SGCI Hosting:
Setup & HubZero Example

Table of Contents

1. Requesting SGCI Hosting Services

Our hosting service provides a limited amount of space on the Rodeo system at the [Texas Advanced Computing Center](#) (TACC). It is available free of charge to US-based gateway projects for up to 6 months of time.

[Rodeo](#) is a powerful cloud resource that allows for the full customization of computational environments and lets users create virtual machines, host data, and provide services of benefit to the science gateway community.

Each project approved for hosting time via SGCI will be given a quota of 3 VMs with each VM consisting of 2 VCPUs, 20 GB of Disk, and 4 GB of RAM in addition to a single public, floating IP with your own private project network. Additional configurations are available upon request. A basic security group allowing traffic on the standard web ports (80 and 443) will be provided with additional configurations available upon request. Additional storage is available (either in the form of volumes or larger instances) upon request.

The Rodeo environment is meant as a test/sandbox environment and does not have any backup capabilities. Please ensure you have backed up any code and services you deploy on the system. Also, the system may be unavailable at times due to maintenance periods. Interested? [Apply using the form on the SGCI Web Site](#)
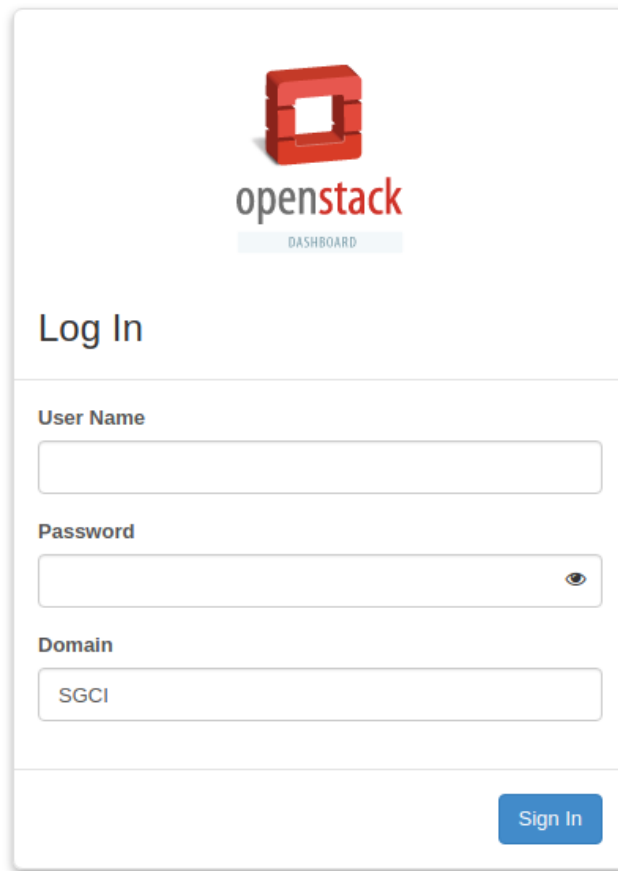
2. Setting Up Account & VMs on Rodeo

2.1 Creating a SGCI Account

In order to access Rodeo, you will need to create an account at: https://sgci.agaveapi.co/create_account

IMPORTANT: Please remember your account credentials from this step and please keep your credentials secure. No administrator will ever ask you for your credentials.
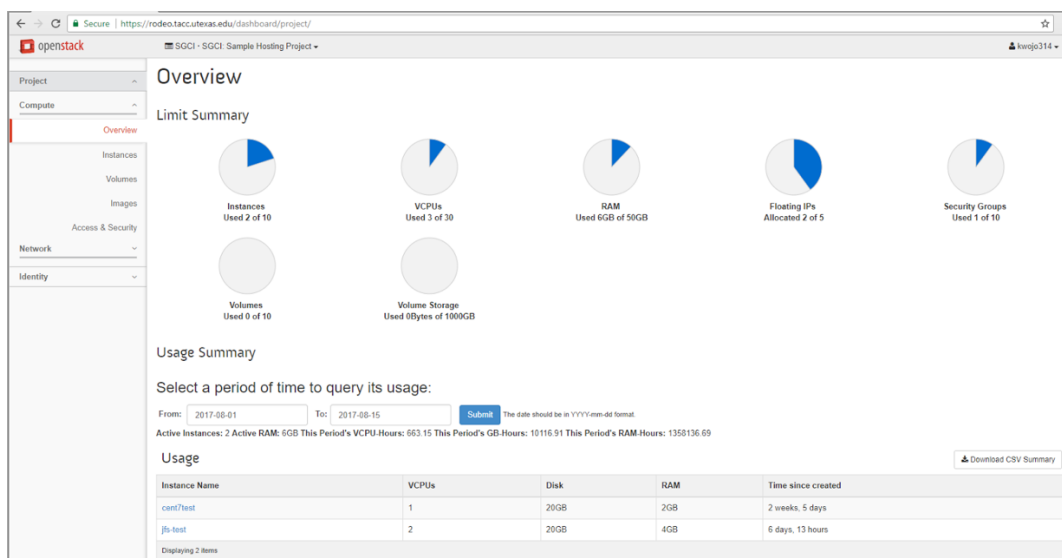
2.2 Setup of OpenStack Domain

