Customer reports a problem when trying to connect using ***Azure Bastion***. Bastion as a Service enables customers to connect via RDP or SSH into the machines which reside on the same Vnet on which the Bastion Host was deployed.

To be able to use Bastion to connect to a VM, the following criteria needs to be met:

1. Bastion needs to be successfully deployed on a subnet named **AzureBastionSubnet** at the same Vnet as the VMs Vnet.
2. Ports 3389 for **Windows** and 22 for **Linux** need to be **opened** at the OS firewall.
3. The VM Network stack at the OS level need to be responding. This means that the VM needs to be all the way boot up and available over the network.

Bastion as a Service is currently supported by the *Azure Networking POD*. However due to the case submission workflow in the portal the **Azure VMPOD** might still get cases to:

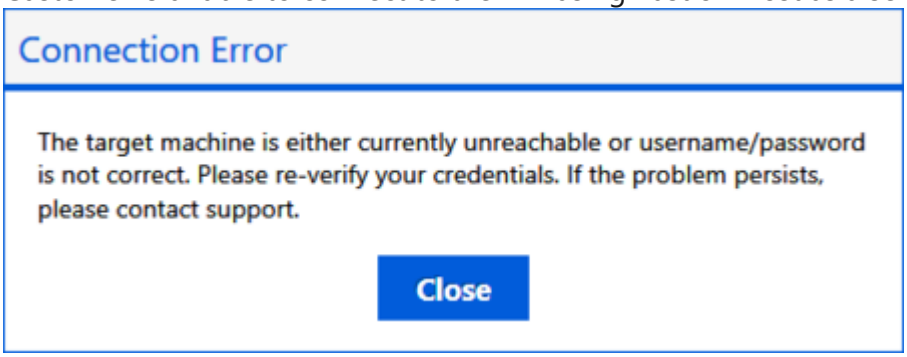
1. Either because the customer wants to use Bastion as a service to connect to the VM and he doesn't know how to file a case to the Bastion product directly
2. Or because the target VM is either not booting or doesn't have connectivity

Azure Bastion is used directly from the portal, and the Sesssion it creates is using https, port 443 on a web browser. On the back-end Bastion reaches out the machines directly on their Vnet using the default SSH (22) or RDP (3389) ports.

During the preview access for this feature, for the customer to be able to see the bastion connection option they will have to access the portal via the link: aka.ms/bastionhost

Symptoms 1

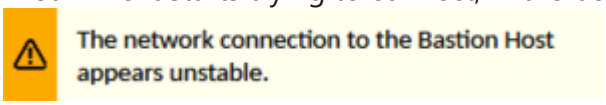
1. Customer is unable to connect to the VM using Bastion Host as a service getting the error:



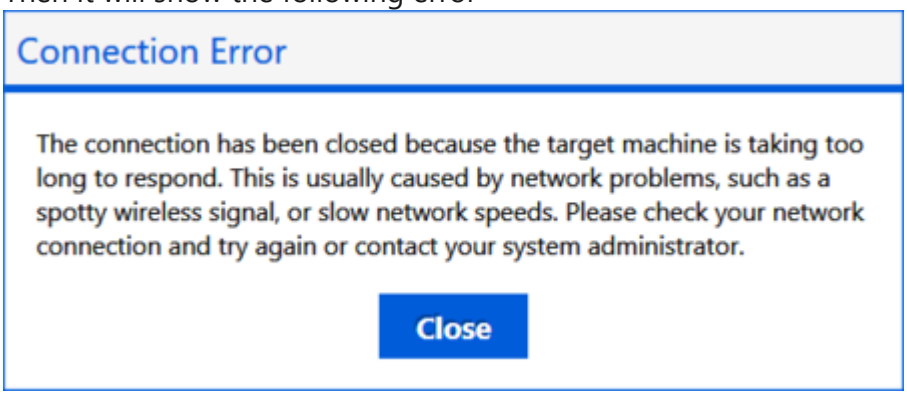
2. If the customer tries to use the normal RDP or SSH on the private/public IP into the Machine directly it fails as well
3. If checked via the Screenshot feature, the OS shows signs of issues.(It could show that the OS did not finish to boot or that there was an Error at the OS level which crashed the machine.)

