

IBM Security Guardium Cloud Deployment for Oracle OCI

Guardium Technical Note
Updated June 10, 2022

©IBM Corporation 2017, 2022

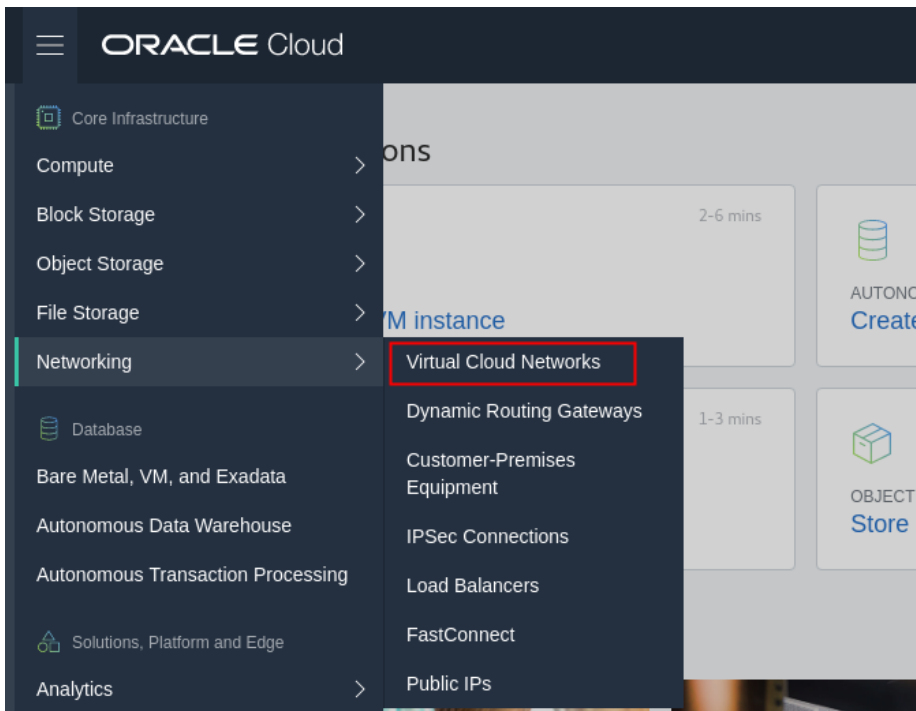
IBM Security Guardium Cloud Deployment Guide for Oracle OCI

Steps to Launch a Guardium instance in Oracle OCI

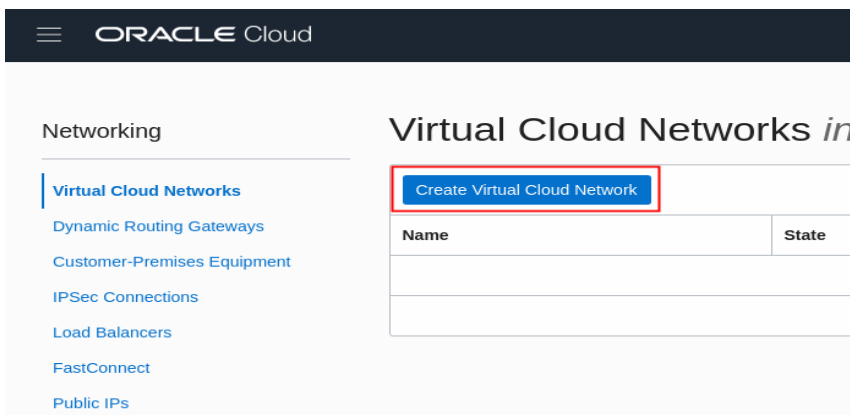
Guardium Collector and Aggregator images are available from the OCI Marketplace: <https://cloudmarketplace.oracle.com/marketplace/oci>.

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.

Create Virtual Cloud Network

NAME

GuardiumVCN

CREATE IN COMPARTMENT

GuardiumOCI

ocicredit4ibm (root)/GuardiumOCI

CREATE VIRTUAL CLOUD NETWORK ONLY
Creates a Virtual Cloud Network only. You'll still need to set up at least one Subnet, Gateway, and Route Rule to have a working Virtual Cloud Network.

CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES
Automatically sets up a Virtual Cloud Network with access to the internet. You can set up firewall rules and Security Lists to control ingress and egress traffic to your Instance.