Navigate to https://rodeo.tacc.utexas.edu enter your username and password that you used in [Creating a SGCI Account](#). Enter "SGCI" for the Domain field.
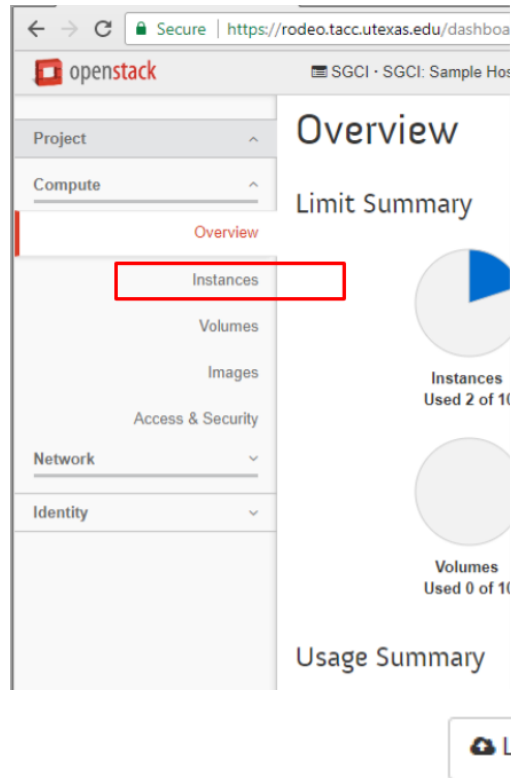
2.2.1 Navigating the Dashboard

Upon successful login, you will be presented with your project's dashboard. This view provides a high-level overview of your allocation on Rodeo.

Creating the Instance

In order to create the instance you will need to navigate to the *Instance* under the *Compute* menu.

From the Instances page, click the **Launch Instance** button.

You will be presented with the Launch Instance wizard which will require filling out few form fields. When launching an instance select *"m1.small"* from **Flavor**, *"Boot from image"* from **Instance Boot Source**, and *"Centos 7"* from **Image Name.**

After populating the Details tab, click the **Access & Security** tab.

Launch Instance

| Details * | Access & Security | Networking * | Post-Creation | Advanced Options |

Availability Zone

nova ▼

Instance Name *

Name

Flavor * ❓

m1.small ▼

Instance Count * ❓

1

Instance Boot Source * ❓

Boot from image ▼

Image Name *

CentOS 7 (962.9 MB) ▼

Specify the details for launching an instance.

The chart below shows the resources used by this project in relation to the project's quotas.

Flavor Details

Name	m1.small
VCPUs	1
Root Disk	20 GB
Ephemeral Disk	0 GB
Total Disk	20 GB
RAM	2,048 MB

Project Limits

Number of Instances   2 of 10 Used

Number of VCPUs   3 of 30 Used

Total RAM   6,144 of 51,200 MB Used

Cancel   Launch

If you already have an SSH key pair, you can import them by clicking the plus (+) button next to the drop-down menu for **Key Pair.** You can also receive instructions on how to generate a key pair if you do not have one already.

The wizard will walk you through how to generate a key pair if you need one. This allows you to access your instance. Password login to the admin account is disabled for security purposes.

Import Key Pair

Key Pair Name *

Public Key *

Description:

Key Pairs are how you login to your instance after it is launched.

Choose a key pair name you will recognise and paste your SSH public key into the space provided.

SSH key pairs can be generated with the ssh-keygen command:

```
ssh-keygen -t rsa -f cloud.key
```

This generates a pair of keys: a key you keep private (cloud.key) and a public key (cloud.key.pub). Paste the contents of the public key file here.

After launching an instance, you login using the private key (the username might be different depending on the image you launched):

```
ssh -i cloud.key <username>@<instance_ip>
```

Cancel   **Import Key Pair**

Once you have configured your Key Pair, you will add your instance to the "default" security group by checking the box under Security Groups.

