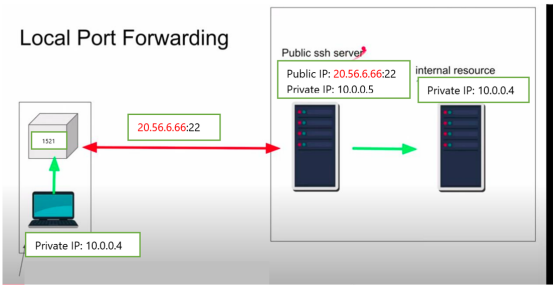
Connecting to ADF via SSH Tunnel

Last updated by | Veena Pachauri | Mar 8, 2023 at 11:23 PM PST

Contents

Scenario

Customer is trying to **copy data from a Database in a private Network without having direct access to it**. To connect to **Oracle, SQL Server, MySQL, PostgreSQL, etc** customers can use SSH tunnel. The image below illustrates such scenario.



For better understanding, I will explain the figure using Azure resources.

- **Azure Windows VM as the internal resource:** This is where customer has the database running. The Azure windows VM with **only private IP**.
- **Azure Linux VM as the public SSH server: This server has access to the DB server(Oracle, SQL Server, MySQL, etc)**. They are part of the same Azure Virtual Network. The SSH server has public static ip and authentication mode ssh key.
- **Azure VM as client machine (10.0.0.4):** In this case the client is a machine in another Azure Virtual Network. **The SHIR is installed here**.
- As you can see in the image above, **for the client 10.0.0.4 to reach the DB Server it must go through the SSH Server**.

Some notes on SSH tunnel

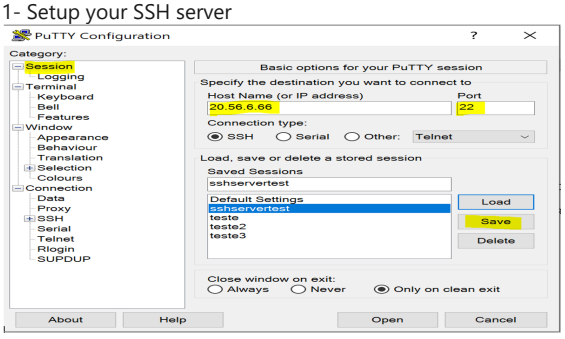
- Connection via SSH tunnel is supported on ADF.
- Port forwarding via SSH (**SSH tunneling**) creates a secure connection between a local computer and a remote machine through which services can be relayed.
- For oracle it allows customers to copy data from oracle in a private Network without having direct access to it.

SSH tunnel setup

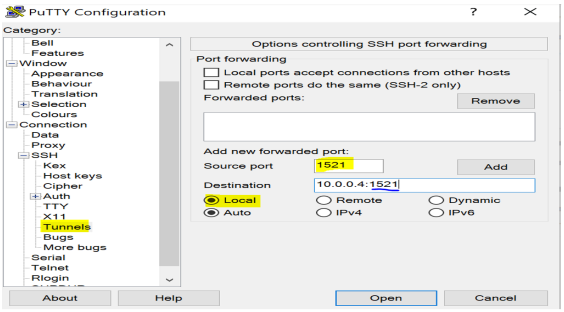
- Customer must ensure that an SSH tunnel is created and that the SSH server can reach the DB server.
- Customer must create the SSH tunnel in the SHIR machine using tools like Putty. You can download and install putty from here.

Creating SSH tunnel using putty

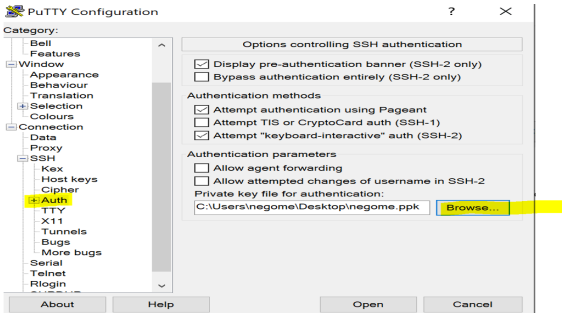
1- Setup your SSH server



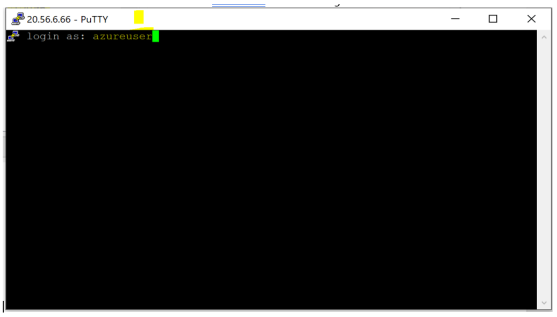
2- Create SSH tunnel Notice, that the destination IP is the IP of the DB server and destination port is port where the DB Server is listening. The source port is the Port where you want the SHIR machine to listen. Click Add.



