



Microsoft Cloud Workshop

Restrict Access to PaaS Services Resources with Virtual
Network Service Endpoints Using the Azure Portal

Hands-on lab step-by-step

October 2018

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2017 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Contents

Restrict Access to PaaS Resources with Service Endpoints hands-on lab step-by-step	1
Abstract and learning objectives	1
Networking References	2
Exercise 1: Log in to Azure	3
Exercise 2: Create a Virtual Network.....	3
Exercise 3: Enable a Service Endpoint	4
Exercise 4: Restrict Network Access for a Subnet	6
Exercise 5: Restrict Network Access to a Resource.....	8
Create a storage account	8
Exercise 6: Create a File Share in the Storage Account	9
Exercise 7: Restrict Network Access to a Subnet	10
Exercise 8: Create Virtual Machines	11
Create the first virtual machine	11
Create the second virtual machine	13
Exercise 9: Confirm Access to Storage Account	14
Exercise 10: Confirm Access is Denied to Storage Account	15
Exercise 11: Clean Up Resources.....	16

Restrict Access to PaaS Resources with Service Endpoints hands-on lab step-by-step

Abstract and learning objectives

Virtual Network (VNet) service endpoints extend virtual network private address space and the identity of VNets to the Azure services, over a direct connection. Endpoints allow customers to secure critical Azure service resources only to their virtual networks. Traffic from each VNet traveling to the Azure service always remains on the Microsoft Azure backbone network.

The student will create a Service Endpoint on a virtual network, restrict access to a file share created inside a storage container, and attempt to gain access in a way that showcases how Service Endpoints lock down access to PaaS services in Azure.

Networking References

- 1) [Azure Virtual Network Overview](#)
- 2) [Azure Virtual Network FAQ](#)
- 3) [IP Addresses](#)
 - a. [Public IP Addresses](#)
 - b. [Internal IP Addresses](#)
- 4) DNS
 - a. [Azure DNS](#)
 - b. [Name Resolution for Azure VNets](#)
- 5) Connectivity for Azure Virtual Networks
 - a. [Site-to-Site VPN](#)
 - b. [VNet-to-VNet VPN](#)
 - c. [Point-to-Site VPN](#)
 - d. [Regional VNet Peering](#)
 - e. [Global VNet Peering](#)
 - f. [ExpressRoute Overview](#)
- 6) Load Balancers
 - a. [Azure Load Balancer](#)
 - b. [Azure Traffic Manager](#)
 - c. [Azure Application Gateway](#)
- 7) Network Security Strategies
 - a. [DMZ Between Azure and On-Premises](#)
 - b. [DMZ Between Azure and the Internet](#)
 - c. [Network Security Groups](#)
 - d. [User Defined Routes](#)
 - e. [Virtual Network Service Tunneling](#)
 - f. [Web Application Firewall](#)
 - g. [Service Endpoints](#)
 - h. [Network Virtual Appliances](#)
- 8) Monitoring
 - a. [Network Watcher](#)
 - b. [Network Performance Monitor Overview & Solution](#)
 - c. [ExpressRoute Monitor](#)
 - d. [DNS Analytics](#)
 - e. [Service Endpoint Monitoring](#)