CIDR BLOCK

10.0.0.0/16

If you plan to peer this VCN with another VCN, the VCNs must not have overlapping CIDRs. [Learn more](#)

DNS RESOLUTION

USE DNS HOSTNAMES IN THIS VCN
Required for instance hostname assignment if you plan to use VCN DNS or a third-party DNS. This choice cannot be changed after the VCN is created. [Learn more](#)

DNS LABEL

GuardiumVCN

Only letters and numbers, starting with a letter. 15 characters max.

DNS DOMAIN NAME *READ-ONLY*

GuardiumVCN.oraclevcn.com

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values. [Learn more about tagging](#)

TAG NAMESPACE KEY

No namespace (Free-Form tag)

VIEW DETAIL AFTER THIS RESOURCE IS CREATED

Create Virtual Cloud Network Cancel

4. Click Create Subnet.

ORACLE Cloud

Networking » Virtual Cloud Networks » Virtual Cloud Network Details

GuardiumVCN

[Add Tag\(s\)](#) [Terminate](#)

VCN Information [Tags](#)

CIDR Block: 10.0.0.0/16
Compartment: GuardiumOCI
Created: Thu, May 16, 2019, 5:15:38 PM UTC

AVAILABLE

Resources

- [Subnets \(0\)](#)
- [Route Tables \(1\)](#)
- [Internet Gateways \(0\)](#)

Subnets *in GuardiumOCI Comp*

[Create Subnet](#)

Name

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

Create Subnet

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, enable Compartment selection for

NAME

guard-subnet

SUBNET TYPE

REGIONAL (RECOMMENDED)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability.

AVAILABILITY DOMAIN-SPECIFIC
Instances in the subnet can only be created in one availability domain in the region.

CIDR BLOCK

10.0.0.0/16

Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)

ROUTE TABLE

Default Route Table for GuardiumVCN

SUBNET ACCESS

PRIVATE SUBNET
Prohibit public IP addresses for Instances in this Subnet

PUBLIC SUBNET
Allow public IP addresses for Instances in this Subnet

DNS RESOLUTION

USE DNS HOSTNAMES IN THIS SUBNET ⓘ
Allows assignment of DNS hostname when launching an Instance

DNS LABEL

guardsubnet

Only letters and numbers, starting with a letter. 15 characters max.

DNS DOMAIN NAME READ-ONLY

guardsubnet.guardiumvcn.oraclevcn.com

DHCP OPTIONS

Default DHCP Options for GuardiumVCN

Security Lists

SECURITY LIST

Default Security List for GuardiumVCN

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

The screenshot shows the Oracle Cloud console interface. At the top, the breadcrumb navigation reads: Networking » Virtual Cloud Networks » Virtual Cloud Network Details » Security Lists. The main heading is "GuardiumVCN". Below the heading are two buttons: "Add Tag(s)" and "Terminate". To the left is a green hexagonal icon with "VCN" and the status "AVAILABLE".

Under "VCN Information", the following details are listed:

- CIDR Block: 10.0.0.0/16
- Compartment: GuardiumOCI
- Created: Thu, May 16, 2019, 5:15:38 PM UTC

On the left side, under "Resources", a list of resource types is shown: Subnets (1), Route Tables (1), Internet Gateways (0), Dynamic Routing Gateways (0), Security Lists (1), and DHCP Options (1). The "Security Lists (1)" link is highlighted with a red box.

The main content area is titled "Security Lists in GuardiumOCI Compartment". It features a "Create Security List" button and a table with one entry:

Name
Default Security List for GuardiumVCN

 The link in the table is highlighted with a red box.

- b. Click Add Ingress Rules.

The screenshot shows the Oracle Cloud console interface for the "Default Security List for GuardiumVCN". The breadcrumb navigation reads: Networking » Virtual Cloud Networks » GuardiumVCN » Security List Details. The main heading is "Default Security List for GuardiumVCN". Below the heading is the text: "Instance traffic is controlled by firewall rules on each Instance in addition to this Security List". There are two buttons: "Add Tag(s)" and "Terminate". To the left is a green hexagonal icon with "SL" and the status "AVAILABLE".

Under "Security List Information", the following details are listed:

- OCID: ...6w3rra [Show](#) [Copy](#)
- Created: Thu, May 16, 2019, 5:15:38 PM UTC

On the left side, under "Resources", a list of resource types is shown: Ingress Rules (3) and Egress Rules (1). The "Ingress Rules (3)" link is highlighted with a red box.