Symptoms 2

1. Customer is unable to connect to the VM using Bastion Host as a service getting the errors:
    1. First while it starts trying to connect, in the bottom right section of the screen it will show:



2. Then it will show the following error

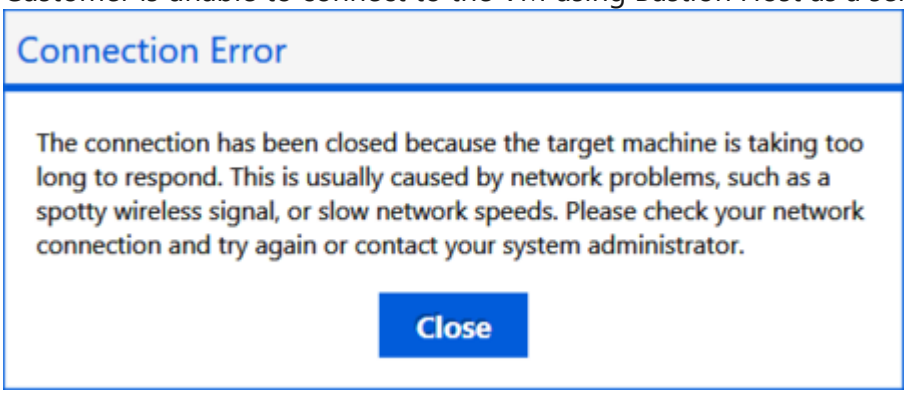


2. VM is reachable on other services via network.
3. If checked via the Screenshot feature, the OS seems to be **Healthy**
4. If the customer tries to connect to the VM directly using RDP/SSH on the private/public IP, it works with no issues

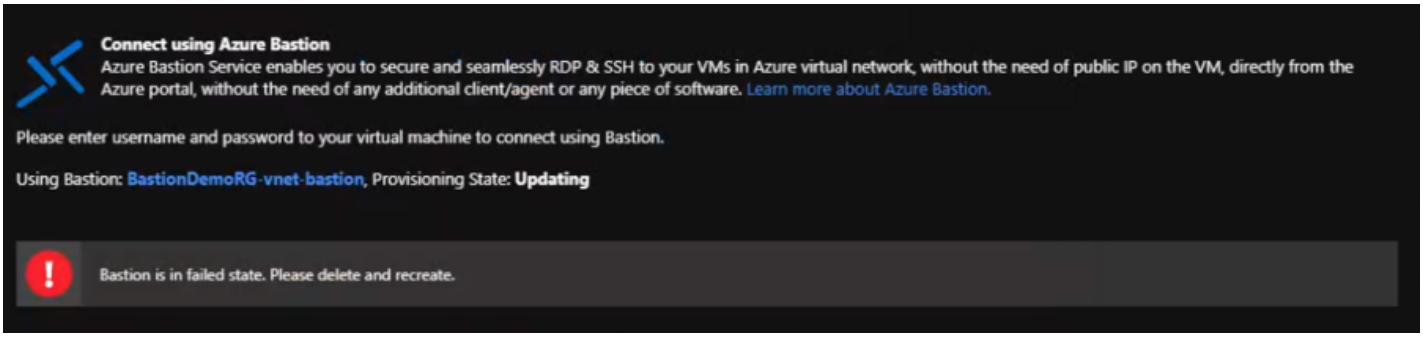
These errors indicates that the machine OS is fully up and running, but that the bastion service is not able to contact the machine on the default RDP or SSH port.

Symptoms 3

1. **If customer tries to RDP or SSH into the machine directly over its private/public IP, it works fine**. The only component not working is the connection using Azure Bastion.
2. Customer is unable to connect to the VM using Bastion Host as a service giving the errors:



or



3. If you are in this scenario, then proceed with *Route Cause Analysis 3* and *Mitigation 3*

Root Cause Analysis

Root Cause Analysis 1

The symptoms indicates that the target VM is healthy and has connectivity but there's connectivity problems between the Bastion host and the VM. In this case, there's some misconfiguration on the Guest OS of the target VM that prevents the connection to the RDP-SSH application. This could be:

1. the default port for RDP/SSH was changed on the Guest OS and the NSGs were not updated properly
2. there's any local firewall not properly updated/open
3. the RDP-SSH port is not working properly
4. etc.

Root Cause Analysis 2

The symptoms indicates that the target VM is healthy and has connectivity but there's connectivity problems between the Bastion host and the VM. In this case, the RDP/SSH port 3389/22 is not opened on the NSG between the Bastion Host and the target VM or there's an UDR messing up the routing between these devices.