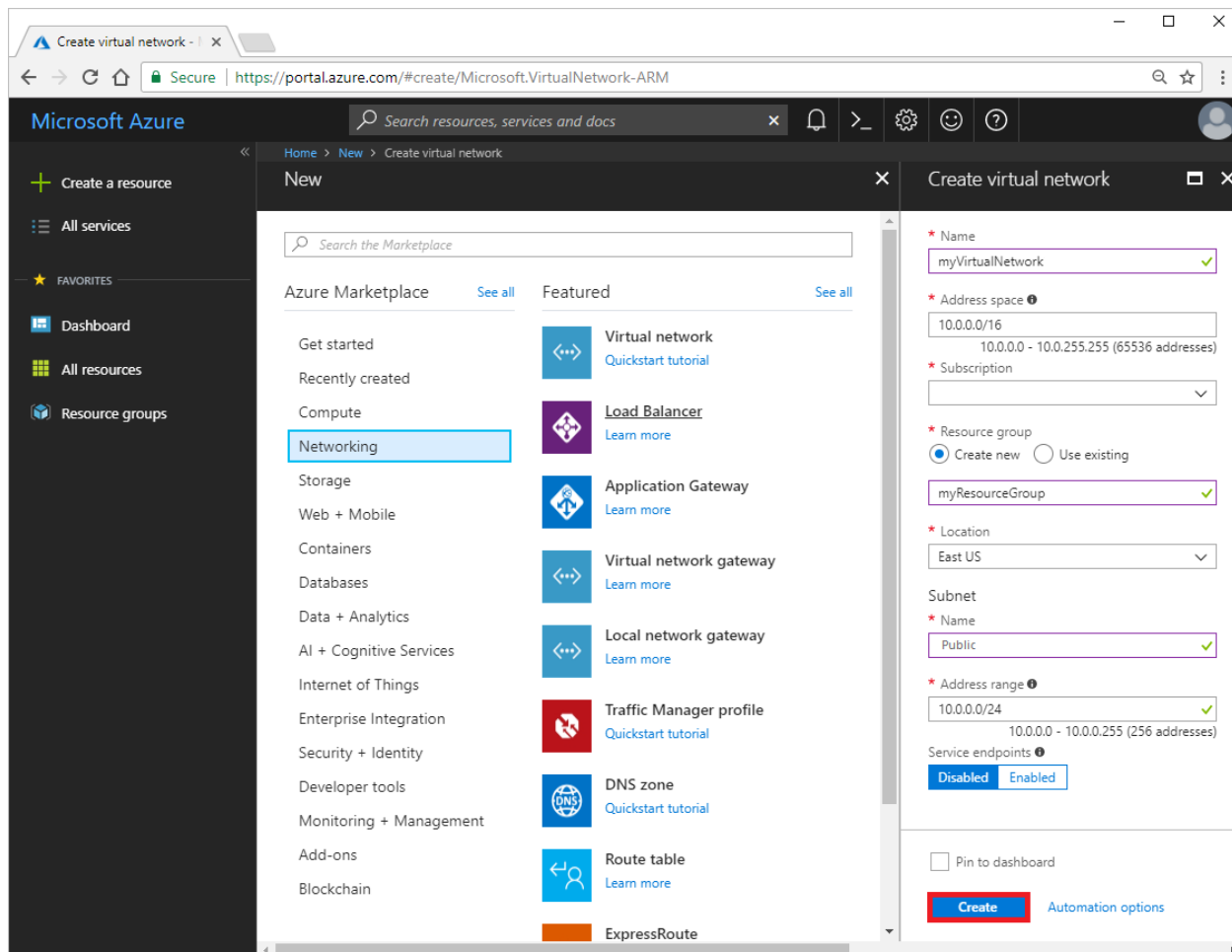
Exercise 1: Log in to Azure

Log in to the Azure portal at <https://portal.azure.com>.

Exercise 2: Create a Virtual Network

1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Networking**, and then select **Virtual network**.
3. Enter, or select, the following information, and then select **Create**:

Setting	Value
Name	myVirtualNetwork
Address space	10.0.0.0/16
Subscription	Select your subscription
Resource group	Select Create new and enter <i>myResourceGroup</i> .
Location	Select East US
Subnet Name	Public
Subnet Address range	10.0.0.0/24
Service endpoints	Disabled

