

Motivation

Lecture Objectives

- We will learn to interact with the cloud in three ways: (1) via a graphical user interface, (2) via command line, and (3) time permitting, via programmatic APIs
- The system with which we communicate is called the cloud infrastructure management software
- A **top-down** learning approach to interacting with the cloud
- Examples of cloud management infrastructure software include OpenStack, Eucalyptus, OpenNebula, proprietary implementations
- We will first use NSF Chameleon, and then Amazon AWS (mostly self-study; numerous online tutorials on AWS to get started)
 - Our NSF's cloud is called Chameleon

We will focus on OpenStack used by Chameleon.

Motivation for Using Multiple Clouds

- NSF Chameleon Cloud is managed by University of Texas and University of Chicago and made available to the academic research community via funds from NSF.
 - A free resource for learning and we are going to use it
- AWS will allow us to play within a real commercial cloud environment while judiciously using our cloud credits.
 - AWS Educate application for educational credit available
 - Projects should use AWS or other cloud platforms.

Motivation

The End

OpenStack Overview

Please note that there may be screenshots that are for our local ISIS' Horizon Cloud or from prior years using NSF Chameleon Cloud, which also uses OpenStack.

OpenStack

- OpenStack is the cloud operating system that manages the infrastructure resources inside a cloud data center
 - Reading assignment is about another academic effort called Eucalyptus
- Open source project
 - Started by NASA and Rackspace in 2010
 - Currently managed by the OpenStack foundation
 - Apache 2.0 license
 - Current releases are called Newton and Ocata
- Different resource types and other aspects of resources in the cloud are handled by individual OpenStack projects

OpenStack Releases

Release Series

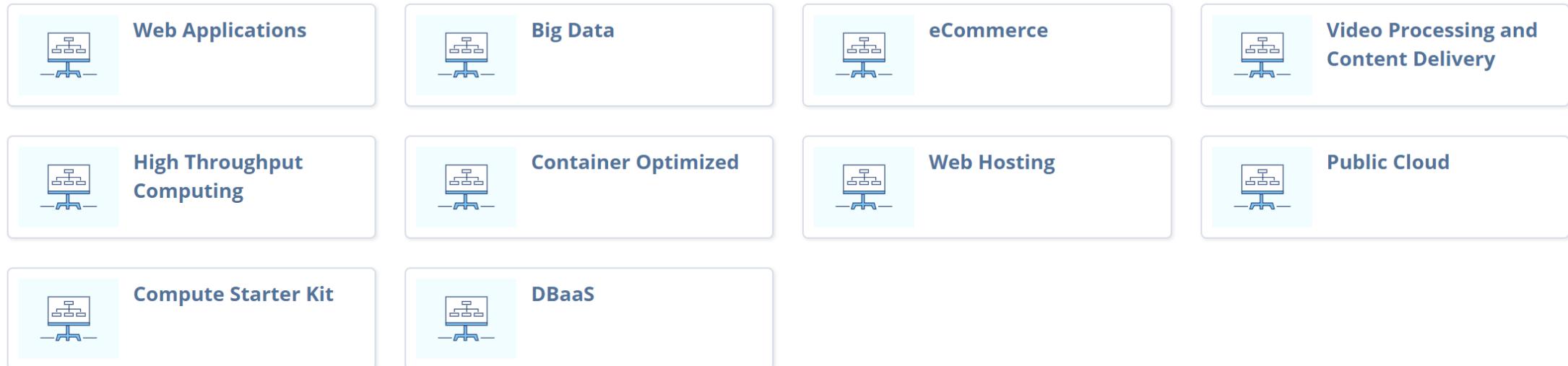
OpenStack is developed and released around 6-month cycles. After the initial release, additional stable point releases will be released in each release series. You can find the detail of the various release series here on their series page. Subscribe to [combined release calendar](#) for continual updates.

Series	Status	Initial Release Date	Next Phase	EOL Date
Train	Development	2019-10-16 <i>estimated schedule</i>	Maintained <i>estimated 2019-10-16</i>	
Stein	Maintained	2019-04-10	Extended Maintenance <i>estimated 2020-10-10</i>	
Rocky	Maintained	2018-08-30	Extended Maintenance <i>estimated 2020-02-24</i>	
Queens	Maintained	2018-02-28	Extended Maintenance <i>estimated 2019-10-25</i>	
Pike	Extended Maintenance	2017-08-30	Unmaintained <i>estimated TBD</i>	
Ocata	Extended Maintenance	2017-02-22	Unmaintained	

Shows a snapshot from 2019

(<https://releases.openstack.org>)

