

IBM Security Guardium Cloud Deployment for IBM Cloud

Guardium Technical Note
Updated June 10, 2022

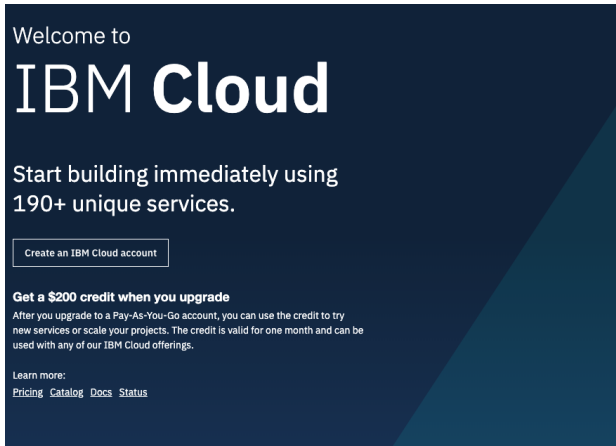
©IBM Corporation 2017, 2022

IBM Security Guardium Cloud Deployment Guide for IBM Cloud

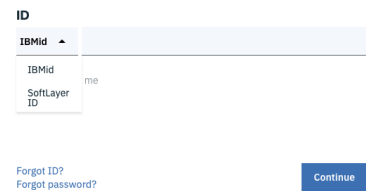
Note: SoftLayer is now IBM Cloud. For Guardium v10.6 (GPU600) and later releases, update your SoftLayer deployment to IBM Cloud.

Deployment Procedure:

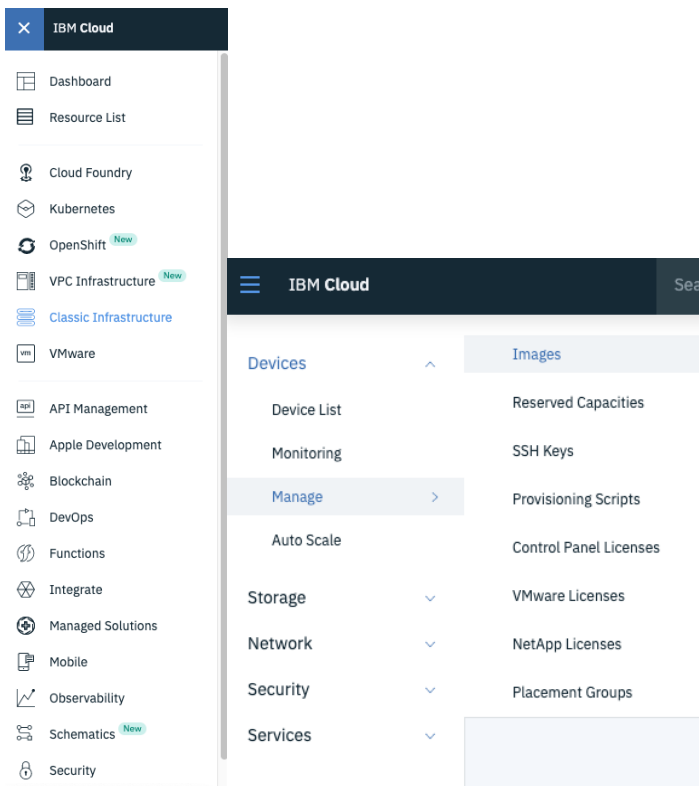
1. Navigate to <https://cloud.ibm.com>.
2. Log into your IBM Cloud account.



