Using Microsoft Azure

to build your own **Test Lab**

Microsoft Azure

Abstract:

(jump to TOC)

This document provides a demonstration of how to use Microsoft Azure to build your own small test lab, at about $20-$40 per month. The intent of this overview is to help people who are new to Azure to get a basic comfort and familiarity with Azure for IaaS (infrastructure as a service).

Intended Audience:

(jump to TOC)

This document is high-level and is intended to be read by persons holding a Windows 2000 or higher MSCE certification, or having equivalent experience.

Document Revision and History:

(jump to TOC)

version	date	description
1.0	9/3/2018	initial publication to blog
1.1	9/4/2018	added descriptions of VM states
1.2	10/1/2018	• added info about standard SSDs for VMs • added info about NSG ACLs • added the '-force' switch to the runbook commands • added a section on Security Center • added a section on VM Update Management
2.0	10/7/2018	• took new screenshots after Microsoft updated the Azure user interface • added information about cost per resource • added information about ARM templates
2.1	10/10/2018	added a section on Azure Advisor

Freeware License and Disclaimer:

(jump to TOC)

This document is freeware, done in the spirit of open-source. You may distribute unchanged copies of this document freely to anyone at any time. Care has been taken to cite contributing sources and individuals, please do the same. If you find errors in anything contained herein, please comment on them and/or contact me so that we may all help the community.

About the Author:

(jump to TOC)

Daniel L. Benway

Active Directory and Information Security Architect / Engineer
BSc CS, MCSE (NT4, 2000), MCTS (SCCM 2012), CISSP, Security+, Network+, CCNA (2.0), CLP (AD R4)

LinkedIn	http://www.LinkedIn.com/in/DanielLBenway
Blog	http://www.DanielLBenway.net
twitter	@Daniel_L_Benway

Special Thanks:

(jump to TOC)

- Special thanks Mike Leary, MS SPFE (Microsoft Senior Premier Field Engineer) for taking the time to answer a few questions on this topic.

Table of Contents:

General Information:

(jump to TOC)

Cost Savings:

- Be sure to use the smallest size VMs that will meet your needs, on the least expensive disks (Standard HDDs < Standard SSDs < Premium SSDs < Ultra SSDs), and deallocate them whenever they're not in use. I found that using Standard B1ms (1 VCPU, 2 GB RAM) VMs on Premium SSDs is about as slow as I can tolerate, but you can go even smaller and cheaper if you are more patient than I am.
- A VM (virtual machine) has three states:
  - **running** - VM is allocated and its OS is online
  - **stopped** - VM is allocated but its OS is offline
  - **stopped (deallocated)** - VM is deallocated, so its OS can't be online. This state is how you save the most on your bill.
- Shutting down a VM within its OS changes the VM's state to 'stopped'. 'Stopping' a VM from within the Azure Portal (or by PowerShell) changes its state to 'stopped (deallocated)'. Based on System Log event ID 6006, it looks like 'stopping' a Windows VM does indeed perform a graceful OS shutdown before the VM changes to 'stopped (deallocated)'.
- Set each VM to auto-shutdown at, say, 02:00AM daily, and write an automation account runbook to 'stop' each VM at, say, 02:15AM daily. This will shutdown and deallocate your VMs in case you forget to 'stop' them yourself (the auto-shutdown isn't technically necessary before the 'stop', but it is good practice).
- When you delete a VM, be sure all of its items in its Resource Group(s) are also deleted, in order to save the most money (simply deleting a VM does NOT remove all of its resources).

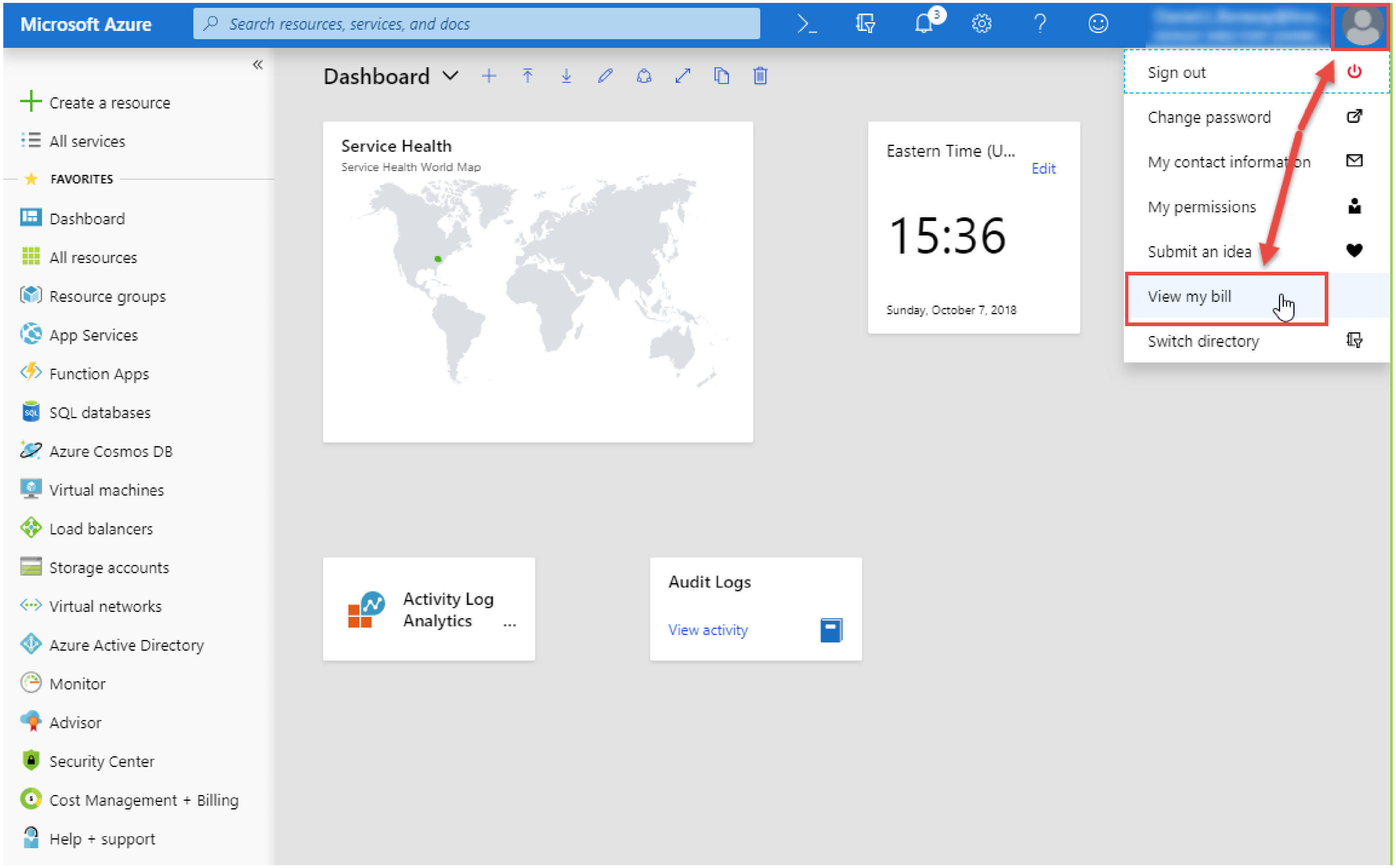
Networking:

- All subnets within a Virtual Network are fully routed amongst themselves by default.
- A VM in Azure, by default, has outgoing Internet access.
- To access your VMs, set up an RDP (remote desktop protocol) jump box that is:
  - within the same Virtual Network as your VMs.
  - has a dynamic public IP using Azure's public DNS, and an open incoming port for RDP (something other than 3389, for obscurity).
- If you want an inexpensive way to connect an on-prem test lab with your Azure test lab, you can use a Unified Secure Gateway to set up a VPN between the two (it looks like there are several vendors, priced $100 - $200 on Amazon).

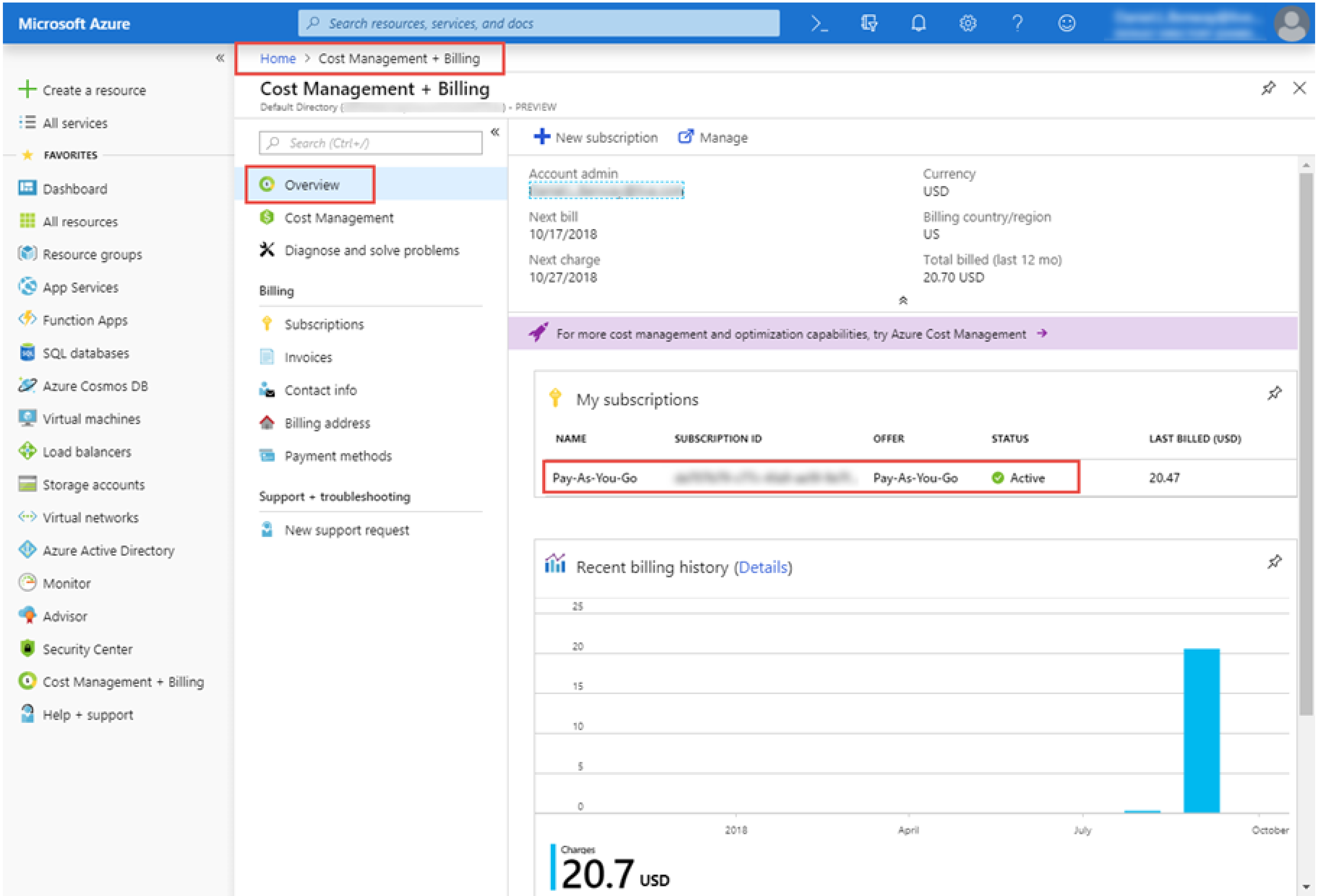
Your Azure Bill:

[(jump to TOC)]

Be sure to check your bill regularly to avoid any surprises. Be sure to read and follow the cost savings steps described earlier in this document!



Go to ‘Overview’ and LC (left click) your subscription…



Cost Management + Billing

Default Directory ([redacted]) - PREVIEW

Account admin
[redacted]

Currency
USD

Next bill
10/17/2018

Billing country/region
US

Next charge
10/27/2018

Total billed (last 12 mo)
20.70 USD

For more cost management and optimization capabilities, try Azure Cost Management →

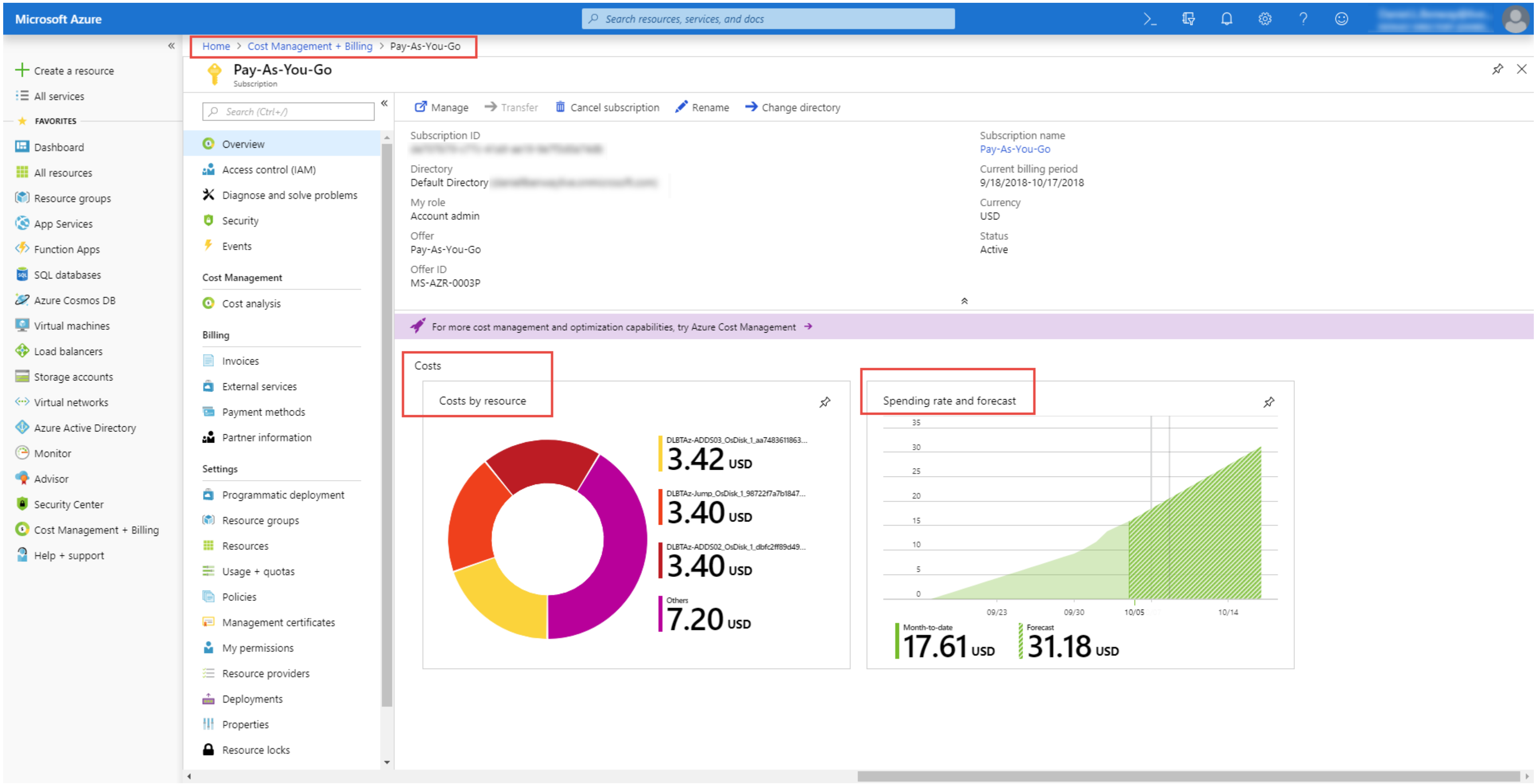
My subscriptions

NAME	SUBSCRIPTION ID	OFFER	STATUS	LAST BILLED (USD)
Pay-As-You-Go	[redacted]	Pay-As-You-Go	✓ Active	20.47

Recent billing history (Details)

Charges
20.7 USD

Use the graphs of costs by resource, and spending rate and forecast:



Subscription ID
[redacted]

Directory
Default Directory [redacted]

My role
Account admin

Offer
Pay-As-You-Go

Offer ID
MS-AZR-0003P

Subscription name
Pay-As-You-Go

Current billing period
9/18/2018-10/17/2018

Currency
USD

Status
Active

For more cost management and optimization capabilities, try Azure Cost Management →

Costs

Costs by resource

DLBTAz-ADDS03_OsDisk_1_aa7483611863...
3.42 USD

DLBTAz-Jump_OsDisk_1_98722f7a7b1847...
3.40 USD

DLBTAz-ADDS02_OsDisk_1_dbfc2ff89d49...
3.40 USD

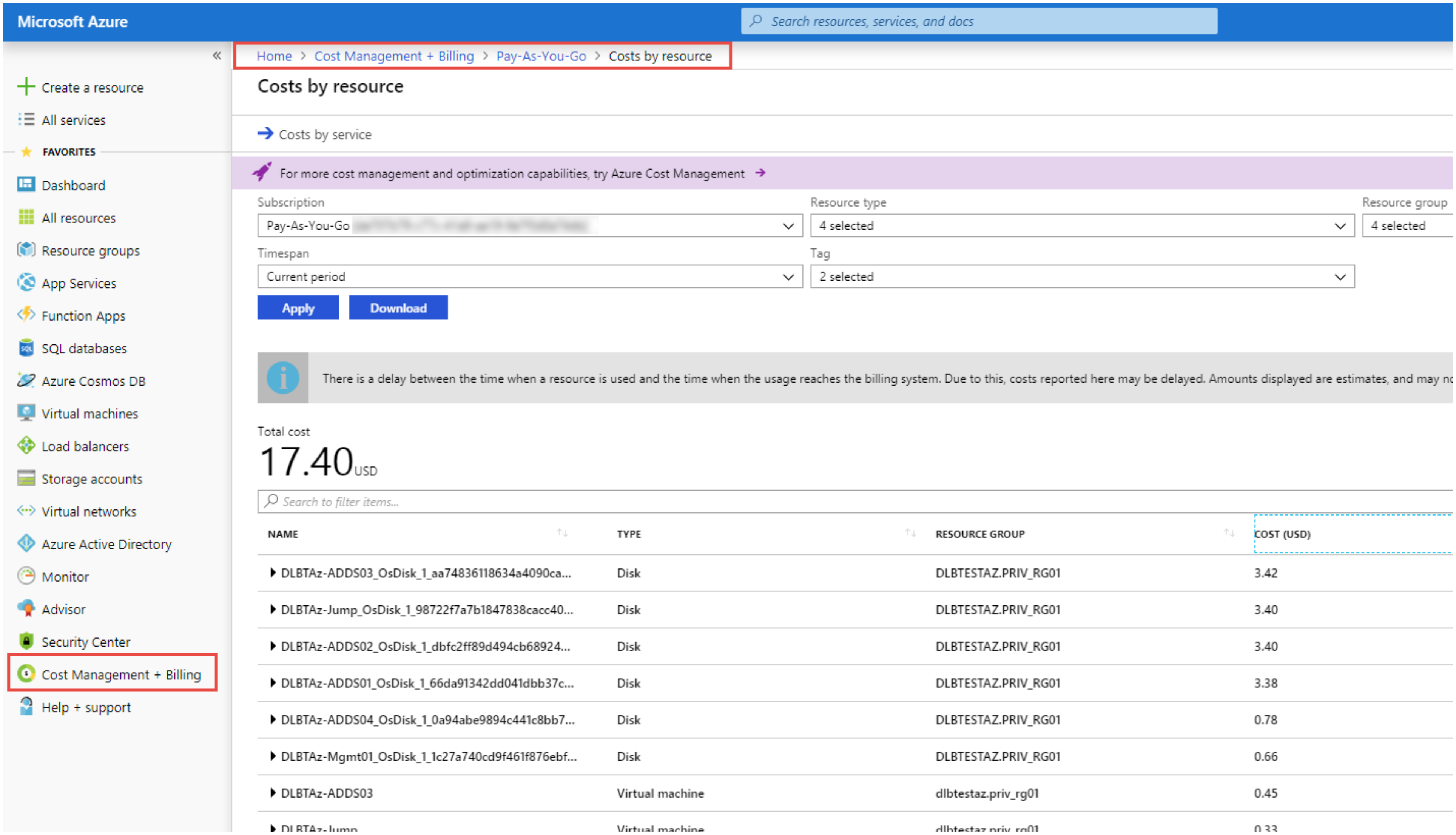
Others
7.20 USD

Spending rate and forecast

Month-to-date
17.61 USD

Forecast
31.18 USD

You can view cost by resource to see how much each of your individual Azure items is costing you:



Costs by resource

Costs by service

For more cost management and optimization capabilities, try Azure Cost Management

