Deployment of the Sentieon software to Azure

Release 202112.07

Sentieon, Inc

Apr 24, 2023

Contents

1 Multi-Availability Zone Deployment on Azure

The Sentieon® software is controlled by a license and requires an active Sentieon® license server to run. Deployment on Azure requires setup and configuration of the Sentieon® license server along with setup and configuration of one or more instances for genomic data processing. A minimum deployment will use the following resources and should take approximately 20 minutes:

- An Azure Virtual Network. The default network configuration with the default subnet(s), internet gateway, and route table is assumed in this deployment guide.
- Security groups that can be used to run the Sentieon® license server and the compute nodes.
- A (Standard_B1s) instance running the Sentieon® license server.

The Sentieon® software can be deployed onto additional instances for additional data processing capacity.

With a minimum deployment, customers will be charged by Azure for the instance running the license server and for outbound communication from the Sentieon® license server to the Sentieon® master license server. Adding additional comptute instances to the deployment will increase costs by the price of those instances. Data processing may incur additional costs for data transfer, etc. The Sentieon® software is a proprietary software and this deployment requires a license for the Sentieon® software.

This deployment is supported in the following Azure Regions:

- (Africa) South Africa North
- (Africa) South Africa West
- (Asia Pacific) Australia Central
- (Asia Pacific) Australia Central 2
- (Asia Pacific) Australia East

- (Asia Pacific) Australia Southeast
- (Asia Pacific) Central India
- (Asia Pacific) East Asia
- (Asia Pacific) Japan East
- (Asia Pacific) Japan West
- (Asia Pacific) Jio India Central
- (Asia Pacific) Jio India West
- (Asia Pacific) Korea Central
- (Asia Pacific) Korea South
- (Asia Pacific) South India
- (Asia Pacific) Southeast Asia
- (Asia Pacific) West India
- (Canada) Canada Central
- (Canada) Canada East
- (Europe) France Central
- (Europe) France South
- (Europe) Germany North
- (Europe) Germany West Central
- (Europe) North Europe
- (Europe) Norway East
- (Europe) Norway West
- (Europe) Sweden Central
- (Europe) Switzerland North
- (Europe) Switzerland West
- (Europe) UK South
- (Europe) UK West
- (Europe) West Europe
- (Middle East) Qatar Central
- (Middle East) UAE Central
- (Middle East) UAE North
- (South America) Brazil South
- (South America) Brazil Southeast
- (US) Central US
- (US) Central US EUAP
- (US) East US
- (US) East US 2
- (US) East US 2 EUAP
- (US) East US STG
- (US) North Central US
- (US) South Central US
- (US) West Central US
- (US) West US
- (US) West US 2
- (US) West US 3

This deployment assumes basic familiarity with the Virtual Network and VM services on Azure and familiarity with the Linux command-line interface.

1.1 Deployment of the Sentieon® license server

In order to use the software on Azure, you will need to follow the following installation instructions to deploy a Sentieon® License server to your Virtual Network.

1. Choose an Azure Region to work in. Choose (or create) the Virtual Network where you will run the Sentieon®

tools.
2. Find and record the CIRD block for your Virtual Network.
3. Launch a Standard_B1s instance to run the license server in the selected Virtual Network.
4. Update the security group for the license server (Fig. 1.1 and Fig. 1.2). The security group must:

- Allow inbound TCP communication at a specific port (we use 8990 by default as it is not typically used by other applications). We highly recommend that users choose a port above 1024 so the license server can be run as a non-root user. This rule is used to accept inbound communication from the compute nodes to the license server. You should open TCP at the desired port across your Virtual Network's CIDR block (172.31.0.0/16 in Fig. 1.1) to whitelist traffic from within your network.
- Allow outbound HTTPS communication to Sentieon® license master at master.sentieon.com (IP 52.89.132.242). This is necessary for license validation.
- Allow inbound SSH. This is necessary for administration.
- (Recommended) Allow ICMP communication. This allows for PMTU discovery.

5. Send your Sentieon® support representative the Private IP address of your instance, together with the TCP port you opened in step 4.
6. Download the Sentieon® tools and your license file to the instance.
7. On the Standard_B1s instance, start the license server with the following command. Note that the license server does not need to be started as a root user if a port above 1024 is chosen in step 4.

```
sentieon licsrvr --start [-l <licsrvr_log>] <license_file>
```

8. (Optional) Confirm the license server is working correctly and serving licenses to the license server instance by running following commands. The second command will return the number of available licenses.

```
sentieon licclnt ping -s <IP_addresss>:<PORT> || (echo "Ping Failed"; exit 1)
sentieon licclnt query -s <IP_address>:<PORT> klib
```

9. Launch a Standard_B1s instance within the same Virtual Network to test the license server.
10. Update the security group for the second Virtual Machine (Fig. 1.3 and Fig. 1.4). The security group should:

- Allow inbound SSH. This is necessary for administration.
- Allow outbound TCP communication at the port chosen in step 3, which will be open across your Virtual Network's CIDR block.
- (Recommended) Allow ICMP communication to facilitate communication between the license server and compute nodes.

