IBM Security Guardium Cloud Deployment for Oracle OCI

Guardium Technical Note

Updated June 10, 2022

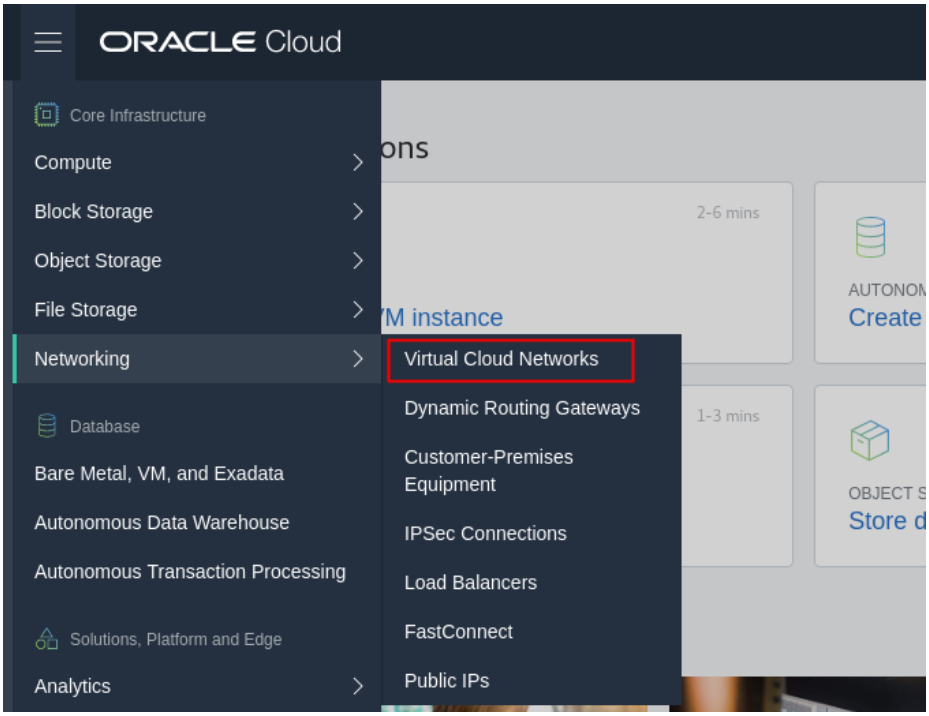
IBM Security Guardium Cloud Deployment Guide for Oracle OCI

Steps to Launch a Guardium instance in Oracle OCI

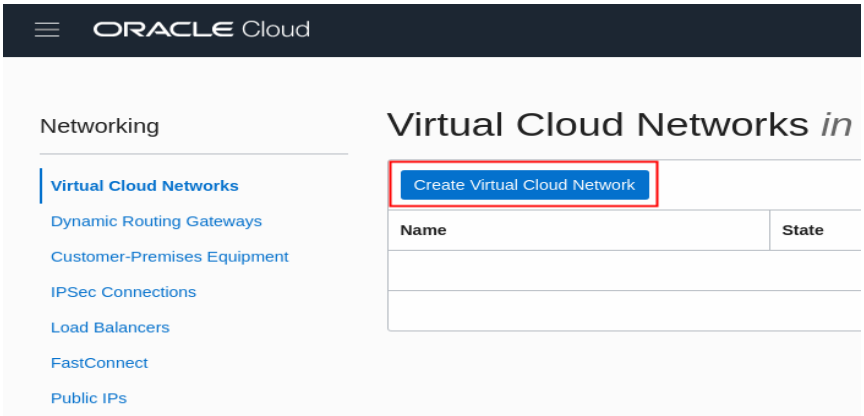
Guardium Collector and Aggregator images are available from the OCI Marketplace: https://cloudmarketplace.oracle.com/marketplace/oci.