The main content area is titled "Ingress Rules". It features an "Add Ingress Rules" button and a table with the following structure:

Stateless	Source	IP Protocol
▼		

 The "Add Ingress Rules" button is highlighted with a red box.

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

Add Ingress Rules [cancel](#)

Ingress Rule 1 ✕

Allows TCP traffic 22 SSH Remote Login Protocol

STATELESS ⓘ

SOURCE TYPE: CIDR

SOURCE CIDR: 10.0.0.0/16
Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)

IP PROTOCOL ⓘ: TCP

SOURCE PORT RANGE OPTIONAL ⓘ: All
Examples: 80, 20-22 or All

DESTINATION PORT RANGE OPTIONAL ⓘ: 22
Examples: 80, 20-22 or All

Ingress Rule 2 ✕

Allows TCP traffic 8443-8445,8447

STATELESS ⓘ

SOURCE TYPE: CIDR

SOURCE CIDR: 10.0.0.0/16
Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)

IP PROTOCOL ⓘ: TCP

SOURCE PORT RANGE OPTIONAL ⓘ: All
Examples: 80, 20-22 or All

DESTINATION PORT RANGE OPTIONAL ⓘ: 8443-8445,8447
Examples: 80, 20-22 or All

Ingress Rule 3 ✕

Allows TCP traffic 16016-16021

STATELESS ⓘ

SOURCE TYPE: CIDR

SOURCE CIDR: 10.0.0.0/16
Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)

IP PROTOCOL ⓘ: TCP

SOURCE PORT RANGE OPTIONAL ⓘ: All
Examples: 80, 20-22 or All

DESTINATION PORT RANGE OPTIONAL ⓘ: 16016-16021
Examples: 80, 20-22 or All

Ingress Rule 4 ✕

Allows TCP traffic 3306

STATELESS ⓘ

SOURCE TYPE: CIDR

SOURCE CIDR: 10.0.0.0/16
Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)

IP PROTOCOL ⓘ: TCP

SOURCE PORT RANGE OPTIONAL ⓘ: All
Examples: 80, 20-22 or All

DESTINATION PORT RANGE OPTIONAL ⓘ: 3306
Examples: 80, 20-22 or All

[+ Additional Ingress Rule](#)

[Add Ingress Rules](#) [Cancel](#)

d. Add Egress Rule Allow all Traffic.

The screenshot shows the 'Add Egress Rules' interface. At the top, it says 'Add Egress Rules' with a 'cancel' link. Below that is 'Egress Rule 1'. A green note says 'Allow TCP traffic for ports: all'. There is a 'STATELESS' checkbox. The 'DESTINATION TYPE' is set to 'CIDR'. The 'DESTINATION CIDR' field contains '10.0.0.0/16' with a note 'Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)'. The 'IP PROTOCOL' is set to 'TCP'. Both 'SOURCE PORT RANGE' and 'DESTINATION PORT RANGE' are set to 'All'. There are 'Add Egress Rules' and 'Cancel' buttons at the bottom left, and an 'Additional Egress Rule' button at the bottom right.

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 Shapes* 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.

ORACLE Cloud

Create Compute Instance

Oracle Cloud Infrastructure Compute lets you provision and manage compute hosts, known as instances. You can launch instances as needed to meet your compute and

Name your instance

Guardium v10.6 Collector

Select an availability domain for your instance

AD 1
xnLH:PHX-AD-1 ✓

AD 2
xnLH:PHX-AD-2

AD 3
xnLH:PHX-AD-3

Choose an operating system or image source

guard-106-collector

Change Image Source

Choose instance type

Virtual Machine
A virtual machine is an independent computing environment that runs on top of physical bare metal hardware. ✓

Bare Metal Machine
A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Choose instance shape

VM.Standard2.2
2 Core OCPU, 30 GB Memory

Change Shape

Configure boot volume

Default boot volume size: 300.0 GB

Custom boot volume size (in GB)

Choose a key from Key Management to encrypt this volume

Add SSH key

Choose SSH key file Paste SSH keys

Choose SSH key file (.pub) from your computer

Choose Files

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

Configure networking

Virtual cloud network compartment

GuardiumOCI

oicredit41bm (root)/GuardiumOCI

Virtual cloud network

GuardiumVCN

Subnet compartment

GuardiumOCI

oicredit41bm (root)/GuardiumOCI

Subnet ⓘ

guard-subnet (Regional)

Show Advanced Options

Create

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

The screenshot displays the Oracle Cloud console interface for an instance named "Guardium v10.6 Collector". The instance is in a "RUNNING" state, indicated by a green square icon with a white vertical bar and the word "RUNNING" below it. The console header shows "ORACLE Cloud" and the breadcrumb "Compute » Instances » Instance Details".