Once the Access & Security information has been collected move to the next tab labeled *Networking* to confirm the networking settings.

There should be only one Available Network. Your instance should be associated with the SGCI: Sample Hosting Project Network.

Once the network has been associated you can click the blue "Launch" button. Your instance will be created and available shortly for access.

2.2.3 Configuring the Firewall (Security Group)

The default security group allows internal traffic. You may need to create rules to allow SSH, HTTP, and HTTPS to your Hub. You can accomplish by going to the *Access & Security* menu under Compute.
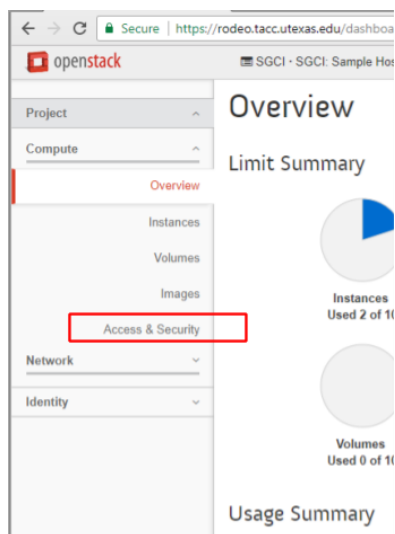
You will see the default security group listed. Click **Manage Rules** to review the security group's policies.

The default security group should look similar to this allowing SSH and HTTPS access.

	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
☐	Egress	IPv6	Any	Any	::/0	-	Delete Rule
☐	Ingress	IPv6	Any	Any	-	default	Delete Rule
☐	Egress	IPv4	Any	Any	0.0.0.0/0	-	Delete Rule
☐	Ingress	IPv4	Any	Any	-	default	Delete Rule
☐	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-	Delete Rule
☐	Ingress	IPv4	TCP	443 (HTTPS)	0.0.0.0/0	-	Delete Rule

Displaying 6 items

If you do not see the appropriate entries you can create the by clicking *Add Rule.*

Once the security group has been configured you can begin building your Sample Portal.

Add Rule

Rule *

SSH

Remote * ❓

CIDR

CIDR ❓

0.0.0.0/0

Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Add

3.   Installing a sample HubZero Portal

The Science Gateway Institute Software Catalog has prepared a Docker containers for the purpose of evaluating the platforms available to build your gateway upon.

3.1 HUBzero Content Management System

The HUBzero Platform allows users to host analytical tools, publish data, share resources, collaborate, and build communities in a single web-based ecosystem.

This sample portal contains the features that facilitate publishing data, sharing resources, collaboration, and community building. The tool hosting functionality is currently not supported in the sample portal, however is available for evaluation on https://hubzero.org

User documentation is available at https://hubzero.org/documentation.

Installing the HUBzero Content Management System will require installing Docker on your CentOS7 instance, cloning a git repository, building the Docker image, and running a command to start the instance.

There are a couple of recommendations that the HUBzero developers recommend for smoothing out the evaluation process for their gateway which are available at the end of the setup procedures.

3.2 Installing Docker on CentOS7

1.   ssh rodeo.129.X.X.X -i ~/.ssh/identity
2.   sudo yum update
3.   sudo yum install docker git -y
4.   sudo systemctl start docker
5.   sudo systemctl enable docker
6.   sudo usermod -aG docker rodeo
7.   exit
8.   Ssh rodeo@129.X.X.X -i ~/.ssh/identity
9.   Docker run hello-world

```
[rodeo@cent7test ~]$ docker run hello-world

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://cloud.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/engine/userguide/
```

3.3 Installing HUBzero Sample Portal Container

The HUBzero Platform is a collection of services which include a web server, a database server, an email server, a dedicated search service, SFTP and WebDav for file transfer, and many other background services that provide a rich set of functionality. It is difficult to distribute many of these services in the form of a container, therefore we make available a virtual machine image or an Amazon Marketplace Image (AMI) available for download at https://hubzero.org/download.

If you are adventurous enough, you may install the HUBzero Platform from packages following the instructions available at https://hubzero.org/documentation.

For the purpose of evaluating the CMS (web server and database server only) a Docker container has been prepared to introduce some of the functionality to a person interested in building a gateway with the HUBzero Platform.

Some caveats of using this Docker Container are:
- Email sending and receiving is not supported.
- Simulation Tool execution is not supported.