Subscription: Pay-As-You-Go [redacted]

Resource type: 4 selected

Resource group: 4 selected

Timespan: Current period

Tag: 2 selected

There is a delay between the time when a resource is used and the time when the usage reaches the billing system. Due to this, costs reported here may be delayed. Amounts displayed are estimates, and may no

Total cost
17.40 USD

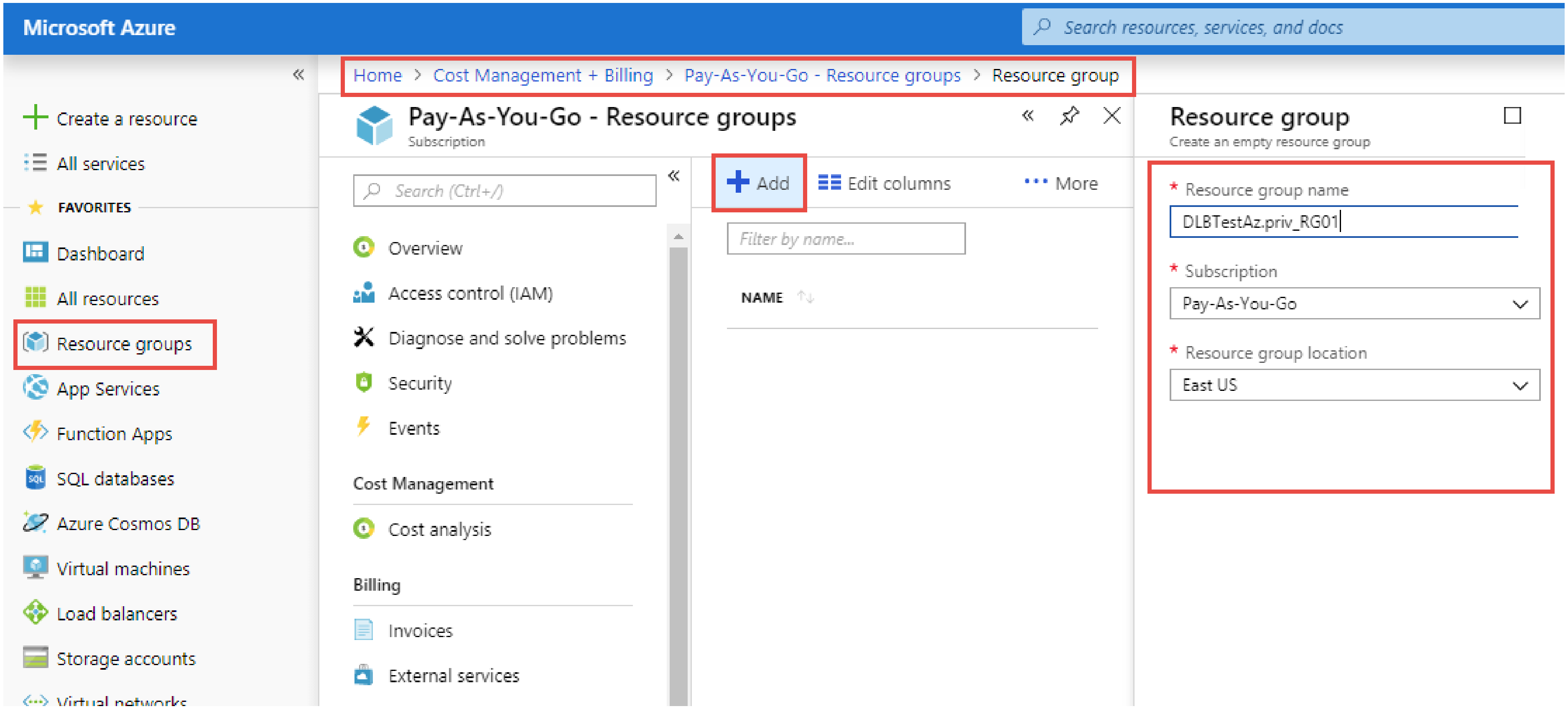
NAME	TYPE	RESOURCE GROUP	COST (USD)
DLBTAz-ADDS03_OsDisk_1_aa74836118634a4090ca...	Disk	DLBTESTAZ.PRIV_RG01	3.42
DLBTAz-Jump_OsDisk_1_98722f7a7b1847838cacc40...	Disk	DLBTESTAZ.PRIV_RG01	3.40
DLBTAz-ADDS02_OsDisk_1_dbfc2ff89d494cb68924...	Disk	DLBTESTAZ.PRIV_RG01	3.40
DLBTAz-ADDS01_OsDisk_1_66da91342dd041dbb37c...	Disk	DLBTESTAZ.PRIV_RG01	3.38
DLBTAz-ADDS04_OsDisk_1_0a94abe9894c441c8bb7...	Disk	DLBTESTAZ.PRIV_RG01	0.78
DLBTAz-Mgmt01_OsDisk_1_1c27a740cd9f461f876ebf...	Disk	DLBTESTAZ.PRIV_RG01	0.66
DLBTAz-ADDS03	Virtual machine	dlbtestaz.priv_rg01	0.45
DLBTAz-Jump	Virtual machine	dlbtestaz.priv_rg01	0.33

Create Your Resource Groups:

(jump to TOC)

You'll need to create three Resource Groups:

1. one for Azure PowerShell -- I named mine: 'AzurePowerShell_RG01', as this is my first Resource Group associated with Azure PowerShell.
2. one for your VMs and associated hardware -- I named mine 'DLBTestAz.priv_RG01' after my test AD Forest name, followed by _RG01 as this is my first Resource Group associated with my AD Forest.
3. one for your Azure Automation Account -- I named mine 'AzureAutomationAccount_RG01', as this is my first Resource Group associated with Azure Automation Accounts.



* Resource group name: DLBTestAz.priv_RG01

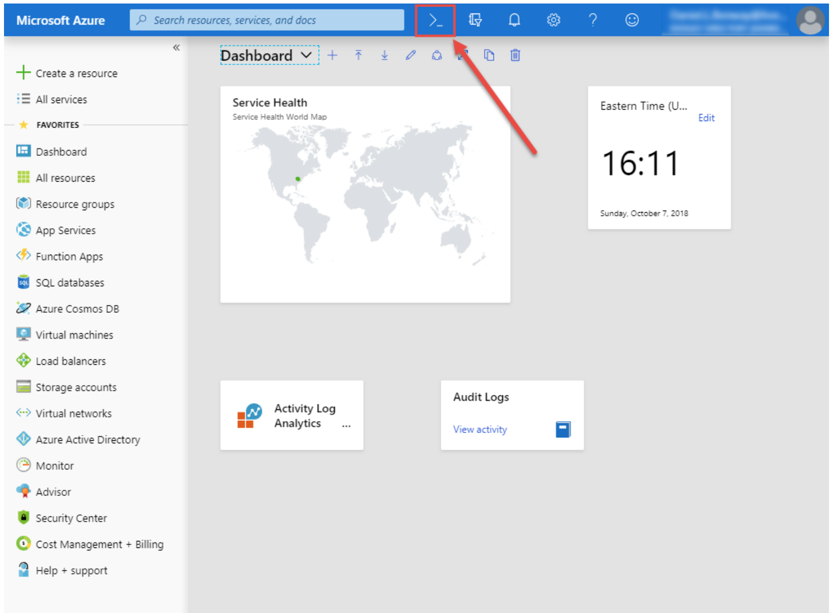
* Subscription: Pay-As-You-Go

* Resource group location: East US

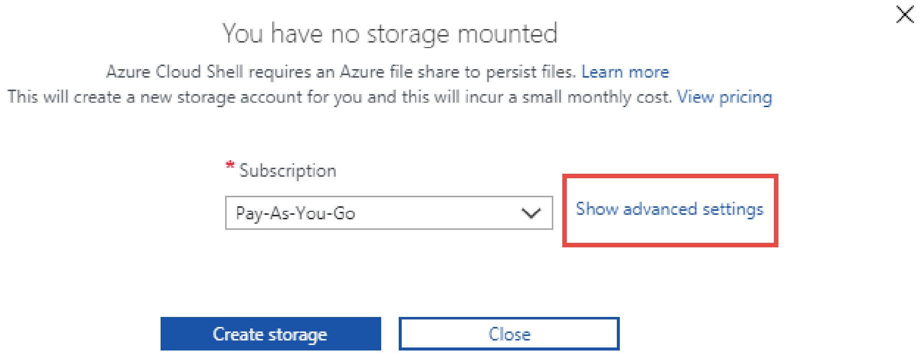
Set Up Azure PowerShell:

[(jump to TOC)]

Click the '>_' in the upper right part of the screen to start the Azure PowerShell creation process...



On the next screen, choose to show advanced settings:



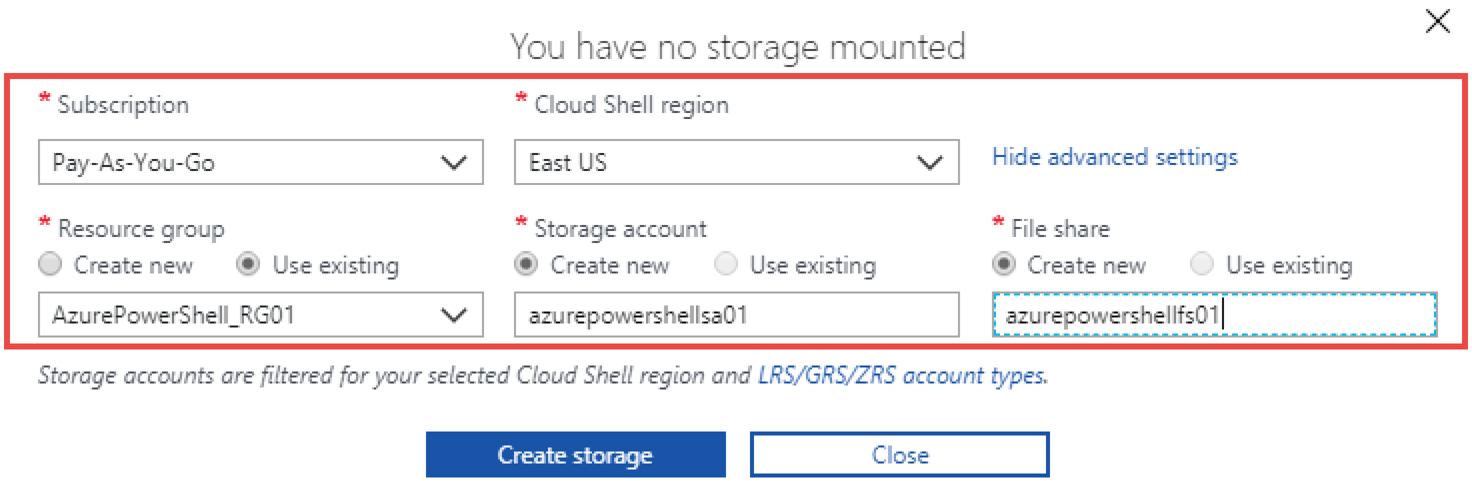
You have no storage mounted

Azure Cloud Shell requires an Azure file share to persist files. Learn more
This will create a new storage account for you and this will incur a small monthly cost. View pricing

* Subscription

Pay-As-You-Go

Choose the Azure PowerShell Resource Group you created earlier, and specify good names for your new ‘storage account’ and ‘file share’:



You have no storage mounted

* Subscription: Pay-As-You-Go

* Cloud Shell region: East US

Hide advanced settings

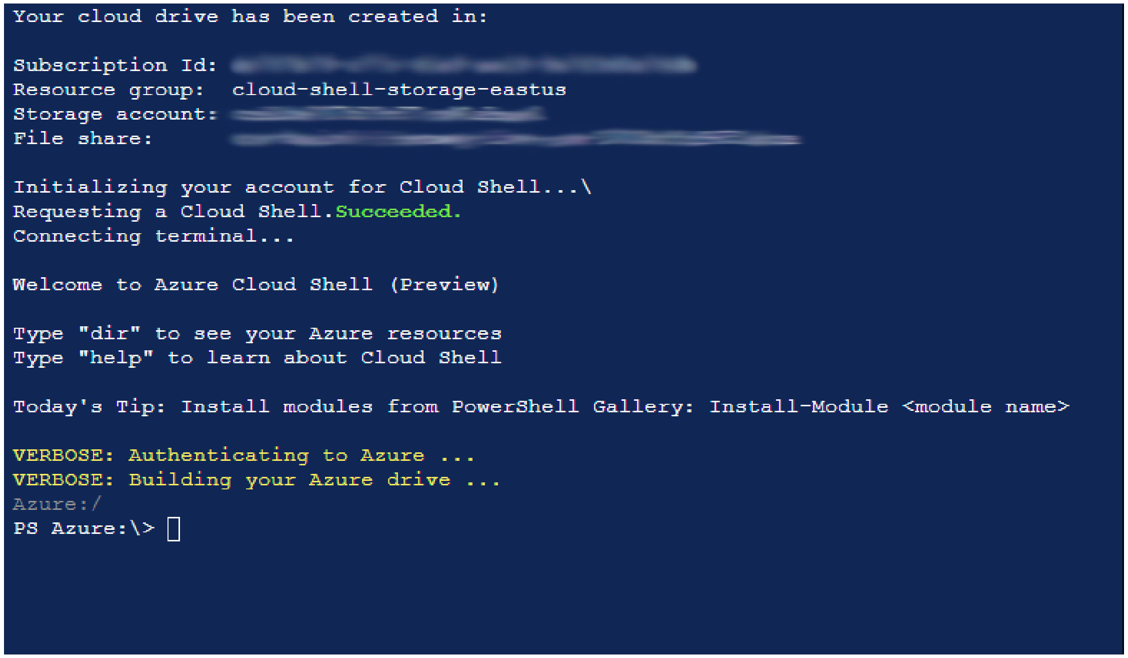
* Resource group: ○ Create new ● Use existing — AzurePowerShell_RG01

* Storage account: ● Create new ○ Use existing — azurepowershellsa01

* File share: ● Create new ○ Use existing — azurepowershellfs01

Storage accounts are filtered for your selected Cloud Shell region and LRS/GRS/ZRS account types.

You should see that your Azure Cloud Shell was created successfully:

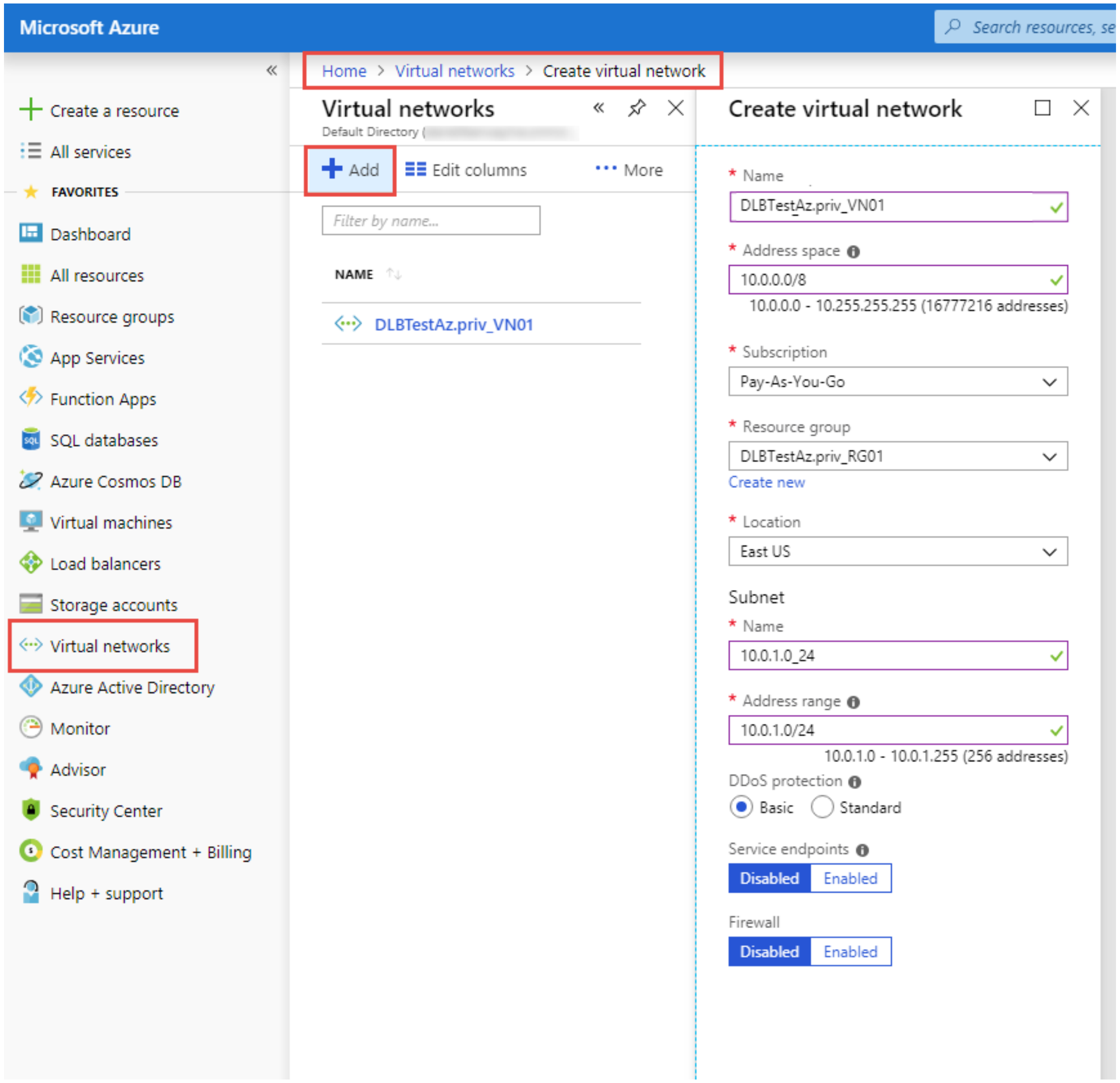


```
Your cloud drive has been created in:

Subscription Id: [redacted]
Resource group:  cloud-shell-storage-eastus
Storage account: [redacted]
File share:      [redacted]

Initializing your account for Cloud Shell...\
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell (Preview)

Type "dir" to see your Azure resources
Type "help" to learn about Cloud Shell

Today's Tip: Install modules from PowerShell Gallery: Install-Module <module name>

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
Azure:/
PS Azure:\>
```

Create Your Virtual Network:

(jump to TOC)

Create your Virtual Network, and first subnet. I chose an address space of 10.0.0.0/8 so that I could use a 24-bit mask and create as many as 65,534 subnets with 254 hosts per subnet. I chose to create three subnets: 10.0.1.0/24, 10.0.2.0/24, and 10.0.3.0/24.



