Datacenter

It takes a few minutes to create the VM and supporting resources. The following example output shows the VM create operation was successful.



```
{
  "fqdns": "",
  "id": "/subscriptions/6d90fe46-87d8-4589-
te/virtualMachines/MyVmCLI",
  "location": "eastus",
  "macAddress": "00-0D-3A-10-F7-A1",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "137.135.74.63",
  "resourceGroup": "MyResourceGroupCLI",
  "zones": ""
}
```

Create a Virtual Machine (CLI)

Open port 80 for web traffic

By default, only RDP connections are opened when you create a Windows VM in Azure. Use az vm open-port to open TCP port 80 for use with the IIS web server:

```
az vm open-port --port 80 --resource-group myResourceGroupCLI --name myVMCLI
```

Connect to virtual machine

Use the following command to create a remote desktop session from your local computer. Replace the IP address with the public IP address of your VM. When prompted, enter the credentials used when the VM was created:

```
mstsc /v:publicIpAddress
```

Azure Security Center for VM

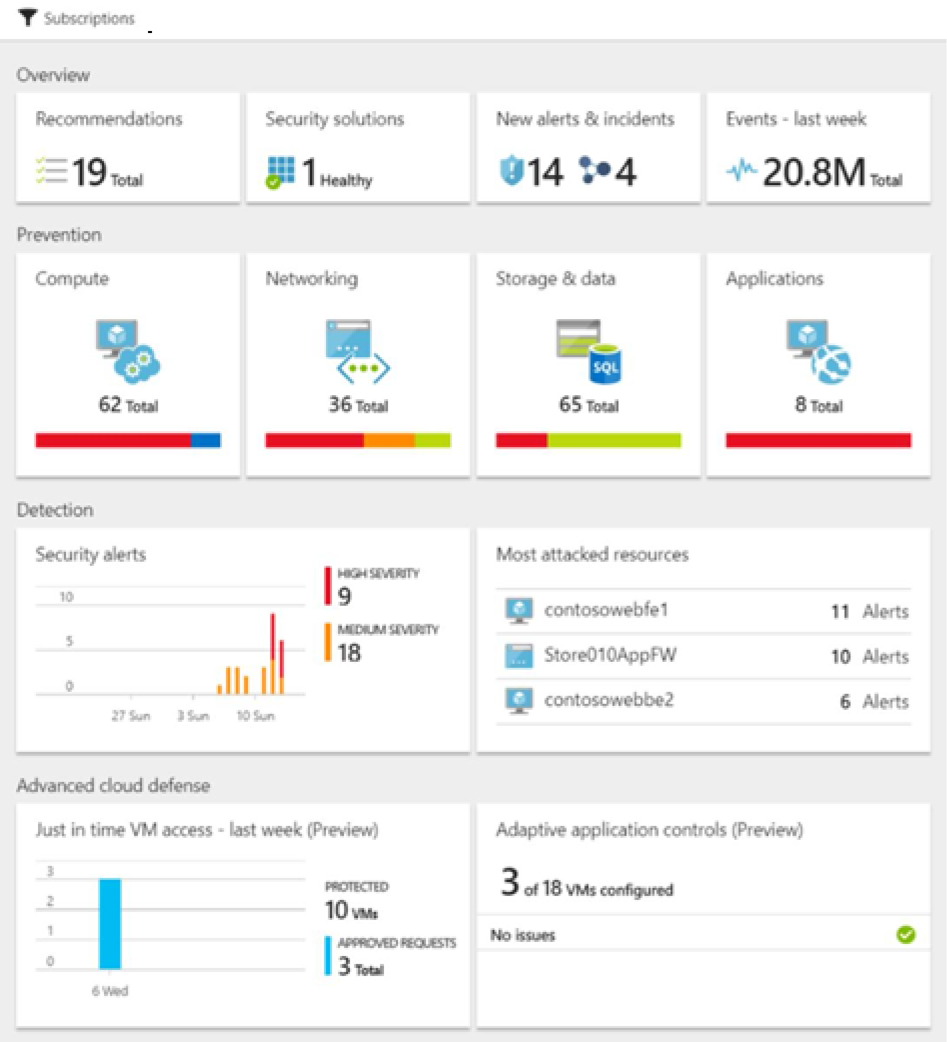
Azure Security Center can help you gain visibility into your Azure resource security practices. Security Center offers integrated security monitoring. It can detect threats that otherwise might go unnoticed. Azure Security Center will help you to:

