IBM Security Guardium Cloud Deployment Guide Google

Prerequisites

• Join the following Google group to gain access to the Google Multi-Cloud Images: <u>https://groups.google.com/forum/#!forum/ibmsecurityguardium</u>

Deployment Procedure:

- 1. Navigate to https://console.cloud.google.com
- 2. Select your Google project to deploy the Guardium appliance(s) on
- 3. In the menu pane, navigate to *Compute Engine*
- 4. Click on VM instances
- 5. Click on Create Instance
 - a. Provide a name for the instance
 - b. Select a zone
 - c. Select a Machine Type

Note: IBM Security Guardium requires a minimum 4 vCPUs and 24 GB RAM

Name 🕜		
guardium-collector-insta	ance	
Zone 🕐		
us-central1-c		•
Machine type		
4 vCPUs 👻	24 GB memory	Customize

d. In the Boot Disk section, click Change

Boot disk 📀		
\bigcirc	New 10 GB standard persistent disk Image Debian GNU/Linux 8 (jessie)	Change

- i. Click the Custom Images tab
- ii. Under Show Images From select the Guardium Images project
- iii. From the images list, select the IBM Security Guardium image per your requirements

Boot disk					
Select an image or snapshot to create a boot disk; or attach an existing disk					
OS images	Application images	Custom images	Snapshots	Existing disks	
Show images	from				
Guardium	Images			•	
guardium -aggregator-1500gb Created from Guardium v1013 Images on Jun 9, 2017, 11:04:54 AM guardium- -aggregator-750gb Created from Guardium v1013 Images on Jun 8, 2017, 1:21:16 PM guardium- -collector-250gb Created from Guardium v1013 Images on Jun 8, 2017, 4:08:39 PM guardium -collector-500gb Created from Guardium v1013 Images on Jun 9, 2017, 11:00:01 AM					

- iv. Click on Select
- e. Click Create to deploy the VM

Configuring the Network

Once the instance is created it will appear listed in the VM Instances page. By default, most ports will be blocked by the firewall. To configure the wire wall rules and open specific ports, follow the steps below.

- 1. Click on the instance name
- 2. Scroll down to Network interfaces and click on the network name



- 3. Scroll down to Firewall rules and click on Add firewall rule
- 4. Enter a Name for the Firewall rule
- 5. Enter a Description
- 6. Under Source Filter select Subnetworks

- 7. Under the *Subnetworks* drop down menu select the subnetworks that apply to your environment
- 8. Under *Protocols and ports* add the following ports: "tcp:8443;udp:8443" to be able to connect to the GUI

Name 🔞	
guardium-gui	
Description (Optional)	
letwork 📀	
default	-
Priority 🕜 Priority can be 0 - 65535 Check priority of other firewall rules	
1000	
Direction of traffic 💿	
Ingress	
) Egress	
Action on match 🕘	
Allow	
Deny	
Targets 🔞	
Specified target tags	
farget tags	
Source filter 🔞	
Subnetworks	
Subnetworks 🕢	
1 selected	
Second source filter 💿	
None	
Protocols and ports 💿	
Allow all	
specified protocols and ports	
tcp:8443;uap:8443	
Create Cancel	

9. Click on **Create**

10. Repeat step 8 for the following ports: For GIM: "tcp:8444-8446; tcp:8081" For FAM: "tcp:16022-16023" For Unix STAP: "tcp:16016-16018" For Windows STAP: "tcp:9500-9501" For Quick Search: "tcp:8983; tcp:9983" For MySQL: "tcp:3306"

For a complete list of ports that are utilized in IBM Security Guardium, please refer to the following Technote: http://www-01.ibm.com/support/docview.wss?uid=swg21973188

Connecting to the Guardium Appliance in the Cloud

To connect to the Guardium appliance configured with the above firewall rules, you will need to establish a VPN connection and connect your existing network to the Google Cloud Platform network. Here are the steps describing how to create a configure a VPN connection In Google Cloud:

https://cloud.google.com/compute/docs/vpn/overview

Connect to the GUI

Once you have a VPN connection established open a web browser to this address: **https://<guardium-ip>:8443**. Login with the credentials provided by Guardium, the system will ask you to change the password upon first login

	IBM Guardium®
Ŀ	
	admin
	•••••
	Login
	Licensed Materials - Property of IBM Corp. IBM Corporation and others (c) Copyright 2002, 2015 IBM Corporation. IBM is a registered trademark of IBM Corporation, in the United States, other countries or both.

Connect to the CLI

To connect to the Guardium CLI, ssh (or use Putty) to the Guardium IP and login as user **cli**. If this is the first-time logging into the system you will be prompted to change the password. Please save this password in a secure location.

Configuring Appliance Network:

- 1. Select the VM on the VM instances page in the Google Cloud Platform
- 2. Scroll down to the *Network interfaces* section
- 3. Make a note of the private IP associated with the VM

Network interfaces

Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
default	default	10.128.0.5	-		Off

4. Configure network settings

- a. SSH into the appliance using the private ip as CLI user
- b. Change your password on first login

ssh cli@10.142.0.2

IBM Guardium, Command Line Interface (CLI)

cli@10.142.0.2's password: Last login: Fri Jan 20 21:12:06 2017 Welcome cli - this is your first login in this system. Your password has expired. Changing password for 'cli'. Enter current password: Enter new password: Re-enter new password: localhost.localdomain>

c. Configure the system IP (use the private or internal ip)

localhost.localdomain> store network interface ip 10.142.0.2 Mar 17 00:55:02 guard-network[13916]: INFO Sanitizing Hosts This change will take effect after the next network restart. ok

d. Configure the netmask

localhost.localdomain> store network interface mask 255.255.255.255 This change will take effect after the next network restart. ok

e. Configure the internal route

localhost.localdomain> store network route default 10.142.0.1 This change will take effect after the next network restart. ok

f. Configure the network resolver

localhost.localdomain> **store network resolver 1 169.254.169.254** This change will take effect after restart network. ok

g. Configure the hostname

localhost.localdomain> store system hostname guardiumcollector Mar 17 00:55:40 guard-network[14237]: INFO set_hostname Mar 17 00:55:40 guard-network[14237]: INFO Host is currently localhost.localdomain Mar 17 00:55:40 guard-network[14237]: INFO Setting hostname to guardiumcollector.yourcompany.com for ip 10.142.0.2 ok

h. Configure the domain

localhost.localdomain> **store system domain guardium.google.cloud.com** Mar 17 00:55:59 guard-network[14277]: INFO set_hostname Mar 17 00:55:59 guard-network[14277]: INFO Host is currently guardiumcollector.yourcompany.com Mar 17 00:55:59 guard-network[14277]: INFO Setting hostname to guardiumcollector.guardium.google.cloud.com for ip 10.142.0.2 ok

i. Restart network in order to apply changes

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. In Standalone clause firewall/iptables rebuilt. setting solr Changing to port 8443 From port 8443 Stopping..... success: true ok localhost.localdomain>

Warning and Known Limitations:

The following CLI commands will not work on an appliance deployed in the Amazon Cloud due to DHCP handling limitations in the appliance:

- store network interface mtu
- show network verify
- Show network interface inventory

The following CLI command should not be run on Oracle Cloud Platform as it may result in the appliance becoming inaccessible:

- store network interface reset
- Store net interface inventory

2018-September-27

IBM Guardium Licensed Materials - Property of IBM. © Copyright IBM Corp. 2018. U.S. 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)