Create a Virtual Cloud Network

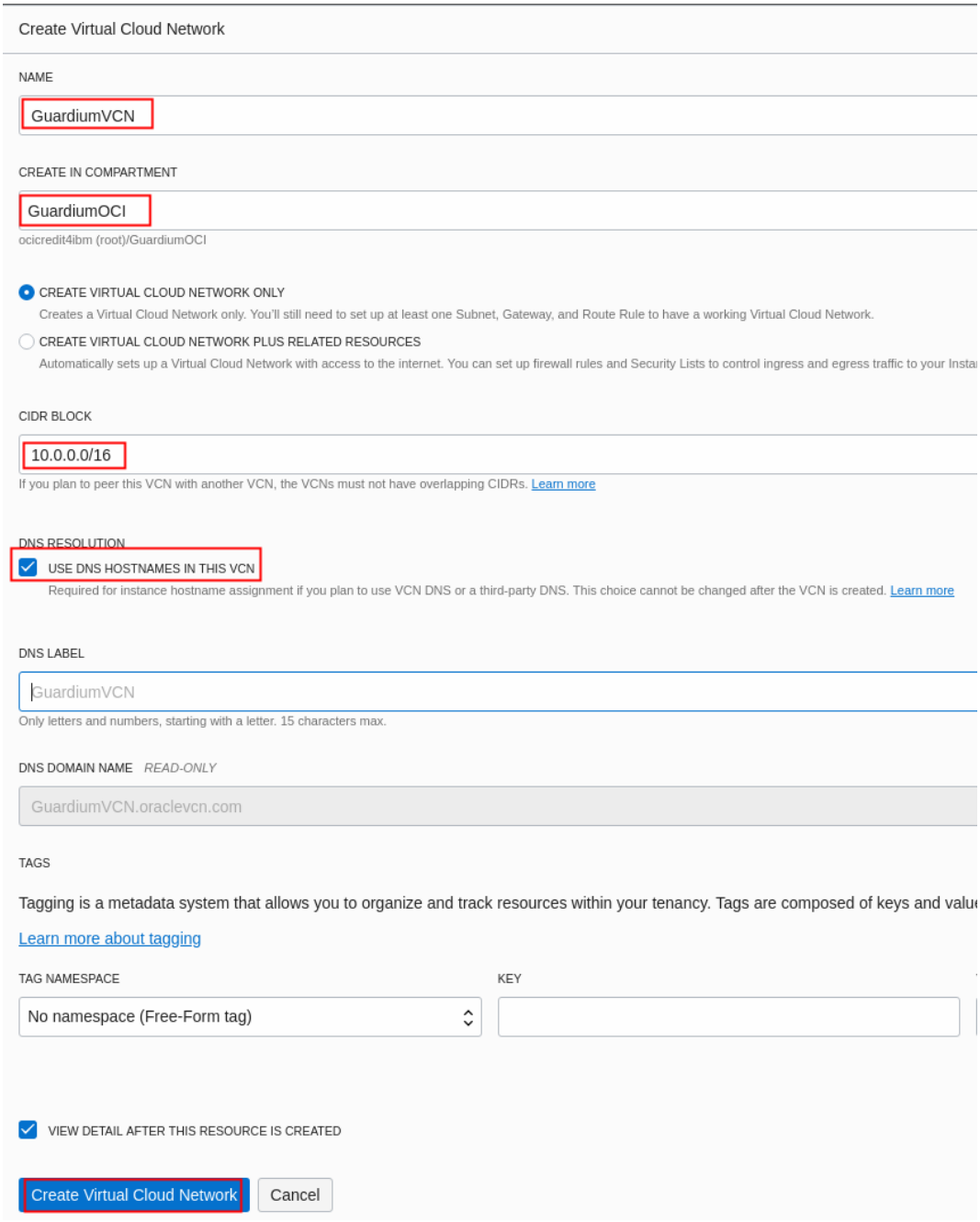
1. From Oracle Cloud, access the Compute Service Console. Go to Networking > Virtual Cloud Networks.



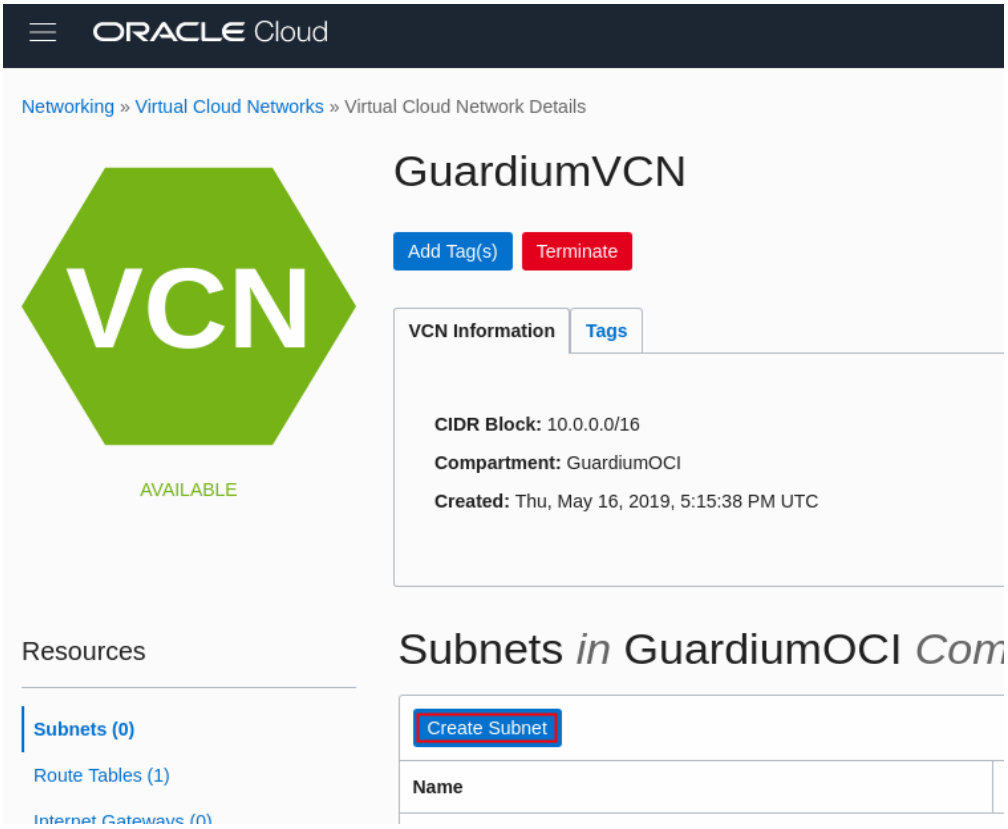
2. Click Create Virtual Cloud Network.



