Efw is the Guest OS firewall and doesn't have the rules to enable SSH traffic.

References

N/A

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*Azure Virtual Machine – Linux*	*Routing Azure Virtual Machine V3\Cannot Connect to my VM\My configuration change impacted connectivity*	*Root Cause - Windows Azure\Compute\Virtual Machines\Guest OS - Linux\Isolated\IPTables stopping connectivity*	

Refresher / Training Template

- For the purpose of training or following along with this TSG, you can use the following link to deploy a VM with this scenario built-in. You will need to enable JIT for the VM. This lab is not to be shared with customers.

  Deploy to Azure

Customer Enablement

N/A

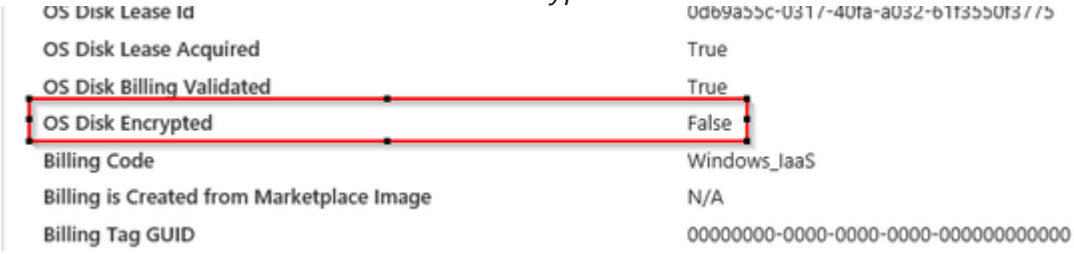
Mitigation

This action plan involves making changes to a Linux file. For that you may want to use vi editor. If you don't know how to use, it, please refer to vi Cheat Sheet

Backup OS disk and setting up the Troubleshooting environment

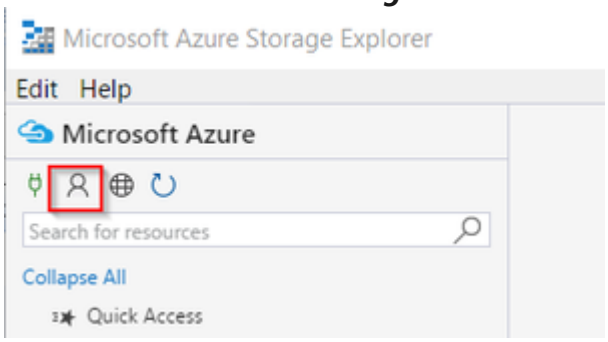
▼ Click here to expand or collapse this section

1. Before doing anything, please validate if this is an encrypted VM. On ASC check on the Resource Explorer on the VMCard for the value *OS Disk Encrypted*