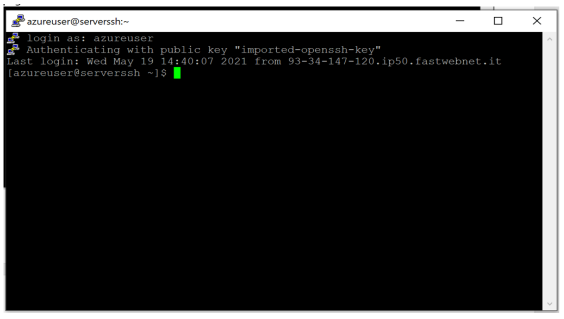
3- Load private key file for authentication It must be a ppk file. If you generate the key using Azure you must convert the .pem file to .ppk format using Putty Gen. Hit open to create the tunnel.



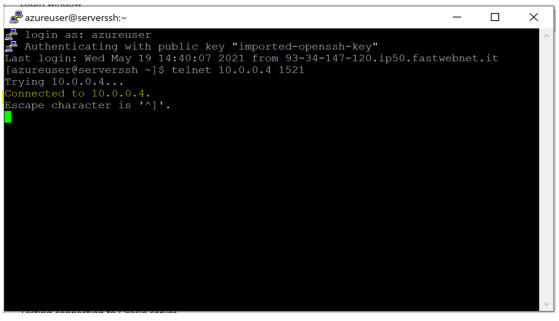
4- Provide the user for Azure VM for the SSH server and hit enter to login



5- Login window



6- Testing connection to DB server Make sure you installed telnet in the SSH server from cmd: **yum install telnet -y**