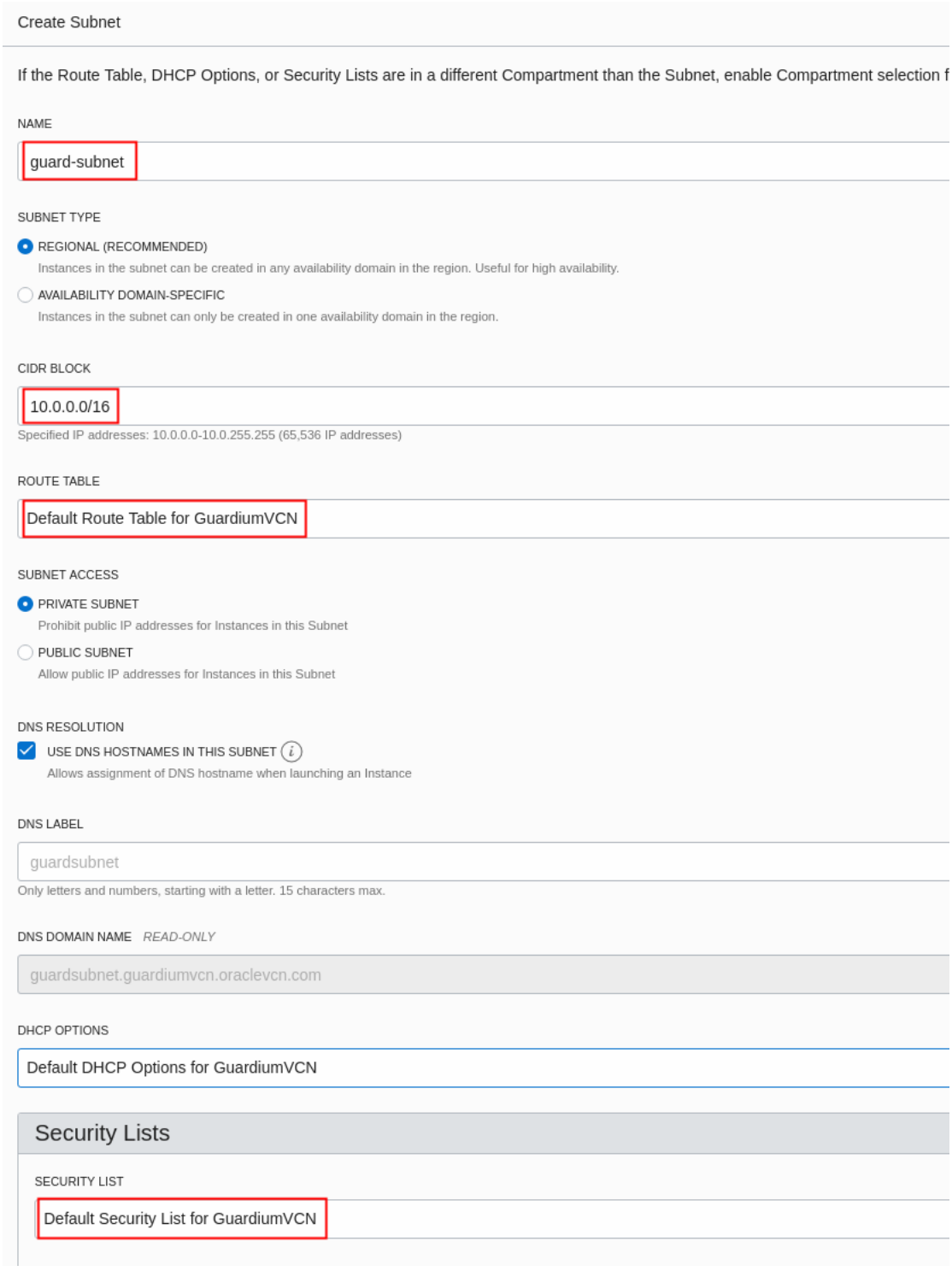
3. Enter the name for the VCN, the name of compartment in which the VCN will be created, and the CIDR block (ex: 10.0.0.0/16). Select Use host name in this VCN, and then click the Create Virtual Cloud Network button.



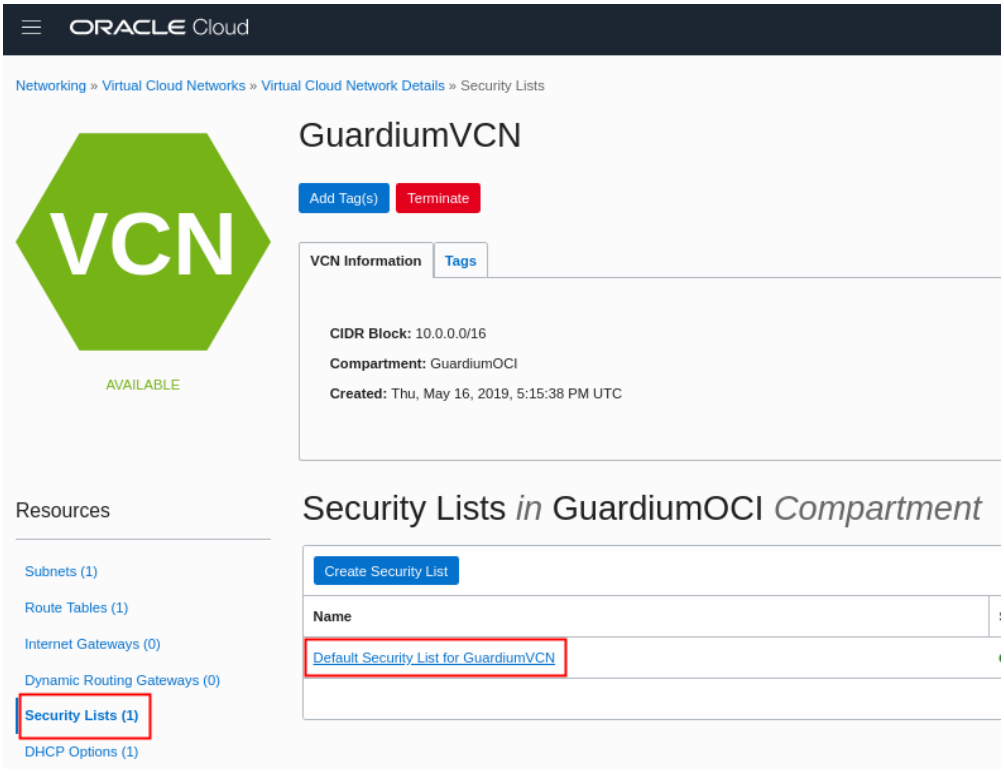
4. Click Create Subnet.