* Name: DLBTestAz.priv_VN01

* Address space: 10.0.0.0/8

10.0.0.0 - 10.255.255.255 (16777216 addresses)

* Subscription: Pay-As-You-Go

* Resource group: DLBTestAz.priv_RG01

Create new

* Location: East US

Subnet

* Name: 10.0.1.0_24

* Address range: 10.0.1.0/24

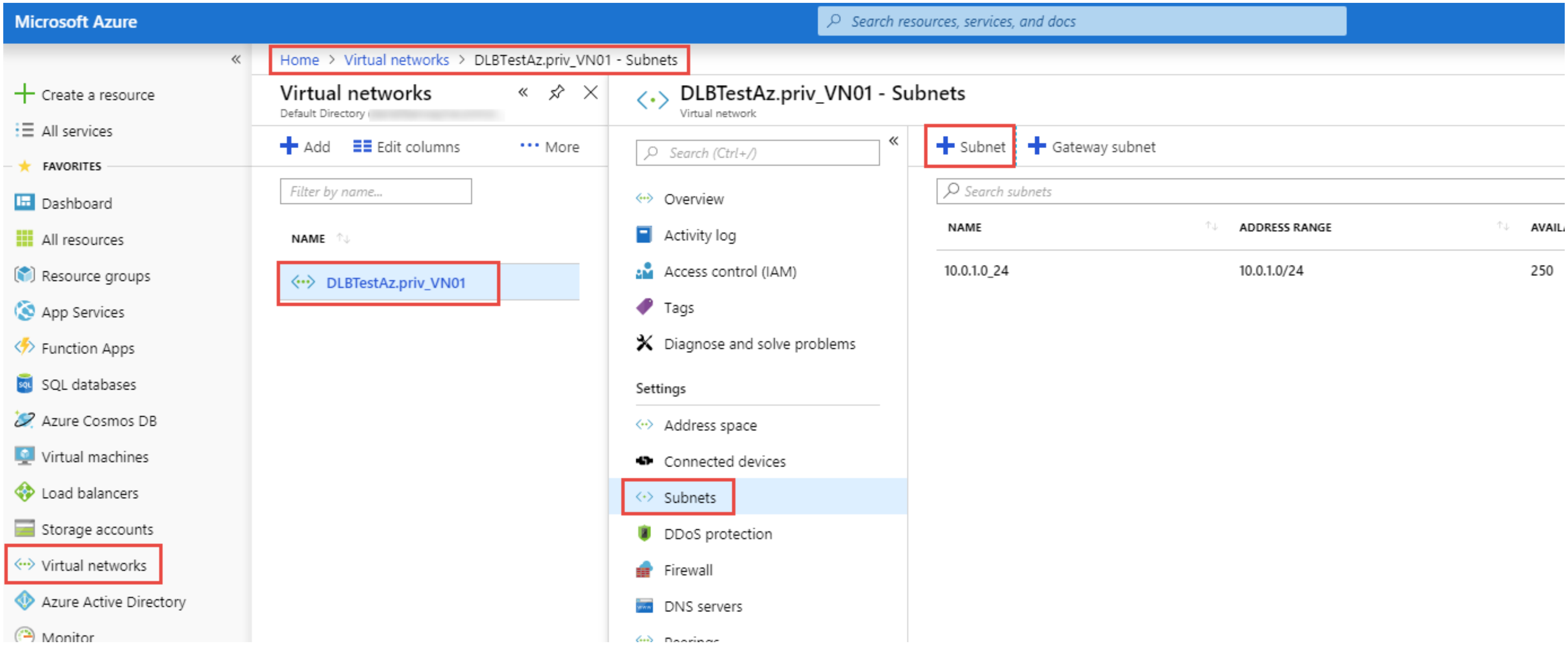
10.0.1.0 - 10.0.1.255 (256 addresses)

DDoS protection: ● Basic ○ Standard

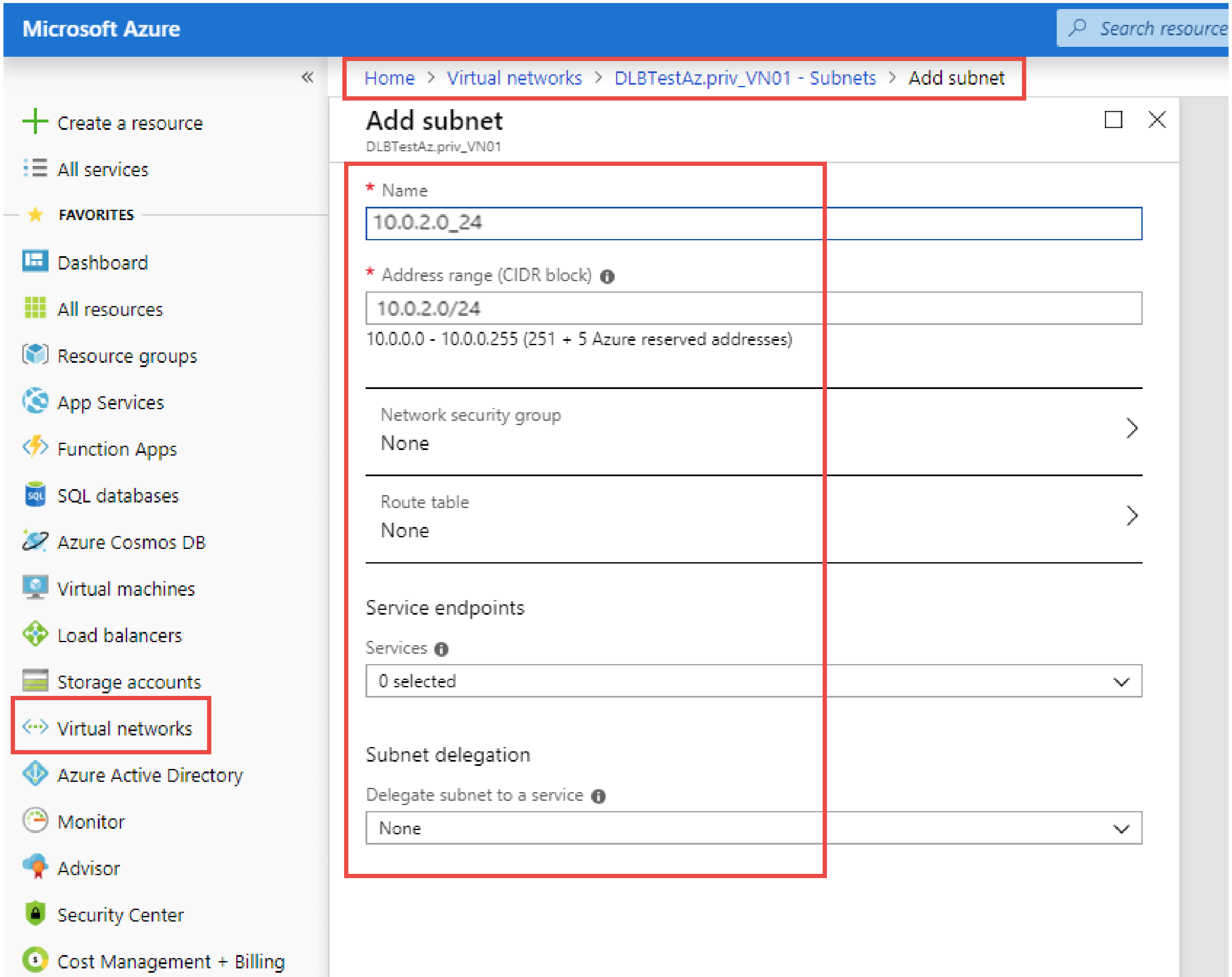
Service endpoints: **Disabled** Enabled

Firewall: **Disabled** Enabled

Create your second subnet:



NAME	ADDRESS RANGE	AVAIL
10.0.1.0_24	10.0.1.0/24	250



Home > Virtual networks > DLBTestAz.priv_VN01 - Subnets > Add subnet

Add subnet

DLBTestAz.priv_VN01

* Name

10.0.2.0_24

* Address range (CIDR block)

10.0.2.0/24

10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses)

Network security group

None

Route table

None

Service endpoints

Services

0 selected

Subnet delegation

Delegate subnet to a service

None

Create your third subnet similarly, using a name of 10.0.3.0_24 with an address range of 10.0.3.0/24.

Create Your VMs:

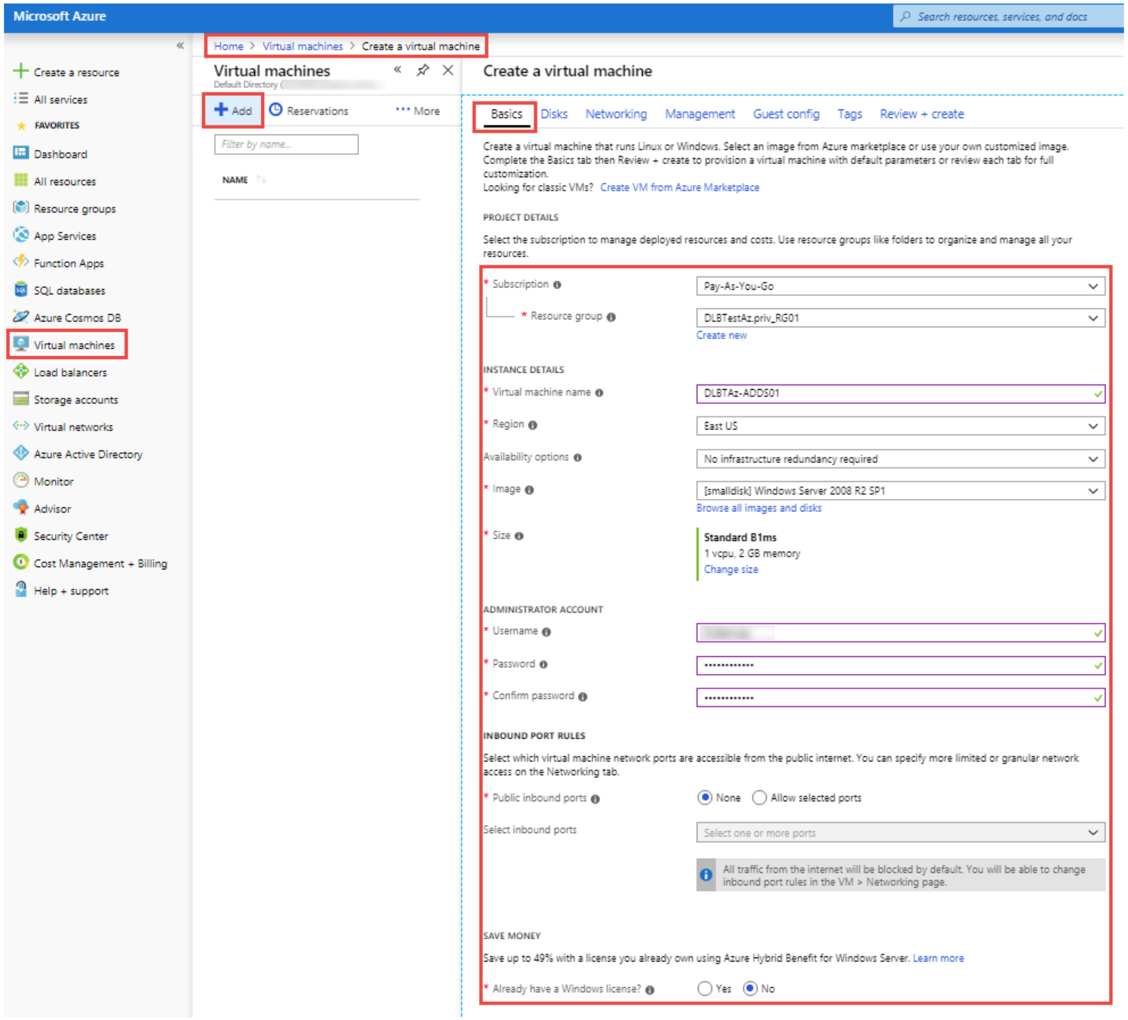
(jump to TOC)

I chose to create six VMs, with the 2008 machines on subnet 1, the 2012 machines on subnet 2, and the 2016 machines on subnet 3:

DLBTAz-ADDS01.DLBTestAz.priv	2008 R2 SP1 DC (domain controller)	10.0.1.0/24 subnet
DLBTAz-ADDS02.DLBTestAz.priv	2012 R2 DC	10.0.2.0/24 subnet
DLBTAz-ADDS03.DLBTestAz.priv	2016 DC	10.0.3.0/24 subnet
DLBTAz-ADDS04.DLBTestAz.priv	1709 SAC (semi-annual channel) DC	10.0.3.0/24 subnet
DLBTAz-Jump.DLBTestAz.priv	RDP jump box (sits on the public Internet, and the 10.0.3.0/24 internal private subnet, and provides front-end access to the back-end VMs of the lab)	10.0.3.0/24 subnet plus a dynamic public IP
DLBTAz-Mgmt01.DLBTestAz.priv	2016 management server (hosting MS Admin Center)	10.0.3.0/24 subnet

Create Your Test VMs (not the RDP Jump Box):

My four DCs and one management server VMs are all created similarly, so use the following steps for each VM you create (the RDP jump box needs additional configuration that will be shown after these first five VMs are created):



Create a virtual machine

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: Pay-As-You-Go
* Resource group: DLBTestAz.priv_RG01
Create new

INSTANCE DETAILS

* Virtual machine name: DLBTAz-ADDS01
* Region: East US
Availability options: No infrastructure redundancy required
* Image: [smalldisk] Windows Server 2008 R2 SP1
Browse all images and disks
* Size: **Standard B1ms**
1 vcpu, 2 GB memory
Change size

ADMINISTRATOR ACCOUNT

* Username: [redacted]
* Password: ••••••••••••
* Confirm password: ••••••••••••

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: Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

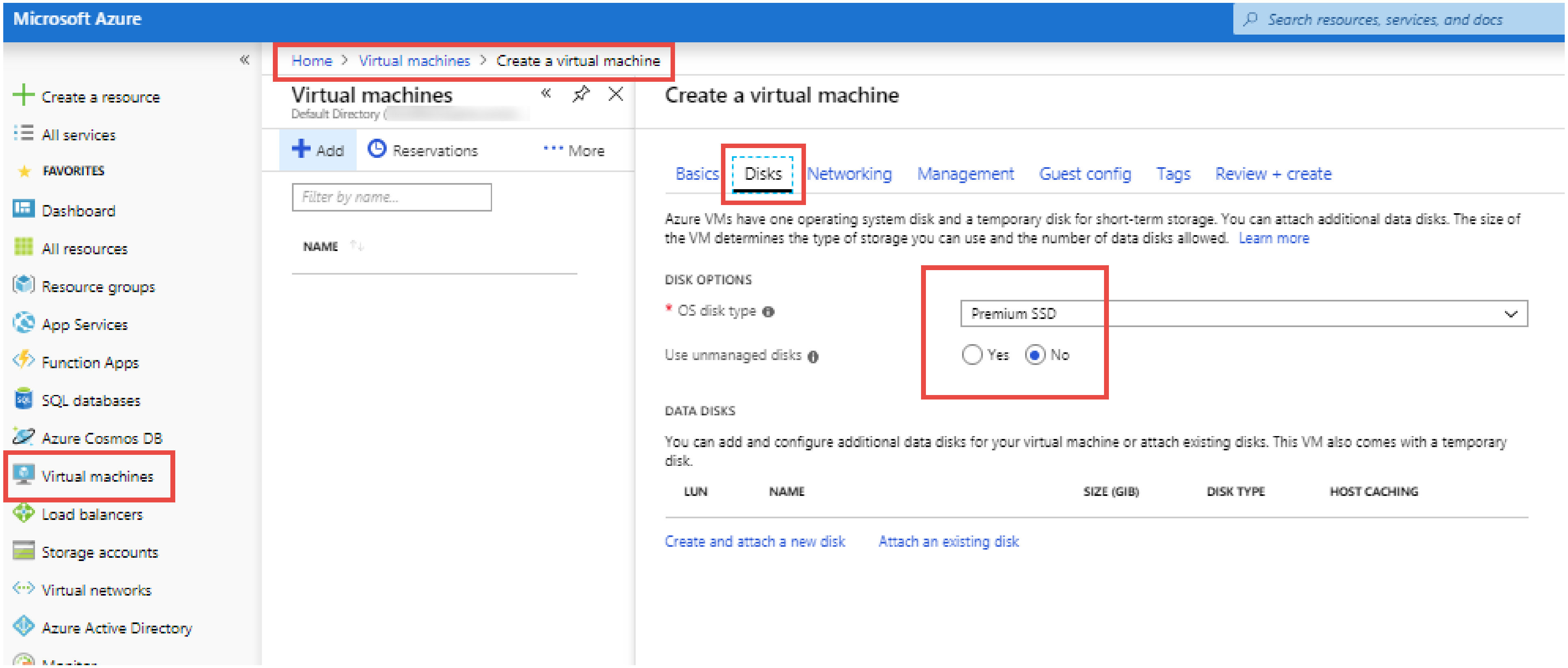
SAVE MONEY

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

* Already have a Windows license? ○ Yes ● No

I chose '[smalldisk]' versions of the operating systems when available because I don't expect to be using much disk at all in this simple lab. I also recommend the B1ms size VM, because the B1 size is just too weak even for a simple test lab.

I recommend you choose Standard SSDs or Premium SSDs (solid state disks) instead of Standard HDDs (spindle and platter drives) because spindles and platters are just too old and slow, even for a simple test lab.



Create a virtual machine

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

DISK OPTIONS

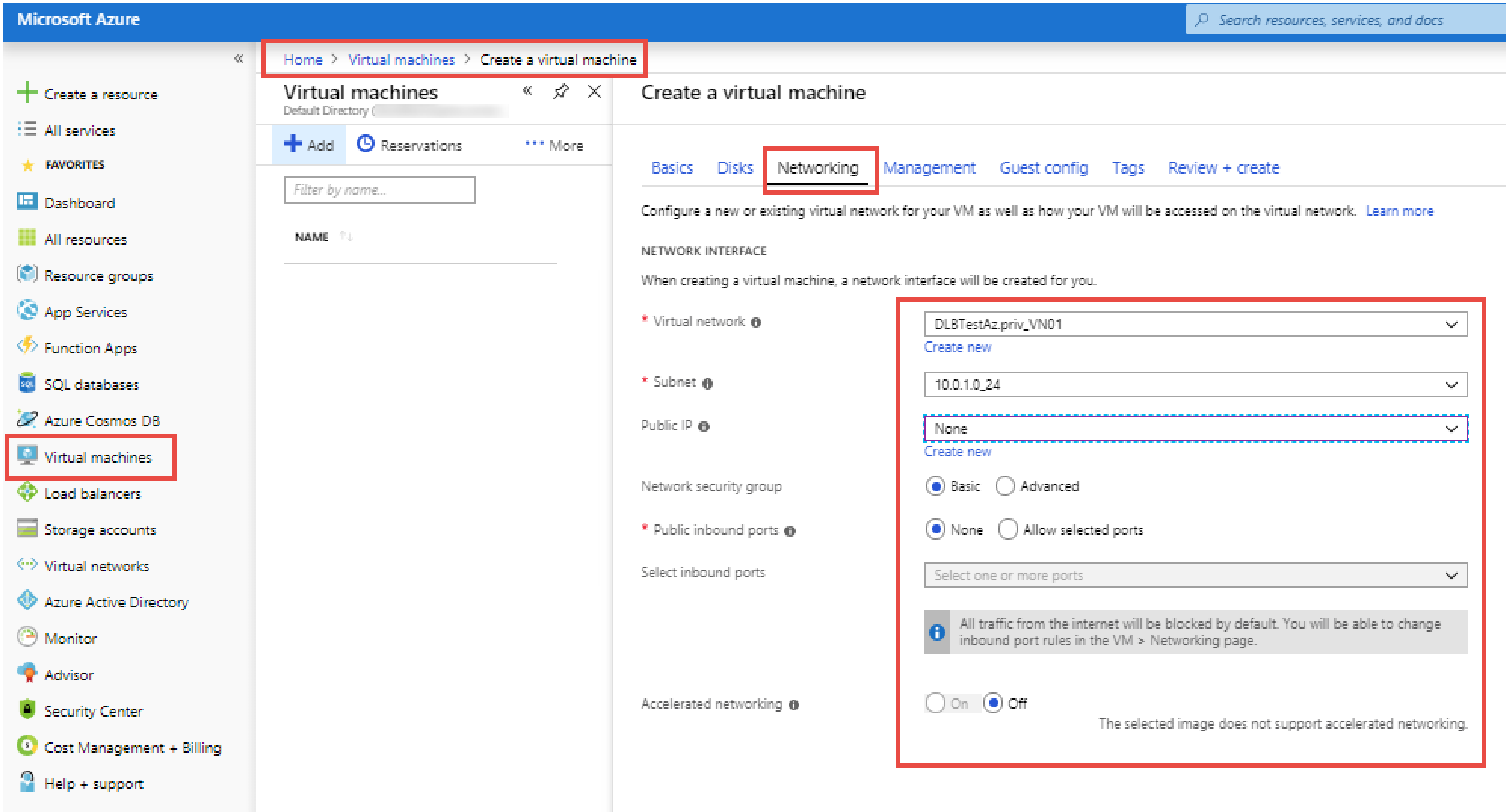
* OS disk type: Premium SSD

Use unmanaged disks: ○ Yes ● No

DATA DISKS

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	NAME	SIZE (GIB)	DISK TYPE	HOST CACHING



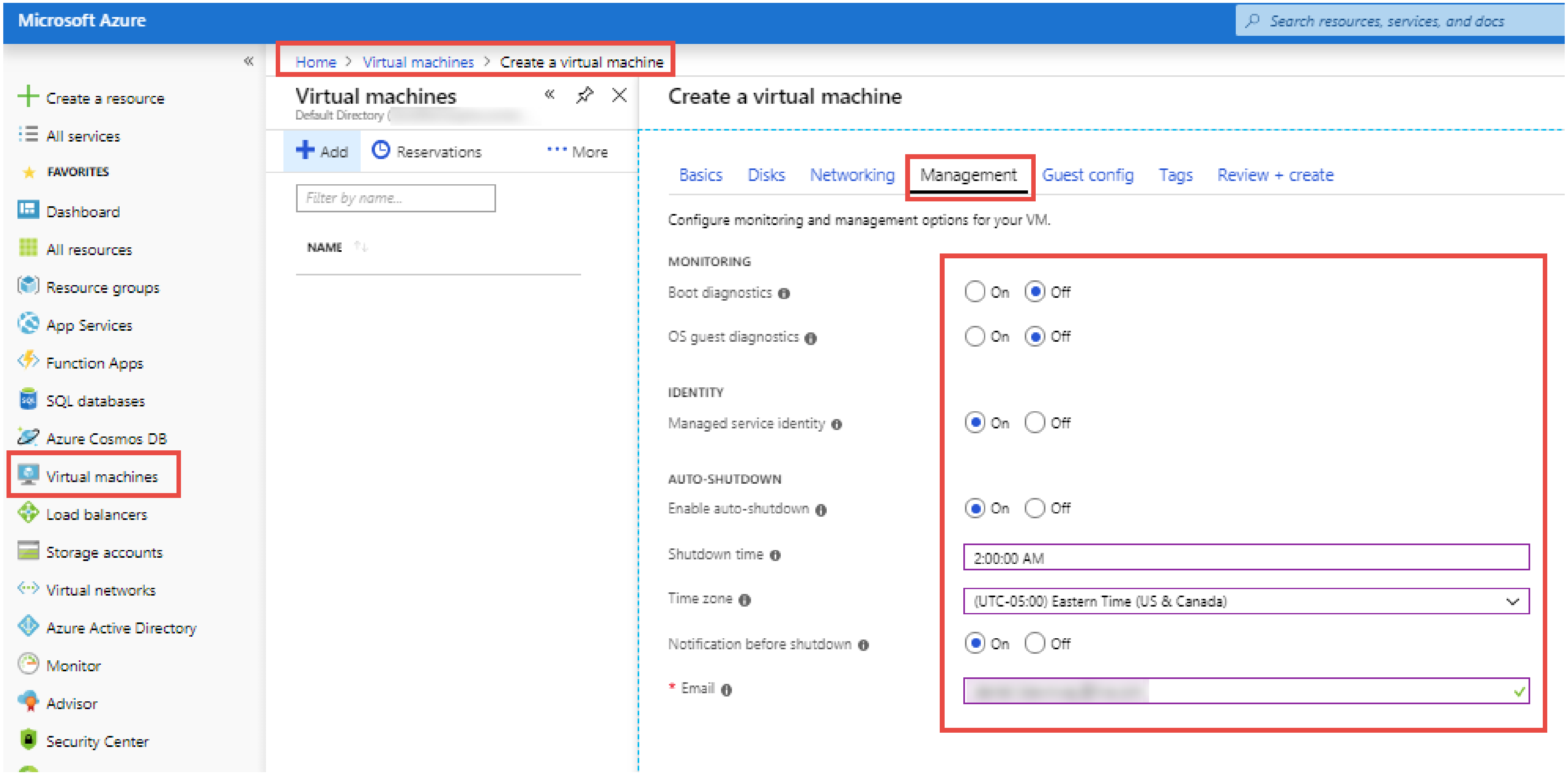
Create a virtual machine

Configure a new or existing virtual network for your VM as well as how your VM will be accessed on the virtual network. Learn more

NETWORK INTERFACE

When creating a virtual machine, a network interface will be created for you.