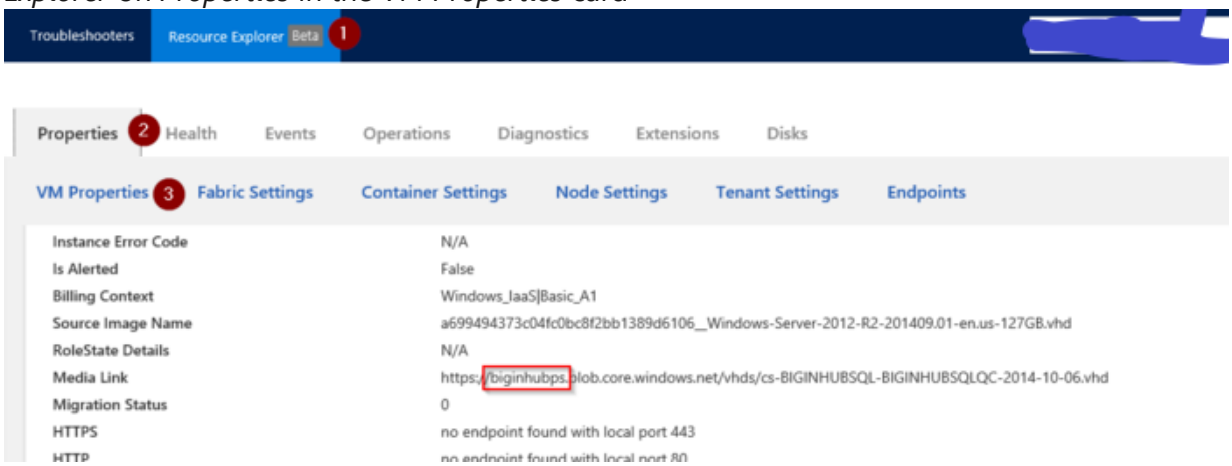


2. If the OS Disk is encrypted, then
    1. Proceed to Unlock an encrypted disk

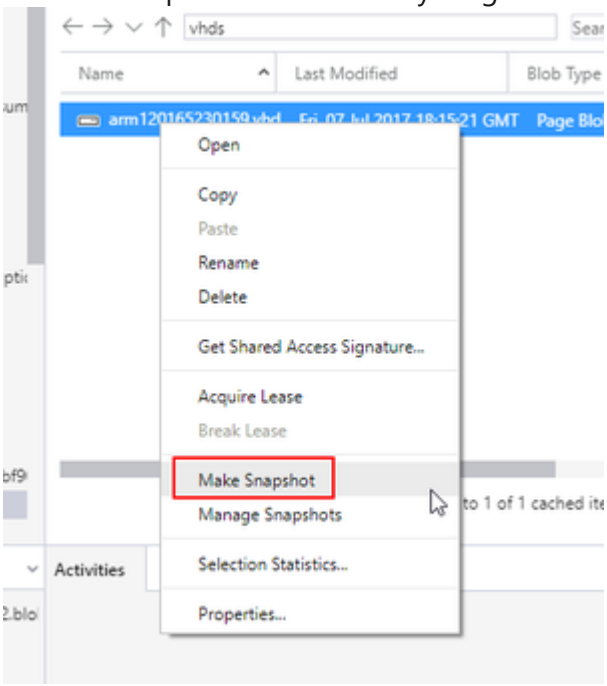
3. Now proceed to do a copy of the OS disk, this will help in case of a rollback for recovery or RCA in a later stage
4. Power the machine down and once it is stopped de-allocated to do the copy.
5. Create a snapshot
    1. If the **disk is unmanaged**, this could be done by using Microsoft Azure Storage Explorer or Azure Powershell
        1. Using Microsoft Azure Storage Explorer
            1. Once the customer download the tool, proceed to add the Azure account details so you can access the storage accounts
            2. Click on ***Add Account Settings*** then ***Add an account...***



            3. Go to the storage account where the OS disk is, you can see this on ASC under *Resource Explorer* on *Properties* in the *VM Properties* card



4. Create a snapshot of this disk by a right click over the disk and select *Make Snapshot*



2. Using Azure Powershell
    1. You can follow How to Clone a disk using Powershell

2. If the **disk is managed**, use Azure portal to take a snapshot
    1. Sign in to the Azure portal.
    2. Starting in the upper-left, click New and search for snapshot.
    3. In the Snapshot blade, click Create.
    4. Enter a Name for the snapshot.
    5. Select an existing Resource group or type the name for a new one.
    6. Select an Azure datacenter Location.
    7. For Source disk, select the Managed Disk to snapshot.
    8. Select the Account type to use to store the snapshot. We recommend Standard_LRS unless you need it stored on a high performing disk.
    9. Click Create.

6. Now prepare your environment to work with your disk
    1. For *CRP (ARM) not encrypted VMs* we could avoid recreating the VM and instead us the OSDisk Swap API tool:
        1. For unmanaged VMs, copy the snapshot that you took on the former step on a different container on the same storage account. It could be a container as *backupvhds*. This will create a clone of the disk on the new container
        2. For managed VMs, use the snapshot you created to attach it on the rescue VM
        3. From now on, ***use this cloned disk*** to perform changes and fix it.
    2. For *CRP (ARM) encrypted VMs*, *RDFE VMs* go ahead and delete the VM keeping the disk and work by attaching this disk on a troubleshooting VM. For the recreation part you will use:
        1. For RDFE VMs refer to Recreate an RDFE Virtual Machine
        2. For CRP (ARM) encrypted VMs, refer to Unlock an encrypted disk

1. Once the broken OS disk is attached to your rescue VM:

1. Get root access

   ```
   sudo su
   ```

2. Locate the drive name to mount the disk on your rescue VM, look in relevant log file note each Linux is slightly different.
   - **For Ubuntu/debian**:

     ```
     grep SCSI /var/log/kern.log
     ```

   - **For Centos/Suse/Oracle/Redhat**:

     ```
     grep SCSI /var/log/messages
     ```

Online Mitigation

Mitigation 1

1. If the VM is accessible via serial console then run following command to check firewall status

```
root@linuxvm:~# ufw status
Status: active
```

2. To check what port ssh is configured

```
root@linuxvm:~# cat /etc/ssh/sshd_config |grep Port
#Port 22
#GatewayPorts no
```

3. To check if configured port is listening by sshd service

```
root@linuxvm:~# sudo netstat -tnlp | grep :22
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2055/sshd
tcp6       0      0 :::22                   :::*                    LISTEN      2055/sshd
```