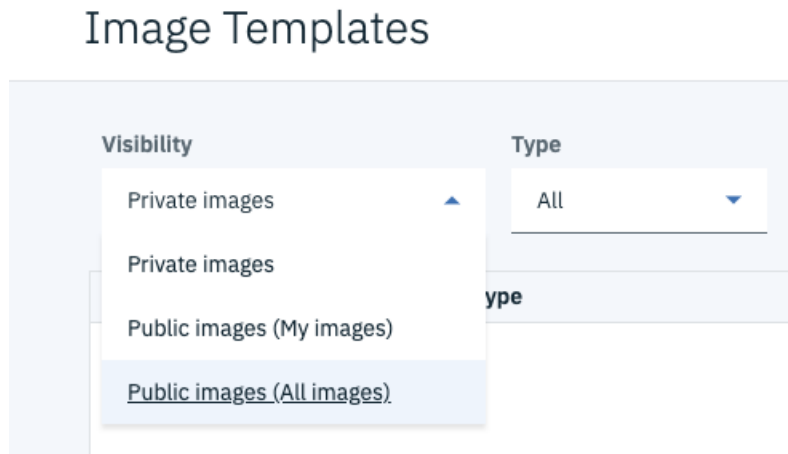
Log in to IBM Cloud

A screenshot of the IBM Cloud login form. The form is titled "Log in to IBM Cloud". It has a field for "ID" with a dropdown menu showing "IBMId" and "SoftLayer ID". There is a "Forgot ID?" link below the ID field. There is a "Forgot password?" link below the ID field. There is a "Continue" button at the bottom right.

3. Navigate to Classic Infrastructure > Devices > Manage > Images.

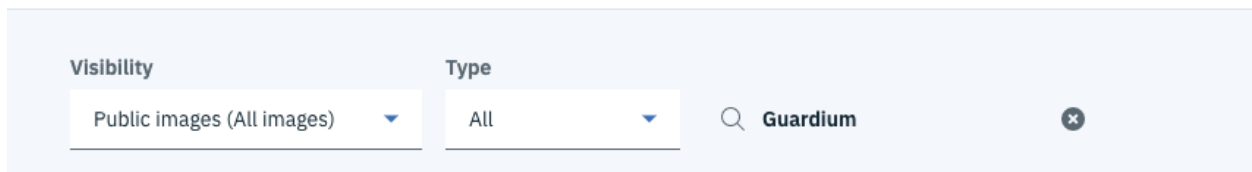


4. On the Images Templates screen, list all Public Images (All images).



5. Filter the list of images using Template Name Guardium.

Image Templates



6. Locate the Guardium image template corresponding to unit type Collector or Aggregator.

7. To order the image, click on the more options icon (...) and select the type of image you need (Public, Reserved, Transient, or Dedicated Virtual Server Instance [VSI]).

Name	Image Type	Created	Summary	Publisher
IBM Security Guardium v10.1.3 Collector - 500 GB	Standard	August 31, 2017	V10.1.3 Collector Image w/ 100 GB first disk, 500 GB second disk	...
IBM Security Guardium v10.1.3 Aggregator - 1.5 TB	Standard	August 31, 2017	V10.1.3 Aggregator Image w/ 100 GB first disk, 1.5 TB second disk	...
IBM Security Guardium v10.1.4 Aggregator - 1.5 TB	Standard	January 23, 2018	IBM Security Guardium v10.1.4 Aggregator - 1.5 TB - BYOL	...
IBM Security Guardium 10.5 Aggregator - Private Only	Standard	May 13, 2019	IBM Security Guardium 10.5 Aggregator - Appliance for IBM Cloud	...
IBM Guardium v11.0 Collector	Standard	July 8, 2019	IBM Guardium v11.0 Collector	...
IBM Guardium v11.0 Aggregator	Standard	July 8, 2019	IBM Guardium v11.0 Aggregator	...
IBM Guardium v10.6 Collector	Standard	July 15, 2019	IBM Guardium v10.6 Collector - 500 GB	...
IBM Guardium v10.6 Aggregator	Standard	July 15, 2019	IBM Guardium v10.6 Aggregator - 1.5 TB	...

8. Specify the following required configuration options:

- a. Type of Virtual Server:
 - i. Public (Multi-tenant)
 - ii. Dedicated (Single-tenant)

- iii. Transient (Multi-tenant, Ephemeral)
- iv. Reserved (Multi-tenant, Term commitment)

b. Billing type

- i. Hourly
- ii. Monthly

Note: Only VSIs based on a monthly billing cycle are eligible for a Hardware Firewall.

c. Hostname

d. Domain

e. Location

- i. Select a Data Center.

f. System Configuration

- i. Select vCPU

Note: IBM Security Guardium recommends a minimum of 4 vCPUs.