Configurations of OpenStack



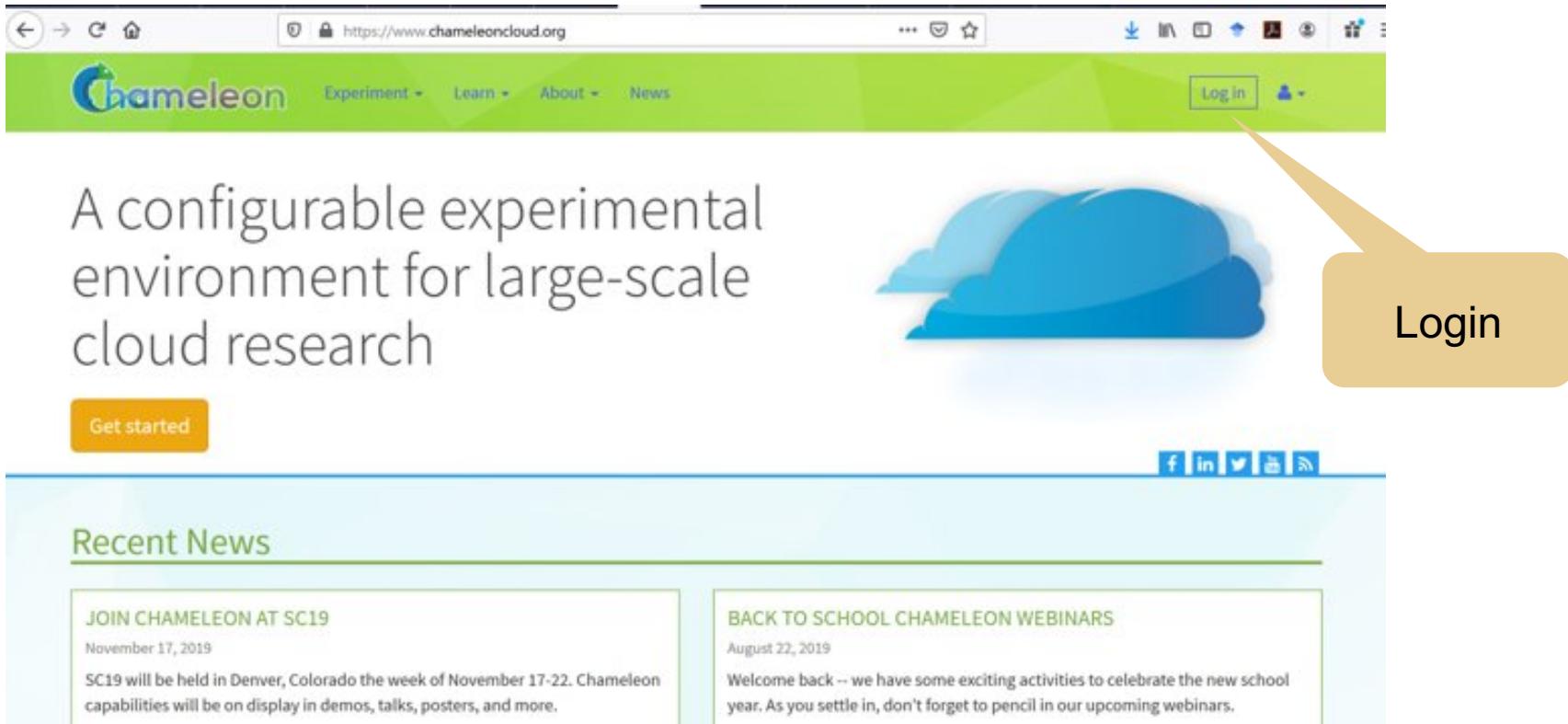
- We do not worry about these configurations.
- We just use what is already configured for us.
 - Here by the NSF Chameleon Cloud managers

OpenStack Overview

The End

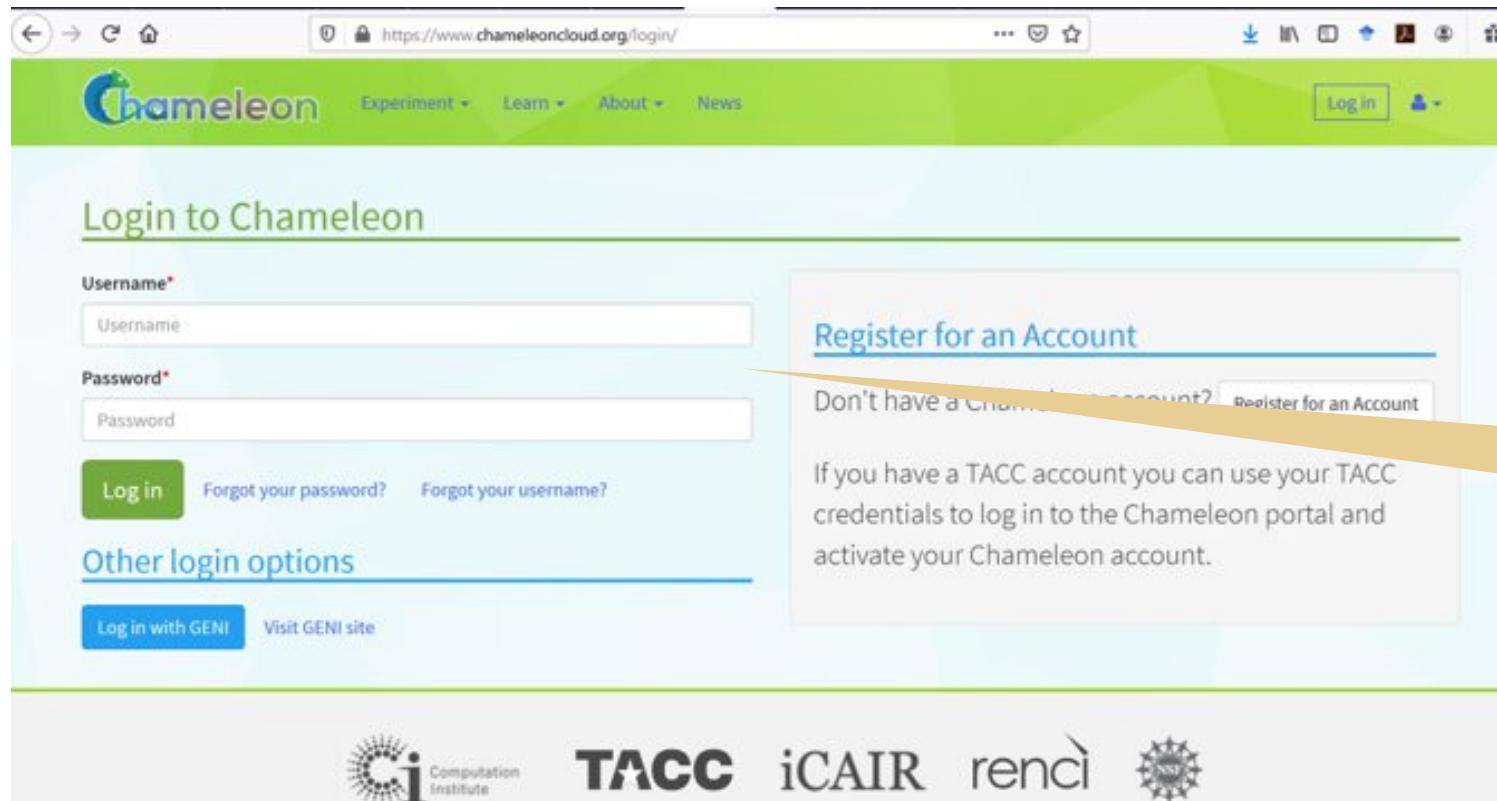
OpenStack GUI

Chameleon Front Page



- This is the view that I see as the project's lead.
- You might see a slightly different view.

Chameleon Signing In



- This is the view that I see as the project's lead.
- You might see a slightly different view.