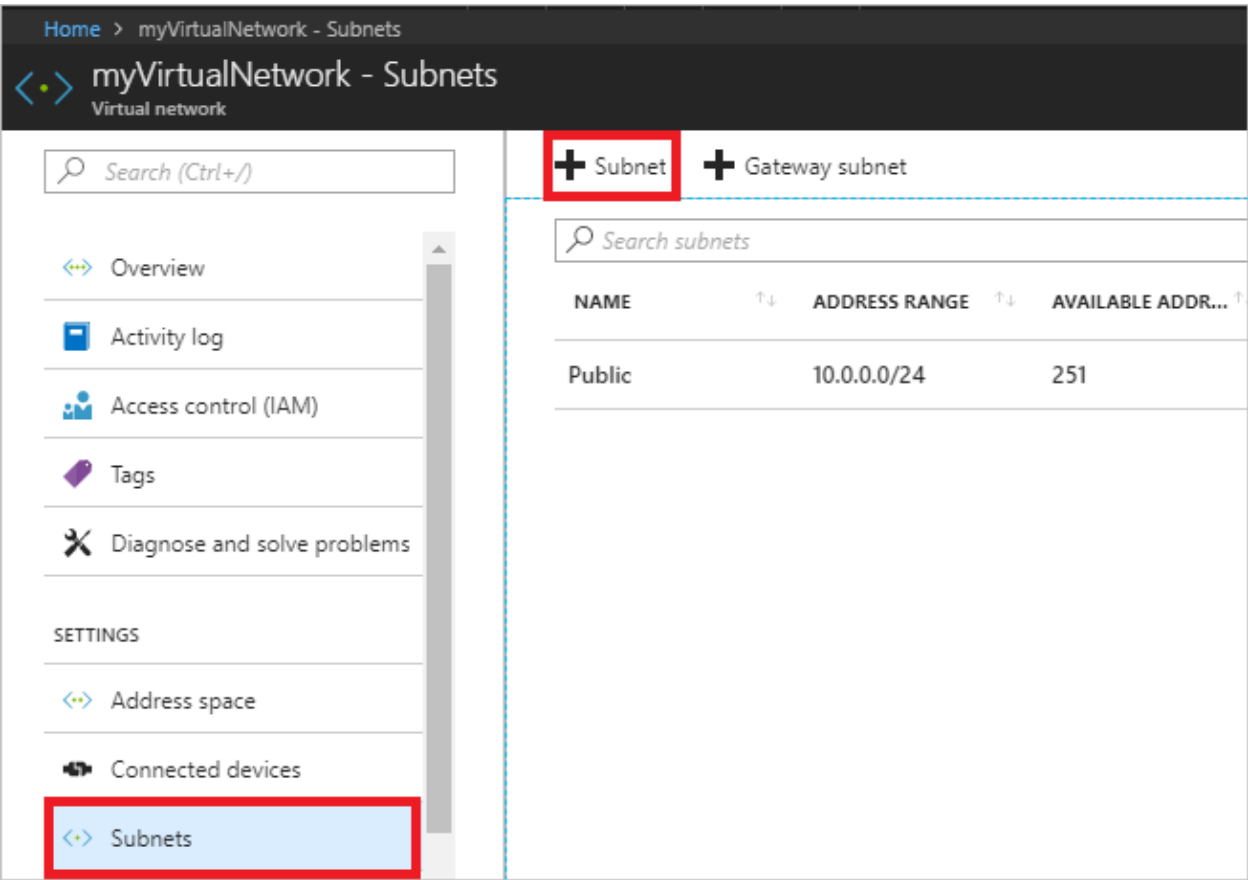


4.

Exercise 3: Enable a Service Endpoint

Service endpoints are enabled per service, per subnet. Create a subnet and enable a service endpoint for the subnet.

1. In the **Search resources, services, and docs** box at the top of the portal, enter *myVirtualNetwork*. When **myVirtualNetwork** appears in the search results, select it.
2. Add a subnet to the virtual network. Under **SETTINGS**, select **Subnets**, and then select **+ Subnet**, as shown in the following picture:



3. Under **Add subnet**, select or enter the following information, and then select **OK**:

Setting	Value
Name	Private
Address range	10.0.1.0/24
Service endpoints	Select Microsoft.Storage under Services

Caution

Before enabling a service endpoint for an existing subnet that has resources in it, see [Change subnet settings](#).

Exercise 4: Restrict Network Access for a Subnet

By default, all VMs in a subnet can communicate with all resources. You can limit communication to and from all resources in a subnet by creating a network security group, and associating it to the subnet.

1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Networking**, and then select **Network security group**.
3. Under **Create a network security group**, enter, or select, the following information, and then select **Create**:

Setting	Value
Name	myNsgPrivate
Subscription	Select your subscription
Resource group	Select Use existing and select <i>myResourceGroup</i> .
Location	Select East US

4. After the network security group is created, enter *myNsgPrivate*, in the **Search resources, services, and docs** box at the top of the portal. When **myNsgPrivate** appears in the search results, select it.
5. Under **SETTINGS**, select **Outbound security rules**.
6. Select **+ Add**.
7. Create a rule that allows outbound communication to the Azure Storage service. Enter, or select, the following information, and then select **Add**:

Setting	Value
Source	Select VirtualNetwork
Source port ranges	*
Destination	Select Service Tag
Destination service tag	Select Storage
Destination port ranges	*