- ii. Select RAM

Note: IBM Security Guardium recommends a minimum of 24 GB of RAM.

g. Network Interface

- i. Uplink port speeds

Note: To deploy a VSI without a Public IP, select a Private Only interface .

- ii. Public egress bandwidth
- iii. Security groups

- After you select configurations, review your order, read and agree to the Third-Party Service Agreement and click Create.

Order summary

1 - Virtual server instance (Dedicated)	\$0.000/hr
4 vCPU	
32 GB RAM	
DAL13 - Dallas	
IBM Guardium v11.0 Collector	
> Add-ons	
Boot disk - 100 GB	\$0.012
Disk 1 - 500 GB	\$0.031
Network interface	\$0.000
1 Gbps non rate-limited public & private network uplinks (Dedicated hosts)	
> Add-ons	

Total due per hour* **\$0.04**
estimated

> Apply promo code

*Price based on average usage and does not include tax.
**Public bandwidth charged per GB

I read and agree to the following Third-Party Service Agreements:
[3rd Party Software Terms CentOS](#)

Create

Save as quote

[Add to estimate](#)

- After the order has been placed, you will be redirected to the Devices page where you can view the provisioned VSI.

Configuring the VM Network:

Note: Hardware Firewall configurations are only possible for a Virtual Server on a monthly billing cycle. Attempting to configure a Hardware Firewall for a Virtual Server on an hourly billing cycle throws the following error:

New Hardware Firewall

Error: Hardware firewalls are not available for hourly-billed servers.

- Click on the Device Name in question

2. Scroll down to the Add-ons section.
3. Click Order Hardware Firewall.

Add-ons

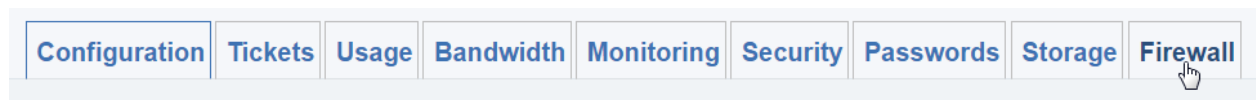
Firewall

Status: Not installed [Order hardware firewall](#)

4. Review the Hardware Firewall configuration, read and agree to the Third-Party Service Agreement and click Create.

Order Summary	USD ▾
100Mbps Hardware Firewall	\$49.00/mo
<hr/>	
Total due per month:	\$49.00 <small>tax not included</small>
Prorated initial charge	\$8.17
<hr/>	
Total due now	\$8.17 <small>tax not included</small>
<p>> Apply promo code</p>	
<p><input checked="" type="checkbox"/> I have read the Master Service Agreement and agree to the terms therein.</p>	
<p>Create</p>	
<p>Add to Estimate</p>	

5. Navigate to the Device Name and then to the Firewall tab.



6. Configure security rules for the following:
 - For UI: “tcp:8443”
 - 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 used in IBM Security Guardium, see [Guardium port requirements](#).

7. Scroll down to the *Network* section and note down the following:

- Public IP Address (if applicable)
- Private IP Address
- Private Default gateway
- Private Subnet Mask

Network		Order IPs	Private	Order IPs
Public			Private	
eth1			eth0	
Status	Private Network Only		Status	Active
IP Address			IP Address	10.70.226.197
Default Gateway			Default Gateway	10.70.226.193
Subnet Mask			Subnet Mask	255.255.255.192
Speed	Disconnected		Speed	10 Mbps
Max Speed	N/A		Max Speed	10 Mbps
VLAN	N/A			Modify Max Speed
N/A			VLAN	ams01bcr02a.1403