11. Download the Sentieon® software to the newly launched instance and confirm the license server is working and serving licenses within the Virtual Network by running the following commands on the instance. The second command will return the number of available licenses.

```
sentieon licclnt ping -s <IP_addresss>:<PORT> || (echo "Ping Failed"; exit 1)
sentieon licclnt query -s <IP_address>:<PORT> klib
```

After the license server has been deployed, the license server can be monitored by running the `sentieon licclnt ping` and `sentieon licclnt query` commands on a separate instance, as described in steps 10 and 11, above.

1.2 Deployment of one or more instances for genomic data processing

After the license server is deployed in your Virtual Network, you can deploy the software to one or more additional instances for genomic data processing. These instances can be deployed to any Availability Zone in the Virtual Network. The following steps provide guidance for deploying the Sentieon® software onto newly launched Azure Virtual Machines:

1. Start an Azure Virtual Machine that meets the platform requirements for the Sentieon® software inside your Virtual Network. Assign the instance to the security group created in *step 10* in the above section on deployment

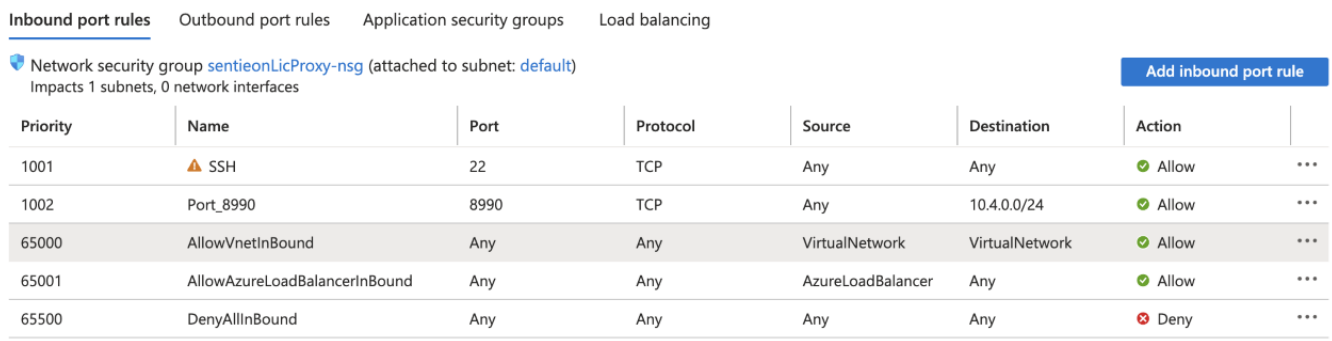

Fig. 1.1: Example license server inbound security group rules

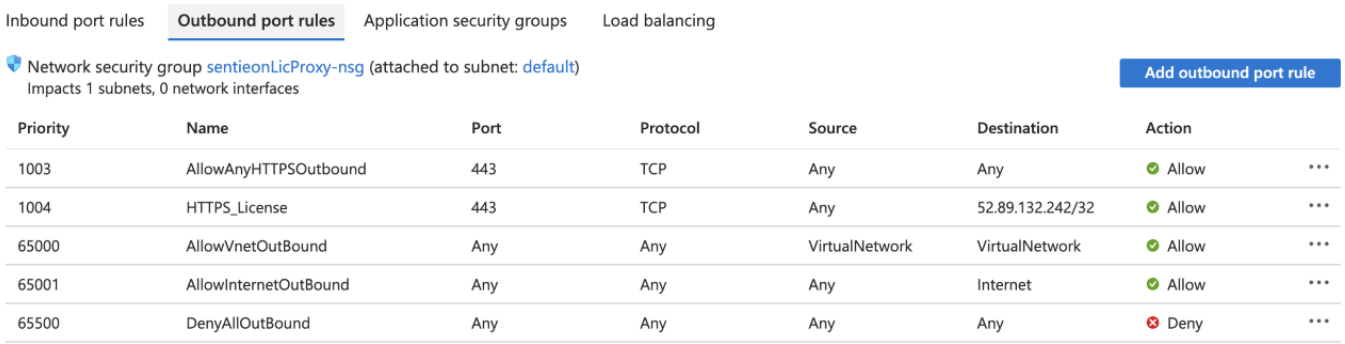

Fig. 1.2: Example license server outbound security group rules

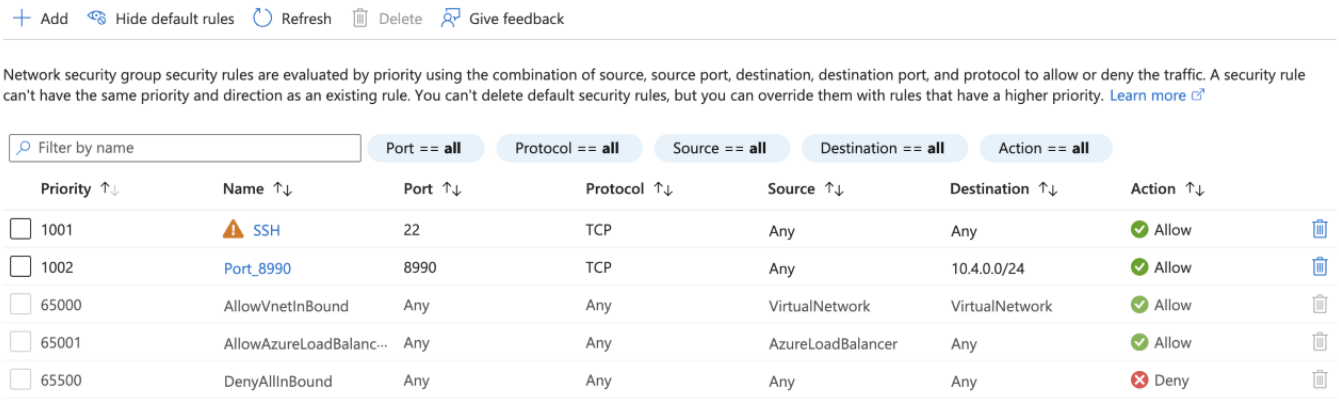

Fig. 1.3: Example compute nodes inbound security group rule

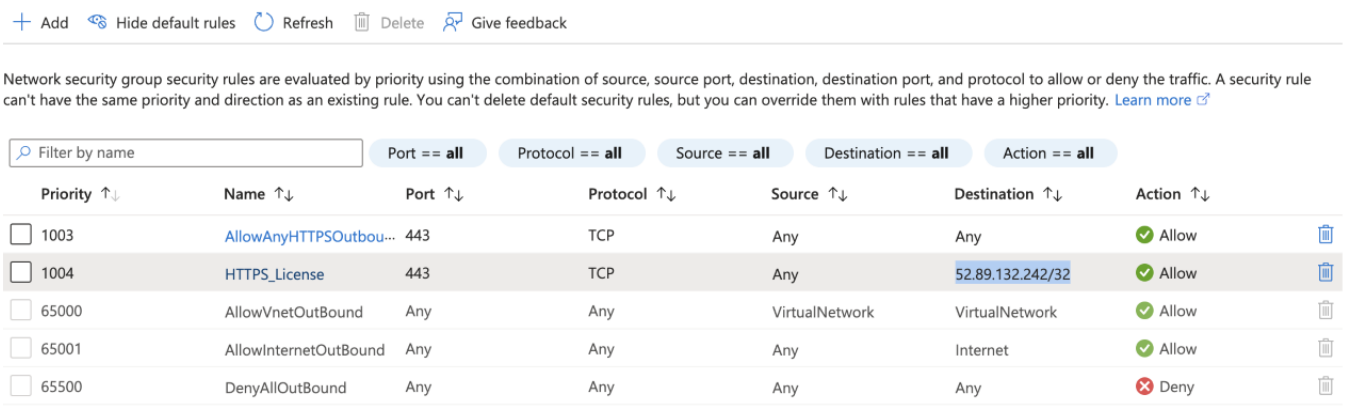

Fig. 1.4: Example compute nodes outbound security group rules

of the license server.

2. Download the Sentieon® tools to the newly launched instance.
3. Set an environment variable in your system to indicate the location of the license server.

```
export SENTIEON_LICENSE=<LICSRVR_INTERNAL_IP>:<LICSRVR_PORT>
```

The new instance is now ready to process data and data processing does not require root privileges. Please see the Sentieon® software manual at, https://support.sentieon.com/manual/ for more information on the functionality included in the Sentieon® software.