Deploying FortiTester-VM on Azure

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

TABLE OF CONTENTS

About FortiTester on Azure

FortiTester™ appliances offer enterprises and service providers a cost-effective solution for performance testing and validating their network security infrastructure and services, providing a comprehensive range of application test cases to evaluate equipment and right-size infrastructure. All test functionality is included in one simple device-based license.

FortiTester provides powerful yet easy-to-use test cases that simulate many applications and a case history browser for simple analysis. It enables you to establish performance standards and run audits to validate they continue to be met. The virtual appliance version provides an ideal tester for NFV and SDN environments.

You deploy FortiTester-VM in the Microsoft Azure cloud platform as part of a virtual network.

Azure CLI on Ubuntu

Azure CLI supports various Linux distributions, and this article describes the installation on ubuntu18.04.

1. Install Azure CLI client. See Azure CLI for details.
2. Log in to Azure platform with the command:
   ```
   az login
   ```
   The web page will pop up, enter the username and password for the Azure platform.

Creating resource groups

Resource groups allow you to organize and manage related Azure resources.

1. Create a resource group with the command:
   ```
   az group create --name [resource group name] --location [location name]
   ```
2. Create a storage account with the command:
   ```
   az storage account create -g [resource group name] -n [storage account name]
   --sku Standard_LRS
   ```
3. Create a container to hold VHD file with the command:
   ```
   az storage container create --account-name [storage account name] -n [storage
   container name]
   ```

Creating the FortiTester Deployment Image

Obtaining the Deployment Image

1. Go to the Fortinet support site (https://support.fortinet.com) and log in.
2. Navigate to **Download > Firmware Images**.
3. Under **Select Product**, select **FortiTester**, then select the firmware version directory.
4. Download the image file **FTS_VM_AZURE_BYOL-vxxx-buildxxxx-FORTINET.out.azure.zip**, where vxxxx is the major version number, and buildxxxx is the build number.

Uploading the FortiTester Deployment Image to Azure

Upload the **boot.vhd** file to Azure platform with the command:

```
az storage blob upload --account-name [storage account name] --container-name
[storage container name] -n [name of the file uploaded to Azure platform] -f ./
[the .vhd file name].
```

Creating the FortiTester Deployment Image

Create images with the command:

```
az image create -g [resource group name] -n [image name]
--os-type linux --source [URL].
```

The default URL is `https://<storage account name>.blob.core.windows.net/<storage container name>/<name of the file uploaded to Azure platform>`.

Creating virtual machine instances

Before creating virtual machines, you need to create virtual networks, network security groups, and network security rules to manage network interfaces and traffic network interfaces. Here are the steps to deploy through the command line interface.

1. Create virtual networks.

   - Create the management network port with the command:
     ```
     az network vnet create -g [resource group name] --name [virtual network name] --address-prefix [address prefix] --subnet-name [management network port subnet name] --subnet-prefix [subnet prefix]
     ```
   - Create the traffic network port with the command:
     ```
     az network vnet subnet create -g [resource group name] --vnet-name [virtual network name] --subnet-name [traffic network port subnet name] --address-prefix [address prefix]
     ```

2. Create network security groups.
   - Create the management network security group with the command:
     ```
     az network nsg create -g [resource group name] --name [management network security group name].
     ```
   - Create the management network security group rules with the command:
     ```
     az network nsg rule create -g [resource group name] --nsg-name [management network security group name] --priority 100 --direction Inbound --source-address-prefixes "*" --source-port-ranges "*" --destination-port-ranges 80 443 22 --access Allow --protocol TCP --description "Allow management port access" --name [management security group rule name]
     ```
   - Create the traffic network security group with the command:
     ```
     az network nsg create -g [resource group name] --name [traffic network security group name].
     ```
   - Create the traffic network security group rules with the two commands below:
     ```
     az network nsg rule create -g [resource group name] --nsg-name [traffic network security group name] --priority 100 --direction Inbound --source-address-prefixes "*" --source-port-ranges "*" --destination-port-ranges "*" --access Allow --protocol "*" --description "Allow traffic port test" --name AllowTrafficInBound