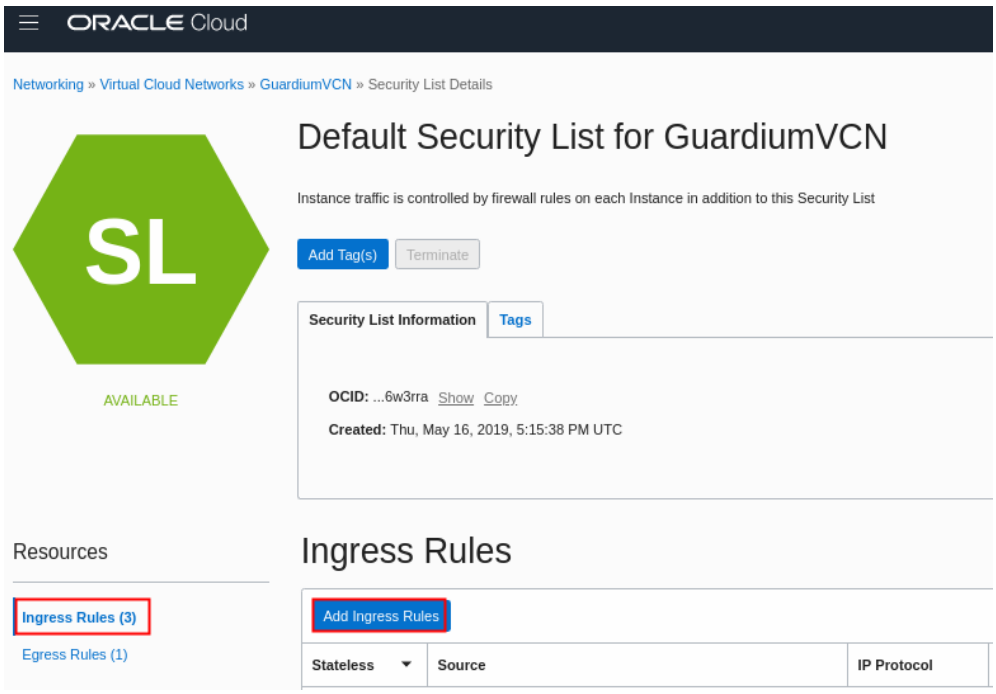
5. Enter the Subnet name, and the CIDR block. Select Default Route Table, and Default Security List. Click Create Subnet.



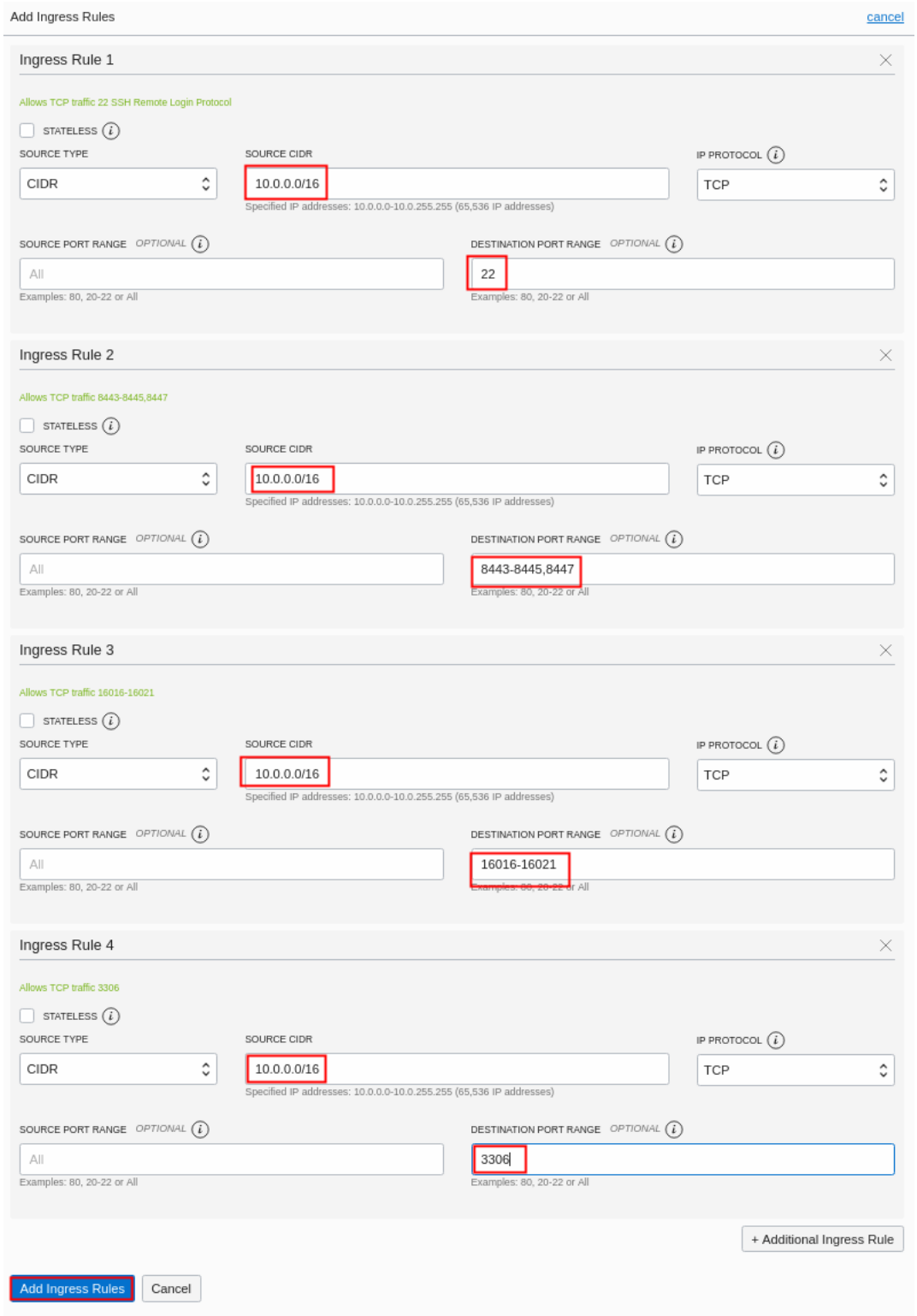
6. Modify the Default Security Rules and open ports needed by Guardium.
   a. Click the Security List link, and then click Default Security List.



