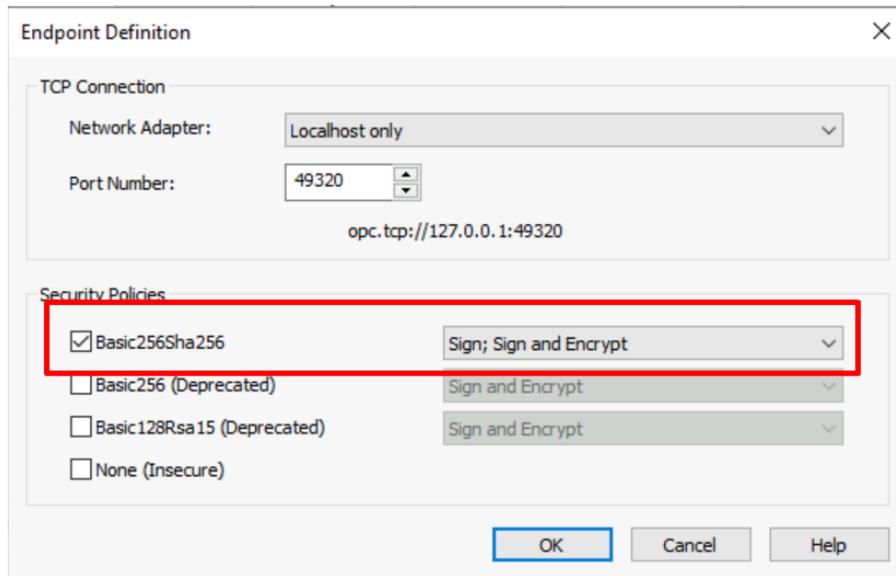


Kepware and Tulip Setup

1. Download Kepware from this [Link](#)
2. Install the latest version of Kepware
3. After Installation, search for the **OPC UA Configuration** in Windows Search Bar
4. Open OPC UA Configuration, go to the Server Endpoints and open the URL having 127.0.0.1:49320 and make the Following Configuration

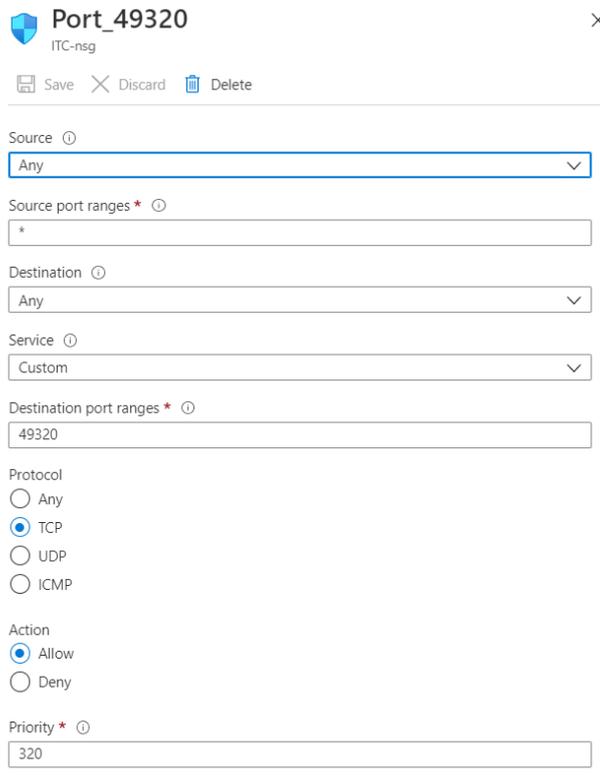


5. Go to Windows Defender Firewall with Advanced Security and create a new Inbound rule with following configurations
 - a. Select TCP
 - b. Select Specific Local Ports 49320
 - c. Select the Allow the Connection
 - d. Unselect Public
 - e. Name it As OPC UA Server Interface (Kepware). (Optional)