* Virtual network	DLBTestAz.priv_VN01 Create new
* Subnet	10.0.1.0_24
Public IP	None Create new
Network security group	● Basic ○ Advanced
* Public inbound ports	● None ○ Allow selected ports
Select inbound ports	Select one or more ports
	All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.
Accelerated networking	○ On ● Off The selected image does not support accelerated networking.



Create a virtual machine

Configure monitoring and management options for your VM.

MONITORING

Boot diagnostics ○ On ● Off

OS guest diagnostics ○ On ● Off

IDENTITY

Managed service identity ● On ○ Off

AUTO-SHUTDOWN

Enable auto-shutdown ● On ○ Off

Shutdown time: 2:00:00 AM

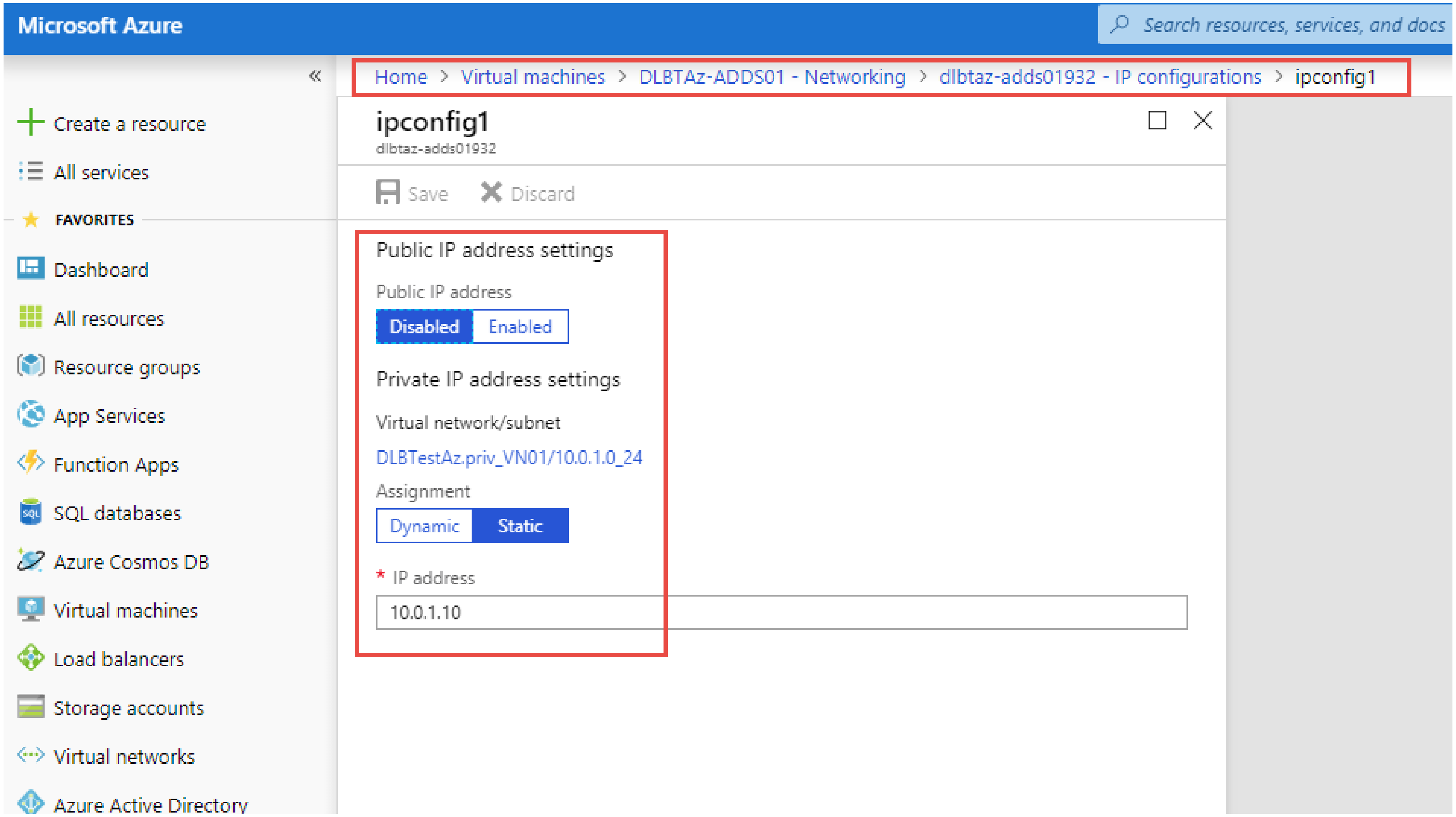
Time zone: (UTC-05:00) Eastern Time (US & Canada)

Notification before shutdown ● On ○ Off

* Email: [redacted] ✓

I set the VMs to auto-shutdown at 02:00AM every day, to keep costs down. This won’t deallocate the VMs (which is the real cost-saver) so in a later step we’ll create an automation account runbook to do that.

The last step for each VM is to change its internal IP from Azure DHCP to static. Look at the path in the following screenshot to see where to do this:



Home > Virtual machines > DLBTAz-ADDS01 - Networking > dlbtaz-adds01932 - IP configurations > ipconfig1

ipconfig1
dlbtaz-adds01932

Public IP address settings

Public IP address: [✓ Disabled] Enabled

Private IP address settings

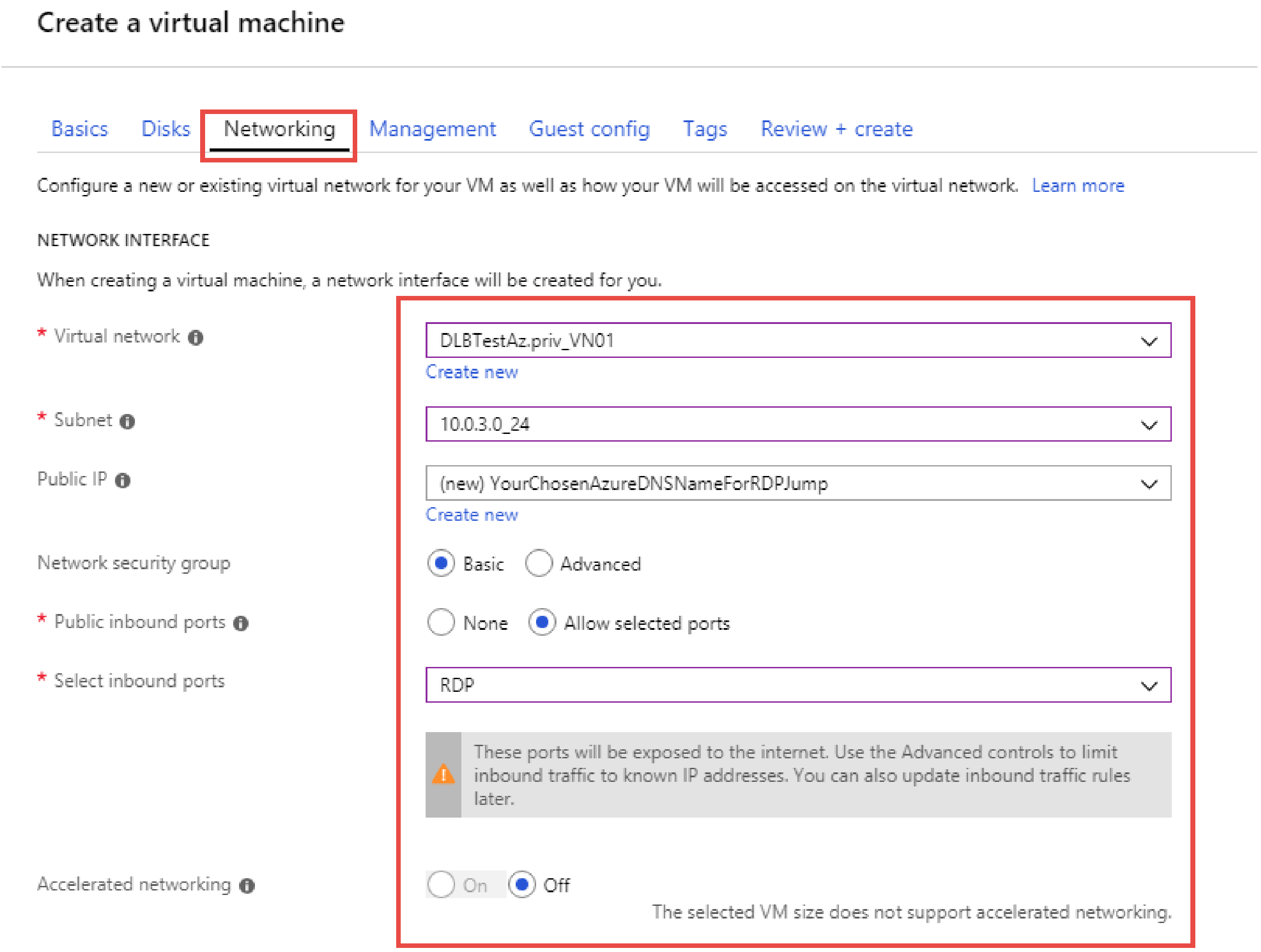
Virtual network/subnet: DLBTestAz.priv_VN01/10.0.1.0_24

Assignment: Dynamic [✓ Static]

* IP address: 10.0.1.10

Create Your RDP Jump Box:

The steps for creating the RDP jump box are similar to those for the other VMs, but there are some changes and additional steps:



Create a virtual machine

Configure a new or existing virtual network for your VM as well as how your VM will be accessed on the virtual network. Learn more

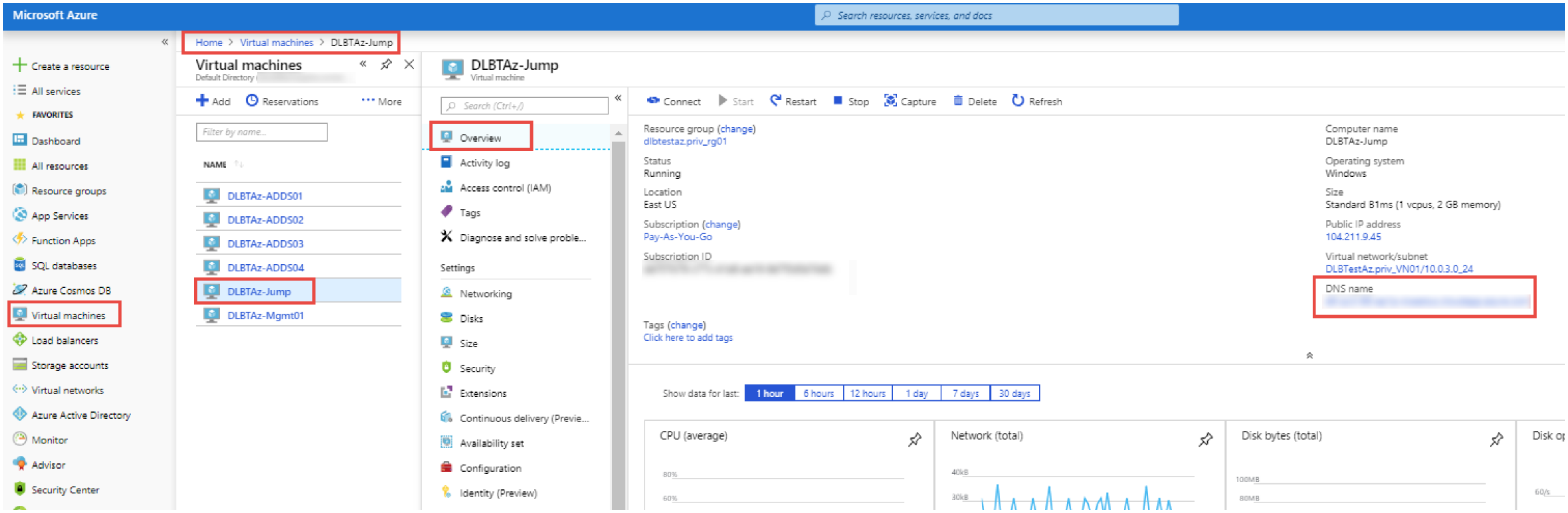
NETWORK INTERFACE

When creating a virtual machine, a network interface will be created for you.

* Virtual network	DLBTestAz.priv_VN01 Create new
* Subnet	10.0.3.0_24
Public IP	(new) YourChosenAzureDNSNameForRDPJump Create new
Network security group	● Basic ○ Advanced
* 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.
Accelerated networking	○ On ● Off The selected VM size does not support accelerated networking.

- Its network interface will have an internal, static, private IPv4 address on one of your Virtual Network's subnets.
- Its network interface will also have an external, dynamic, public IPv4 address which will be open on port 3389 for incoming RDP. Because this address will be dynamic, you will access it by a DNS name you choose that will be published automatically into Azure's public DNS. You should make this name long and complex (lower case, numbers, and dashes).
- The configuration to allow port 3389 inbound occurs as an NSG (Network Security Group) ACL (Access Control List). These configurations are NOT part of any 'Azure Firewall' per se, nor are they part of the VM's OS firewall (which we will configure in a later step).

Add a public DNS name (make it long and complex for obscurity) into the 'DNS name' field. This will be the public Internet name by which you access your RDP jump box's external, dynamic, public, IPv4 address:



Resource group (change)
dlbtestaz.priv_rg01

Status
Running

Location
East US

Subscription (change)
Pay-As-You-Go

Subscription ID
[redacted]

Tags (change)
Click here to add tags

Computer name
DLBTAz-Jump

Operating system
Windows

Size
Standard B1ms (1 vcpus, 2 GB memory)

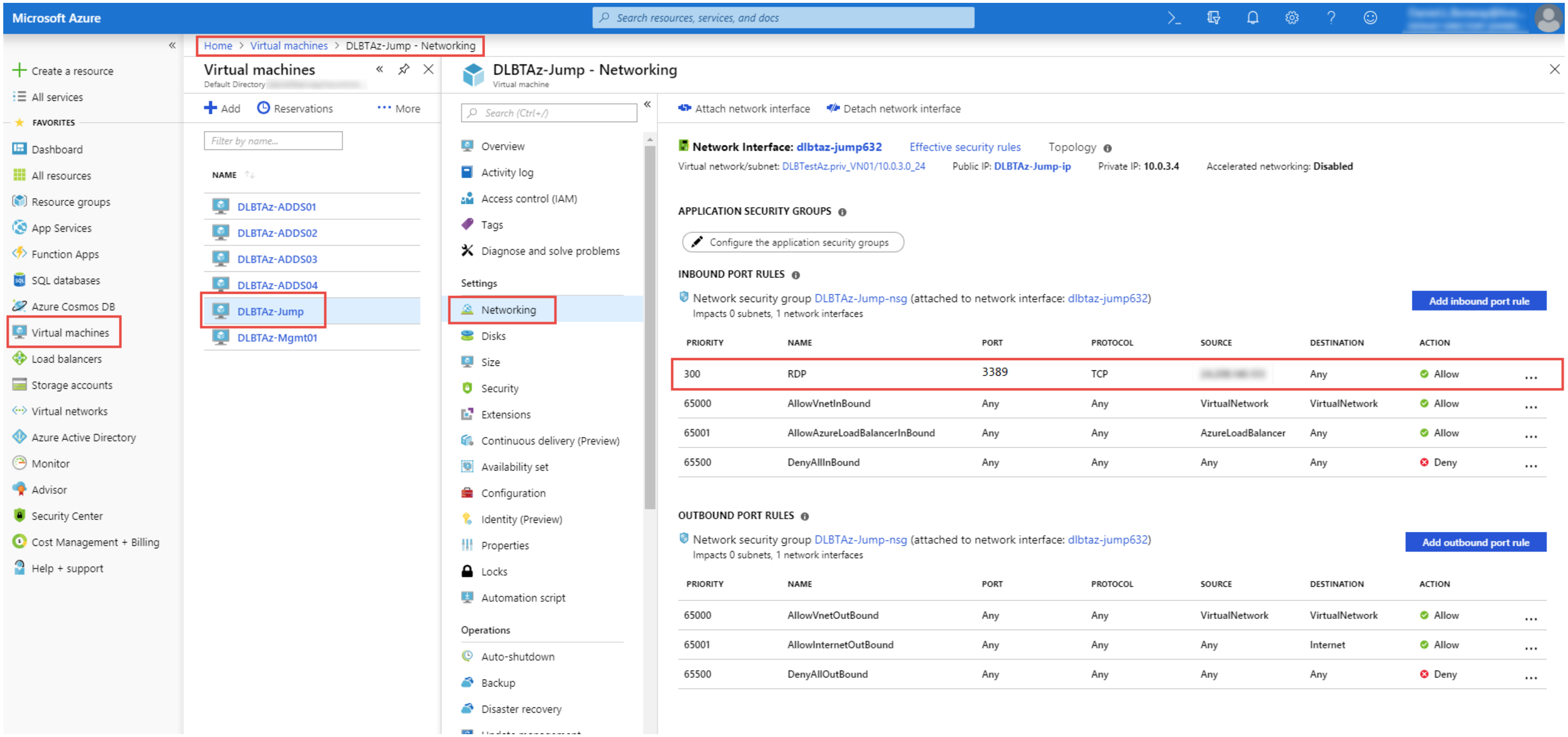
Public IP address
104.211.9.45

Virtual network/subnet
DLBTestAz.priv_VN01/10.0.3.0_24

DNS name
[redacted]

Set your RDP jump box's internal, static, private IPv4 address as described in previous steps.