     az network nsg rule create -g [resource group name] --nsg-name [traffic network security group name] --priority 100 --direction Outbound --source-address-prefixes "*" --source-port-ranges "*" --destination-port-ranges "*" --access Allow --protocol "*" --description "Allow traffic port test" --name AllowTrafficOutBound
     ```
3. Create a public IP with the command:
   ```
   az network public-ip create -g [resource group name] --name [public IP name].
   ```
4. Create network interfaces.
   a. Create a management port with the command:
      ```
      az network nic create -g [resource group name] --name [management port network interface name] --vnet-name [virtual network name] --subnet
      ```

```
[management network port subnet name] --accelerated-networking true --
public-ip-address [public IP name] --network-security-group [management
network security group name].
```

b. Create traffic port1 with the command:

```
az network nic create -g [resource group name] --name [traffic port1 name]
--vnet-name [virtual network name] --subnet [traffic network port subnet
name] --accelerated-networking true --network-security-group [traffic
network security group name].
```

c. Create traffic port2 with the command:

```
az network nic create -g [resource group name] --name [traffic port2 name]
--vnet-name [virtual network name] --subnet [traffic network port subnet
name] --accelerated-networking true --network-security-group [traffic
network security group name].
```

5. Create virtual machines with the command:

```
az vm create -g [resource group name] --image [image name] --data-disk-sizes-
gb [data disk size in gb] --size [instance size] --name [product name-
version] --authentication-type password --admin-username [admin username] --
nics [management port network interface name] [traffic port1 name] [traffic
port2 name].
```

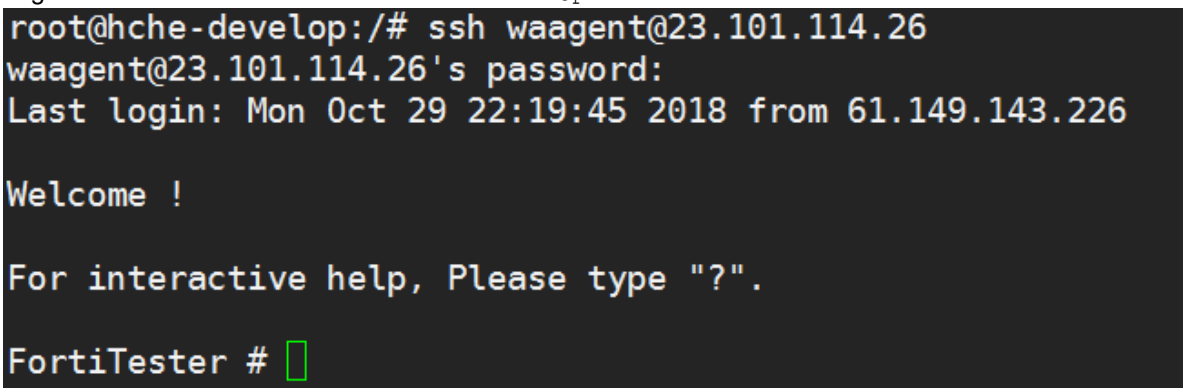
Enter the password twice.

The FortiTester should be deployed on instances that support hyperthreading, and accelerated networking. Supported series are: D/Dsv3, E/Esv3, Fsv2, Lsv2, Ms/Mms and Ms/Mmsv2. The recommend instance is Standard_Ds3_v2.

The value of parameter `--data-disk-sizes-gb` should be 64 GB or larger.

Launching the FortiTester instance

1. Navigate to Dashboard > [instance name], click **Start** to start the instance.
2. Login via SSH with the command `ssh username@publicIP`.



3. Login via the web with the username and password.
   Use the password in Step 5 of Creating virtual machine instances on page 8.