6. Create the Inbound rule for the Azure VM by going to Networking Tab as Shown below

Priority	Name	Port	Protocol	Source	Destination	Ac
300	▲ RDP	3389	TCP	Any	Any	✓
310	Port_4334	4334	TCP	Any	Any	✓
320	Port_49320	49320	TCP	Any	Any	✓
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓

Keeware and Tulip Setup



Port_49320 ITC-nsg

Save Discard Delete

Source ⓘ
Any

Source port ranges * ⓘ
*

Destination ⓘ
Any

Service ⓘ
Custom

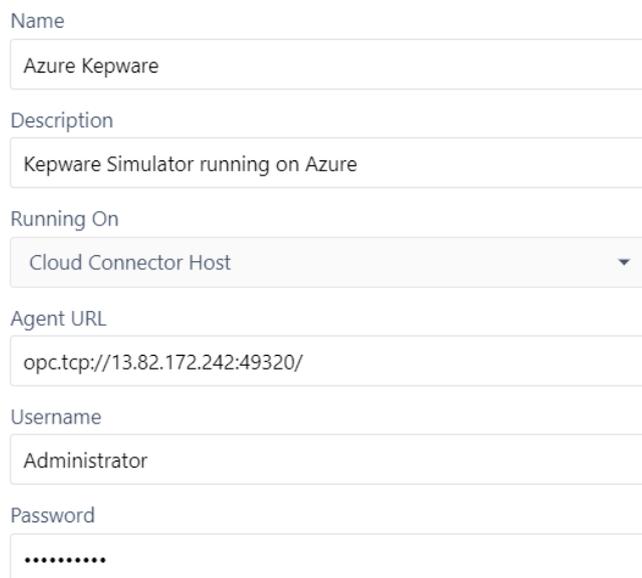
Destination port ranges * ⓘ
49320

Protocol
 Any
 TCP
 UDP
 ICMP

Action
 Allow
 Deny

Priority * ⓘ
320

7. Go to Tulip Environment and go to the Shop Floor → Machines → Machine Data Sources
8. Press on **Create Connector** and type the following configurations:



Name
Azure Keeware

Description
Keeware Simulator running on Azure

Running On
Cloud Connector Host

Agent URL
opc.tcp://13.82.172.242:49320/

Username
Administrator

Password
.....

9. Press on Test, if everything goes as Documented then test gets passed and save button gets enabled.

Kepware and Tulip Setup

Even after this changes the Tulip is not able to connect, then do the follow the below steps

1. Disable the Firewall in the Azure VM:

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer. [Use recommended settings](#)

[What are the recommended settings?](#)

Private networks Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state: Off

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: Network

Notification state: Notify me when Windows Defender Firewall blocks a new app

Guest or public networks Not connected

2. Enable the of the Server Endpoints in the OPC UA Configuration

URL	Security
opc.tcp://kepware-sim-vm:49320	None, Basic128Rsa15 (SE), Basic256 (SE), Basic256Sha256...
opc.tcp://127.0.0.1:49320	None, Basic128Rsa15 (S,SE), Basic256 (S,SE), Basic256Sh...

Enable both of them

Kepware and Tulip Setup

3. Enable all of the Security Policies that are present in the Server EndPoints:

Endpoint Definition ✕

TCP Connection

Network Adapter: Localhost only ▼

Port Number: 49320 ▲▼

opc.tcp://127.0.0.1:49320

Security Policies

<input checked="" type="checkbox"/> Basic256Sha256	Sign; Sign and Encrypt ▼
<input checked="" type="checkbox"/> Basic256 (Deprecated)	Sign; Sign and Encrypt ▼
<input checked="" type="checkbox"/> Basic128Rsa15 (Deprecated)	Sign; Sign and Encrypt ▼
<input checked="" type="checkbox"/> None (Insecure)	

OK Cancel Help

Resources:

https://www.youtube.com/watch?v=pumlhz_h0Qs