Setting	Value
Protocol	Any
Action	Allow
Priority	100
Name	Allow-Storage-All

8. Create another outbound security rule that denies communication to the internet. This rule overrides a default rule in all network security groups that allows outbound internet communication. Complete steps 5-7 again, using the following values:

Setting	Value
Source	Select VirtualNetwork
Source port ranges	*
Destination	Select Service Tag
Destination service tag	Select Internet
Destination port ranges	*
Protocol	Any
Action	Deny
Priority	110
Name	Deny-Internet-All

9. Under **SETTINGS**, select **Inbound security rules**.

10. Select **+ Add**.
11. Create an inbound security rule that allows Remote Desktop Protocol (RDP) traffic to the subnet from anywhere. The rule overrides a default security rule that denies all inbound traffic from the internet. Remote desktop connections are allowed to the subnet so that connectivity can be tested in a later step. Under **SETTINGS**, select **Inbound security rules**, select **+Add**, enter the following values, and then select **Add**:

Setting	Value
Source	Any
Source port ranges	*
Destination	Select VirtualNetwork
Destination port ranges	3389
Protocol	Any
Action	Allow
Priority	120
Name	Allow-RDP-All

12. Under **SETTINGS**, select **Subnets**.
13. Select **+ Associate**
14. Under **Associate subnet**, select **Virtual network** and then select **myVirtualNetwork** under **Choose a virtual network**.
15. Under **Choose subnet**, select **Private**, and then select **OK**.

Exercise 5: Restrict Network Access to a Resource

The steps necessary to restrict network access to resources created through Azure services enabled for service endpoints varies across services. See the documentation for individual services for specific steps for each service. The remainder of this tutorial includes steps to restrict network access for an Azure Storage account, as an example.

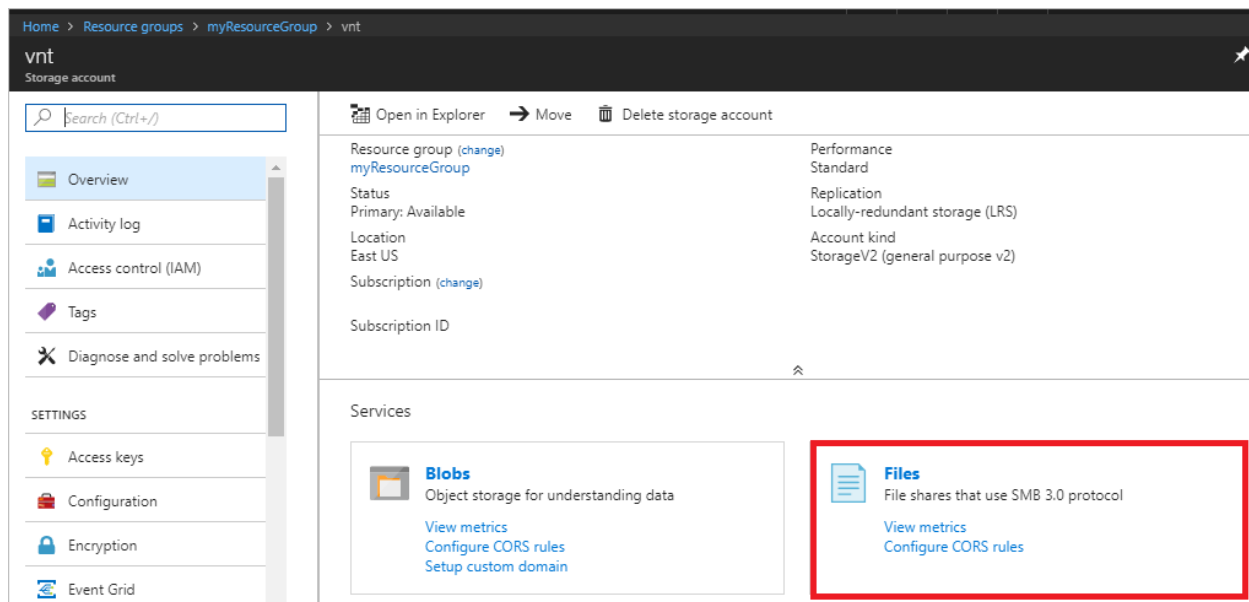
Create a storage account

1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Storage**, and then select **Storage account - blob, file, table, queue**.
3. Enter, or select, the following information, accept the remaining defaults, and then select **Create**:

Setting	Value
Name	Enter a name that is unique across all Azure locations, between 3-24 characters in length, using only numbers and lower-case letters.
Account kind	StorageV2 (general purpose v2)
Location	Select East US
Replication	Locally-redundant storage (LRS)
Subscription	Select your subscription
Resource group	Select Use existing and select <i>myResourceGroup</i> .