The files to build the docker image are available on Github at https://github.com/hubzero/hzcms-sgi-docker.git. The instructions for using the docker image are available on the README and are adapted for use on the SGCI Instance below.
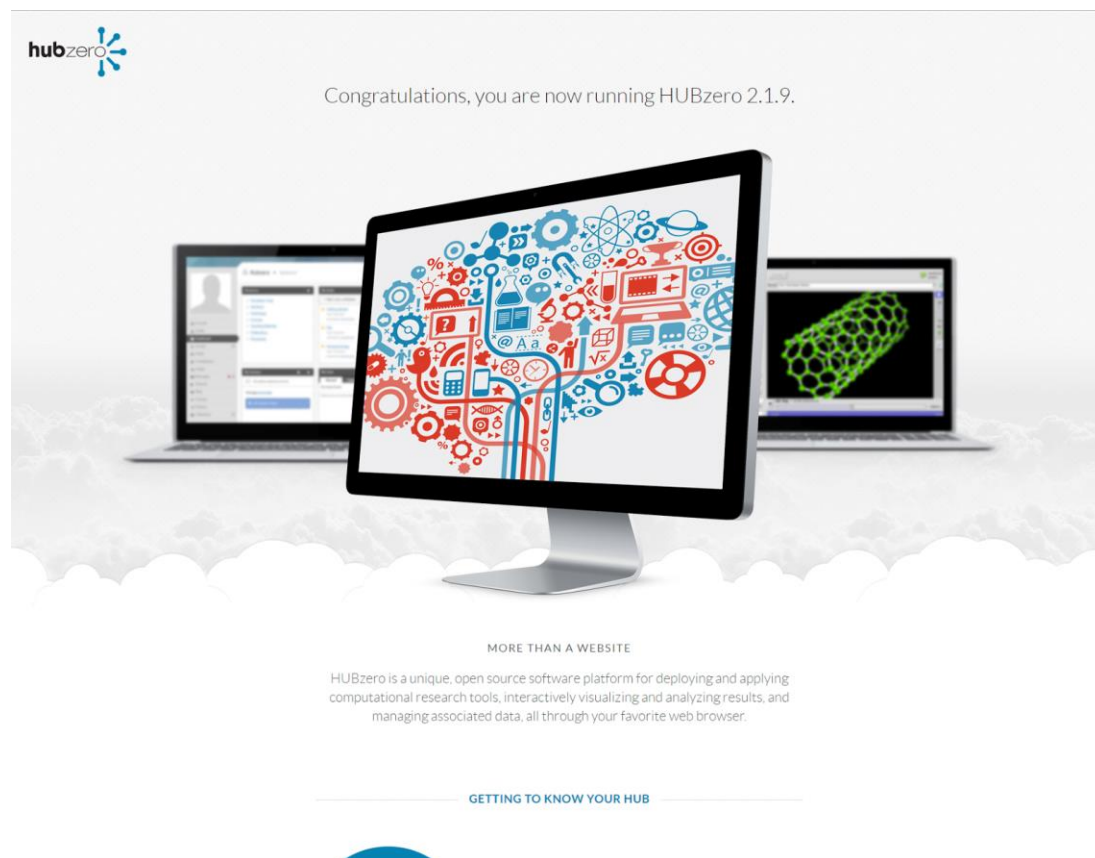1. Clone this repository: git clone https://github.com/hzcms-sgi-docker

2. Build the container: `cd hzcms-sgi-docker && docker build -t hubzero-cms ./`
3. Run the container: `docker run -p 443:443 hubzero-cms -d`
4. In your browser, navigate to *https://<floating ip address*

3.4 First-time Configuration of the HUBzero Sample Portal

The HUBzero Platform is a highly-configurable platform used to build gateways. There are a couple of first-time configuration items you will need to change in order to more fully evaluate the system.

3.5 The Landing Page

Upon successful launching of the HUBzero Container, visiting https://<floating_ip_address> will display a splash page that discusses some of the high-level features the full platform has to offer.

MORE THAN A WEBSITE

HUBzero is a unique, open source software platform for deploying and applying computational research tools, interactively visualizing and analyzing results, and managing associated data, all through your favorite web browser.