- Set up data collection
- Set up security policies
- View and fix configuration health issues
- Review detected threats

Security Center overview

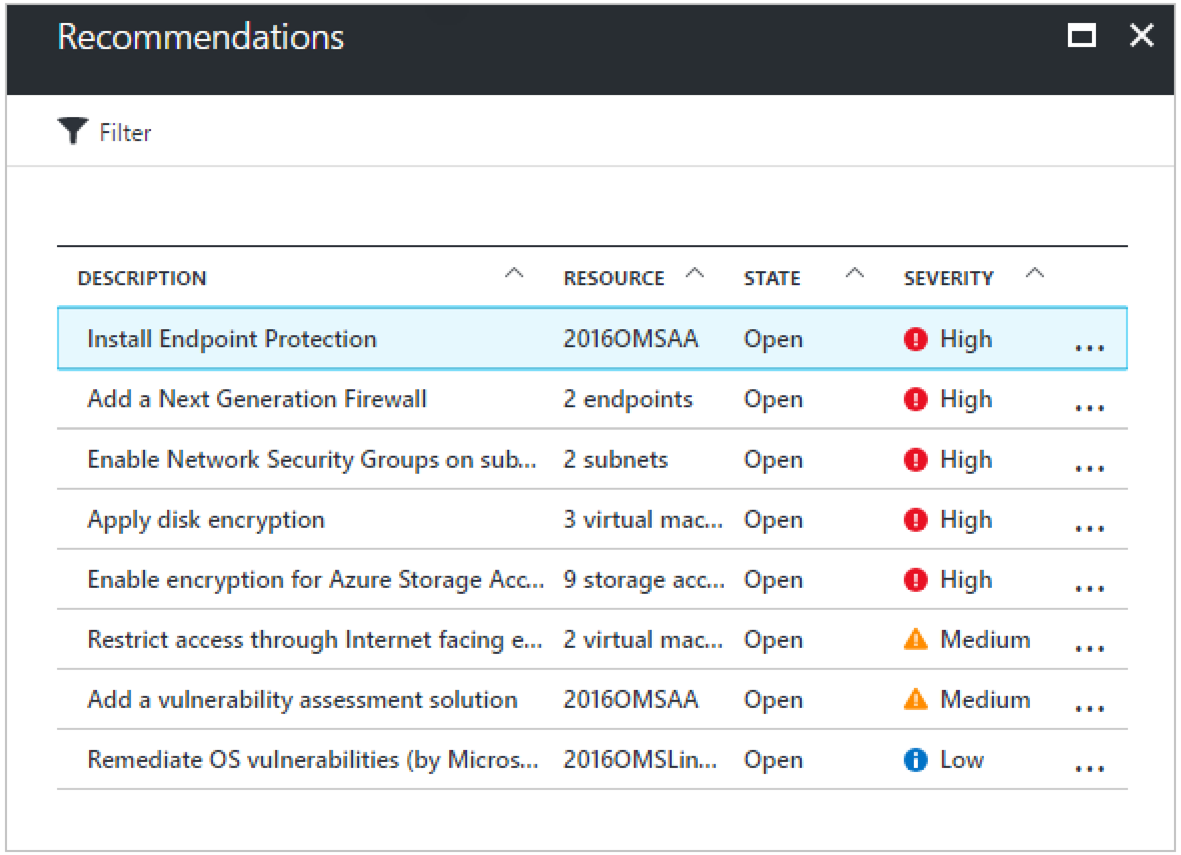
Security Center identifies potential virtual machine (VM) configuration issues and targeted security threats. These might include VMs that are missing network security groups, unencrypted disks, and brute-force Remote Desktop Protocol (RDP) attacks. The information is shown on the Security Center dashboard in easy-to-read graphs.