4. Add rule to allow ssh

```
root@linuxvm:~# sudo ufw allow ssh
root@linuxvm:~# #sudo ufw reload
```

5. Verify if the rule is added

```
root@ubuntufirewall:~# ufw status
Status: active

To                         Action      From
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
```

6. check if you are able to ssh

Mitigation 2

1. Disable ufw

```
root@linuxvm:~# sudo ufw disable
Firewall stopped and disabled on system startup
```

2. Check if you are able to ssh

Offline mitigation

1. Mount the attached disk onto mountpoint **/rescue**

```
df -h
mkdir /rescue
```

   - **For Red Hat 7.2+**

     ```
     mount -o nouuid /dev/sdc2 /rescue
     ```

   - **For CentOS 7.2+**

     ```
     mount -o nouuid /dev/sdc1 /rescue
     ```

   - **For Debian 8.2+, Ubuntu 16.04+, SUSE 12 SP4+**

     ```
     mount /dev/sdc1 /rescue
     ```

2. Change into */etc/ufw* directory where the original OS disk from resides

```
cd /rescue/etc/ufw/
cp ufw.conf ufw.conf_orig
```

3. Now that you have made a backup of you config you can proceed to make the changes you require using vi, nano or your favorite text editor:

```
vi ufw.conf
```

4. Now you can disable ufw by just changing *enabled* from *yes* to *no*

```
enabled=no
```

5. Umount the disk

```
cd /
umount /rescue
```

6. Detach the now fixed OS disk from the recovery VM

7. Reassemble the original VM

Re-Assemble the original VM

▼ Click here to expand or collapse this section

1. If this is a *CRP (ARM) VMs* and you are following the OSDisk Swap API tool to fix a cloned of the disk, then you can reassemble your VM by:
    1. For **Unmanaged VMs**
        1. Using Powershell run the following:

```
$subscriptionID = "<Subscription ID>"
$rgname = "<Resource Group name>"
$vmname = "<VM Name>"
$vhduri = '<VHD URI of the fixed OS disk>'

Add-AzureRmAccount
Select-AzureRmSubscription -SubscriptionID $subscriptionID
Set-AzureRmContext -SubscriptionID $subscriptionID

$vm = Get-AzureRMVM -ResourceGroupName $rgname-Name $vmname
$vm.StorageProfile.OsDisk.Vhd.Uri = $vhduri
Update-AzureRmVM -ResourceGroupName $rgname -VM $vm
```

        2. Using Cloud Shell (CLI 2.0)

```
az vm update -g <<RESOURCE GROUP>> -n <<VM NAME>> --set StorageProfile.OsDisk.Vhd.Uri=<<VHD
```

    2. For **Managed VMs**
        1. Using Powershell run the following:

```
$name = '<VM Name>'
$resourceGroupName = '<Resource Group name>'
$diskname='<Disk Name>'
$diskResourceInstanceID="<Resource instance ID of the fixed disk>"

#Get the VM details
$vm = get-azurermvm -ResourceGroupName $resourceGroupName -Name $name

#Set the new disk properties and update the VM
Set-AzureRmVMOSDisk -VM $vm -Name $diskname  -ManagedDiskId $diskResourceInstanceID | Update
```

        2. Using Cloud Shell (CLI 2.0)

```
az vm update --name <<VM NAME>> --resource-group <<RESOURCE GROUP>> --os-disk <<RESOURCE INS
```

2. For *RDFE VMs* just go ahead recreate your VM normally. Please refer to How to recreate an RDFE Virtual Machine

After work - Cleanup

If you are uncertain that we may need this snapshot by the end of this case for RCA purposes, then just leave it.

1. If the issue is already fix and no further RCA analysis is needed, then proceed to remove the OS Disk backup we created at the beginning of the case

1. If the **disk is managed** using the portal so the snapshot section and select the snapshot you created previously as a backup.
2. If the **disk is unmanaged** then
    1. If this is an CRP Machine - ARM, then no further action is required
    2. If this is an Classic - RDFE machine, then
        1. Check the storage account where the OS disk of this machine is hosted using Microsoft Azure Storage Explorer right click over the disk and select *Managed Snapshots*
        2. Proceed to delete the snapshot of the broken machine

Need additional help or have feedback?

To engage the Azure RDP-SSH SMEs...	*To provide feedback on this page...*	*To provide kudos on this page...*
Please reach out to the **RDP-SSH SMEs** for faster assistance. Make sure to use the **Ava process** for faster assistance.	Use the **RDP-SSH Feedback** form to submit detailed feedback on improvements or new content ideas for RDP-SSH. ***Please note*** the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.	Use the **RDP-SSH Kudos** form to submit kudos on the page. Kudos will help us improve our wiki content overall! ***Please note*** the link to the page is required when submitting kudos!