Go to https://www.whatismyip.com/ to learn your own workstation's external, dynamic, public, IPv4 address, and change the jump box's inbound RDP rule to accept from that address only (you will have to do this step whenever your workstation's external address changes from your ISP):



Home > Virtual machines > DLBTAz-Jump - Networking

Virtual machines
Default Directory [redacted]

- DLBTAz-ADDS01
- DLBTAz-ADDS02
- DLBTAz-ADDS03
- DLBTAz-ADDS04
- DLBTAz-Jump
- DLBTAz-Mgmt01

DLBTAz-Jump - Networking
Virtual machine

Network Interface: dlbtaz-jump632 Effective security rules Topology

Virtual network/subnet: DLBTestAz.priv_VN01/10.0.3.0_24 Public IP: DLBTAz-Jump-ip Private IP: 10.0.3.4 Accelerated networking: Disabled

APPLICATION SECURITY GROUPS

INBOUND PORT RULES

Network security group DLBTAz-Jump-nsg (attached to network interface: dlbtaz-jump632)
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
300	RDP	3389	TCP	[redacted]	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✕ Deny

OUTBOUND PORT RULES

Network security group DLBTAz-Jump-nsg (attached to network interface: dlbtaz-jump632)
Impacts 0 subnets, 1 network interfaces

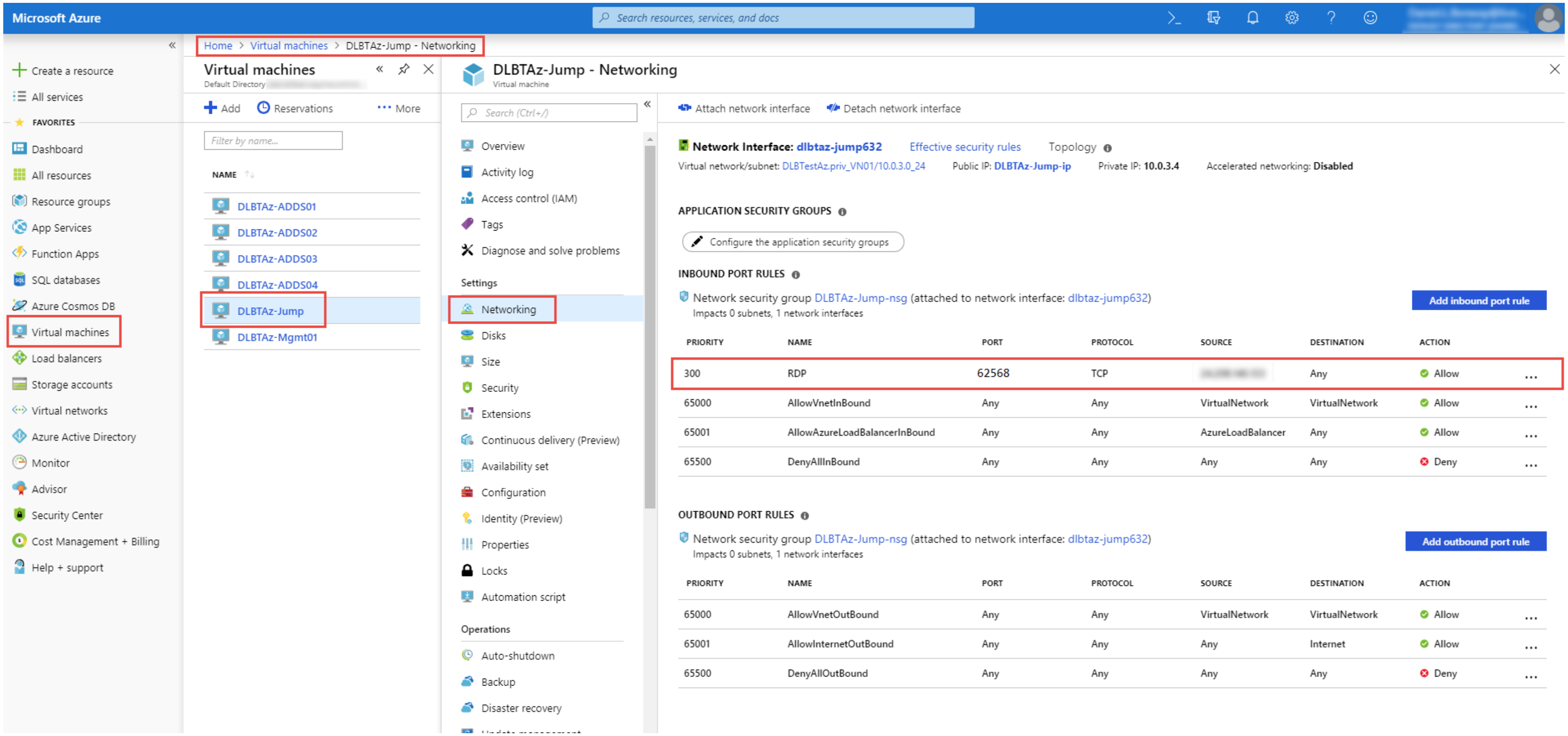
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✕ Deny

Remember, these configurations are NOT part of any 'Azure Firewall' per se, nor are they part of the VM's OS firewall (which we will configure in a later step), but rather they are implemented through an NSG (Network Security Group) ACL (Access Control List).

RDP into your RDP jump box on 3389, and run the following PSh script (in PowerShell ISE as an Administrator) to change the jump box’s RDP port to, say, 62,568, and reboot (it changes the RDP jump box’s registry and its local OS firewall):

```
-----------------------------------------------------------------------------------------------------------------------
https://blogs.technet.microsoft.com/drew/2017/04/14/1195/
-----------------------------------------------------------------------------------------------------------------------
# Paste this line first
Write-host "What Port would you like to set for RDP: " -ForegroundColor Yellow -NoNewline;$RDPPort = Read-Host

# Paste these two lines next
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-TCP\" -Name
PortNumber -Value $RDPPort
New-NetFirewallRule -DisplayName "RDP HighPort" -Direction Inbound –LocalPort $RDPPort -Protocol TCP -Action
Allow

Write-host "port number is $RDPPORT" -ForegroundColor Magenta
Write-host "Launch RDP with IP:$RDPORT or cmdline MSTSC /V [ip]:$RDPORT"
-----------------------------------------------------------------------------------------------------------------------
```

Change your RDP jump box's inbound port rules from 3389 to whatever port you chose, say 62,568, and restart your jump box:



Network Interface: dlbtaz-jump632

Virtual network/subnet: DLBTestAz.priv_VN01/10.0.3.0_24 Public IP: **DLBTAz-Jump-ip** Private IP: **10.0.3.4** Accelerated networking: **Disabled**

APPLICATION SECURITY GROUPS

INBOUND PORT RULES

Network security group DLBTAz-Jump-nsg (attached to network interface: dlbtaz-jump632)
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
300	RDP	62568	TCP	[redacted]	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

OUTBOUND PORT RULES

Network security group DLBTAz-Jump-nsg (attached to network interface: dlbtaz-jump632)
Impacts 0 subnets, 1 network interfaces

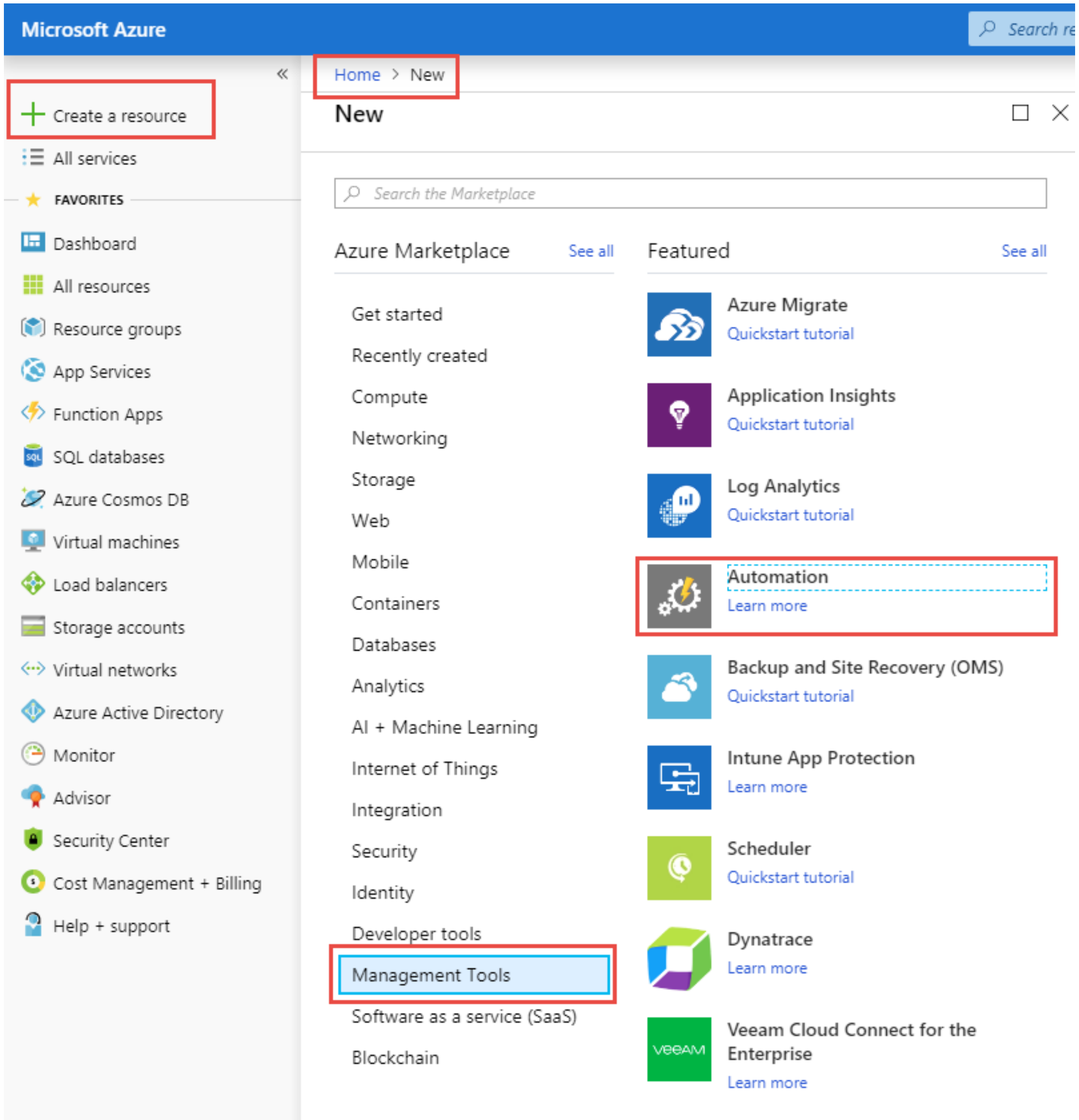
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Remember, these configurations are NOT part of any ‘Azure Firewall’ per se, nor are they part of the VM’s OS firewall, but rather they are implemented through an NSG (Network Security Group) ACL (Access Control List).

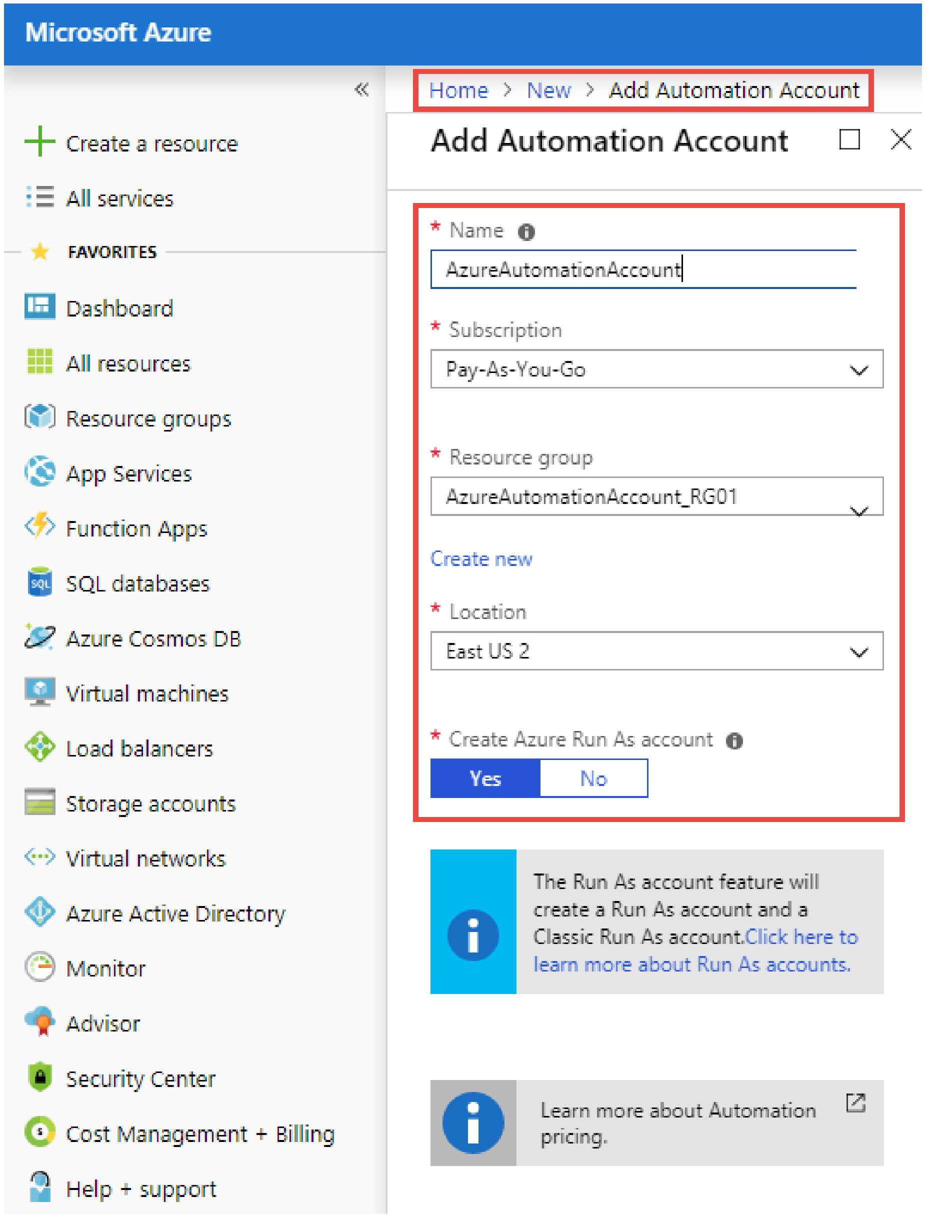
Now, RDP into your RDP jump box using its long and complex public DNS name and its new RDP port. This VM is exposed to the public Internet, so rename the jump box’s local user ID to something long and complex, with a long and complex password.

Create Automation Account and Runbook for Automatic Deallocation:

[(jump to TOC)](#)



Give your Automation Account a good name, and assign it to the Automation Group you created earlier:



* Name: AzureAutomationAccount

* Subscription: Pay-As-You-Go

* Resource group: AzureAutomationAccount_RG01

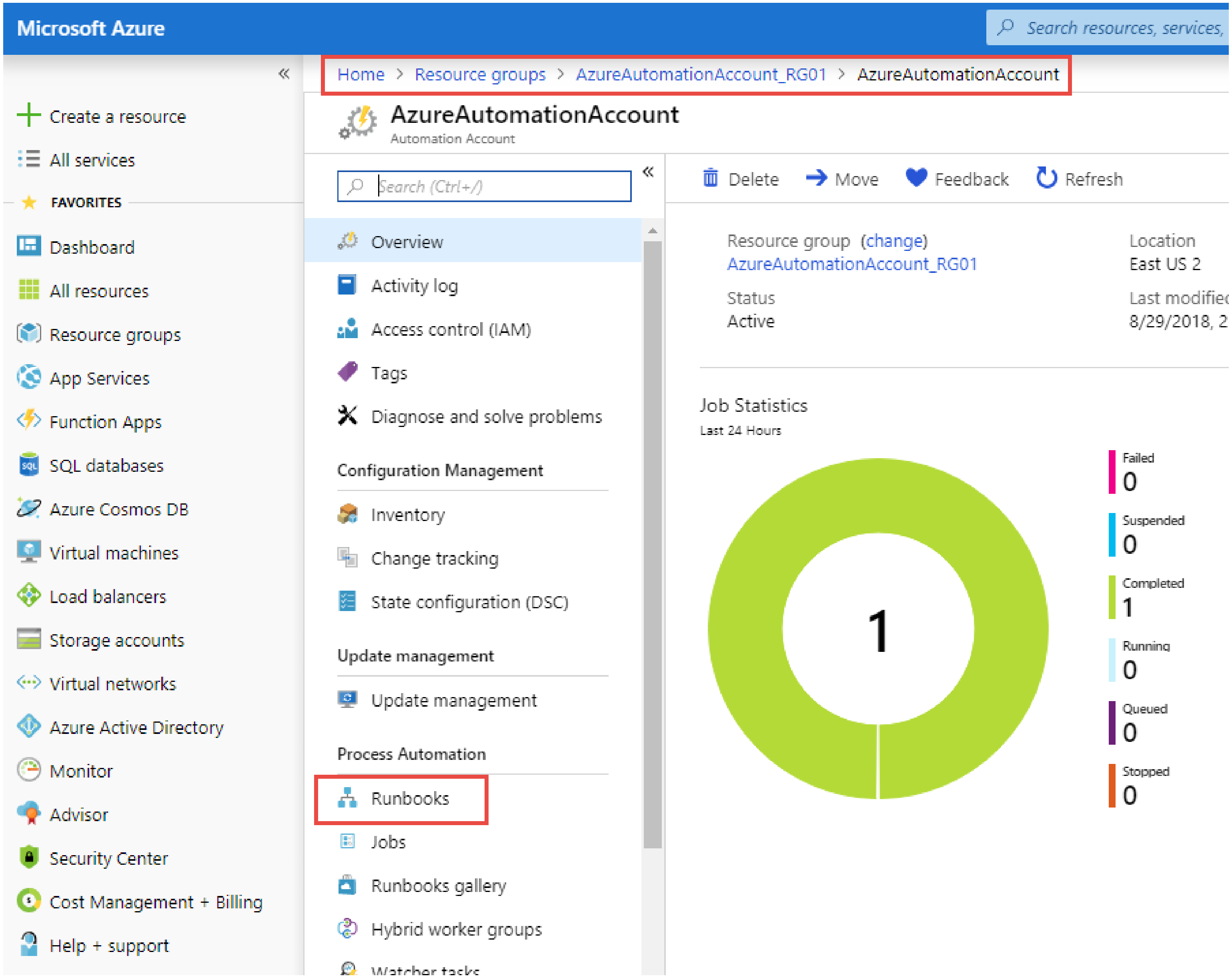
* Location: East US 2

* Create Azure Run As account: [✓ Yes] No

The Run As account feature will create a Run As account and a Classic Run As account.Click here to learn more about Run As accounts.

Learn more about Automation pricing.