GETTING TO KNOW YOUR HUB

3.6 Getting the Admin Credentials

The HUBzero CMS default management user is called 'admin'. The password used for the 'admin' account can be found by running `docker exec CONTAINERNAME cat /etc/hubzero.secrets` The password for 'admin' is listed under JOOMLA_ADMIN.

```
[rodeo@cent7test ~]$ docker ps
CONTAINER ID        IMAGE           COMMAND              CREATED        STATUS         PORTS                     NAMES
3647fc42cb2c        hubzero-cms     "/bin/sh -c /run.sh" 5 hours ago    Up 5 hours     0.0.0.0:443->443/tcp      suspicious_mahavira
[rodeo@cent7test ~]$ docker exec suspicious_mahavira cat /etc/hubzero.secrets
[DEFAULT]
HUBDB=9cVCf2vFyUHnu8
JOOMLA-ADMIN=rSpmHT9WvSSw29
MYSQL-ROOT=9yJ9xwSD2CNCA5
MYSQL-ROOT-USER=root
```

3.7 Logging into the Administrator Panel

Navigating to https://<floating_ip_address>/administrator will bring you to a login page where you will enter the admin credentials. Upon successful login you will be taken to the Dashboard.
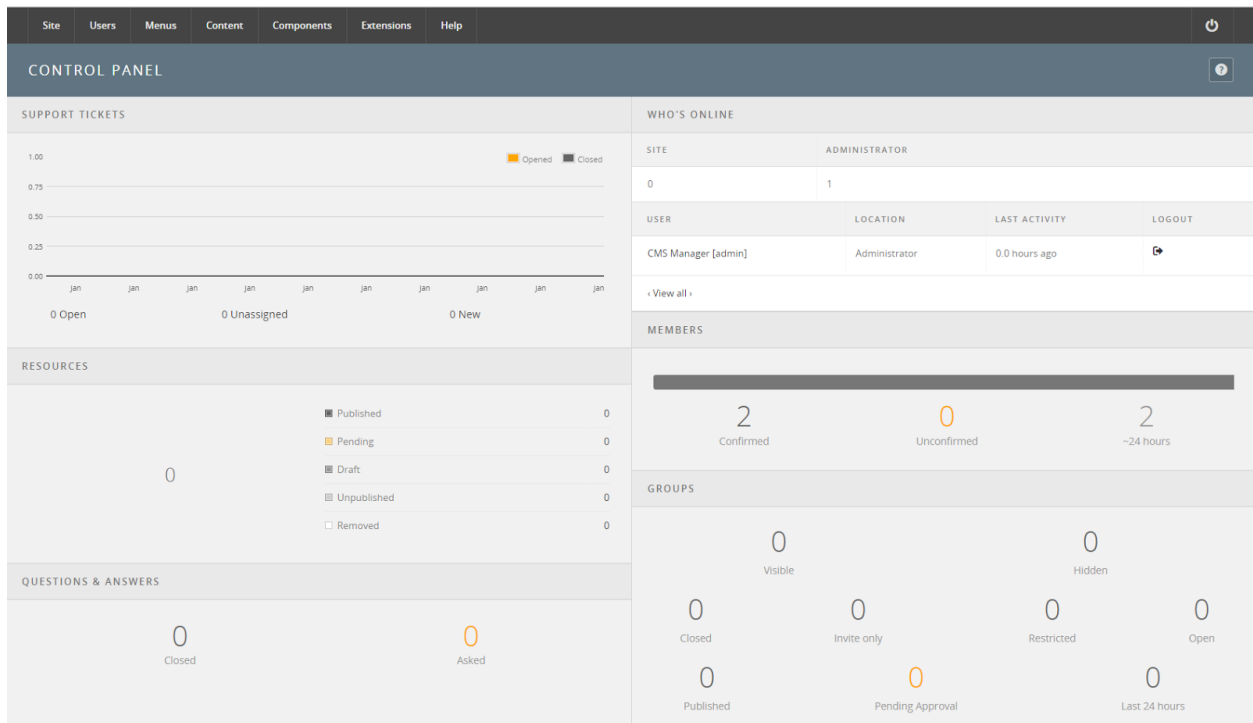
3.8 Changing the Template

To change the template from the Welcome landing page to the default template, use the Extensions Menu and then navigate to the Template Manager menu item. Click the Star Next to "HUBzero Standard Site Template 2015 (Kimera)" to change the template.

Reloading the front page at https://<floating_ip_address> should show the Kimera template.

More information on templates can be found here:
https://help.hubzero.org/documentation/2.1.0/webdevs/templates

3.9 Registering a User Account

A user may register by going to https://<floating_ip_address>/register and filling out the form.

Notice: Email is not supported in the container environment. Normally an email will be sent to the user's email address asking them to confirm their email address using a registration code. They will confirm their account via the registration code and be granted access to your hub.

Workaround: An admin can go into the backend and approve users manually. From the administrative backend go to the Users menu and click Members. Clicking the Registered column will confirm the user's email.

3.9.1 The Member Dashboard

The member dashboard is an area where you can get a high-level overview of happenings on the hub. You can enter any area on the Hub from the dashboard. For a full overview of features and capabilities, review the HUBzero documentation at https://hubzero.org/documentation