To access the Security Center dashboard, in the Azure portal, on the menu, select **Security Center**. On the dashboard, you can see the security health of your Azure environment, find a count of current recommendations, and view the current state of threat alerts. You can expand each high-level chart to see more detail.



Security Center overview

Security Center goes beyond data discovery to provide recommendations for issues that it detects. For example, if a VM was deployed without an attached network security group, Security Center displays a recommendation, with remediation steps you can take. You get automated remediation without leaving the context of Security Center.



Recommendations

Filter

DESCRIPTION	RESOURCE	STATE	SEVERITY	
Install Endpoint Protection	2016OMSAA	Open	❗ High	...
Add a Next Generation Firewall	2 endpoints	Open	❗ High	...
Enable Network Security Groups on sub...	2 subnets	Open	❗ High	...
Apply disk encryption	3 virtual mac...	Open	❗ High	...
Enable encryption for Azure Storage Acc...	9 storage acc...	Open	❗ High	...
Restrict access through Internet facing e...	2 virtual mac...	Open	⚠ Medium	...
Add a vulnerability assessment solution	2016OMSAA	Open	⚠ Medium	...
Remediate OS vulnerabilities (by Micros...	2016OMSLin...	Open	ℹ Low	...

Set up data collection

Before you can get visibility into VM security configurations, you need to set up Security Center data collection. This involves turning on data collection which automatically installs the Microsoft Monitoring Agent on all the VMs in your subscription.

1. On the Security Center dashboard, click **Security policy**, and then select your subscription.
2. For **Data collection**, in **Auto Provisioning** select **On**.
3. For **Default workspace configuration** leave it as **Use workspace(s) created by Security Center (default)**.
4. Under **Security Events** keep the default option of **Common**.
5. Click **Save** at the top of the page.

The Security Center data collection agent is then installed on all VMs, and data collection begins.

Set up a security policy

Security policies are used to define the items for which Security Center collects data and makes recommendations. You can apply different security policies to different sets of Azure resources. Although by default Azure resources are evaluated against all policy items, you can turn off individual policy items for all Azure resources or for a resource group.

To set up a security policy for an entire subscription:

1. On the Security Center dashboard, select **Security policy** and then select your subscription.
2. On the **Security policy** blade, select **Security policy**.
3. On the ** Security policy - Security policy ** blade, turn on or turn off policy items that you want to apply to the subscription.
4. When you're finished selecting your settings, select **Save** at the top of the blade.