Go into your AzureAutomationAccount and create a Runbook to perform the nightly deallocation of your VMs:



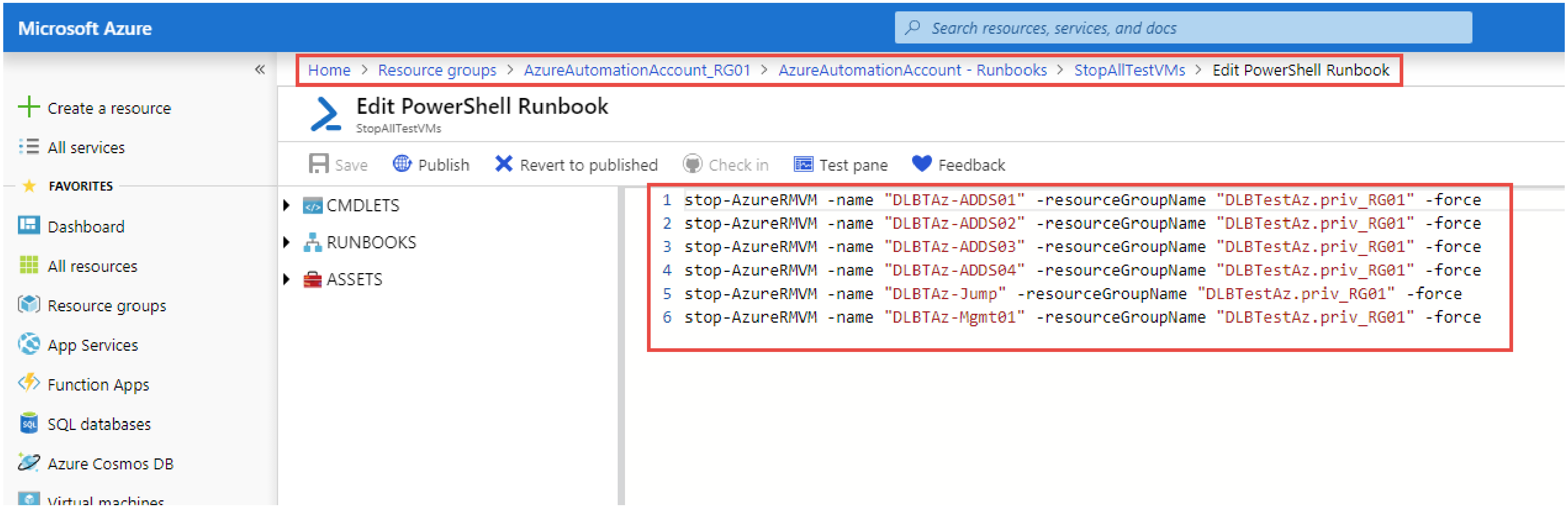
Resource group (change)
AzureAutomationAccount_RG01

Location
East US 2

Status
Active

Last modifiec
8/29/2018, 2

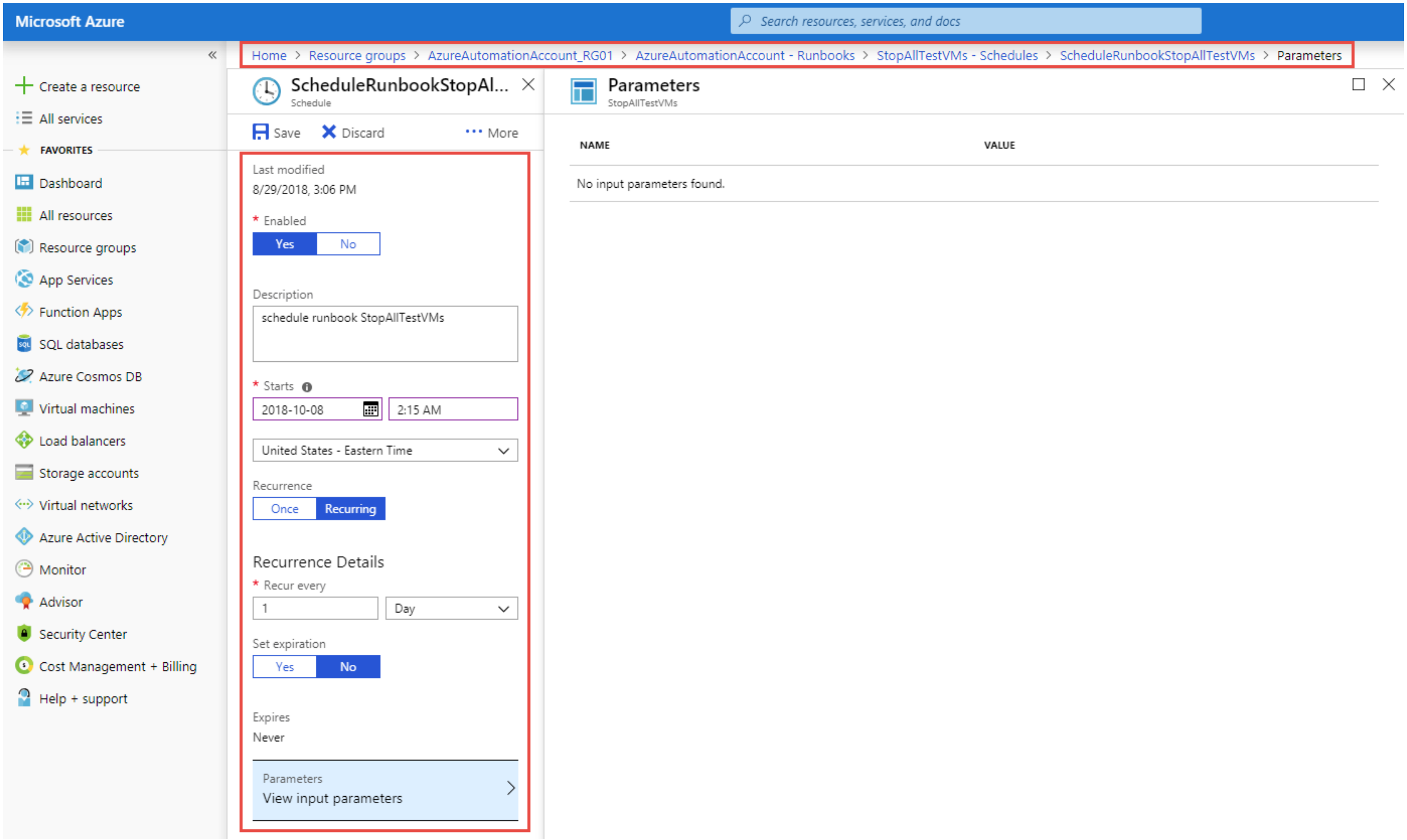
Edit your runbook to contain Azure PowerShell commands similar to these, and then publish it (these commands stop/deallocate each of my six VMs, all of which are in the same Resource Group).



```
stop-AzureRMVM -name "DLBTAz-ADDS01" -resourceGroupName "DLBTestAz.priv_RG01" -force
stop-AzureRMVM -name "DLBTAz-ADDS02" -resourceGroupName "DLBTestAz.priv_RG01" -force
stop-AzureRMVM -name "DLBTAz-ADDS03" -resourceGroupName "DLBTestAz.priv_RG01" -force
stop-AzureRMVM -name "DLBTAz-ADDS04" -resourceGroupName "DLBTestAz.priv_RG01" -force
stop-AzureRMVM -name "DLBTAz-Jump" -resourceGroupName "DLBTestAz.priv_RG01" -force
stop-AzureRMVM -name "DLBTAz-Mgmt01" -resourceGroupName "DLBTestAz.priv_RG01" -force
```

Note: When you start a runbook in Azure Automation, a job is created. A job is a single execution instance of a runbook. (https://docs.microsoft.com/en-us/azure/automation/automation-runbook-execution)

Schedule your runbook to run, say, fifteen minutes after your VMs perform their auto-shutdown each night:



Home > Resource groups > AzureAutomationAccount_RG01 > AzureAutomationAccount - Runbooks > StopAllTestVMs - Schedules > ScheduleRunbookStopAllTestVMs > Parameters

ScheduleRunbookStopAl...
Schedule

Last modified
8/29/2018, 3:06 PM

* Enabled: [✓ Yes] No

Description: schedule runbook StopAllTestVMs

* Starts: 2018-10-08 2:15 AM

United States - Eastern Time

Recurrence: Once [✓ Recurring]

Recurrence Details

* Recur every: 1 Day

Set expiration: Yes [✓ No]

Expires
Never

Parameters
View input parameters

Parameters
StopAllTestVMs

NAME	VALUE
No input parameters found.	

Verify your runbook schedule after you create it, and **test it** one night to make sure your VMs shut down, and the runbook deallocates them.

Supporting Documents:

https://docs.microsoft.com/en-us/azure/automation/automation-quickstart-create-account
Create an Azure Automation account

https://docs.microsoft.com/en-us/azure/automation/automation-quickstart-create-runbook
Create an Azure Automation Runbook

https://docs.microsoft.com/en-us/azure/automation/automation-solution-vm-management
Start/Stop VMs during off-hours solution in Azure Automation

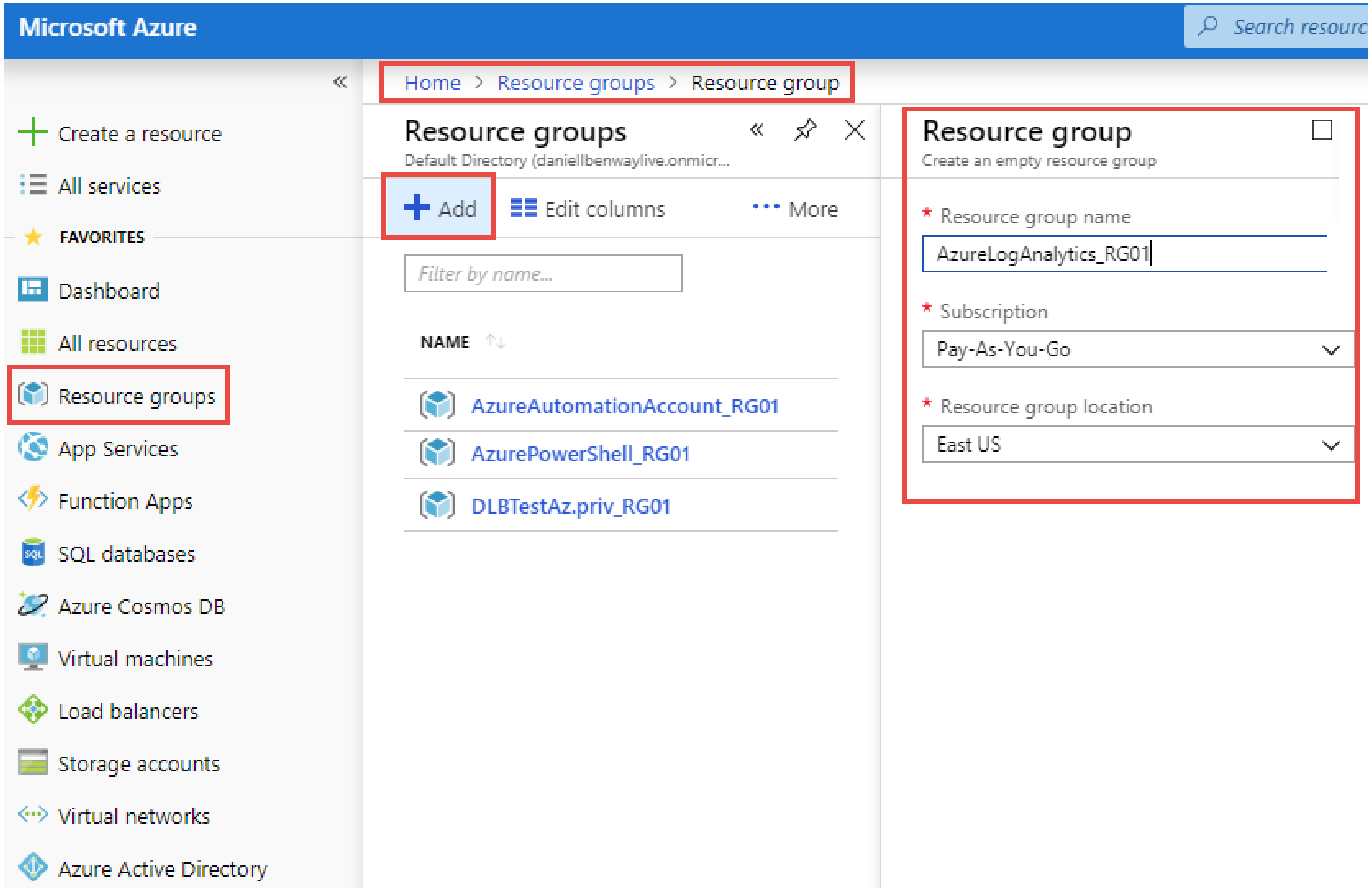
(https://docs.microsoft.com/en-us/azure/automation/automation-runbook-execution
Runbook execution in Azure Automation

Security Center:

(jump to TOC)

Azure Security Center is offered in two tiers: Free and Standard. The Standard tier is free for the first 60 days, and any usage beyond 60 days will be automatically charged per a fee schedule. So for your test lab, make sure you use and configure at least the free tier.

Create a new Resource Group for your Log Analytics Workspaces:



Resource groups
Default Directory (daniellbenwaylive.onmicr...

NAME
AzureAutomationAccount_RG01
AzurePowerShell_RG01
DLBTestAz.priv_RG01

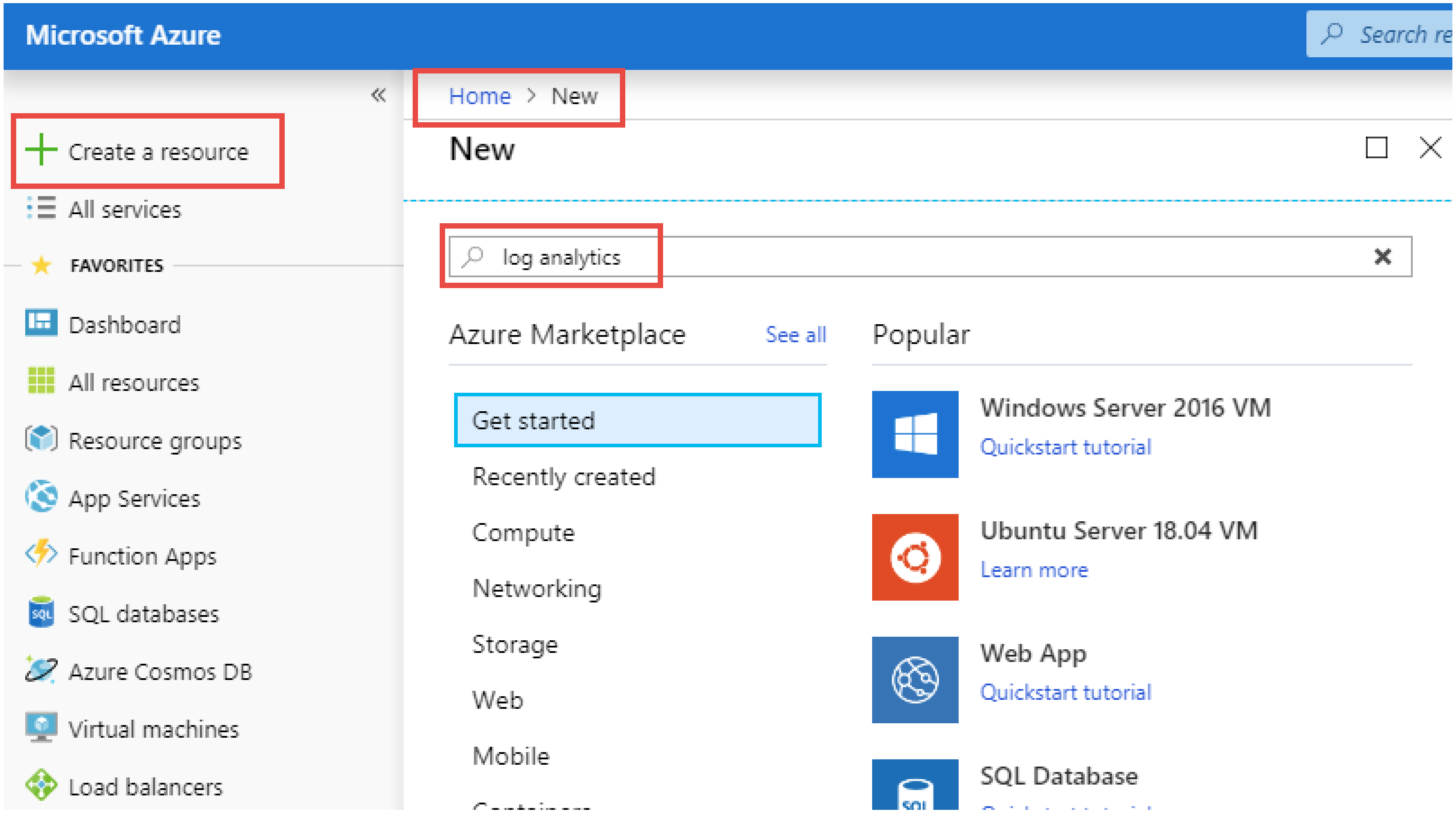
Resource group
Create an empty resource group

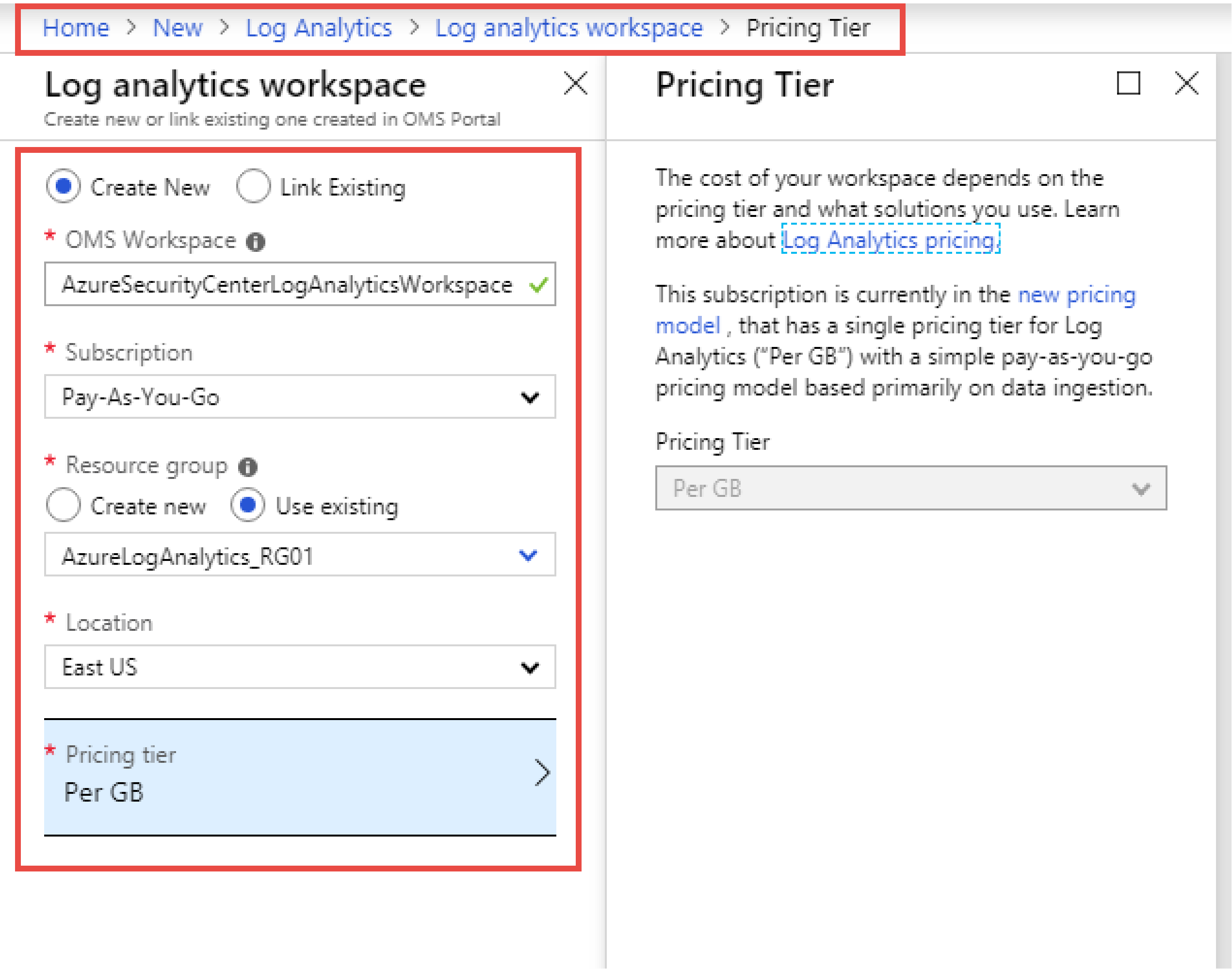
* Resource group name: AzureLogAnalytics_RG01

* Subscription: Pay-As-You-Go

* Resource group location: East US

Create a Log Analytics Workspace for Security Center:





Home > New > Log Analytics > Log analytics workspace > Pricing Tier

Log analytics workspace

Create new or link existing one created in OMS Portal

● Create New ○ Link Existing

* OMS Workspace

AzureSecurityCenterLogAnalyticsWorkspace ✓

* Subscription

Pay-As-You-Go

* Resource group

○ Create new ● Use existing

AzureLogAnalytics_RG01

* Location

East US

* Pricing tier

Per GB

Pricing Tier

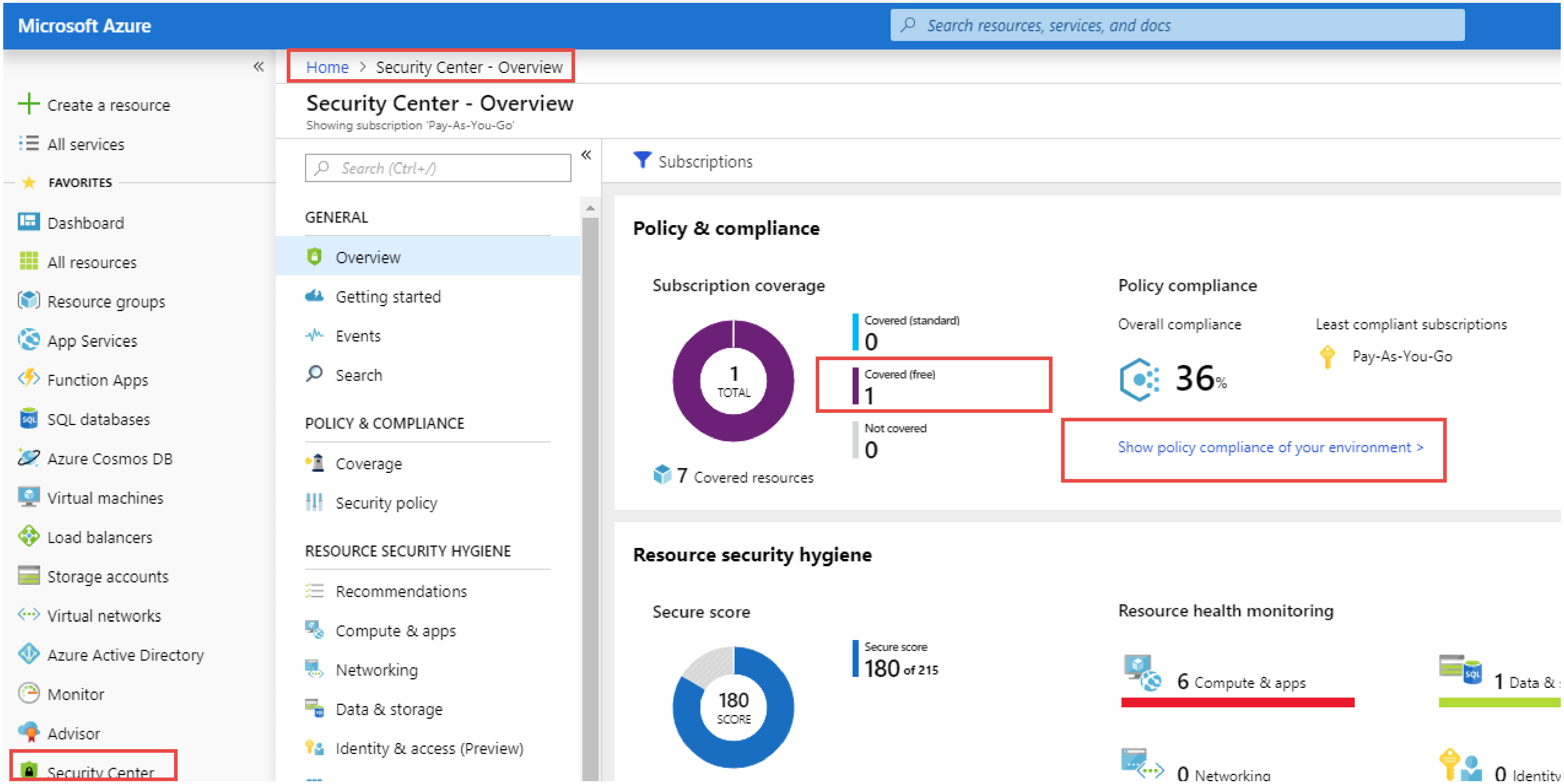
The cost of your workspace depends on the pricing tier and what solutions you use. Learn more about Log Analytics pricing.