Exercise 6: Create a File Share in the Storage Account

1. After the storage account is created, enter the name of the storage account in the **Search resources, services, and docs** box, at the top of the portal. When the name of your storage account appears in the search results, select it.
2. Select **Files**, as shown in the following picture:



3. Select **+ File share**.

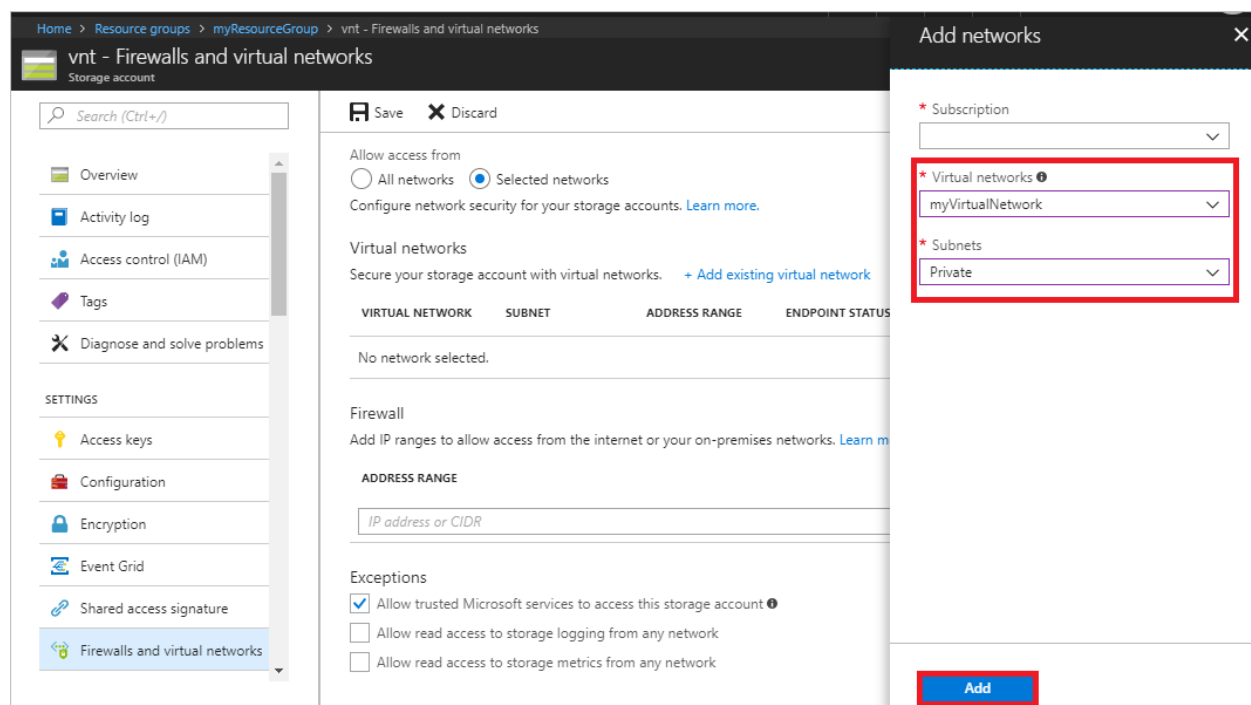
4. Enter *my-file-share* under **Name**, and then select **OK**.
5. Close the **File service** box.