Chameleon Front Page Post Signing In

The screenshot shows the Chameleon cloud website's front page. At the top, there is a navigation bar with links for Appliances, Hardware, News, About, Blog, Documentation, Webinars, and a user account dropdown labeled 'agokhale'. Below the navigation bar, a large green header features the Chameleon logo and the text 'A configurable experimental environment for large-scale cloud research'. A prominent orange 'Get started' button is located below the text. To the right of the text, there is a graphic of three blue clouds. A yellow callout bubble with a black border points from the bottom right towards the user account dropdown. Inside the bubble, the text reads: 'Select dashboard from the pull-down menu.' Below the main header, there is a section titled 'Recent News' with two items: 'BACK TO SCHOOL CHAMELEON WEBINARS' (August 22, 2019) and 'CHAMELEON TO PRESENT AT PEARC19 HARC WORKSHOP' (July 27, 2019).

A yellow callout bubble with a black border points from the bottom right towards the user account dropdown.

Select dashboard from the pull-down menu.

- This is the view that I see as the project's lead.
- You might see a slightly different view.

Chameleon Dashboard Page

The screenshot shows the Chameleon dashboard with the following sections:

- Active Projects:** Displays two projects: CH-817567 and CH-819381.
- Ongoing outages:** Shows "Network maintenance at TACC December 15 8am-4pm CDT".
- Open tickets:** Displays one ticket: #57516 - Deleting users and instances, last updated 9 seconds ago, with a "Reply" link.

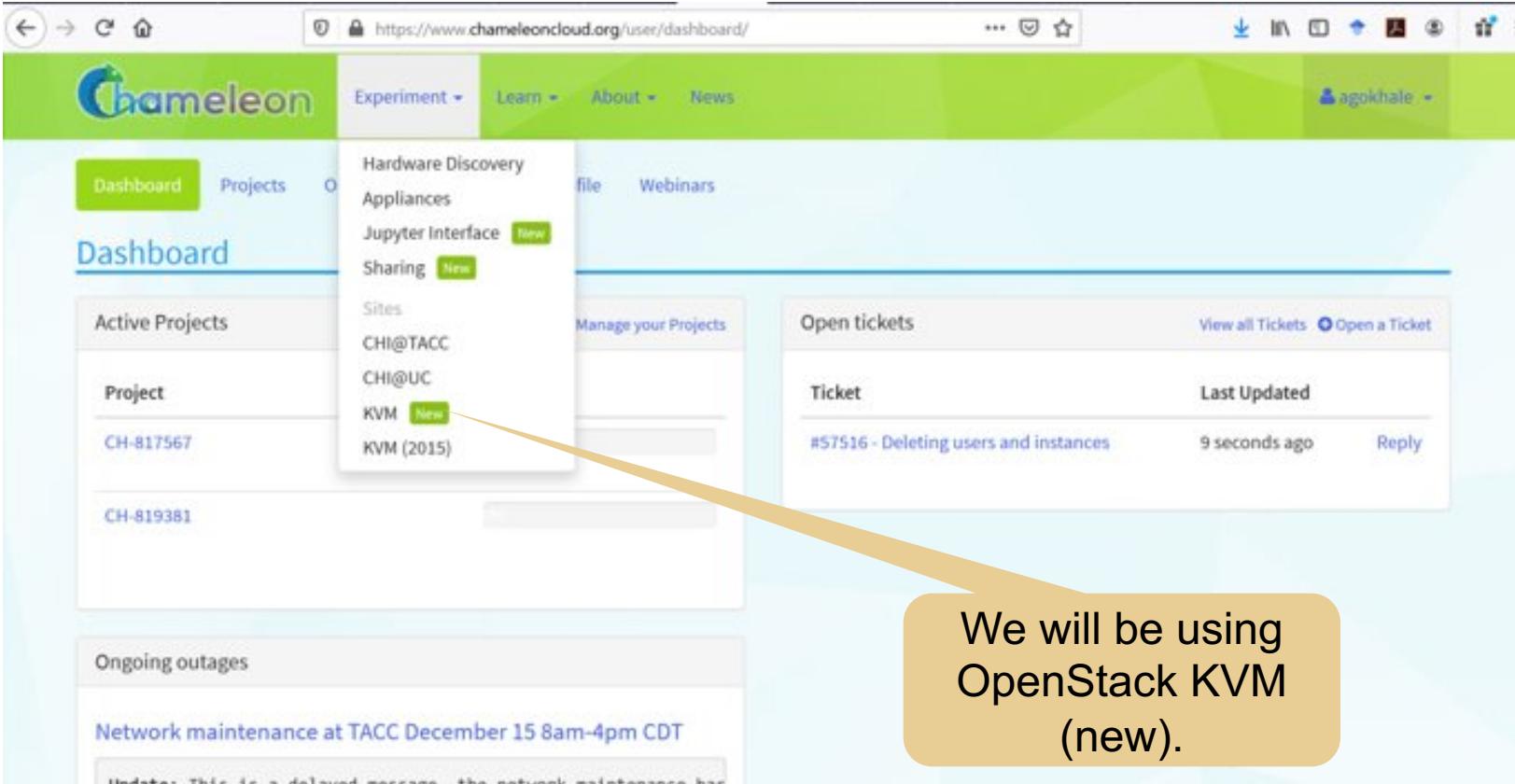
Experiment selection menu.

These are my projects.

These are any tickets you may have open in the system.

Our class project is CH-819381.