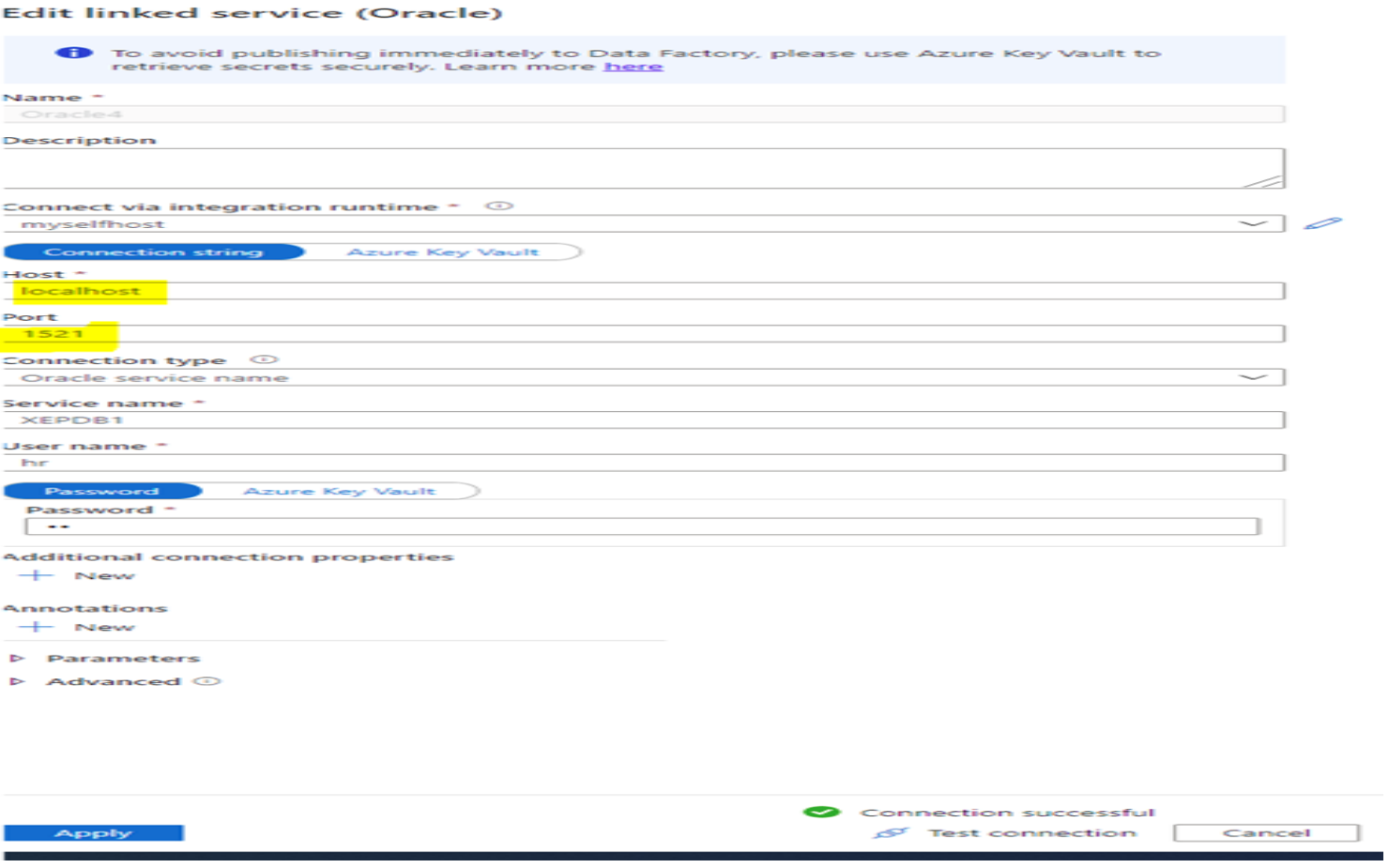
Oracle Scenario repro

You can use the following steps to create an Oracle testing scenario.

1. **Oracle env**: Leverage our Advanced Lab to create an oracle environment. Please, check the step by step here
2. **SSH server:** In Virtual Network created in step, create the SSH server as well.
   - Choose SSH key as authentication mode.
   - Setup NIC network security group as basic.
   - When asked, saved the private key in your local machine. You will need it to connect from the SHIR machine.
3. Make sure that the Oracle VM can be accessed from SSH VM. For testing purpose, you can disable the SHIR machine firewall.
4. **SHIR machine:** use the temple below to create a vm with a SHIR installed. Use the data factory created in step 1 and a different Virtual Network from the one created in one. shir template
5. RDP to your SHIR machine and copy the private key created in step 2. This will be used when creating the SSH tunnel using Putty.
6. Create the SSH tunnel using Putty as indicated in previously and create a new linked service in your ADF using this new SHIR. You should be able to access the oracle DB using the SHIRs created in step 1 and step 4.

Oracle Linked service setup

Provide the oracle linked service details as usually. Notice, that this time your host will be localhost or 127.0.0.1.



Possible issues for incorrect SSH tunnel setup

1. ERROR [08001] [Microsoft][ODBC Oracle Wire Protocol driver][Oracle]Unexpected Network Error
2. ERROR [08001] [Microsoft][ODBC Oracle Wire Protocol driver]Connection refused. Verify Host Name and Port Number.

Ensuring that SSH tunnel is always enabled

Sometimes the SSH tunnel connection closes or the SHIR machine can be restarted. To ensure that there is always a SSH tunnel enabled in the SHIR machine, you can proceed as below.

1. **Create a bat file to start a SSH tunnel** if it does not exist already. Adjust the code below with your inputs. The while section is to ensure that you keep alive the connection. Create a bat file and name it **SSHCreatetunnel.bat** for instances. Please, check here for more about **Plink Non-Interactive SSH Session**.

```
QPROCESS "plink.exe">NUL
IF "%ERRORLEVEL%" == "0"  GOTO SSHtunnelDoesExist
ECHO "starting SSH tunnel"
"C:\Program Files\PuTTY\plink.exe" -batch -i "C:\Users\negome\Desktop\negome.ppk" -L 1521:10.0.0.4:1521 azureuser@20.56.6.66:22  -C -T while true; do echo "ke
GOTO end
:SSHtunnelDoesExist
ECHO "There is already a SSH tunnel established"
:end
```

2. **Create a task schedule to run every 5 minutes**. This will call the bat file created in 1. Please, find a step by step on how to schedule a task here. Please, choose the method 2 as you want to schedule every 5 minutes and only the method 2 allows to configure that.

- **Author:** negome
- **Reviewer:** davzhao
- **Keywords:**

How good have you found this content?