Exercise 7: Restrict Network Access to a Subnet

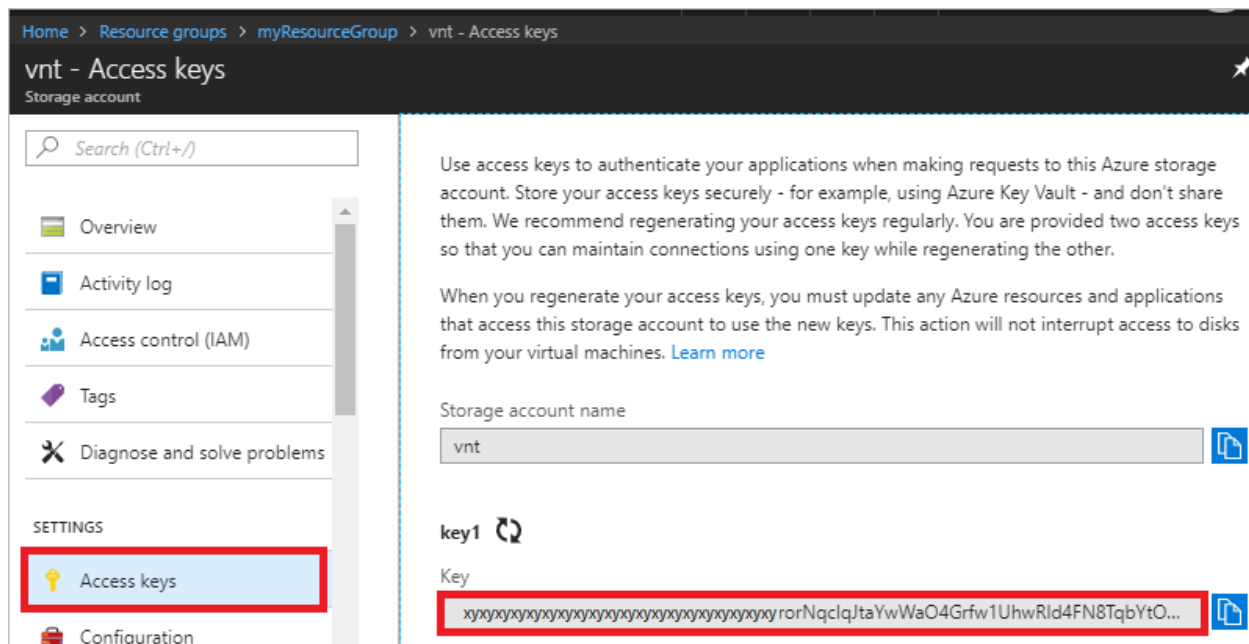
By default, storage accounts accept network connections from clients in any network, including the internet. Deny network access from the internet, and all other subnets in all virtual networks, except for the *Private* subnet in the *myVirtualNetwork* virtual network.

1. Under **SETTINGS** for the storage account, select **Firewalls and virtual networks**.
2. Select **Selected networks**.
3. Select **+Add existing virtual network**.
4. Under **Add networks**, select the following values, and then select **Add**:

Setting	Value
Subscription	Select your subscription.
Virtual networks	Select myVirtualNetwork , under Virtual networks
Subnets	Select Private , under Subnets



5. Select **Save**.
6. Close the **Firewalls and virtual networks** box.
7. Under **SETTINGS** for the storage account, select **Access keys**, as shown in the following picture:



- Note the **Key** value, as you'll have to manually enter it in a later step when mapping the file share to a drive letter in a VM.

Exercise 8: Create Virtual Machines

To test network access to a storage account, deploy a VM to each subnet.

Create the first virtual machine

1. Select **+ Create a resource** found on the upper, left corner of the Azure portal.
2. Select **Compute**, and then select **Windows Server 2016 Datacenter**.
3. Enter, or select, the following information and then select **OK**:

Setting	Value
Name	myVmPublic
User name	Enter a user name of your choosing.
Password	Enter a password of your choosing. The password must be at least 12 characters long and meet the defined complexity requirements .
Subscription	Select your subscription.

Setting	Value
Resource group	Select Use existing and select myResourceGroup .
Location	Select East US .

Home > New > Create virtual machine > Basics

Create virtual machine

Basics

- 1 Basics**
Configure basic settings
- 2 Size**
Choose virtual machine size
- 3 Settings**
Configure optional features
- 4 Summary**
Windows Server 2016 Datacen...