This subscription is currently in the new pricing model , that has a single pricing tier for Log Analytics ("Per GB") with a simple pay-as-you-go pricing model based primarily on data ingestion.

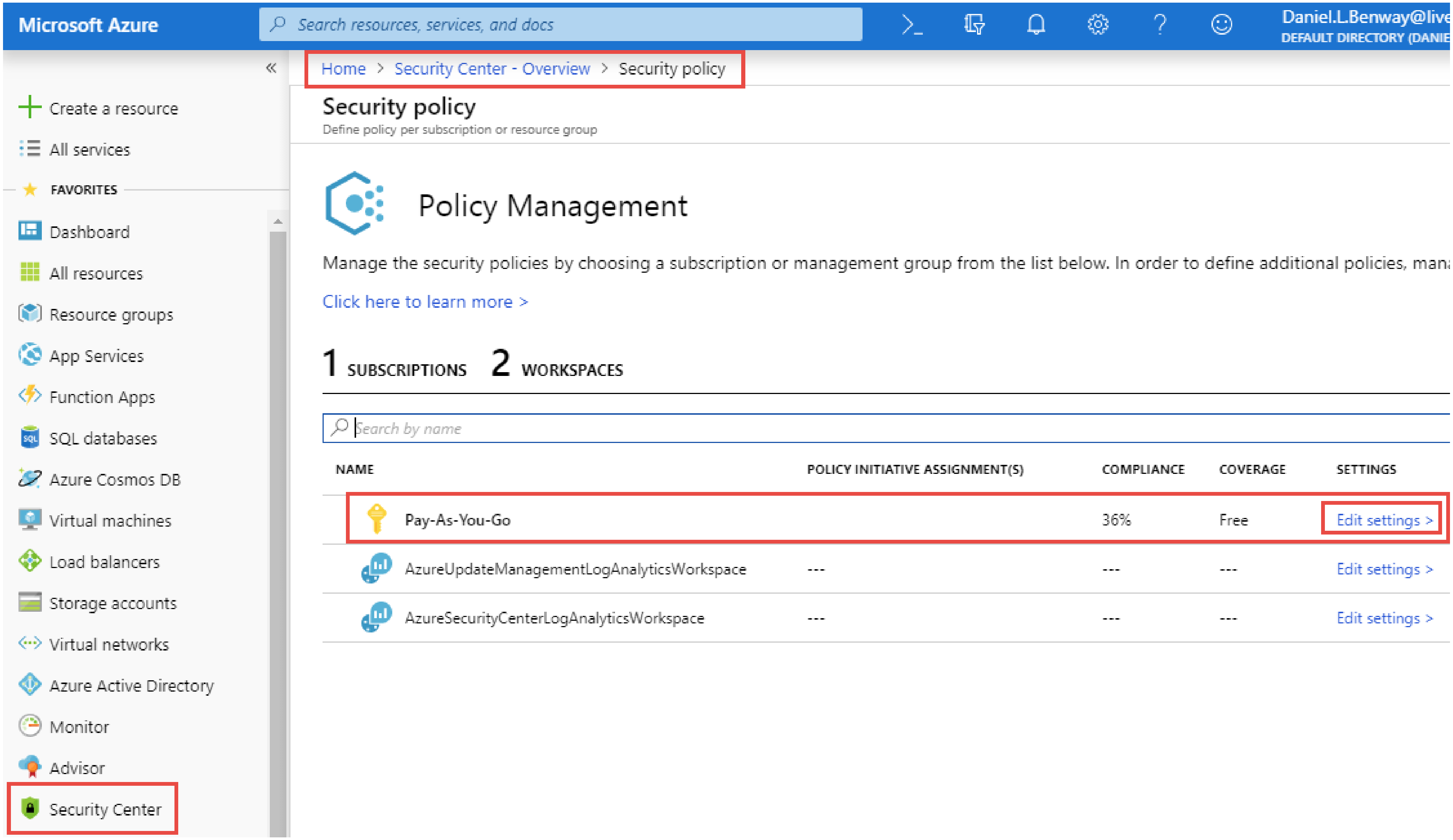
Pricing Tier

Per GB

Now configure Security Center:



My test lab is pretty simple, so I will just configure the Security Center settings on my subscription, and allow each item therein inherit its configuration from the subscription:



Security policy

Define policy per subscription or resource group

Policy Management

Manage the security policies by choosing a subscription or management group from the list below. In order to define additional policies, mana

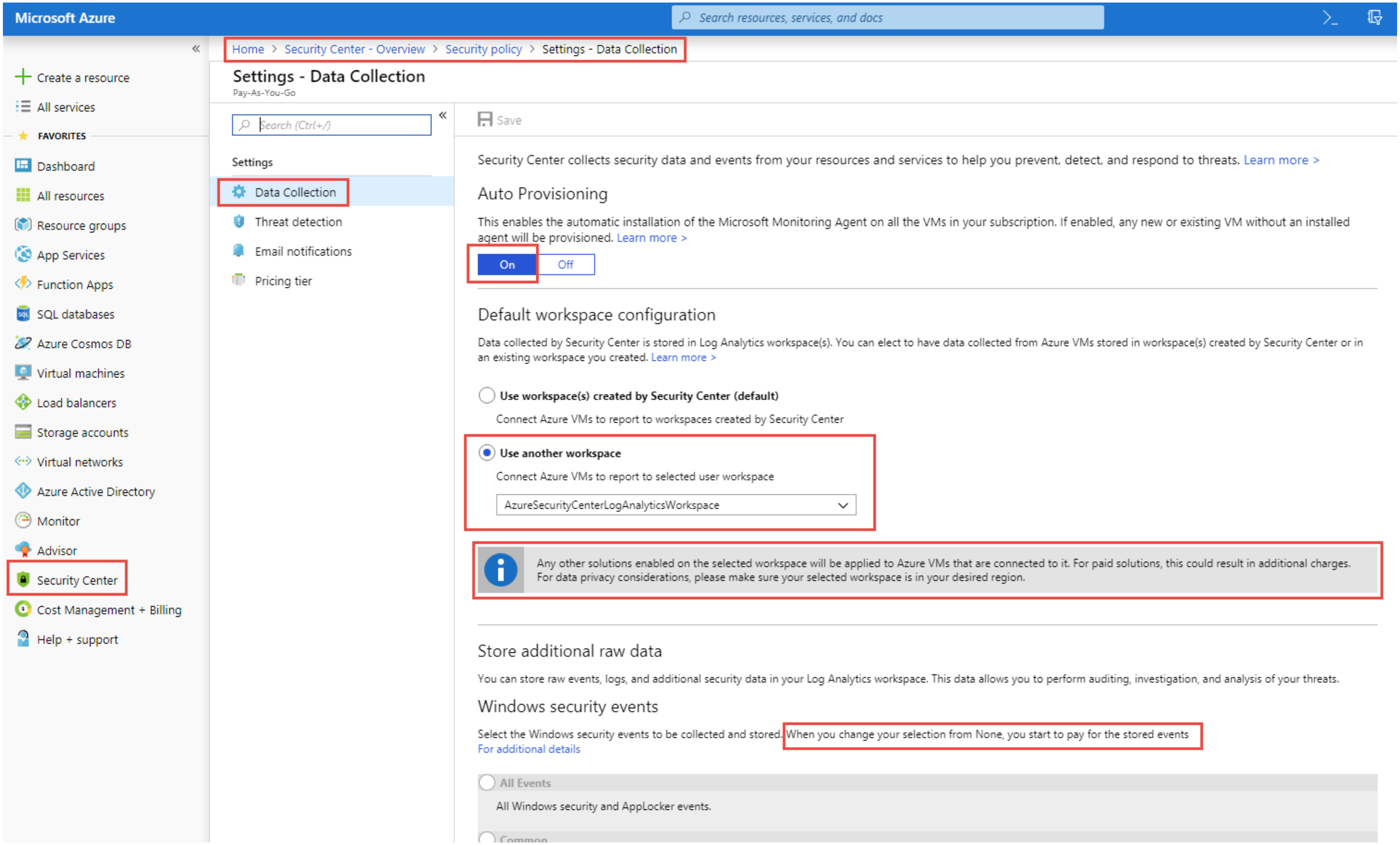
Click here to learn more >

1 SUBSCRIPTIONS 2 WORKSPACES

Search by name

NAME	POLICY INITIATIVE ASSIGNMENT(S)	COMPLIANCE	COVERAGE	SETTINGS
Pay-As-You-Go		36%	Free	Edit settings >
AzureUpdateManagementLogAnalyticsWorkspace	---	---	---	Edit settings >
AzureSecurityCenterLogAnalyticsWorkspace	---	---	---	Edit settings >

Enable Auto Provisioning, so that the MS Monitoring Agent gets installed onto your current and future VMs:



Settings - Data Collection
Pay-As-You-Go

Security Center collects security data and events from your resources and services to help you prevent, detect, and respond to threats. Learn more >

Auto Provisioning

This enables the automatic installation of the Microsoft Monitoring Agent on all the VMs in your subscription. If enabled, any new or existing VM without an installed agent will be provisioned. Learn more >

[✓ On] Off

Default workspace configuration

Data collected by Security Center is stored in Log Analytics workspace(s). You can elect to have data collected from Azure VMs stored in workspace(s) created by Security Center or in an existing workspace you created. Learn more >

○ **Use workspace(s) created by Security Center (default)**
Connect Azure VMs to report to workspaces created by Security Center

● **Use another workspace**
Connect Azure VMs to report to selected user workspace
AzureSecurityCenterLogAnalyticsWorkspace

Any other solutions enabled on the selected workspace will be applied to Azure VMs that are connected to it. For paid solutions, this could result in additional charges. For data privacy considerations, please make sure your selected workspace is in your desired region.

Store additional raw data

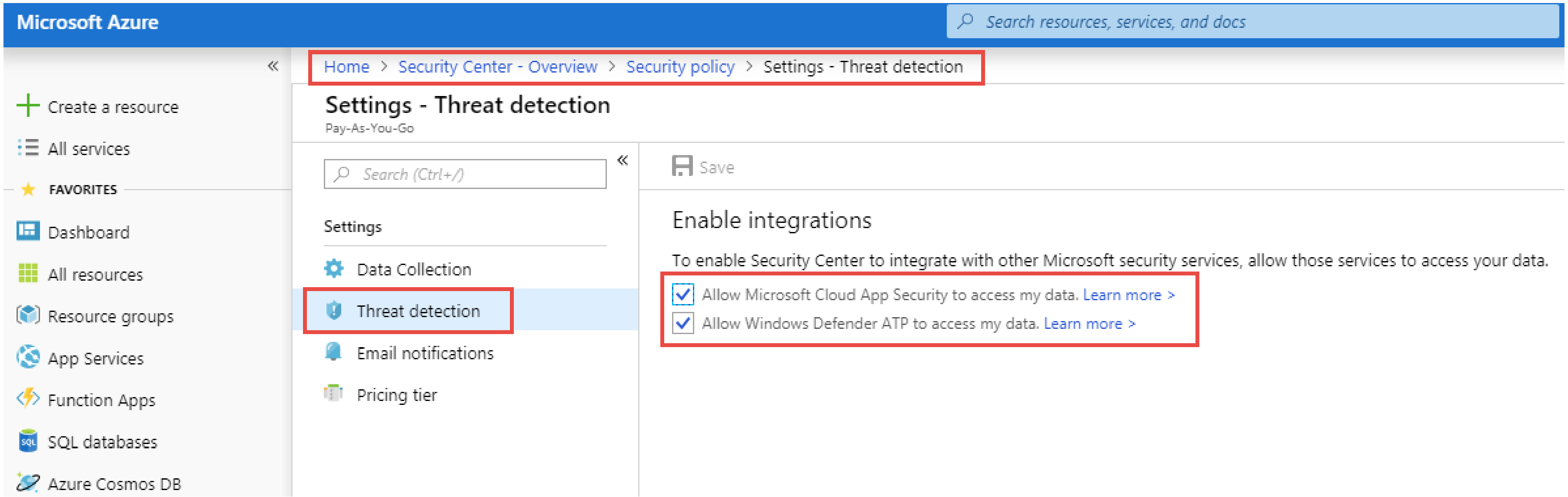
You can store raw events, logs, and additional security data in your Log Analytics workspace. This data allows you to perform auditing, investigation, and analysis of your threats.

Windows security events

Select the Windows security events to be collected and stored. When you change your selection from None, you start to pay for the stored events
For additional details

○ All Events
All Windows security and AppLocker events.

○ Common



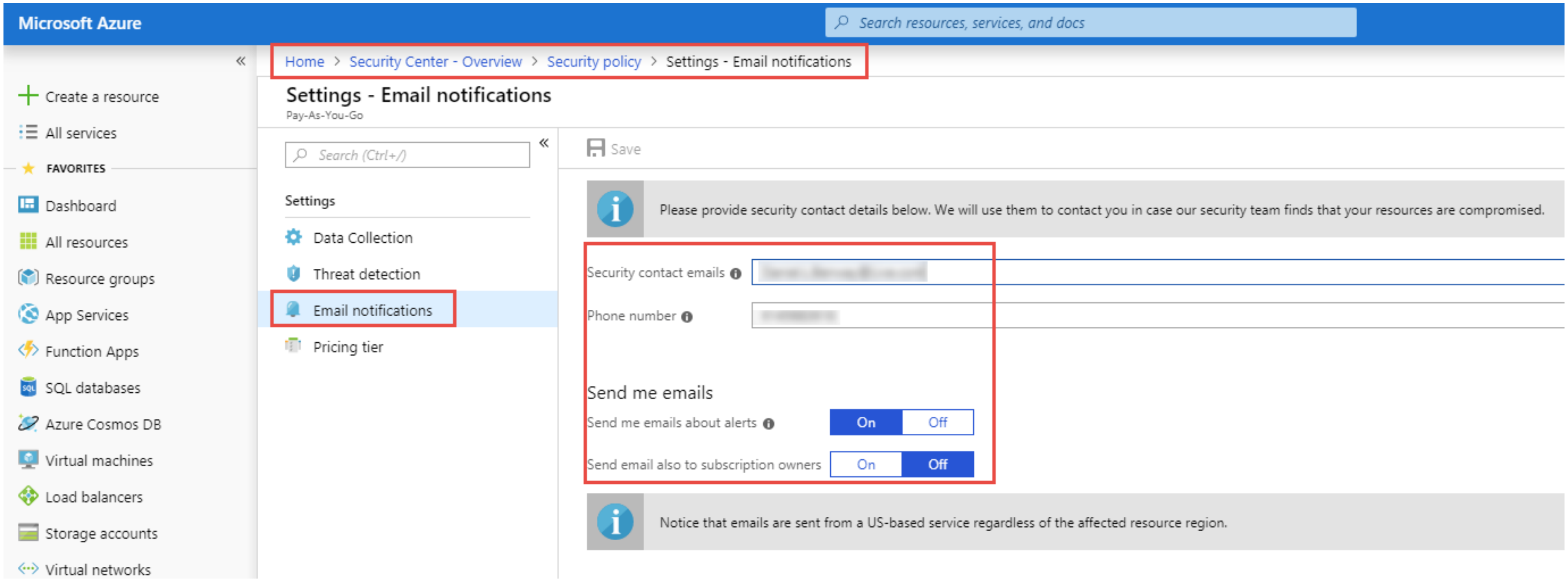
Home > Security Center - Overview > Security policy > Settings - Threat detection

Settings - Threat detection
Pay-As-You-Go

Enable integrations

To enable Security Center to integrate with other Microsoft security services, allow those services to access your data.

☑ Allow Microsoft Cloud App Security to access my data. Learn more >
☑ Allow Windows Defender ATP to access my data. Learn more >



Home > Security Center - Overview > Security policy > Settings - Email notifications

Settings - Email notifications
Pay-As-You-Go

Please provide security contact details below. We will use them to contact you in case our security team finds that your resources are compromised.

Security contact emails: [redacted]

Phone number: [redacted]

Send me emails

Send me emails about alerts: [✓ On] Off

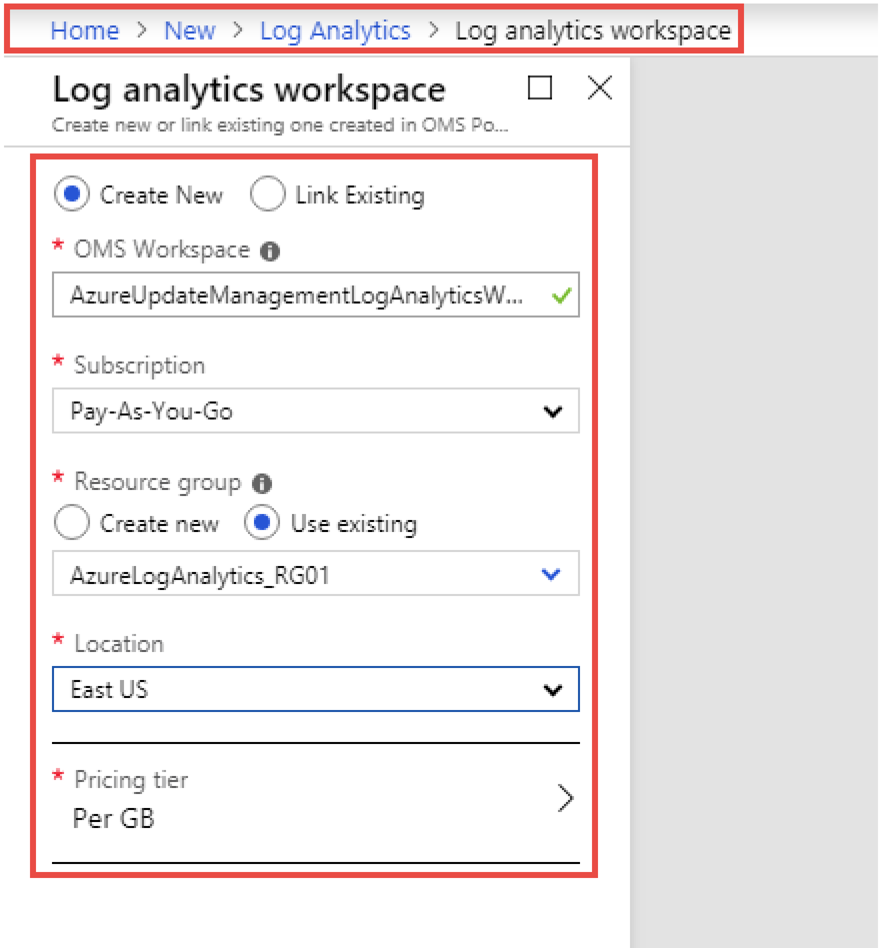
Send email also to subscription owners: On [✓ Off]

Notice that emails are sent from a US-based service regardless of the affected resource region.