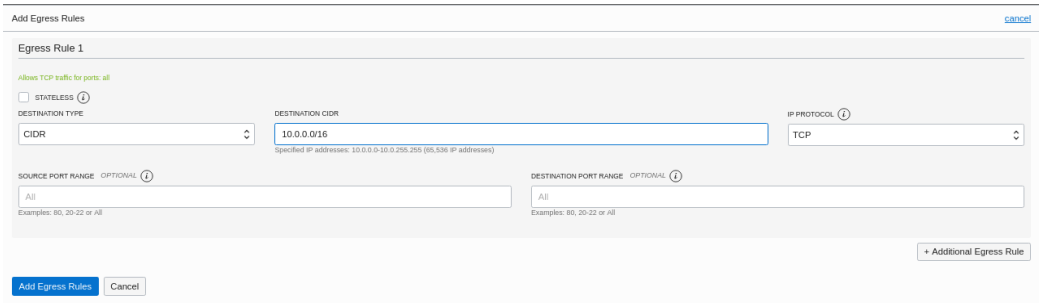
   b. Click Add Ingress Rules.



c. Add Ingress rules for ports 22,3306,8081, 8443-8445,8447, and 16016-16021.



d. Add Egress Rule Allow all Traffic.



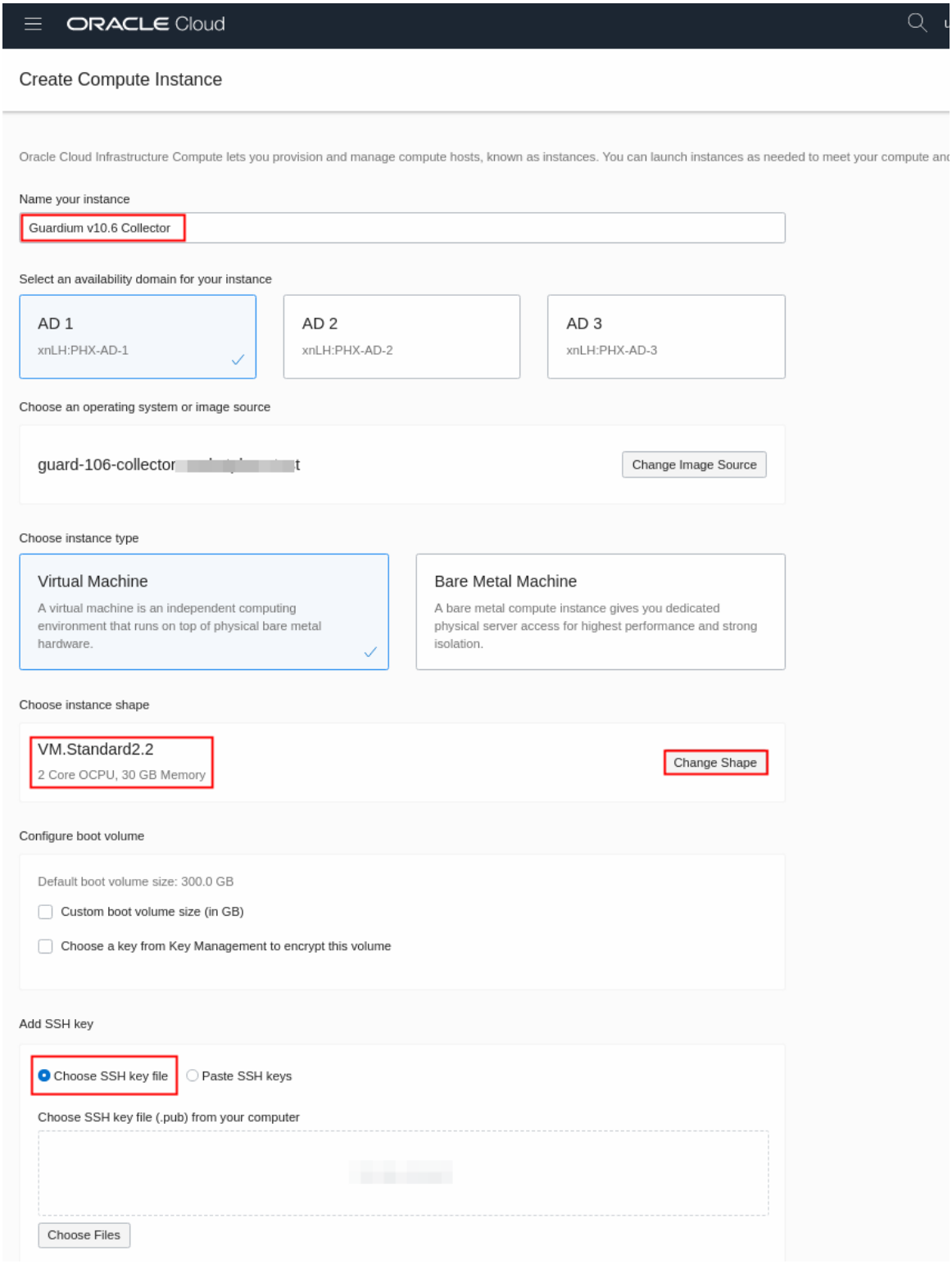
Launch Instance

Navigate to the Oracle OCI Marketplace, and search for Guardium. Select the Guardium