Root Cause Analysis 3

If the VM was proven to be healthy and the setup seems to be right, then this will require further investigation. This needs to be provided by the **Azure Networking POD**

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*Bastion - Preview*	*Routing Azure\Connectivity\Failure to connect using RDP*	*Root Cause - Windows Azure\Azure Bastion\Connectivity Issues\RDP\No Connectivity to Workload\Target VM Issues - RDP not configured properly on target VM*	
	Bastion - Preview	*Routing Azure\Connectivity\Failure to connect using SSH*	*Root Cause - Windows Azure\Azure Bastion\Connectivity Issues\SSH\No Connectivity to Workload\Target VM Issues - SSH not configured properly on target VM*	
2	*Bastion - Preview*	*Routing Azure\Connectivity\Failure to connect using RDP*	*Root Cause - Windows Azure\Azure Bastion\Connectivity Issues\SSH\No Connectivity to Workload\Target VM Issues - NSG/UDR*	
	Bastion - Preview	*Routing Azure\Connectivity\Failure to connect using SSH*	*Root Cause - Windows Azure\Azure Bastion\Connectivity Issues\SSH\No Connectivity to Workload\Target VM Issues - NSG/UDR*	
3	*Bastion - Preview*	*Routing Azure\Connectivity\Failure to connect using RDP*	This will depend on the investigation	
	Bastion - Preview	*Routing Azure\Connectivity\Failure to connect using SSH*	This will depend on the investigation	

To know how to flag a bug on a case please refer to How to do Proper Case Coding

Mitigation

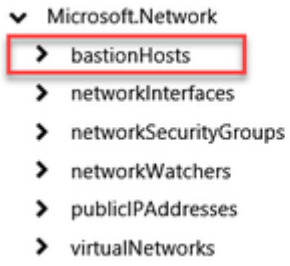
How to validate if customer have Bastion host on their environment

1. In **ASC** go to the affected machine under resource explorer and make a note of the Vnet on which the nic of this machine is configured.

VM Properties

VM Name	Ubuntu18
Resource Group	Bastion
State	Converged
Cluster	N/A
AZSM Cluster Name	N/A
AZSM Cluster	False
Deployment Id / Tenant Name	3ebd922b[redacted]
Id	[redacted]
Deployment Model	Resource Manager
Region	westus
OS	Linux
HyperV Generation Type	Gen1
Create Option	FromImage
Current Power State	deallocated
Provision VMAgent	N/A
Scheduled Events Enabled	N/A
DIPs	N/A
Instance Public IPs	N/A
Load Balancer Public IPs	N/A
Application Gateway Public IPs	N/A
VM Instance Time Created	04/10/2019 15:27:21
Network Interfaces	UBUNTU1879
Virtual Network	Bastion-vnet
Private IP Allocation Method	Dynamic
Subnets	default
Network Security Groups	N/A

2. Now that you have the Vnet name, you can go to **Resource Provider** and select **Microsoft.Networking** in there, if Bastion Host is enable you will see an object type called **BastionHost**.



3. Click on it, and validate the ones that are deployed, as each bastion Host is deployed on a single Vnet, you just need to search for one that shares the same Vnet with your affected machine.

Mitigation 1

1. If the machine have a private IP, then test by doing a direct RDP-SSH connection attempt
    1. If this works, then continue with *Mitigation 2*
    2. If this fails, then follow then
        1. If you find the VM is boot all the way up and has connectivity, then
            1. Check the local firewall is not blocking the RDP-SSH connections
            2. Check that RDP-SSH app is working. Check the if the port number of the app was changed and if that change was reflected on the local firewall and NSGs
            3. Validate if the issue is related to CredSSP. Currently Bastion Host is not patched for CredSSP, hence if the server that is receiving the connection, forces the client to be patched the connection will fail. **This will be addressed before the Feature goes into GA**.
            4. If you found problems on the above items and fix those out and fix the connection attempt, then proceed to close out this case as codded on the *Tracking close code for this volume* section
        2. Re-code the case as
            - Product: *Azure Virtual Machine* `&#xfffd;` *Windows* or *Azure Virtual Machine* `&#xfffd;` *Linux* as appropriate
            - Support Area Path: *Routing Azure Virtual Machine V3\Cannot connect to my VM\Failure to connect using RDP or SSH port*
        3. Continue with RDP-SSH Basic Workflow to determine the reason behind why the machine is not able to accept the requests
2. If the machine have a public IP, you can do the same test as above and see if the connection works
3. If both the public AND private IP works to do a direct RDP-SSH connection, then you successfully ruled out problems with the target VM and Bastion needs to be further investigated. Continue on *Mitigation 3*

Mitigation 2

1. Check the NSGs configuration between the Bastion Host and the target VM and ensure you have the RDP-SSH ports enable.
2. If they are not open, set those up and retry your connection. If it works, then proceed to code the case properly as explained on the *Tracking close code for this volume* section
3. If update the NSGs and you are still unable to connect then proceed with following mitigation

Mitigation 3

1. The Azure Bastion connection needs further investigation. Please update the case with
    - Product: *Bastion - Preview*
    - Support Area Path: *Connectivity\Failure to connect using RDP* or *Connectivity\Failure to connect using SSH* as appropriate
2. Transfer the whole case to *Azure Networking POD*

Escalation

1. If this doesn't work out, please reach out to the Unable to RDP-SSH SME channel on teams for advise providing the case number, issue description and your question

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!