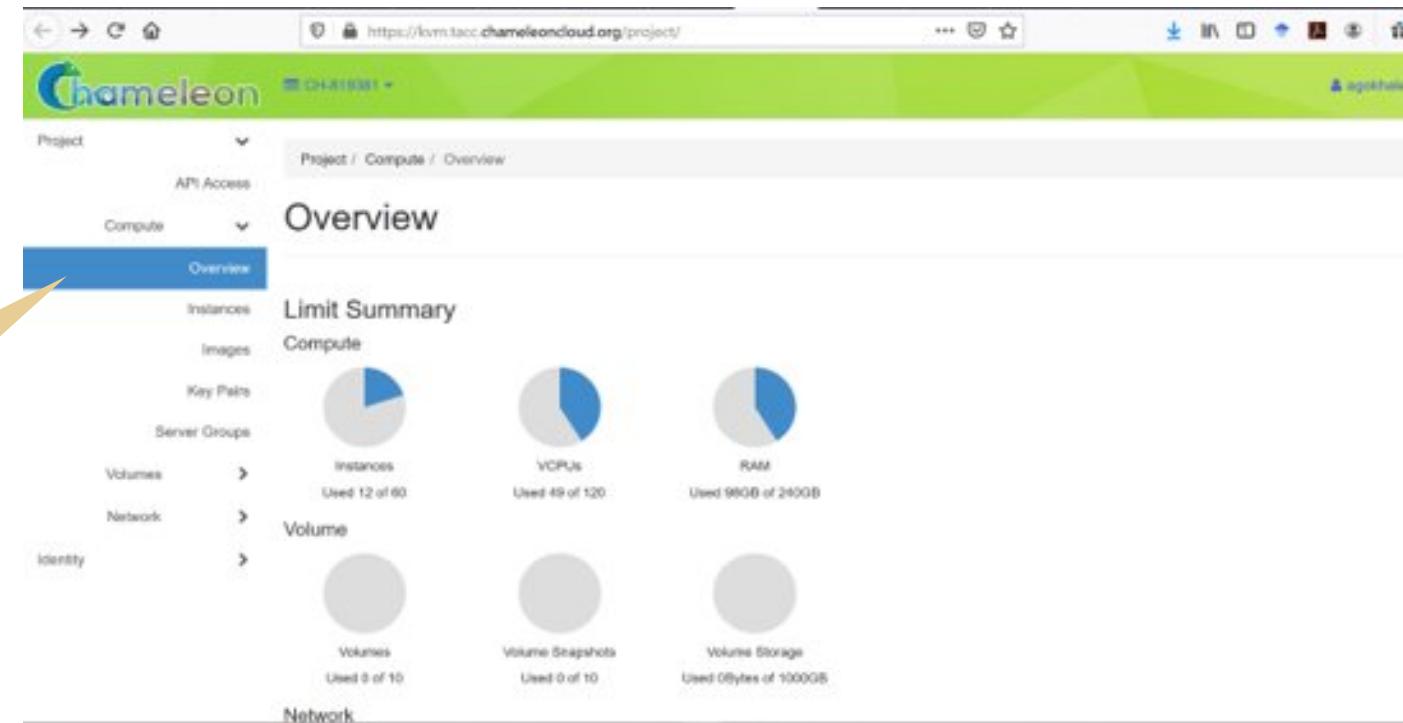
Experimenting With the Chameleon Cloud



The screenshot shows the Chameleon Cloud user dashboard at <https://www.chameleoncloud.org/user/dashboard/>. The dashboard has a green header with the Chameleon logo, navigation links for Experiment, Learn, About, News, and a user profile for agokhale. The main area is titled "Dashboard". On the left, there's a sidebar with "Active Projects" showing "Project" and two entries: "CH-817567" and "CH-819381". To the right of the sidebar is a "Manage your Projects" section with a "Hardware Discovery" dropdown menu open, showing options like Appliances, Jupyter Interface (New), Sharing (New), and Sites (CHI@TACC, CHI@UC). Below this is an "Open tickets" section with one ticket listed: "#57516 - Deleting users and instances" last updated 9 seconds ago with a "Reply" button. At the bottom, there's an "Ongoing outages" section mentioning "Network maintenance at TACC December 15 8am-4pm CDT". A large orange callout bubble points from the "KVM (2015)" entry in the sidebar to the text "We will be using OpenStack KVM (new).".

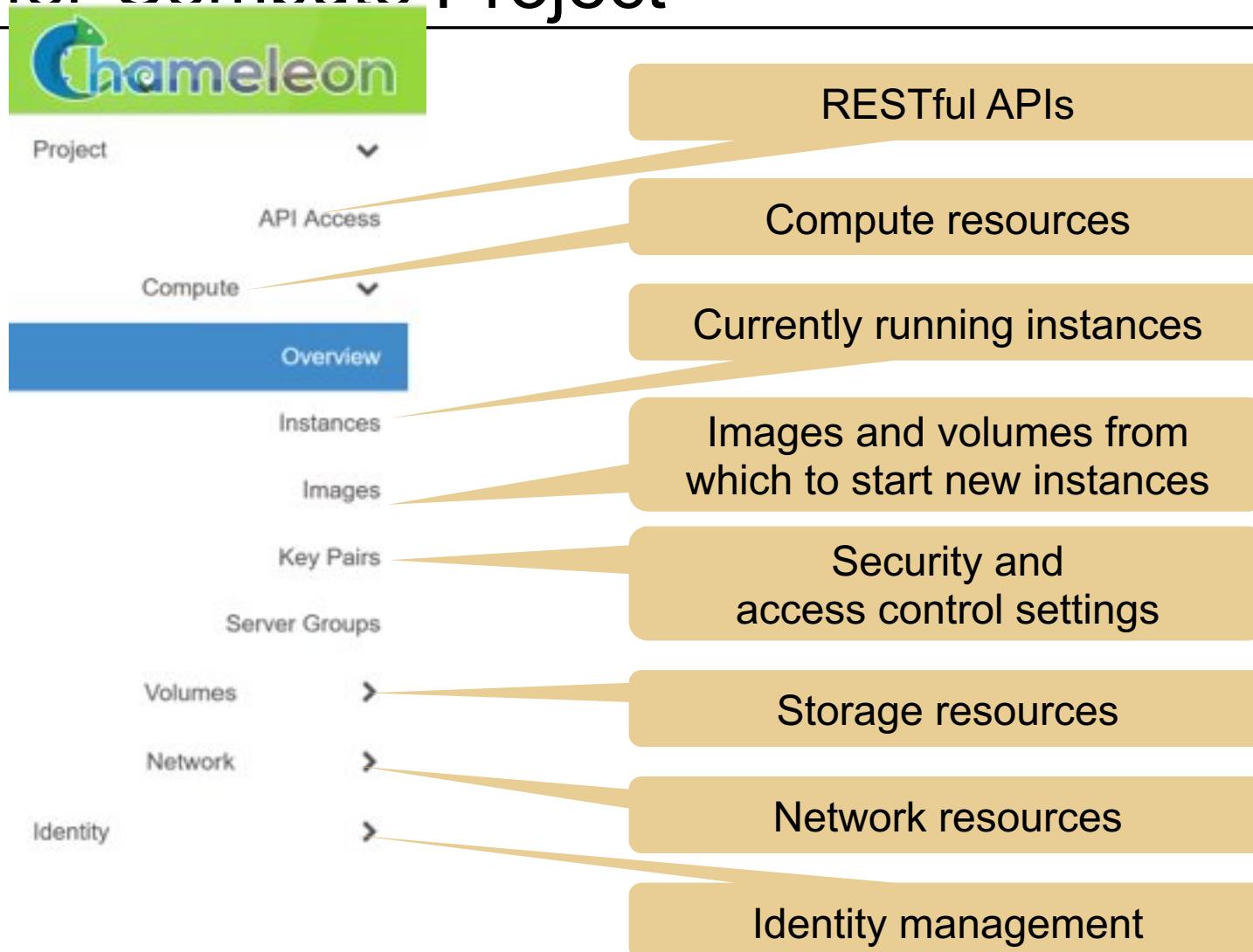
We will be using
OpenStack KVM
(new).