version (ex: 10.6), Type either Collector or Aggregator. Select the OCI Compartment in which the instance will be created, and then click Launch Instance.

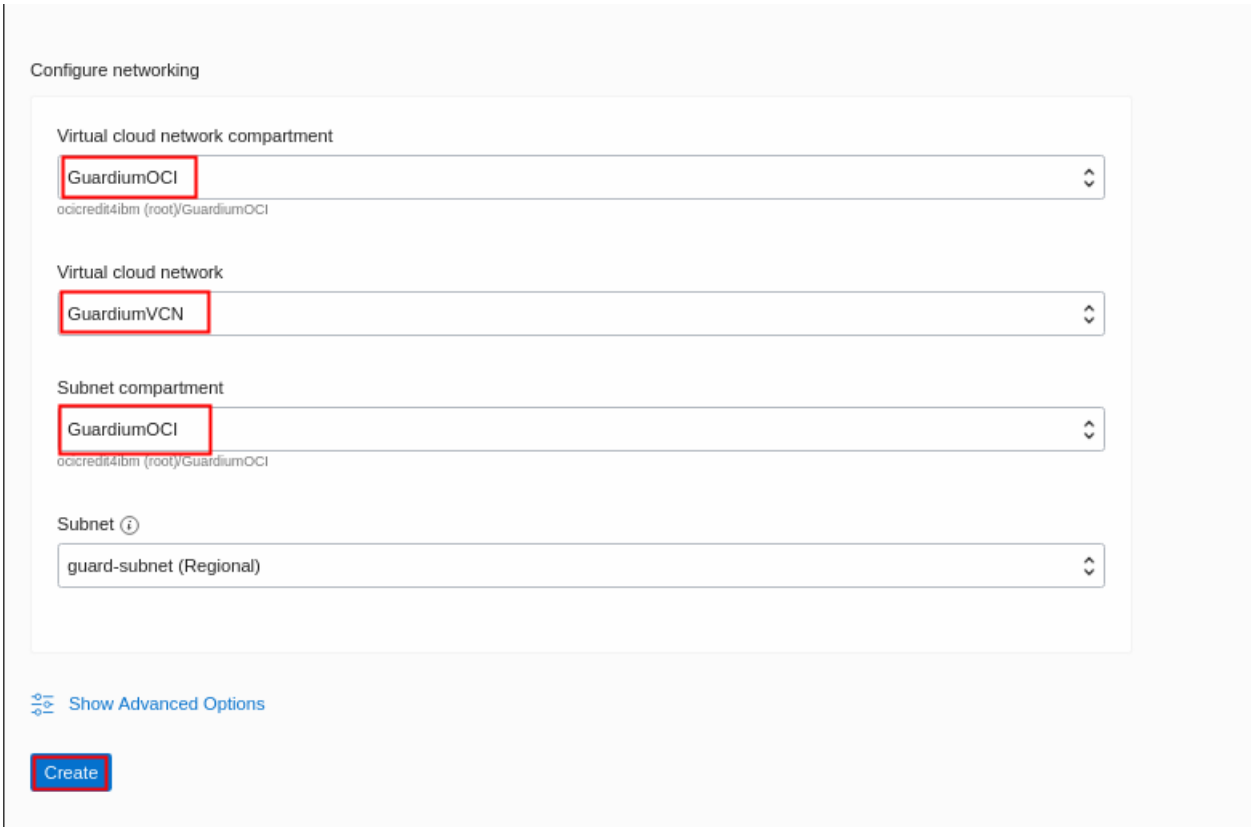
1. Enter the name of the instance, then select the instance shape. Guardium recommends *Compute Shape*s with at least 8vCPUs and 32GB RAM.