* Name
myVmPublic ✓

VM disk type ⓘ
SSD ▼

* User name
azureuser ✓

* Password
..... ✓

* Confirm password
..... ✓

Subscription
▼

* Resource group ⓘ
☐ Create new ☒ Use existing
 myResourceGroup ▼

* Location
East US ▼

OK

- 4.
5. Select a size for the virtual machine and then select **Select**.
6. Under **Settings**, select **Network** and then select **myVirtualNetwork**. Then select **Subnet**, and select **Public**, as shown in the following picture:

Home > New > Create virtual machine > Settings

Create virtual machine

1 Basics Done ✓

2 Size Done ✓

3 Settings Configure optional features >

4 Summary Windows Server 2016 Datacenter >

Settings

High availability

Availability zone (Preview) ⓘ

None ▾

No availability zones are available for the location you have selected. Current supported locations are: East US 2, Central US, West Europe, France Central.

* Availability set ⓘ >

None

Storage

Use managed disks ⓘ

No Yes

Network

* Virtual network ⓘ >

myVirtualNetwork

* Subnet ⓘ >

Public (10.0.0.0/24)

OK

7. Under **Network Security Group**, select **Advanced**. The portal automatically creates a network security group for you that allows port 3389, which you'll need open to connect to the virtual machine in a later step. Select **OK** on the **Settings** page.
8. On the **Summary** page, select **Create** to start the virtual machine deployment. The VM takes a few minutes to deploy, but you can continue to the next step while the VM is creating.

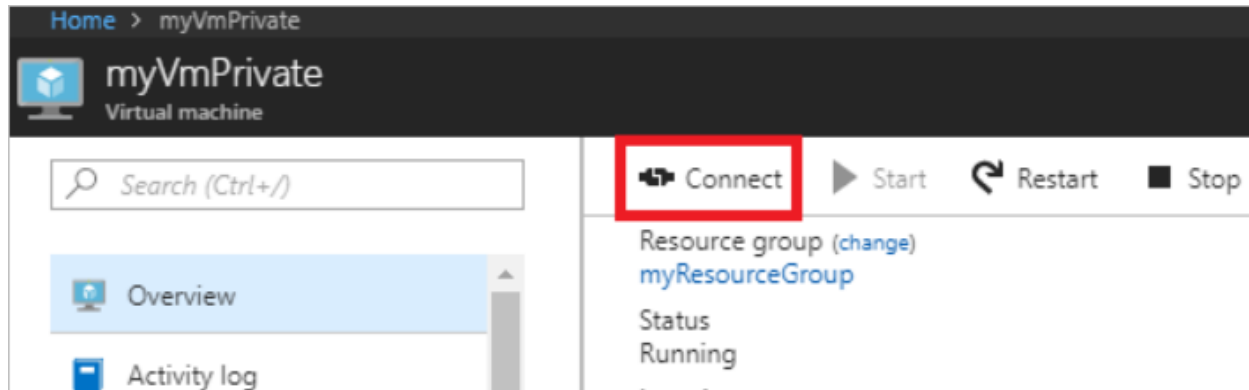
Create the second virtual machine

Complete steps 1-7 again, but in step 3, name the virtual machine *myVmPrivate* and in step 5, select the **Private** subnet.

The VM takes a few minutes to deploy. Do not continue to the next step until it finishes creating and its settings open in the portal.

Exercise 9: Confirm Access to Storage Account

1. Once the *myVmPrivate* VM finishes creating, Azure opens the settings for it. Connect to the VM by selecting the **Connect** button, as shown in the following picture:



2. After selecting the **Connect** button, a Remote Desktop Protocol (.rdp) file is created and downloaded to your computer.
3. Open the downloaded rdp file. If prompted, select **Connect**. Enter the user name and password you specified when creating the VM. You may need to select **More choices**, then **Use a different account**, to specify the credentials you entered when you created the VM.
4. Select **OK**.
5. You may receive a certificate warning during the sign-in process. If you receive the warning, select **Yes** or **Continue**, to proceed with the connection.
6. On the *myVmPrivate* VM, map the Azure file share to drive Z using PowerShell. Before running the commands that follow, replace `<storage-account-key>` and `<storage-account-name>` with values you supplied and retrieved in Create a storage account.

```
$acctKey = ConvertTo-SecureString -String "<storage-account-key>" -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential -ArgumentList
"Azure\<storage-account-name>", $acctKey

New-PSDrive -Name Z -PSProvider FileSystem -Root "\\<storage-account-
name>.file.core.windows.net\my-file-share" -Credential $credential
```

PowerShell returns output similar to the following example output:

Name	Used (GB)	Free (GB)	Provider	Root
----	-----	-----	-----	----
Z			FileSystem	\\vnt.file.core.windows.net\my-
f...				