VM Update Management:

(jump to TOC)

Create a Log Analytics Workspace for Update Management:



Home > New > Log Analytics > Log analytics workspace

Log analytics workspace

Create new or link existing one created in OMS Po...

● Create New ○ Link Existing

* OMS Workspace: AzureUpdateManagementLogAnalyticsW... ✓

* Subscription: Pay-As-You-Go

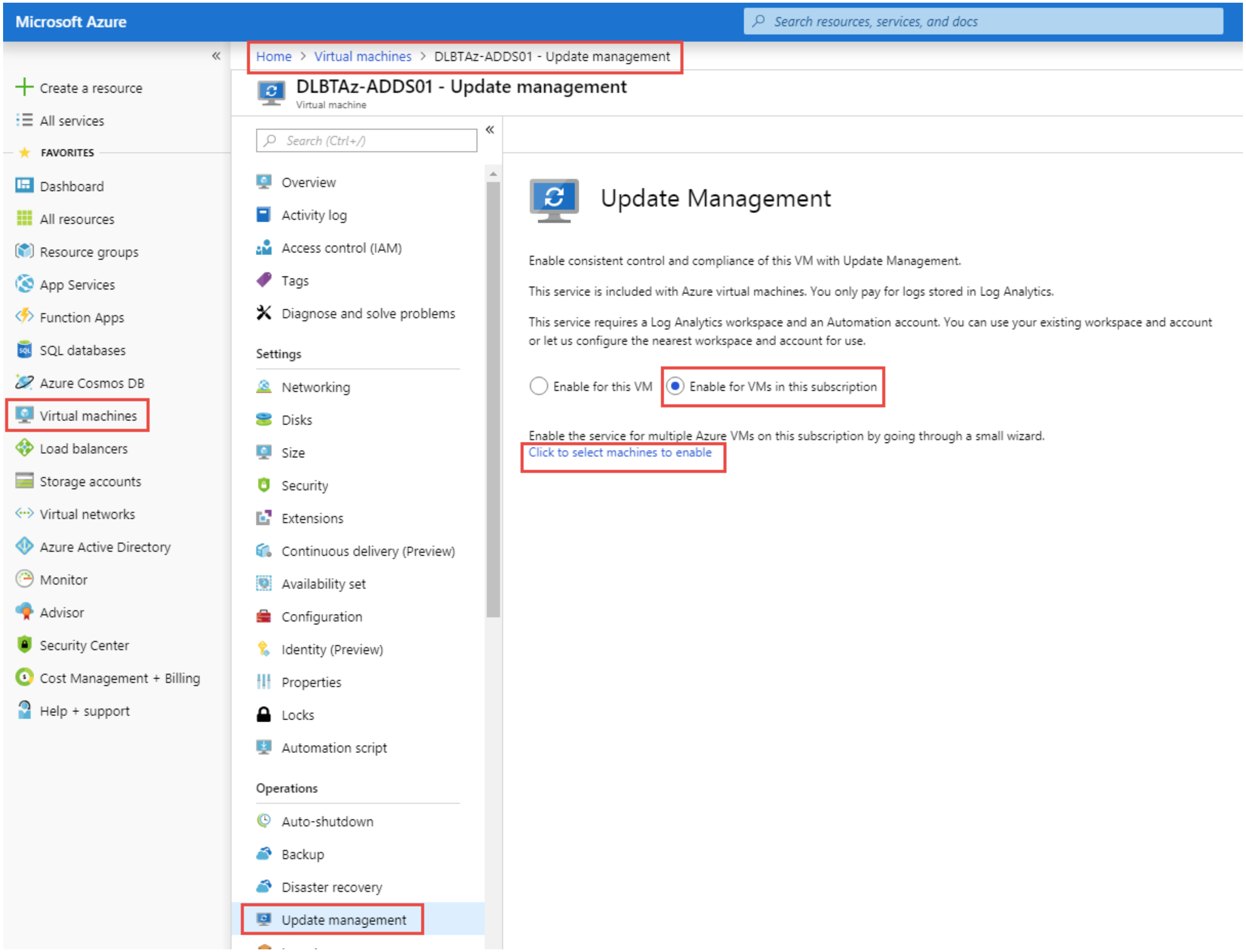
* Resource group: ○ Create new ● Use existing

AzureLogAnalytics_RG01

* Location: East US

* Pricing tier: Per GB

Go into ‘Update Management’ for any one of your VMs, and choose to enable it for all VMs in your subscription:



Update Management

Enable consistent control and compliance of this VM with Update Management.

This service is included with Azure virtual machines. You only pay for logs stored in Log Analytics.

This service requires a Log Analytics workspace and an Automation account. You can use your existing workspace and account or let us configure the nearest workspace and account for use.

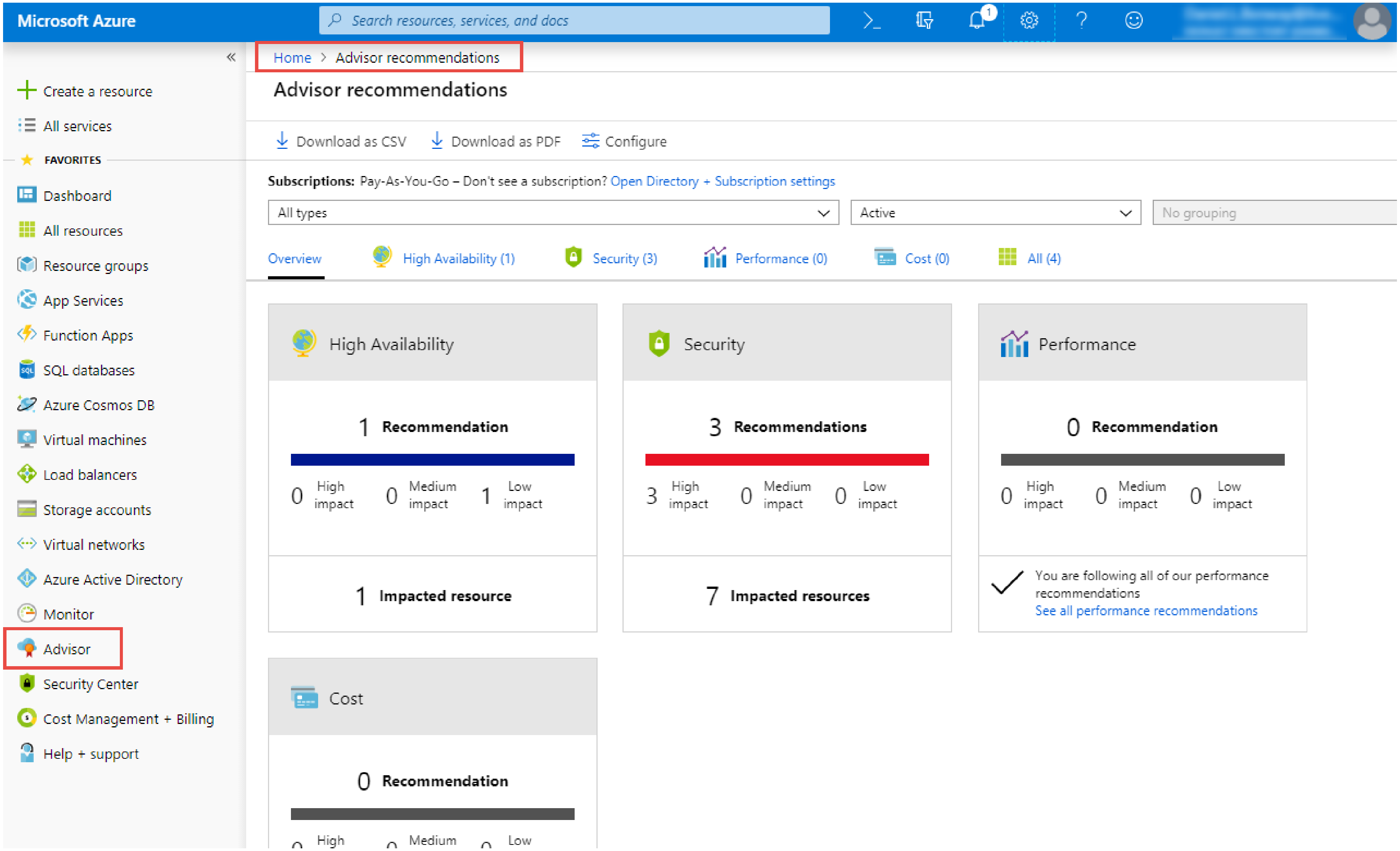
○ Enable for this VM ● Enable for VMs in this subscription

Enable the service for multiple Azure VMs on this subscription by going through a small wizard.
Click to select machines to enable

Azure Advisor:

(jump to TOC)

Be sure to periodically look at the recommendations from Azure Advisor:



Advisor recommendations

Subscriptions: Pay-As-You-Go – Don't see a subscription? Open Directory + Subscription settings

All types | Active | No grouping

High Availability

1 **Recommendation**

0 High impact | 0 Medium impact | 1 Low impact

1 **Impacted resource**

Security

3 **Recommendations**

3 High impact | 0 Medium impact | 0 Low impact

7 **Impacted resources**

Performance

0 **Recommendation**

0 High impact | 0 Medium impact | 0 Low impact

✓ You are following all of our performance recommendations

See all performance recommendations

Cost

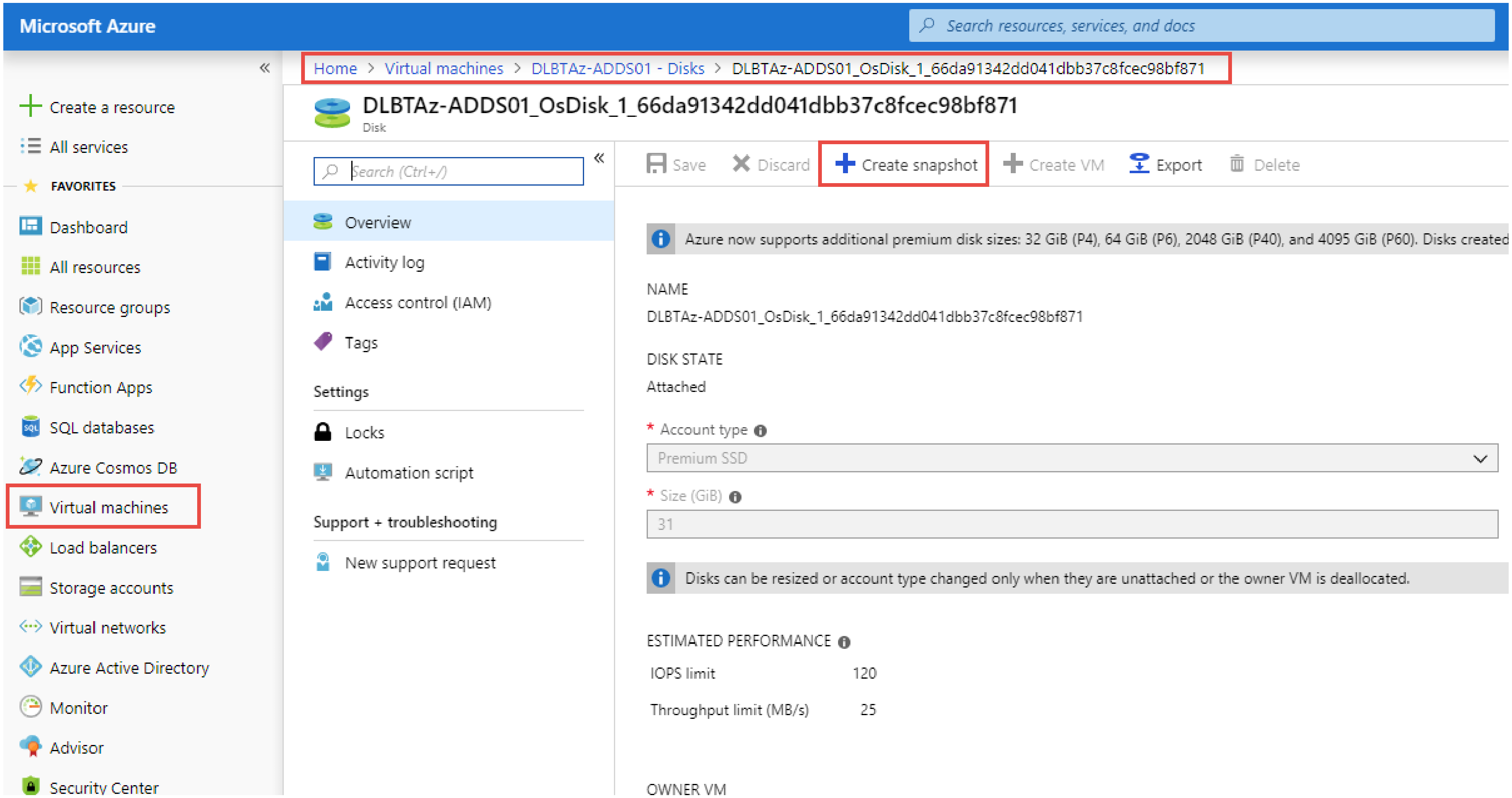
0 **Recommendation**

0 High | 0 Medium | 0 Low

Snapshotting Your VMs:

(jump to TOC)

Here’s where you create snapshots of your VMs:



DLBTAz-ADDS01_OsDisk_1_66da91342dd041dbb37c8fcec98bf871
Disk

Azure now supports additional premium disk sizes: 32 GiB (P4), 64 GiB (P6), 2048 GiB (P40), and 4095 GiB (P60). Disks created

NAME
DLBTAz-ADDS01_OsDisk_1_66da91342dd041dbb37c8fcec98bf871

DISK STATE
Attached

* Account type
Premium SSD

* Size (GiB)
31

Disks can be resized or account type changed only when they are unattached or the owner VM is deallocated.

ESTIMATED PERFORMANCE

IOPS limit	120
Throughput limit (MB/s)	25

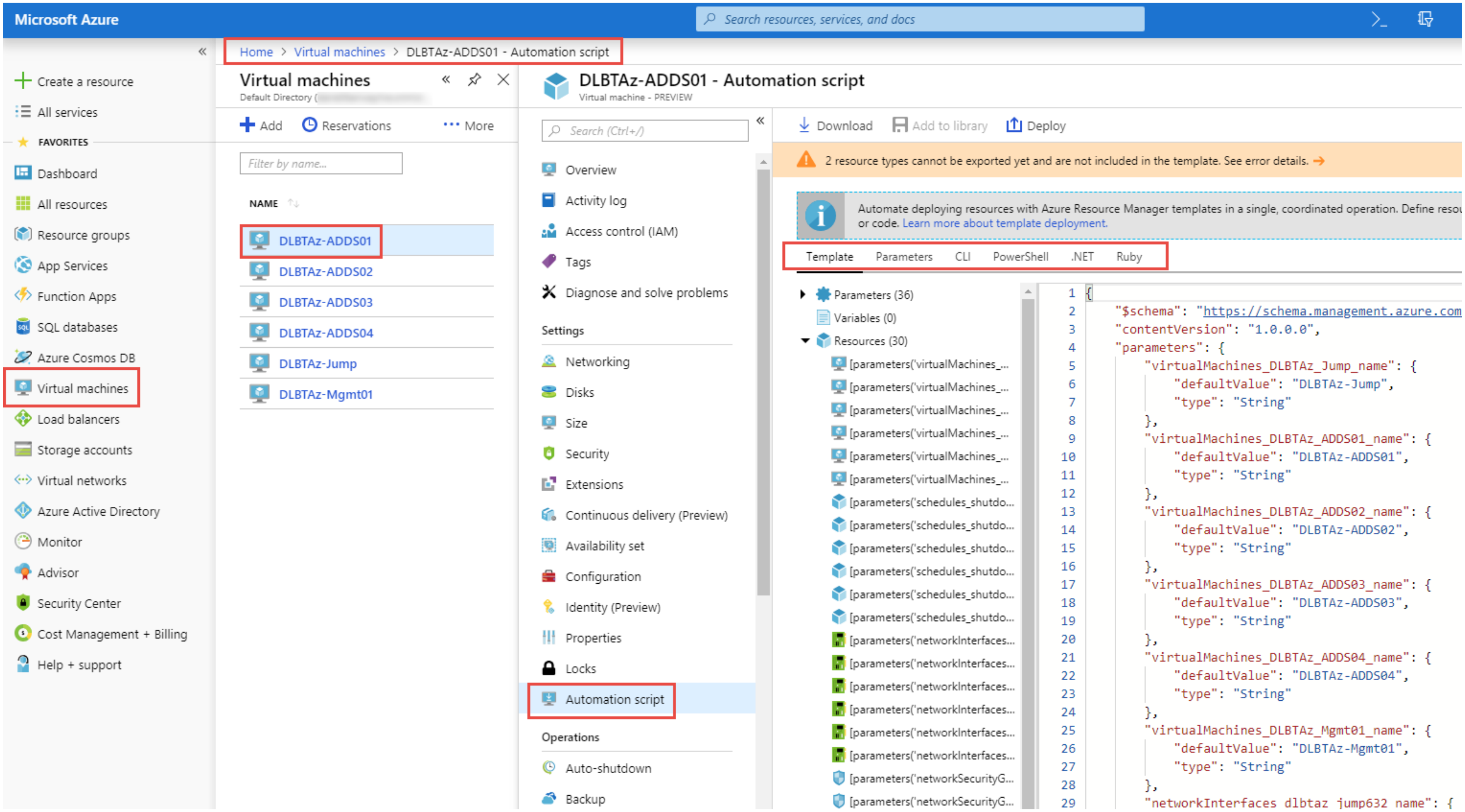
OWNER VM

NOTE: if your VM has more than just an OS drive, you’ll need to snapshot each drive if you want the whole VM to be shapshotted.

ARM Templates:

(jump to TOC)

An ARM template is the JSON (JavaScript Object Notation) code that can be used to deploy your VMs (instead of clicking through the GUI). If you'd like to see the ARM template associated with your VMs, go into 'Automation script' under 'Settings' as shown here:


Microsoft Azure
Search resources, services, and docs
Home > Virtual machines > DLBTAz-ADDS01 - Automation script
Create a resource
All services
FAVORITES
Dashboard
All resources
Resource groups
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Virtual machines
Default Directory (
Add
Reservations
More
Filter by name...
NAME
DLBTAz-ADDS01
DLBTAz-ADDS02
DLBTAz-ADDS03
DLBTAz-ADDS04
DLBTAz-Jump
DLBTAz-Mgmt01
DLBTAz-ADDS01 - Automation script
Virtual machine - PREVIEW
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Disks
Size
Security
Extensions
Continuous delivery (Preview)
Availability set
Configuration
Identity (Preview)
Properties
Locks
Automation script
Operations
Auto-shutdown
Backup
Download
Add to library
Deploy
Template
Parameters
CLI
PowerShell
.NET
Ruby
Parameters (36)
Variables (0)
Resources (30)
[parameters('virtualMachines_...
[parameters('virtualMachines_...
[parameters('virtualMachines_...
[parameters('virtualMachines_...
[parameters('virtualMachines_...
[parameters('virtualMachines_...
[parameters('schedules_shutdo...
[parameters('schedules_shutdo...
[parameters('schedules_shutdo...
[parameters('schedules_shutdo...
[parameters('schedules_shutdo...
[parameters('schedules_shutdo...
[parameters('networkInterfaces...
[parameters('networkInterfaces...
[parameters('networkInterfaces...
[parameters('networkInterfaces...
[parameters('networkInterfaces...
[parameters('networkInterfaces...
[parameters('networkSecurityG...
[parameters('networkSecurityG...

2 resource types cannot be exported yet and are not included in the template. See error details. →

Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Define resou
or code. Learn more about template deployment.

```
{
    "$schema": "https://schema.management.azure.com
    "contentVersion": "1.0.0.0",
    "parameters": {
        "virtualMachines_DLBTAz_Jump_name": {
            "defaultValue": "DLBTAz-Jump",
            "type": "String"
        },
        "virtualMachines_DLBTAz_ADDS01_name": {
            "defaultValue": "DLBTAz-ADDS01",
            "type": "String"
        },
        "virtualMachines_DLBTAz_ADDS02_name": {
            "defaultValue": "DLBTAz-ADDS02",
            "type": "String"
        },
        "virtualMachines_DLBTAz_ADDS03_name": {
            "defaultValue": "DLBTAz-ADDS03",
            "type": "String"
        },
        "virtualMachines_DLBTAz_ADDS04_name": {
            "defaultValue": "DLBTAz-ADDS04",
            "type": "String"
        },
        "virtualMachines_DLBTAz_Mgmt01_name": {
            "defaultValue": "DLBTAz-Mgmt01",
            "type": "String"
        },
        "networkInterfaces_dlbtaz_jump632_name": {
```