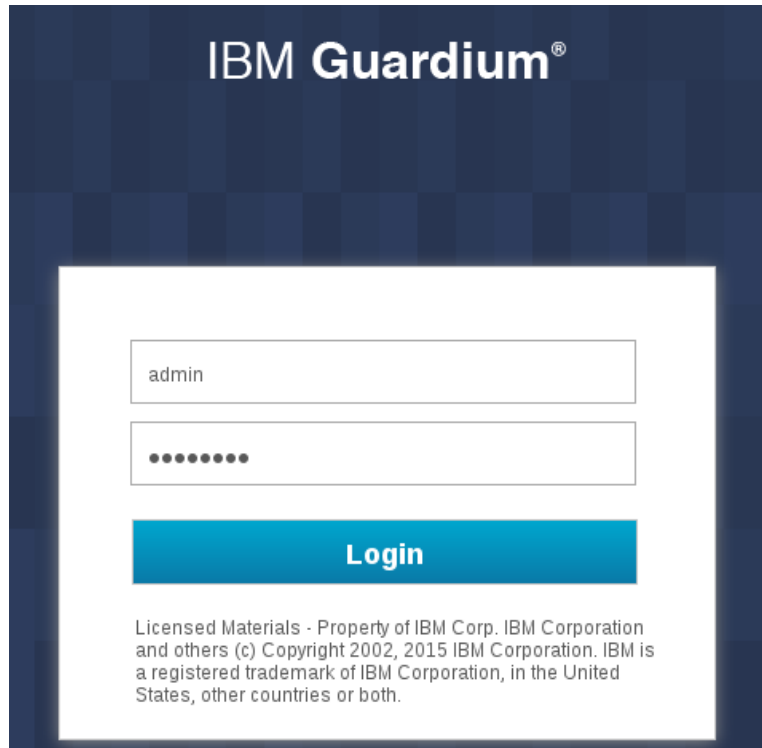
Connecting to the Guardium Appliance in the Cloud

To connect to the Guardium appliance via the Private IP, you need to establish a VPN connection to the IBM Cloud Network.

1. Verify that your User account has VPN access credentials by navigating to Manage > Access (IAM) > Users.
2. Click on your User account and scroll down to the VPN password section to set your VPN credentials.
3. Navigate to <https://www.ibm.com/cloud/vpn-access>.
4. Choose the VPN portal for your desired Datacenter.
5. Provide your VPN login credentials that you set in step 2.
6. After you connect to the VPN client, you can SSH and connect to the GUI of your Guardium instance.

Connect to the GUI

After you establish a VPN connection, open a web browser to this address: <https://<private-ip>:8443>. Login with the credentials provided by Guardium, the system requires that you change the password upon first login.



IBM Guardium®

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.