The Azure file share successfully mapped to the Z drive.

7. Confirm that the VM has no outbound connectivity to the internet from a command prompt:
ping bing.com

You receive no replies, because the network security group associated to the *Private* subnet does not allow outbound access to the internet.

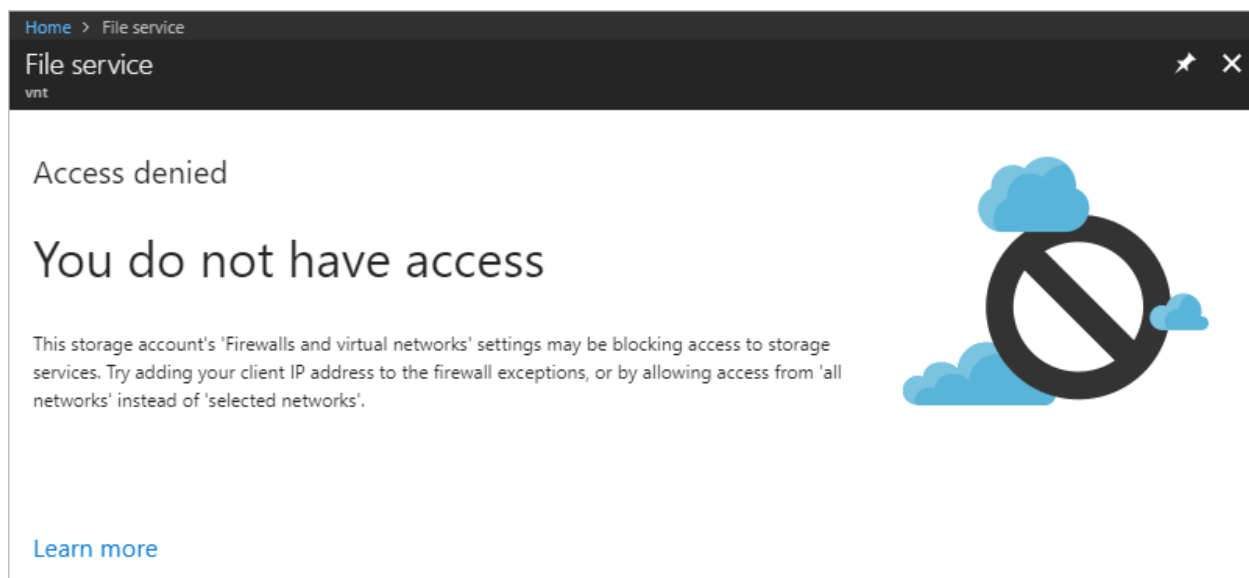
8. Close the remote desktop session to the *myVmPrivate* VM.

Exercise 10: Confirm Access is Denied to Storage Account

1. Enter *myVmPublic* In the **Search resources, services, and docs** box at the top of the portal.
2. When **myVmPublic** appears in the search results, select it.
3. Complete steps 1-6 in [Confirm access to storage account](#) for the *myVmPublic* VM.

After a short wait, you receive a `New-PSDrive : Access is denied` error. Access is denied because the *myVmPublic* VM is deployed in the *Public* subnet. The *Public* subnet does not have a service endpoint enabled for Azure Storage. The storage account only allows network access from the *Private* subnet, not the *Public* subnet.

4. Close the remote desktop session to the *myVmPublic* VM.
5. From your computer, browse to the Azure [portal](#).
6. Enter the name of the storage account you created in the **Search resources, services, and docs** box. When the name of your storage account appears in the search results, select it.
7. Select **Files**.
8. You receive the error shown in the following picture:



Access is denied, because your computer is not in the *Private* subnet of the *MyVirtualNetwork* virtual network.

Exercise 11: Clean Up Resources

When no longer needed, delete the resource group and all resources it contains:

1. Enter *myResourceGroup* in the **Search** box at the top of the portal. When you see **myResourceGroup** in the search results, select it.
2. Select **Delete resource group**.
3. Enter *myResourceGroup* for **TYPE THE RESOURCE GROUP NAME:** and select **Delete**.