HAMMERSPACE

Deployment Guide

Hammerspace 4.1

Google Cloud Platform

Introduction

This guide details step by step instructions for deploying Hammerspace 4.1 in the Google Cloud Platform using Marketplace.

Solution Overview

Hammerspace is a set of software services that are deployed as virtual machines in order to manage data in a single global namespace.

The Hammerspace solution consists of the following main components:

Metadata Server (MDS) deployed as a service and is responsible for managing all the metadata for the namespace.

Data Services (DSX) includes several different components:

- **Portal** - Enables protocol access for NFS v3 and SMB clients. The portal is stateless except for SMB file locks that are maintained across portals.
- **Mover** - The mover is stateless and runs on each DSX instance. It moves files non-disruptively between storage volumes within the global namespace.
- **Cloud Connector -** The cloud connector provides connectivity to S3 compatible object storage and cloud storage from Amazon AWS, Microsoft Azure and Google GCP.
- **Store -** The store service makes block storage available for use in the global namespace. Using DSX Store is a simple way to include local NVMe drives and cloud block volumes in the global namespace.

Deploying Hammerspace Solution

1. In GCP console, select the project where you want to deploy Hammerspace

2. Select Marketplace

3. Search for Hammerspace and select 'Hammerspace' as the solution you want to deploy

4. Click on 'Launch on Compute Engine'

5. Enter a name for your deployment and select a zone where it will be created.
   Note that due to the character limit restriction for an FQDN, Hammerspace will truncate end of the deployment name if the generated hostname is longer than 63 characters. It is recommended to keep the deployment name short in order to avoid running into this situation.

6. A Hammerspace solution comprises one Metadata Server (MDS) Instance and one or more Data Services (DSX) Instances.
   The default Machine type created for the MDS and DSX(s) is 8vCPUs with 30 GB. It is recommended to use the default configuration or bigger for large environments, but in the event that it needs to be changed, the minimum supported configuration is 4vCPUs and 15GB.
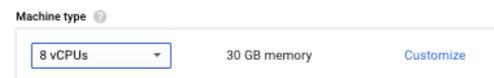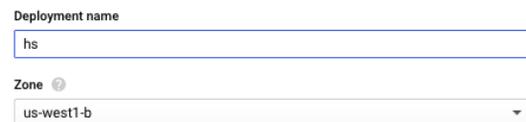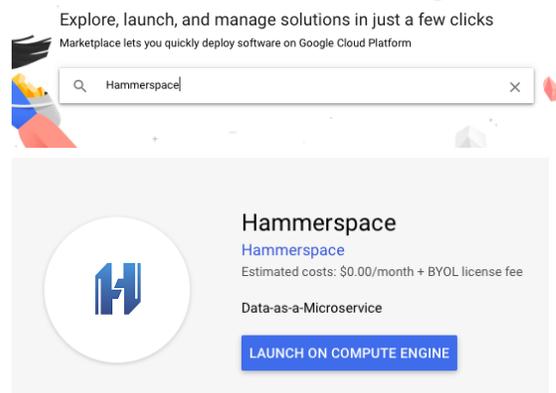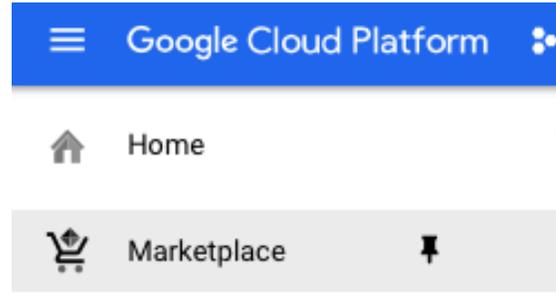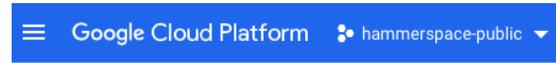
7. To create a Hammerspace solution, select 'Deployment type' as 'Create a new Hammerspace solution' and specify the number of DSX instances to be created as part of the solution in 'Data Services (DSX) instance count'.
A minimum of 1 DSX instance needs to be created for a Hammerspace solution.