Below the instance name, there are several action buttons: "Create Custom Image", "Start", "Stop", "Reboot", "Terminate" (highlighted in red), "Apply Tag(s)", and "Create Instance Configuration".

The "Instance Information" tab is selected, showing the following details:

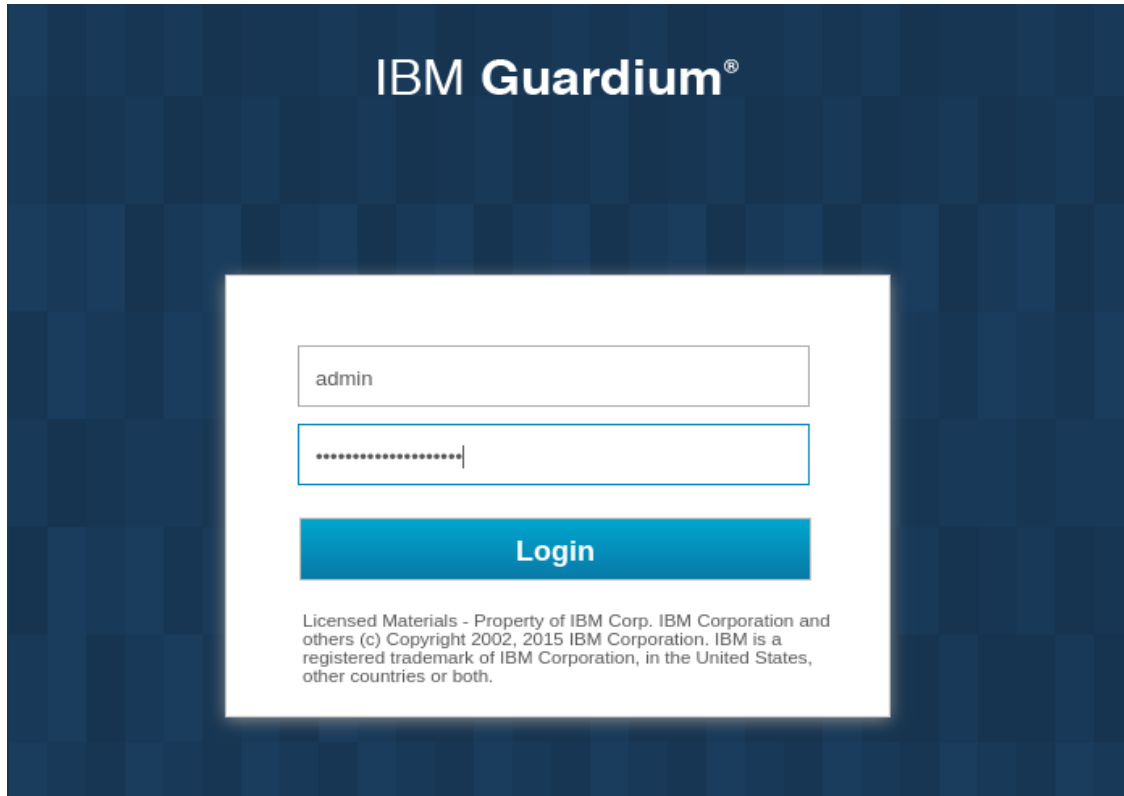
- Availability Domain: xnLH:PHX-AD-1
- Fault Domain: FAULT-DOMAIN-2
- Region: phx
- Shape: VM.Standard2.2
- Virtual Cloud Network: [GuardiumVCN](#)
- Maintenance Reboot: -

The "Primary VNIC Information" section shows the Private IP Address and Public IP Address, both of which are currently blank.

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](#).

IBM Security Guardium Licensed Materials - Property of IBM. © Copyright IBM Corp. 2017, 2019. US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" (www.ibm.com/legal/copytrade.shtml)