OpenStack User Dashboard



- The GUI is called Horizon.
- This is our view when we log into Chameleon.
 - Right now, there still are several instances from last year that are running and that need to be deleted.
- User guide is available here: [OpenStack Train Project User Guides](#).

OpenStack Project Tab: Expanded for Compute Project



Overview of OpenStack Compute Tab

The screenshot shows the Chameleon OpenStack Compute tab with the following data points:

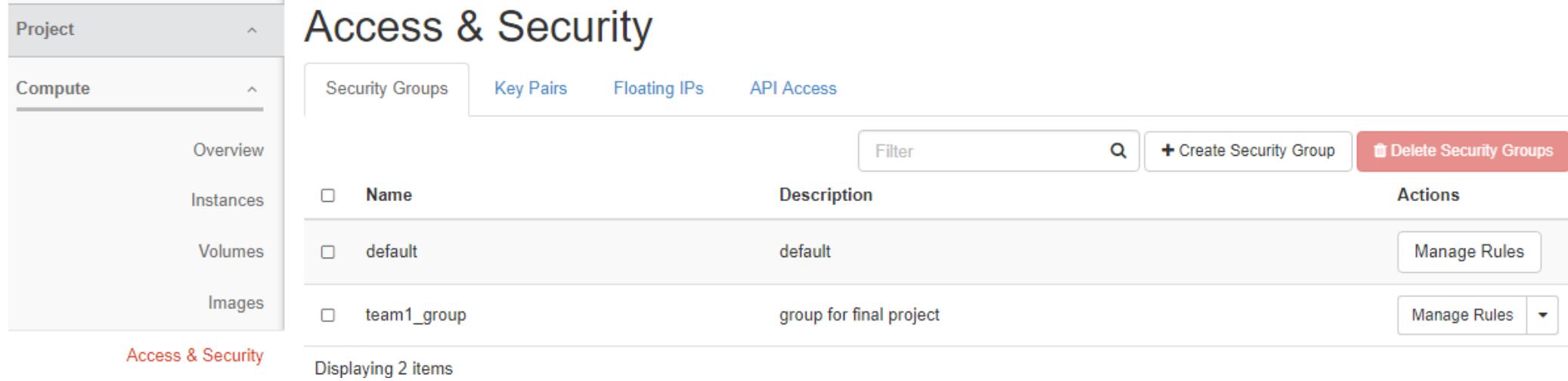
- Instances:** Used 12 of 60
- VCPUs:** Used 49 of 120
- RAM:** Used 98GB of 240GB
- Volume:** Used 0 of 10
- Volume Snapshots:** Used 0 of 10
- Volume Storage:** Used 0Bytes of 1000GB
- Floating IPs:** Used 0 of 10
- Security Groups:** Used 0 of 10
- Security Group Rules:** Used 0 of 10
- Networks:** Used 0 of 10
- Ports:** Used 0 of 10
- Routers:** Used 0 of 10

Annotations with callouts point to specific metrics:

- The project that we belong to (CH-819381)
- Number of running instances and upper limit (Instances: Used 12 of 60)
- Number of running virtual CPUs and upper limit (VCPUs: Used 49 of 120)
- Amount of RAM used and upper limit (RAM: Used 98GB of 240GB)
- Number of configured security groups (Security Groups: Used 0 of 10)
- Number of floating IP addresses and their limit (Floating IPs: Used 0 of 10)

We will all be in the CH-819381 project.

Security and Access Control



The screenshot shows the AWS CloudFormation interface with the 'Compute' project selected. The left sidebar shows 'Compute' expanded, with 'Access & Security' highlighted in red. The main area is titled 'Access & Security' and contains tabs for 'Security Groups', 'Key Pairs', 'Floating IPs', and 'API Access'. The 'Security Groups' tab is active. It displays two security groups: 'default' and 'team1_group'. Each group has a checkbox next to its name, a 'Description' field, and an 'Actions' section with a 'Manage Rules' button. A 'Filter' input field and a search icon are at the top right, along with buttons for '+ Create Security Group' and 'Delete Security Groups'.

Name	Description	Actions
default	default	Manage Rules
team1_group	group for final project	Manage Rules ▾

Displaying 2 items

- Click on the access and security tab.
- Before doing anything else, we must set up security and access control policies.
 - Set up groups (if any).
 - We need Secure Shell (SSH) key pairs so you can log into an instance remotely.
 - Assign public floating IP address so you can communicate to an instance from outside.