Features

Deployment type

Create a new Hammerspace solution

Internal IP of deployed Hammerspace solution (if adding DSX)

192.169.0.2

Data Services (DSX) instance count

1

8. A boot disk and an additional data disk needs to be created for each MDS and DSX. The boot disks are sized at 100GB and their size is non-configurable.
All data disks for MDS and DSX in a deployment are created with the same size, specified by the 'Data disk size in GB' field. If you want different data disk sizes for MDS and DSX or between DSX nodes, create the MDS and DSX in separate deployments. Please look at step 16 for more details on how to do that. The same applies to creating different nodes with different 'Machine types' as mentioned in the previous step.
The minimum supported size for data disks is 100GB and the maximum supported size is 100TB. Also note that the DSX comes in two configurations: with and without Data Store. If you don't want to configure the DSX as a Data Store, you can delete the storage provisioned by the initial deployment at a later time. Similarly, additional storage can be added to a DSX at any later time.

Boot Disk

Boot disk type

Standard Persistent Disk

Data Disk

Data disk type

SSD Persistent Disk

Data disk size in GB

200

9. Setup the Network where the instance should be created. Note that MDS and DSX IP addresses will be dynamically assigned by GCP based on the network listed in the 'Subnetwork' field.
Select 'Ephemeral' from the 'External IP' drop down in order to allow access through Hammerspace GUI. Make sure to keep the 'Allow HTTPS traffic' checkbox checked, otherwise GUI access will not be provided. If you want to restrict GUI access to certain hosts, add their IPs in the field 'Source IP ranges for HTTPS traffic'. Note that

Networking

Network

default

Subnetwork

default (10.138.0.0/20)

External IP

Ephemeral

Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
☑ Allow HTTPS traffic
Source IP ranges for HTTPS traffic

0.0.0.0/0, 192.169.0.2/24

HTTPS access is only for the MDS node, these
options don't have any bearing on the DSX nodes.

10. Click 'Deploy'. The deployment will show up under the 'Deployments' section

-

11. To access Hammerspace through the GUI, click
     on the "Management URL" link on the
     Deployment page. Note that this link only
     applies to an MDS instance and is N/A for DSX
     instances.

12. Note: Be patient after deployment is completed,
     it will take up to 5 minutes before the login page
     is available. If your web browser still can't get to
     the login page then it is possible that https traffic
     was not enabled in your setup for the
     Hammerspace server.
     Go to the VM instance details and check the
     firewall checkboxes for http and https.

13. Login through the CLI or GUI using the Admin user and password provided on the Deployment page. Make sure to change the password after logging into the system.
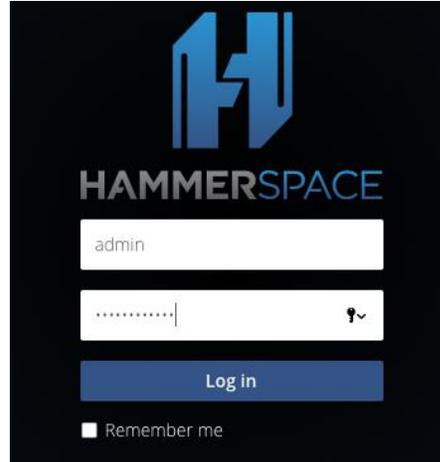
14. Accept the EULA and you will be able to access the Hammerspace Graphical User Interface. You can also manage Hammerspace using the CLI, simply SSH into the same IP as the web UI. See step 18 for additional details using ssh.

15. Add the DSX node(s) to Hammerspace by clicking on the '+' icon under Actions and then following the prompts to add volumes. Consult the 'Getting Started with Hammerspace Guide' for additional options and step by step instructions on how to add storage to the Hammerspace solution.

    This step must be completed before data can be stored using the Hammerspace solution.

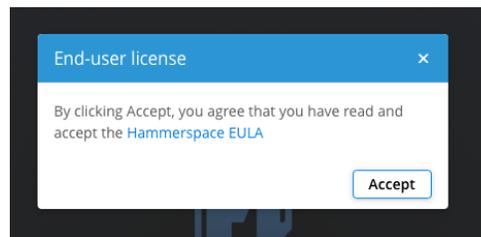   Managed Objects: Infrastructure & Data

    | Shares | Storage Systems | Volume Groups | Volumes |

Add Storage System							Search			
Name	**Volumes**	**Volume Status**	**Type**	**Used**	**Free**	**Total**	**Percentage Used**			**Actions**
hs-mds-dsx0.us-...ernal	0	🟢 🟡 🔴 ⚪	Hammerspace	0.00 B	0.00 B	0.00 B		0%		👁 ➕

16. **OPTIONAL**: Adding additional DSX nodes
    In order to add additional DSX Instances to an existing Hammerspace Solution, create a new Deployment by launching the Hammerspace Solution in Marketplace. Make sure to choose the same project and zone for deployment. Choose 'Add Data Services (DSX) to a Hammerspace solution' from the 'Deployment Type' drop down menu.