View VM configuration health

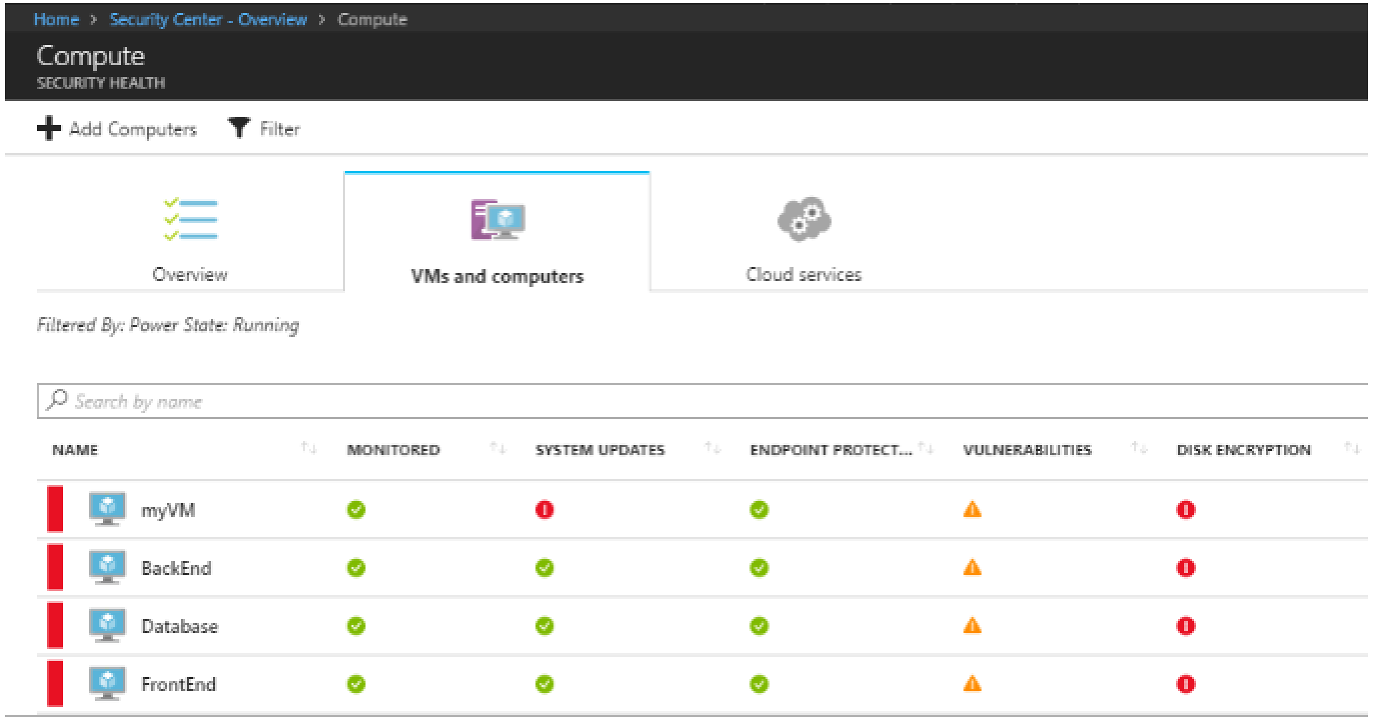
After you've turned on data collection and set a security policy, Security Center begins to provide alerts and recommendations. As VMs are deployed, the data collection agent is installed. Security Center is then populated with data for the new VMs. For in-depth information about VM configuration health, see Protect your VMs in Security Center.

As data is collected, the resource health for each VM and related Azure resource is aggregated. The information is shown in an easy-to-read chart.

View VM configuration health

To view resource health:

1. On the Security Center dashboard, under **Prevention**, select **Compute**.
2. On the **Compute** blade, select **VMs and computers**. This view provides a summary of the configuration status for all your VMs.