OpenStack GUI

The End

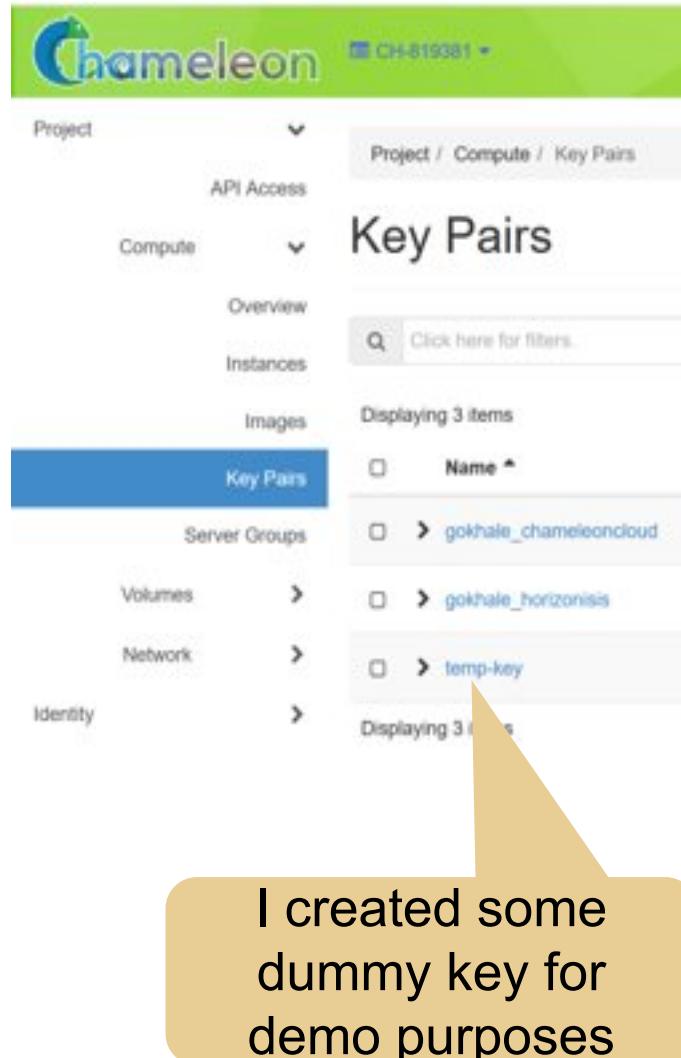
Setting Up Key Pairs

Setting Up Key Pairs (Creation)

The screenshot shows a web browser window for the Chameleon Cloud platform at the URL https://kvm.tacc.chameleoncloud.org/project/key_pairs. The page title is "Key Pairs". On the left, there's a navigation sidebar with "Project", "API Access", "Compute" (selected), "Overview", "Instances", and "Images". Under Compute, "Key Pairs" is also selected. The main content area displays a table with two items, filtered by "Name". A modal dialog box titled "Create Key Pair" is open in the foreground. It has a field labeled "Key Pair Name *". A tooltip for this field says: "Key Pairs are how you login to your instance after it is launched. Choose a key pair name you will recognize. Names may only include alphanumeric characters." Below the dialog is a "Cancel" button. At the top of the main page, there are buttons for "Create Key Pair" (highlighted with a yellow arrow), "Import Public Key", and "Delete Key Pairs". A large yellow callout bubble on the right side of the screen contains the text "Create or import key pair." Another yellow callout bubble points to the "Key Pair Name" field in the dialog with the text "Give some name for your key pair."

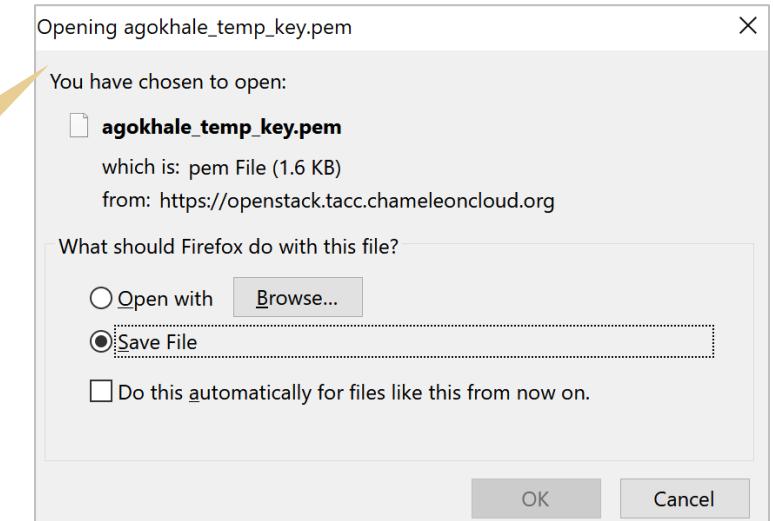
- You can create a new private-public key pair, or import if you have created one previously.
- Private key is stored in a *.pem file that gets downloaded (move it to your .ssh folder; on Windows I keep this under C:\Users\<mylogin>\.ssh; on Linux/Mac, put it in .ssh directory of home directory).

Setting Up Key Pairs (Creation) (cont.)



The screenshot shows the Chameleon cloud provider's web interface. The top navigation bar includes 'Project' (CH-819381), 'API Access', 'Compute' (selected), 'Overview', 'Instances', 'Images', 'Key Pairs' (selected), 'Server Groups', 'Volumes', 'Network', and 'Identity'. The 'Key Pairs' section displays a table with one item: 'gokhale_chameleondcloud'. A yellow callout bubble at the bottom left states: 'I created some dummy key for demo purposes'.

- Your generated key should then be saved in a folder, such as the .ssh folder.
- This is your private key (a *.pem file).
- **Never disclose this key.**
- Save it in a special folder.
 - For example, on Linux, usually in the .ssh folder of your home directory



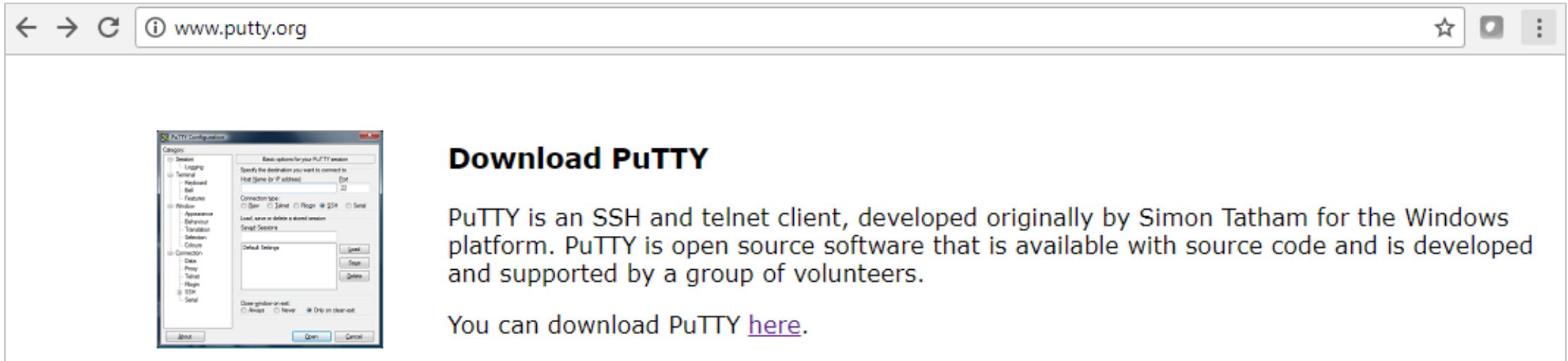
Setting Up Key Pairs

The End

Importing Key Pairs

For Windows Users Running PuTTY

- On Windows, we will use PuTTY to remotely connect to our cloud-based VM.
- You can download PuTTY [here](#).
- Follow the download link and install it via the installer.
- A bunch of executables will be installed and your PATH will be updated.
 - Putty.exe, pageant.exe, pscp.exe, puttygen.exe



