SSH to the DB System.

```
ssh -i <private_key_path> opc@<db_system_ip_address>
```

Log in as opc and then sudo to the root user.

```
login as: opc
[opc@dbsys ~]$ sudo su -
```

Save a copy of iptables as a backup.

```
[root@dbsys ~] # iptables-save > /tmp/iptables.orig
```

(If necessary, you can restore the original file by using the command iptables-restore < /tmp/iptables.orig.)

Dynamically add a rule to iptables to allow inbound traffic on the console port, as shown in the following sample. Change the port number and comment as needed.

```
[root@dbsys ~] # iptables -I INPUT 8 -p tcp -m state --state NEW -m tcp --dport 5500 -j ACCEPT -m comment --comment "Required for EM Express."
```

Make sure the rule was added.

```
[root@dbsys ~] # service iptables status
```

Save the updated file to /etc/sysconfig/iptables.

```
[root@dbsys ~] # /sbin/service iptables save
```

The change takes effect immediately and will remain in effect when the node is rebooted.

Update the DB system's security list as described in Updating the Security List for the DB System.

```
cool@fpe~
[opc@fpe ~]$ sudo su -
[root@fpe ~]# service iptables status | grep 1521
6 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:1521
[root@fpe ~]#
```

sudo su – service iptables status | grep 1521

## Opening Ports on the DB System

Open the following ports as needed on the DB system:

- 6200 For Oracle Notification Service (ONS).
- 5500 For EM Express. 5500 is the default port, but each additional EM Express console enabled
  on the DB system will have a different port. If you're not sure which port to open for a particular
  console, see Monitoring a Database with Enterprise Manager Express.
- 1158 For Enterprise Manager Database Control. 1158 is the default port, but each additional
  console enabled on the DB system will have a different port. If you're not sure which port to open
  for a particular console, see Monitoring a Database with Enterprise Manager Database Control.

For important information about critical firewall rules, see Essential Firewall Rules.

To open ports on the DB system

## Updating the Security List for the DB System

Review the list of ports in Opening Ports on the DB System and for every port you open in iptables, update the security list used for the DB system, or create a new security list.

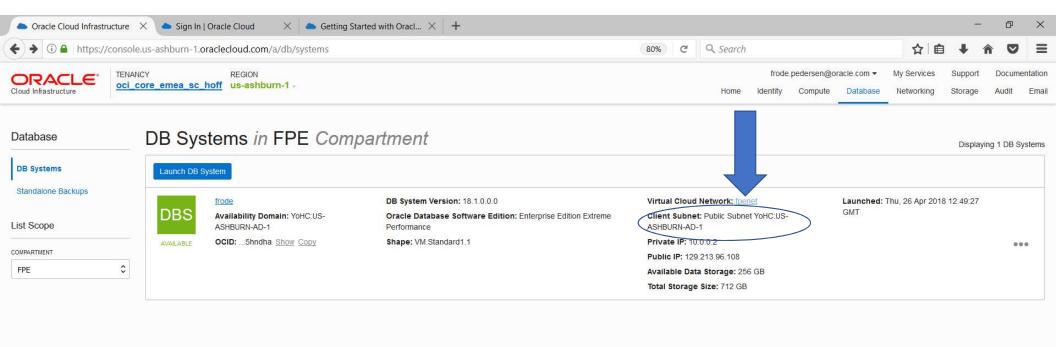
Note that port 1521 for the Oracle default listener is included in iptables, but should also be added to the security list.

## To update an existing security list

- 1. In the Console, click **Database** and locate the DB system in the list.
- Note the DB system's Subnet name and click its Virtual Cloud Network.
- Locate the subnet in the list, and then click its security list under Security Lists.
- Click Edit All Rules and add an ingress rule with source CIDR=<source CIDR>, protocol=TCP, and port=<port number or port range>.

The source CIDR should be the CIDR block that includes the ports you open for the client connection.

For detailed information about creating or updating a security list, see Security Lists.



Tenancy OCID: ocid1.tenancy.oc1..aaaaaaaaat4jhcns2fqgrwwrfpuj5grhxqpcxeg5ajsywekcwgpqfznr4smvq

About Oracle Contact Us Service Health Dashboard Legal Notices Terms of Use Privacy

https://console.us-ashburn-1.oraclecloud.com/a/networking/vcns/ocid1.vcn.oc1.iad.aaaaaaaqk2smzp5azx2ayxwrqlopvf33baf4skrzznextnwpu3oumi5jqqq