   Compute Shapes: VM.Standard2.4, VM.Standard2.8, VM.Standard2.16, VM.Standard2.24, VM.Standard.E2.4, VM.Standard.E2.8, VM.DenseIO2.8, VM.DenseIO2.16, VM.DenseIO2.24

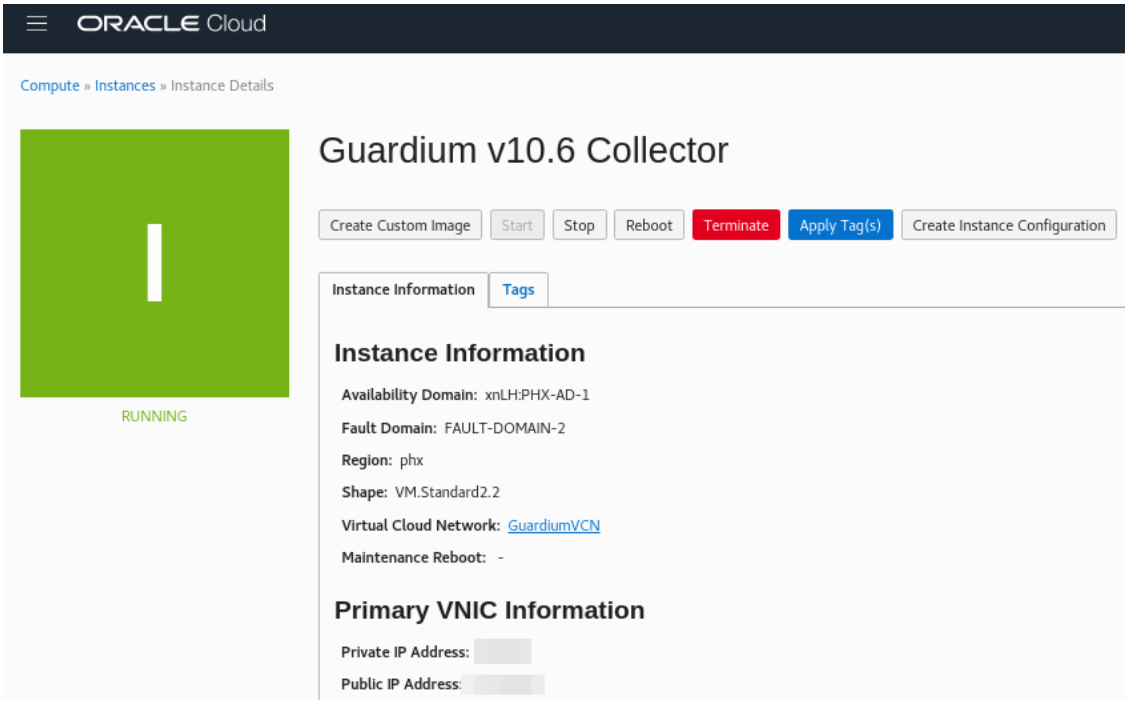
2. Choose the SSH public key that is used to connect to the instance.



3. Configure the Networking. Select the VCN and Subnet created in the previous step. Then click Create.



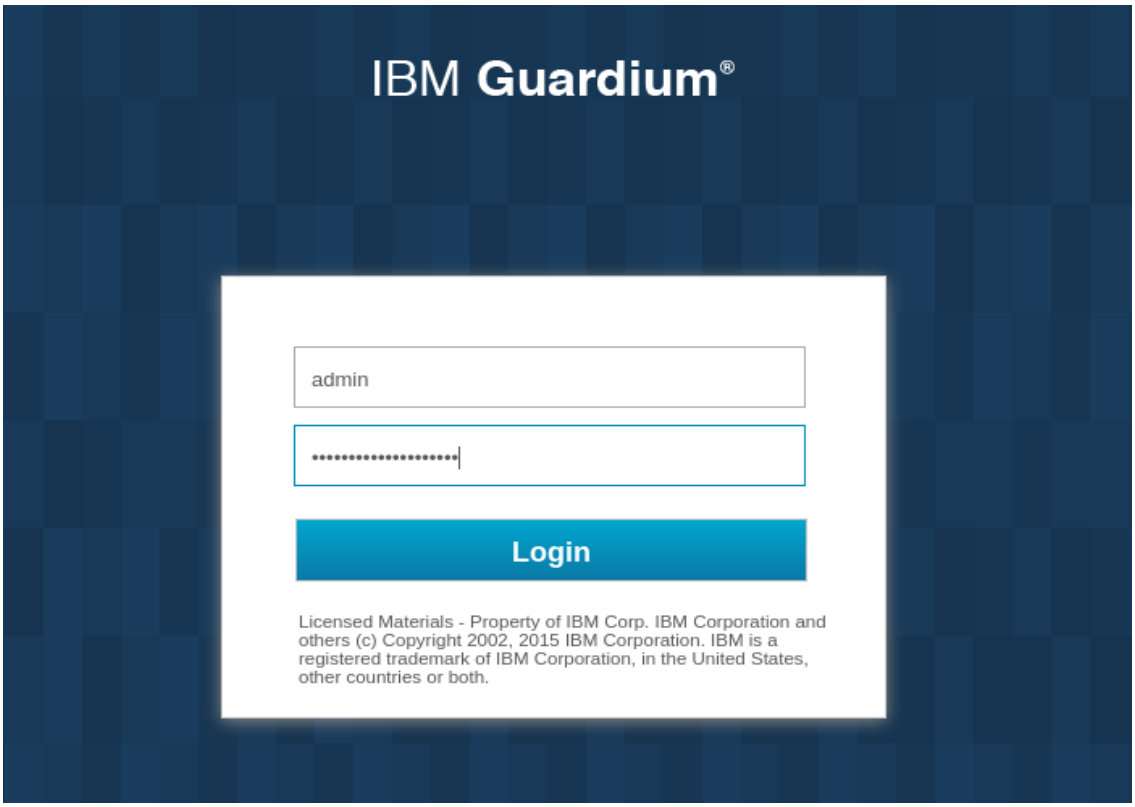
4. Once deployment is ready, the status should update to “Running”.