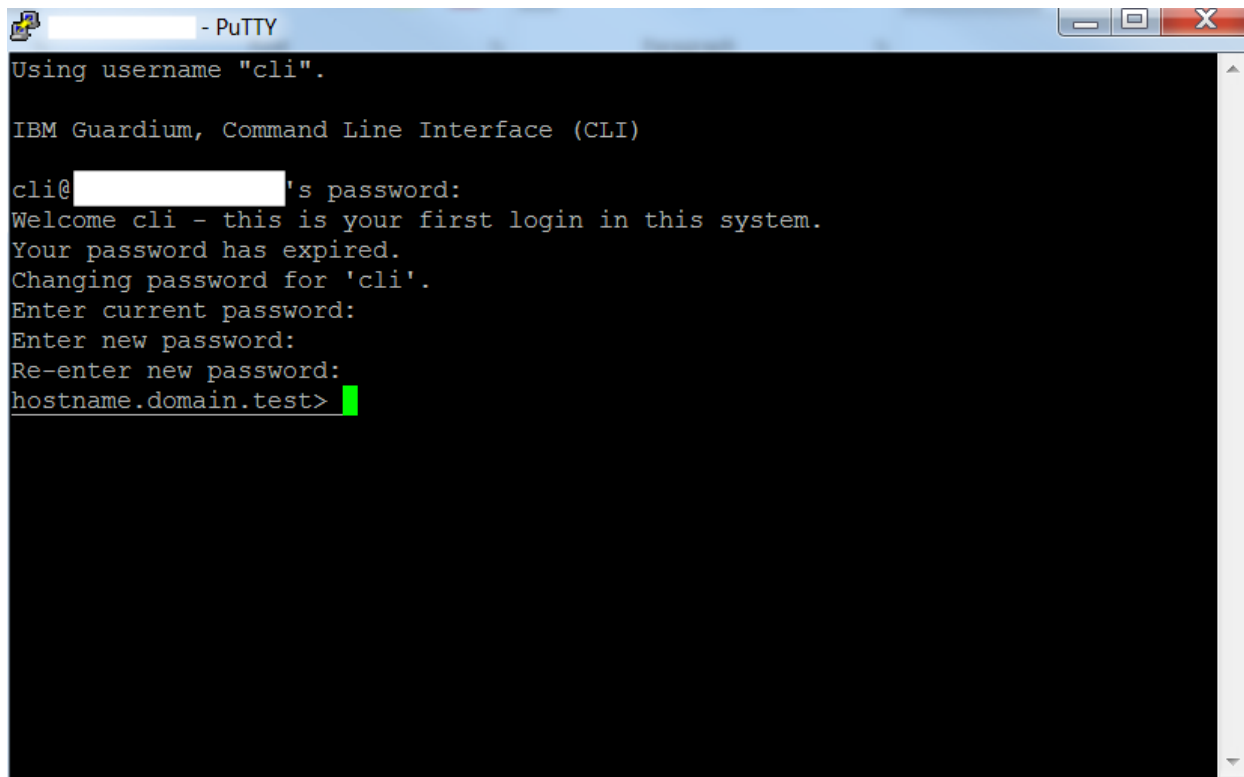
Connect to CLI

To connect to the Guardium CLI, ssh (or use Putty) to the private IP and login as user cli. The first time you log in, the system requires that you to change the password. Change it and store it in a secure place.

Configuring the Appliance Network:

1. Verify that you can SSH into the appliance via CLI user.

Note: The default password is *guardium*. You will be prompted to change your password on first login.



```
Using username "cli".
IBM Guardium, Command Line Interface (CLI)
cli@ [redacted]'s password:
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:
hostname.domain.test>
```

2. Configure network settings.
 - a. SSH into the appliance using the private ip as CLI user.
 - b. Change your password on first log in.

```
cli@10.70.226.197
```

```
IBM Guardium, Command Line Interface (CLI)
```

```
cli@10.70.226.197 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'
```

```
IBM Guardium, Command Line Interface (CLI)
```

```
cli@10.70.226.197 password:
```

- c. Configure the system IP (use the private ip).

```
localhost.domain.test> store network interface ip
10.70.226.197
Mar 29 21:51:40 guard-network[2847]: INFO Sanitizing Hosts
This change will take effect after the next network
restart.
ok
```

- d. Configure the netmask.

```
localhost.domain.test> 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.domain.test> store network route default
10.70.226.1
This change will take effect after the next network
restart.
ok
```

- f. Configure the network resolver.

```
localhost.domain.test> store network resolver 1 10.0.80.11
This change will take effect after restart network.
ok
localhost.domain.test> store network resolver 2 10.0.80.12
This change will take effect after restart network.
ok
```

- g. Configure the hostname.

```
localhost.domain.test> store system hostname
guardiumcollector
Mar 29 14:23:06 guard-network[23308]: INFO set_hostname
Mar 29 14:23:06 guard-network[23308]: INFO Host is
currently localhost.domain.test
Mar 29 14:23:06 guard-network[23308]: INFO Setting
hostname to guardiumcollector.domain.test for ip
10.70.226.197
ok
```

- h. Configure the domain.

```
localhost.domain.test> store system domain
guardium.ibmcloud.com
```

```
Mar 29 14:23:37 guard-network[23836]: INFO set_hostname
Mar 29 14:23:37 guard-network[23836]: INFO Host is
currently guardiumcollector.domain.test
Mar 29 14:23:37 guard-network[23836]: INFO Setting
hostname to guardiumcollector.guardium.ibmcloud.cloud.com
for ip 10.70.226.197
ok
```

- i. Restart the network to apply changes.

```
localhost.domain.test> restart network
Do you really want to restart network? (Yes/No)
yes
Restarting network
Shutting down interface eth0: RTNETLINK answers: No such
file or director

[ 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
```

Warnings and Known Limitations:

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

- show network verify
- show network interface inventory

Do not run the following CLI commands on the IBM Cloud platform as it may result in the appliance becoming inaccessible:

- store network interface reset
- store net interface inventory

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)