    Features

    Deployment type

    Add Data Services (DSX) to a Hammerspace solution

    Internal IP of deployed Hammerspace solution (if adding DSX)

    192.169.0.2

    Data Services (DSX) instance count

    1

In order for the MDS to discover the DSX, you need to specify the 'Internal IP' of the MDS in the field 'Internal IP of deployed Hammerspace solution (if adding DSX)'. Click on the MDS 'Instance' on the Deployment page and look for the 'Primary Internal IP' listed under "Network Interfaces". Add that IP in this field.

Specify the number of DSX nodes to be added to the Hammerspace Solution in the 'Data Service (DSX) instance count' field.

Follow the instructions for filling in the remaining fields as outlined earlier and click Deploy. It is recommended to use labels on deployments that might be sharing a Hammerspace solution.

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP
nic0	default	default	10.138.0.3	—	35.227.169.205 (ephemeral)

17. The new DSX Instance(s) will show up in the Hammerspace solution and can be added as DSX node by clicking on the '+' icon under Actions as mentioned earlier. Follow the 'Getting Started with Hammerspace Guide' to setup the Hammerspace solution.

Managed Objects: Infrastructure & Data

Shares	Storage Systems	Volume Groups	Volumes

⊕ Add Storage System   🔍 Search

Name	Volumes	Volume Status	Type	Used	Free	Total	Percentage Used	Actions
mds-test-dsx0.u...ernal	1	1 0 0 0	Hammerspace	782 MB	107 GB	107 GB	1%	👁
dsx-test-dsx0.u...ernal	1	1 0 0 0	Hammerspace	782 MB	107 GB	107 GB	1%	👁

18. In order to manage Hammerspace using the CLI interface, connect using ssh:

gcloud compute ssh --project <project-name> --zone <zone> admin@<mds instance name>

e.g.
gcloud compute ssh --project hammerspace-public --zone us-west1-b admin@hammerspace-b5-mds

Once connected, you can traverse into the /opt/pd/mgmt/webapps/webui/legal directory to access and/or download the EULA, Licenses and Source files.

Alternately, you can access this information on the GUI by clicking on the 'About Hammerspace' link shown below.
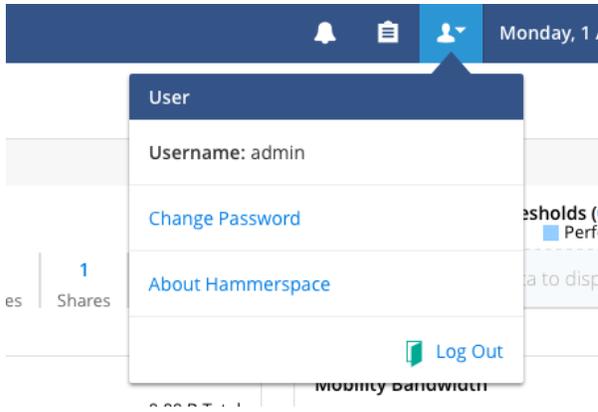
Clicking on this link will show the following screen.
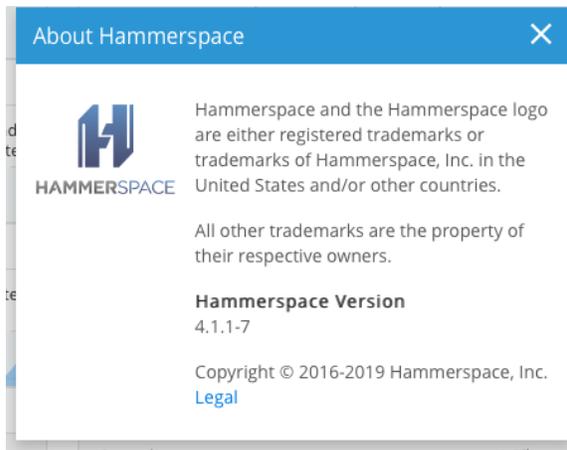
Click on 'Legal' to access and/or download the EULA, Licenses and Source files.