Home > Security Center - Overview > Compute

Compute

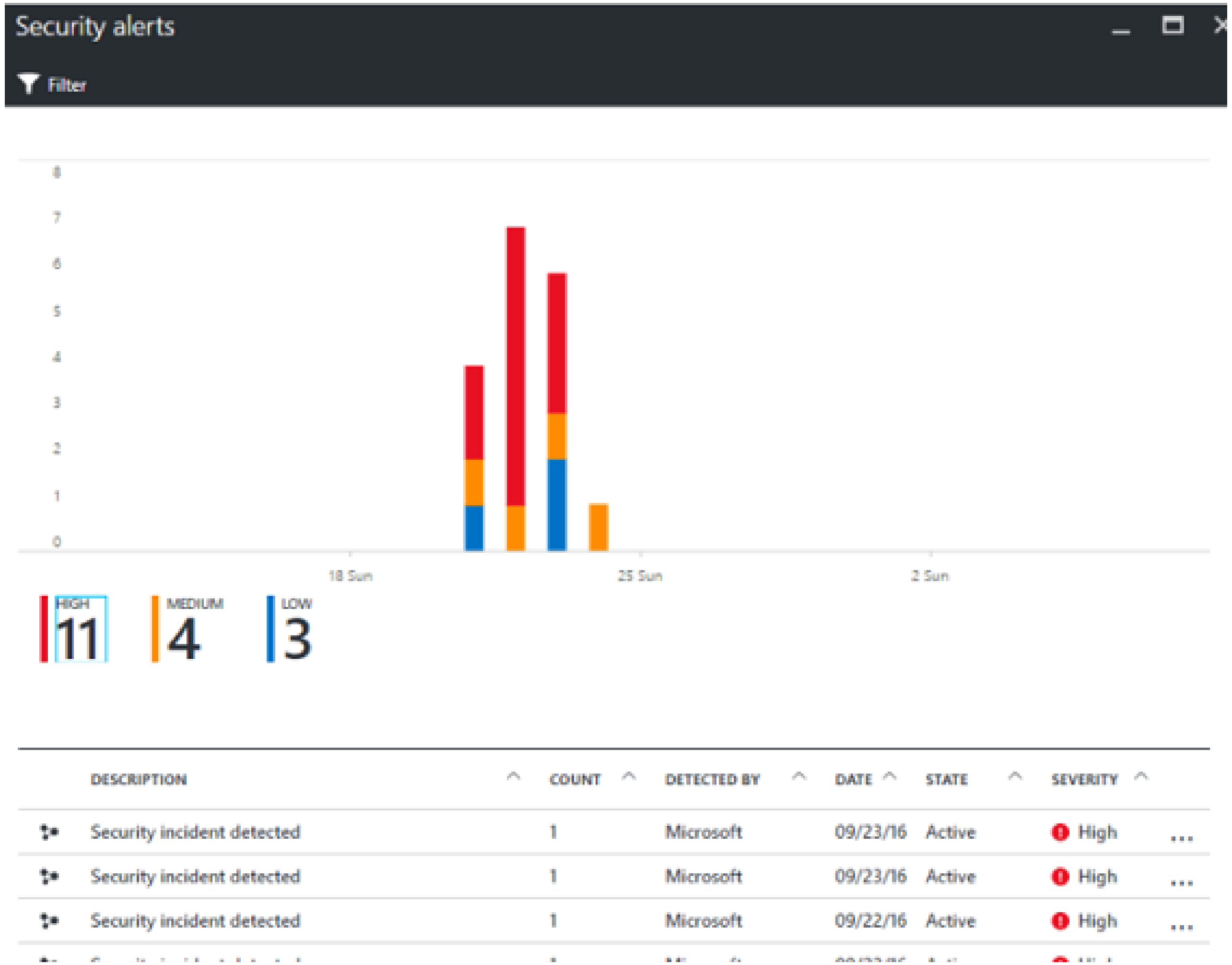
SECURITY HEALTH

Filtered By: Power State: Running

NAME	MONITORED	SYSTEM UPDATES	ENDPOINT PROTECT...	VULNERABILITIES	DISK ENCRYPTION
myVM	✓	❗	✓	⚠	❗
BackEnd	✓	✓	✓	⚠	❗
Database	✓	✓	✓	⚠	❗
FrontEnd	✓	✓	✓	⚠	❗

View detected threats

In addition to resource configuration recommendations, Security Center displays threat detection alerts. The security alerts feature aggregates data collected from each VM, Azure networking logs, and connected partner solutions to detect security threats against Azure resources. For in-depth information about Security Center threat detection capabilities.



DESCRIPTION	COUNT	DETECTED BY	DATE	STATE	SEVERITY
Security incident detected	1	Microsoft	09/23/16	Active	● High
Security incident detected	1	Microsoft	09/23/16	Active	● High
Security incident detected	1	Microsoft	09/22/16	Active	● High