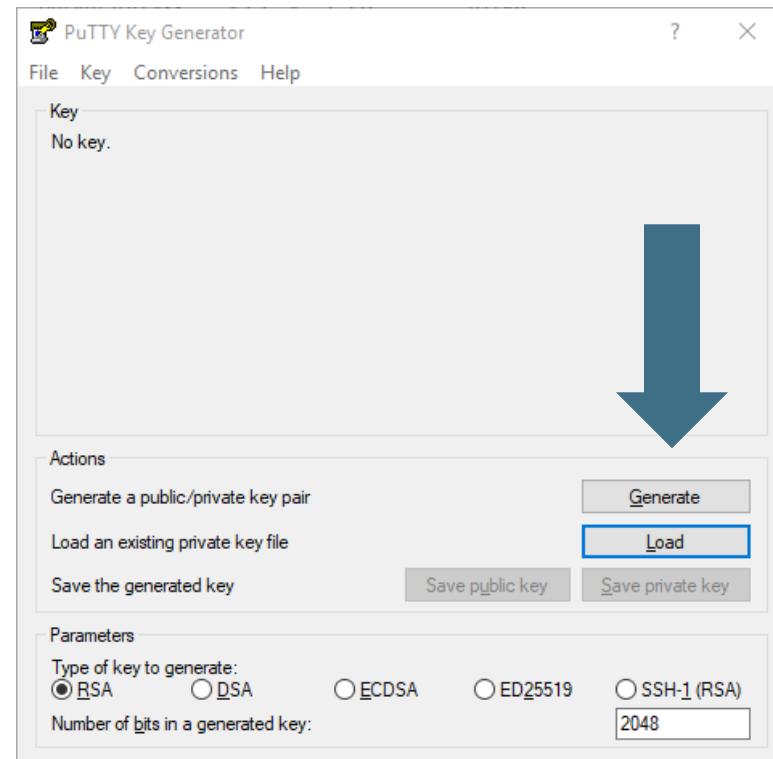
The screenshot shows a web browser window with the URL www.putty.org in the address bar. The main content area displays the PuTTY Configuration dialog box, which is a Windows application window titled "PuTTY Configuration". The dialog box has a tree view on the left under "Category" with items like Session, Logging, Terminal, Appearance, Connection, Date, Proxy, Telnet, SSH, and Serial. The "Session" node is expanded, showing fields for "Host (name or IP address)" (set to "10.0.2.2") and "Connection type" (set to "SSH"). Below these are buttons for "Open" and "Cancel". To the right of the dialog box, there is descriptive text about PuTTY and a download link.

Download PuTTY

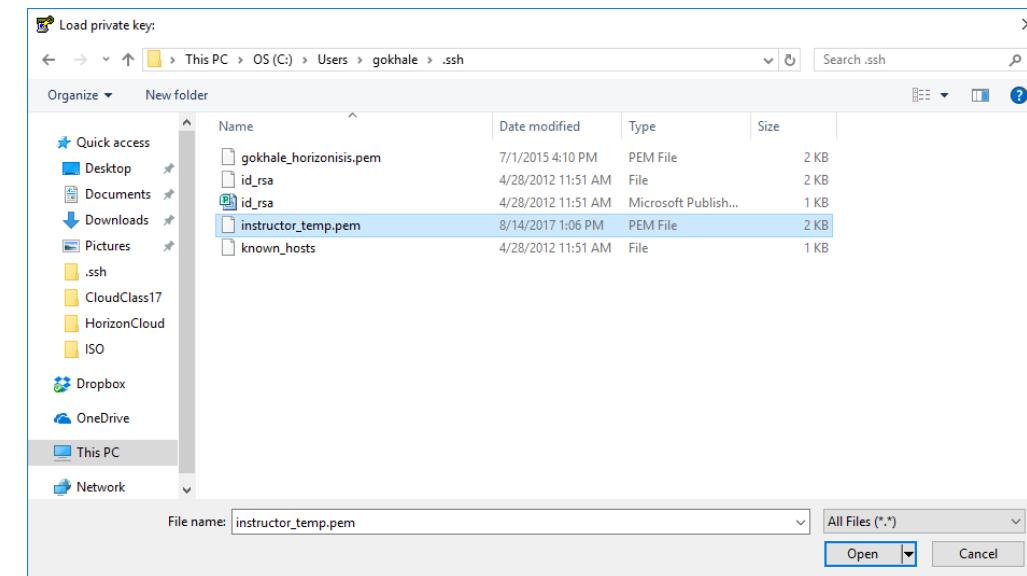
PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is available with source code and is developed and supported by a group of volunteers.

You can download PuTTY [here](#).