Filename	Size	Last Modified
EULA	8.1 kb	Mon, 01 Apr 2019 05:10:54 GMT
opensource/		Mon, 01 Apr 2019 19:01:21 GMT
LICENSE	4944.5 kb	Mon, 01 Apr 2019 19:01:21 GMT

Apache Tomcat/8.0.24

FIREWALL REQUIREMENTS

The following ports must be open for Hammerspace and DSX nodes to communicate between each other, and for management and protocol access.

Services running on Storage, Hammerspace and DSX nodes

Node	Ports	Protocol	Service	Description
Hammerspace	22	TCP	Management Console	Secure Shell for CLI
Hammerspace	111	TCP & UDP	Storage	RPC (rpcbind)
Hammerspace	123	UDP	NTP	NTP
Hammerspace/DSX	137, 138, 139	TCP & UDP	Samba	SMB file sharing
Hammerspace	161, 445	TCP & UDP	SNMP	SNMP (optional)
External Syslog	514	UDP	syslogd	Syslog (optional)
Storage/DSX/ Hammerspace	2049, 20490, 20491	TCP	NFS	NFS (Network File System)
Hammerspace/DSX	4379	TCP	CTDB	SMB High Availability, CTDB in and outbound
Hammerspace/DSX	4505, 4506	TCP	SALT	Node management, SALT
Hammerspace/DSX	80, 443, 8443	TCP	Management Console	Web management interface
Hammerspace/DSX	9090	TCP	DSX/Hammerspace	Services management
Hammerspace/DSX	9093	TCP	Kafka	Services monitoring, Kafka
DSX	9094, 9095, 9096	TCP	Data Mover	Data Mobility
Object Store/DSX	9098	TCP	Cloud Mover	Object Storage (S3), Cloud mobility
Hammerspace/DSX	9099	TCP	HMDB	Cloud mobility
Hammerspace/DSX	20048	TCP & UDP	Mount	Mount
Hammerspace/DSX	32803	TCP & UDP	NLM	NFS File Locking

Table 1 Incoming firewall port settings

Connections to and from DSX and Hammerspace nodes

Source	Destination	Protocol	Ports	Description
Management Console	Hammerspace	TCP	22	Secure Shell for CLI
DSX/Hammerspace	Mail Server(s)	TCP	25	Alerting
Storage	Hammerspace	TCP & UDP	111	RPC (rpcbind)
NTP	Hammerspace	UDP	123	NTP
SNMP	Hammerspace	UDP	161	SNMP (optional)
Syslog	External syslog	TCP & UDP	514	Syslog (optional)
Storage	Hammerspace	TCP & UDP	2049, 20490, 20491	NFS (Network File System)
DSX/Hammerspace	Hammerspace/DSX	TCP	4379	SMB High Availability (CTDB)
DSX/Hammerspace	Hammerspace/DSX	TCP & UDP	4505, 4506, 5405	Node management
Management Console	Hammerspace	TCP	80, 443, 8443	Web management interface
DSX/Hammerspace	Hammerspace/DSX	TCP	9090	Services management
DSX/Hammerspace	Hammerspace/DSX	TCP	9092	Services monitoring
DSX/Hammerspace	Hammerspace/DSX	TCP	9093	Event monitoring (Kafka)
DSX/Hammerspace	Hammerspace/DSX	TCP	9094, 9095, 9096	Data Mobility
DSX/Object Store	Object Store/DSX	TCP	9098	Object Storage (S3)
DSX/Hammerspace	Hammerspace/DSX	TCP	9099	Cloud Mobility

Table 2 Outgoing firewall port settings

An example of a firewall rule that would open up a subset of these ports for all nodes on the subnet 10.138.0.0/20 would be:

← Firewall rule details   ✎ EDIT   🗑

hs-rules

Logs ⊙
Off
view

Network
default

Priority
1000

Direction
Ingress

Action on match
Allow

Source filters

IP ranges	10.138.0.0/20

Protocols and ports
tcp:22
tcp:111
tcp:139
tcp:161
tcp:445
tcp:662
tcp:875
tcp:892
tcp:2049
tcp:4505
tcp:4506
tcp:4379
tcp:8443
tcp:9054
tcp:9093
tcp:9094
tcp:9095
tcp:9096
tcp:9098
tcp:9099
tcp:20048
tcp:20491
tcp:32803
udp:111
udp:123
udp:137
udp:138
udp:161
udp:662
udp:875
udp:892
udp:4379
udp:20048
udp:32803

Enforcement
Enabled

Applicable to instances

Licensing

Hammerspace requires a valid license to use the software. The installation should be activated using the license CLI. Without a license, the software will operate without warnings for 30 days.