Connecting to the instance

1. Connect to the Guardium GUI: In a browser to go the URL: https://<ip-of-gmachine>:8443.

   Note: The default password for admin, accessmgr, and Guardium UI users is the last 20 characters of the instance OCI ID. After you login the first time, you are prompted to change the password.



2. Connect to the CLI. From a terminal, connect via ssh to the cli using the private key corresponding to the public key selected when launching the instance:

```
ssh  -i /path/to/private-key  cli@<ip-of-gmachine>
```

Guardium Network Setup

1. From the Compute Service Console page, find the values for the private IP, subnet mask, internal gateway IP and Internal FQDN of the instance. Then run the following CLI network commands to configure the appliance.

   Answer yes to the question “Is it a newly cloned appliance?”.

2. Finally, run the `restart network` CLI command for the changes to take effect.

```
localhost.localdomain> store network interface ip 10.0.0.30
May 16 23:13:08 guard-network[6292]: INFO Sanitizing Hosts
This change will take effect after the next network restart.
ok
localhost.localdomain> store network interface mask
255.255.0.0
This change will take effect after the next network restart.
ok
localhost.localdomain> store network route def 10.0.0.1
This change will take effect after the next network restart.
ok
localhost.localdomain> store system hostname guardium-v10-6-
collector
Is it a newly cloned appliance (y/n)?y
May 16 23:35:31 guard-network[15980]: INFO set_hostname
May 16 23:35:31 guard-network[15980]: INFO Host is currently
localhost.localdomain
May 16 23:35:31 guard-network[15980]: INFO Setting hostname to
guard-106-coll-marketplace.yourcompany.com for ip 10.0.0.30
May 16 23:35:32 guard-network[15980]: INFO findhosts: Did not
find hostname localhost
May 16 23:35:32 guard-network[15980]: ERROR Localhost not in
/etc/hosts, adding it.
ok
localhost.localdomain> store system domain
guardsubnet.guardiumvcn.oraclevcn.com
May 16 23:36:05 guard-network[24976]: INFO set_hostname
May 16 23:36:05 guard-network[24976]: INFO Host is currently
guard-106-coll-marketplace.yourcompany.com
May 16 23:36:05 guard-network[24976]: INFO Setting hostname to
guard-106-coll-marketplace.subnet1.guard2network.oraclevcn.com
for ip 10.0.0.30
ok
localhost.localdomain> restart network
Do you really want to restart network? (Yes/No)
yes
Restarting network
Shutting down interface eth0:  RTNETLINK answers: No such file
or directory
```

```
                                                                    [
OK  ]
Shutting down loopback interface:                                   [
OK  ]
Bringing up loopback interface:                                     [
OK  ]
Bringing up interface eth0:
Determining IP information for eth0... done.
                                                                    [
OK  ]
Network System Restarted.

kafka is not running
In Standalone clause

conntrack is : conntrack on
 appending :
 -A PREROUTING -p tcp -d THIS_HOST -m state --state
ESTABLISHED,RELATED -j ACCEPT
-A PREROUTING -p tcp -d SECOND_HOST -m state --state
ESTABLISHED,RELATED -j ACCEPT

firewall/iptables rebuilt.
setting solr
Changing to port 8443
From port 8443
Stopping.......
success: true

ok
localhost.localdomain>
```

3. Aggregation/CM outside the internal network. In order to connect to an Aggregator or central manager outside the internal network, you need to enable PasswordAuthentication for that specific IP/network. Run the following CLI command to enable PasswordAuthentication:

```
guardium-v10-6-
collector.guardsubnet.guardiumvcn.oraclevcn.com> store system
ssh-match-address ?
USAGE: store system ssh-match-address <ADDR EXPR,...>
       The match patterns may consist of single entries or
comma-separated
       lists and may use the wildcard and negation operators
described
       in the PATTERNS section of ssh_config(5)
Example: store system ssh-match-address
*,!192.168.1.0/24,192.168.3.6
ok
guardium-v10-6-
collector.guardsubnet.guardiumvcn.oraclevcn.com> store system
ssh-match-address 10.0.0.0/8
This command will restart the sshd service, your session may
get logged out


Continue (y/n)? y
restarting ssh service
Stopping sshd:                                             [
OK  ]
Starting sshd:                                             [
OK  ]
ok
```

Working with Guardium support

If you need to contact Guardium support, the support team might need to access your system for debugging purposes. You can grant temporary access to the support team by running the following CLI command:

```
cli> support reset-password cloudsupport
```

To see the current passkey for cloudsupport, run the following CLI command:

```
cli> show passkey cloudsupport
```

When requested, copy and paste the passkey that is returned in the output and send it to Guardium Support.

For more information about the CLI commands, see Support CLI commands.