Each customer is provided an account on the Delivery & License Portal where release images and documentation can be found and downloaded. Information about entitlements associated with the customer account are also available on this portal.

An entitlement e-mail is sent to the customer owner and lists one or more Activation IDs associated with each product when an entitlement is created, updated or renewed.

Subject: Entitlement ID(s): zzzz-yyyy-xxxx-wwww-vvvv-uuuu-tttt-ssss from Hammerspace

Dear <User>,

Below are the Entitlement ID(s) that you can use to activate the licenses you recently purchased from Hammerspace under Sales Order ID: < Sales Order ID>.

These entitlements are granted to:
Org Name: <Company Name>
Contact Name: <Contact Name>
Contact Email: <user@customer_domain>

Subject to the terms of your purchase agreement with Hammerspace, you hereby have the right to activate the following product license(s):

ActivationID: aaaa-bbbb-cccc-dddd-eeee-ffff-gggg-hhhh
Product Name: Hammerspace
Version: 4.1.1
Total Quantity: 2
Start Date: Feb 5, 2019
Expiration Date: Sep 30, 2019

Duration: 237 Days

…

Activating Hammerspace Licenses

To activate your Hammerspace licenses please refer to the entitlement email received from Hammerspace, note the ActivationID and follow the steps below.
Please contact your Hammerspace representative if you did not receive an ActivationID.

1. Login to Hammerspace via ssh as an admin user.
2. Enter your ActivationID using the 'license-activate' command, example:

license-activate --activation-id aaaa-bbbb-cccc-dddd-eeee-ffff-gggg-hhhh

3. Validate Hammerspace licenses using the 'cluster-view' command, example:

cluster-view

```
ID:                        3aedcc9e-21d6-42f4-8d6f-66150f6a645c
Name:                      PD242010A8A0FC2
State:                     Standalone
IP:                        10.138.15.194/32
Cluster floating IPs:      [10.138.15.194/32]
Portal floating IPs:       []
Since:                     2019-03-29 17:35:31 UTC
Timezone:                  UTC
VVOL support:              true
EULA accepted date:        2019-03-29 17:36:28 UTC
Online activation support: true
Activation ID:             aaaa-bbbb-cccc-dddd-eeee-ffff-gggg-hhhh
License activation date:   2019-03-29 17:55:16 UTC
License details:
            Name:          DataSphere_Enterprise
            Status:        VALID
            Expiration:    2019-03-29 23:59:59 UTC
            Number of acquired licenses: 1
Data directors:
            [Object type: DATA_SPHERE, Node name: hs-mds-mds.us-west1-b.c.hammerspace-
dev.internal, Role: PRIMARY, Oper state: UP, Admin state: UP]
            [Object type: DATA_SPHERE, Node name: ds-001.tme.local, Role: SECONDARY, Admin
state: UP]
```

If you attempt to use a license that the Hammerspace is already using, you will see similar results to those shown below:

license-activate --activation-id aaaa-bbbb-cccc-dddd-eeee-ffff-gggg-hhhh

license-activate: Already licensed with aaaa-bbbb-cccc-dddd-eeee-ffff-gggg-hhhh on 2018-02-16 17:34:19 UTC

If you attempt to use an already expired license, you will see similar results to those shown below:

license-activate --activation-id aaaa-bbbb-cccc-dddd-eeee-ffff-gggg-hhhhlicense-activate: License activation failed, The activation ID was denied, All features of entitlement, aaaa-bbbb-cccc-dddd-eeee-ffff-gggg-hhhh, are expired.

If you attempt to use a license with the wrong format, you will see similar results to those shown below:

license-activate --activation-id 1234

license-activate: activationId invalid activation-id format

            Try 'license-activate --help' for more information.