Convert .pem File to PuTTY Format, Part I

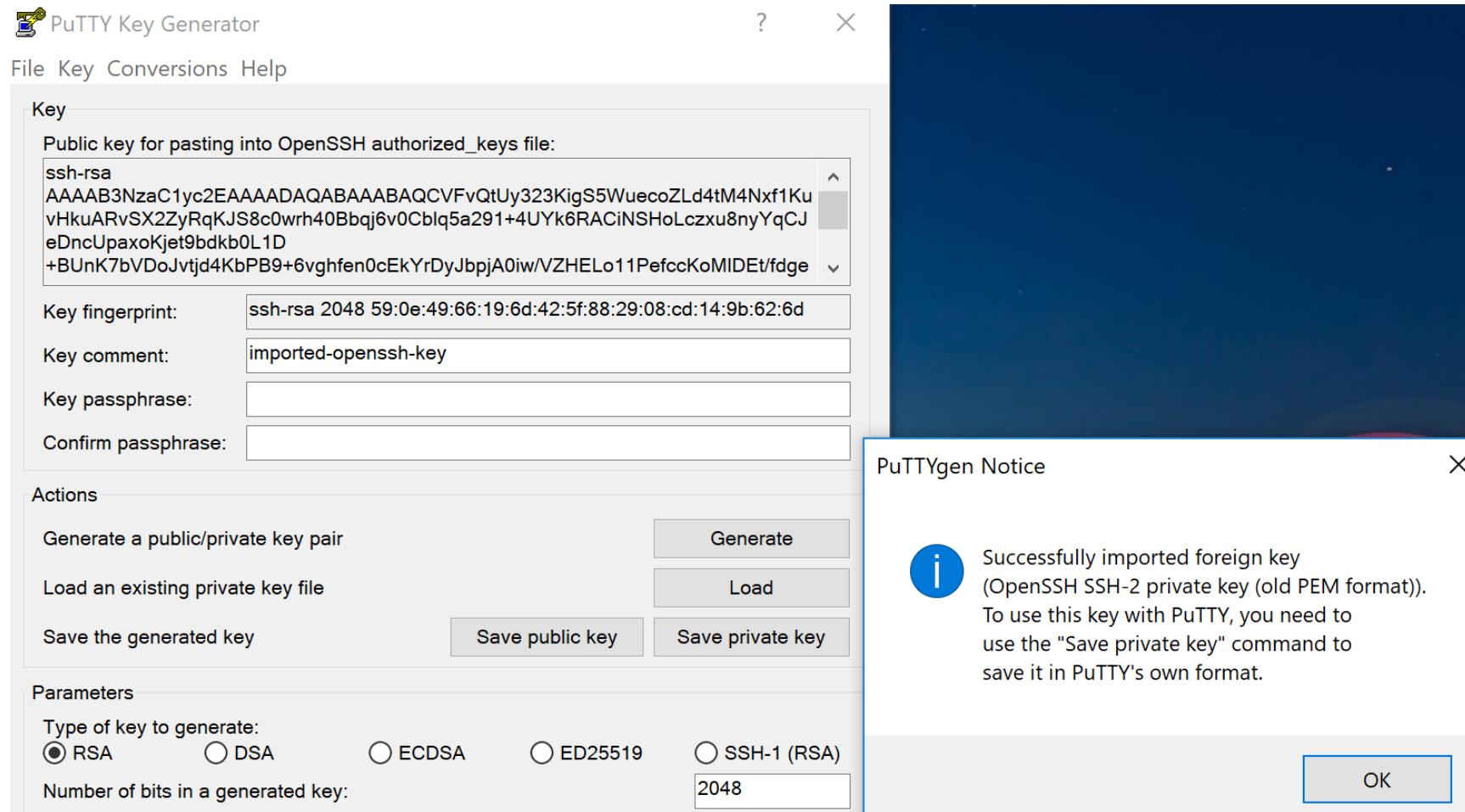


- We need the private key in a format that PuTTY can understand.
- Start the puttygen program that was just installed.
- Click load as shown on left.
- Browse to the directory where you downloaded the *.pem file when you created the key pair.



- Select the .pem file you just created, and click open

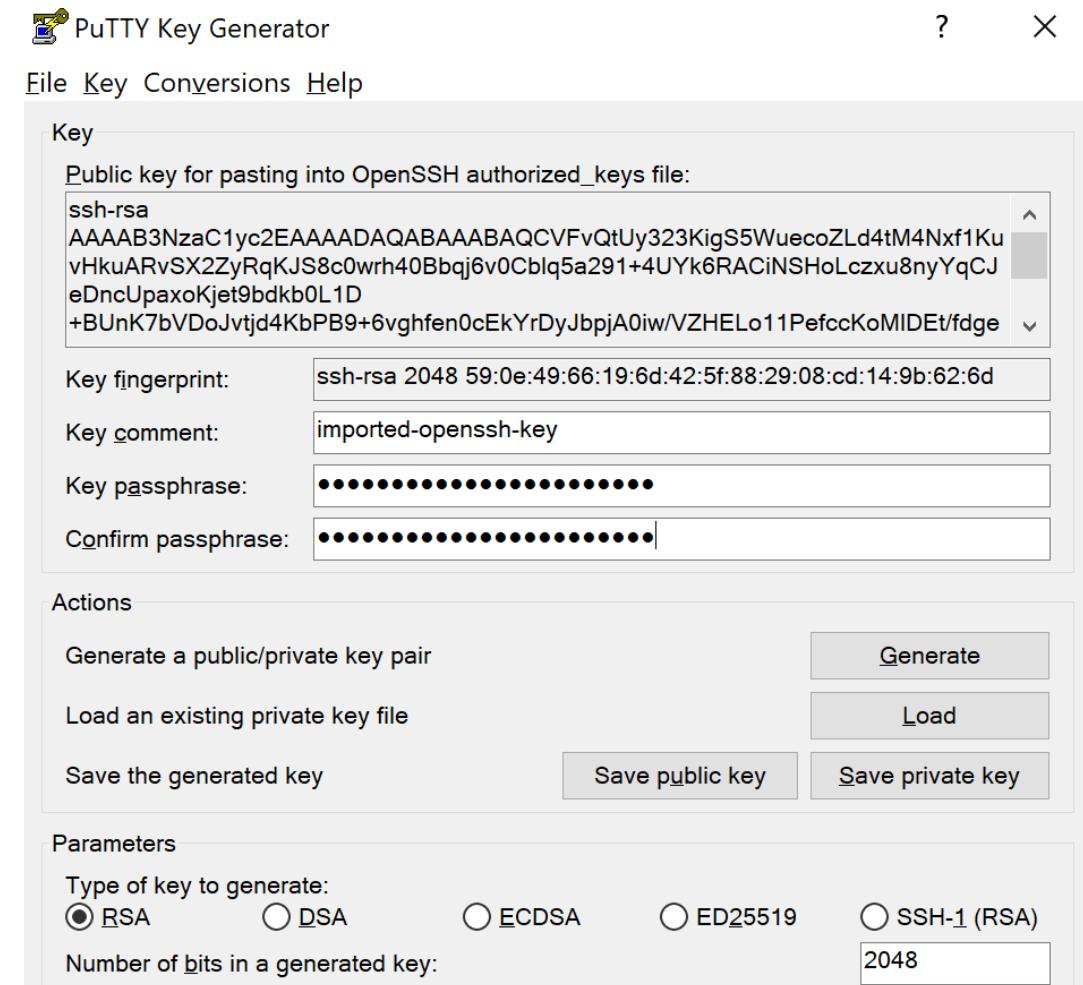
Convert .pem File to PuTTY Format, Part II



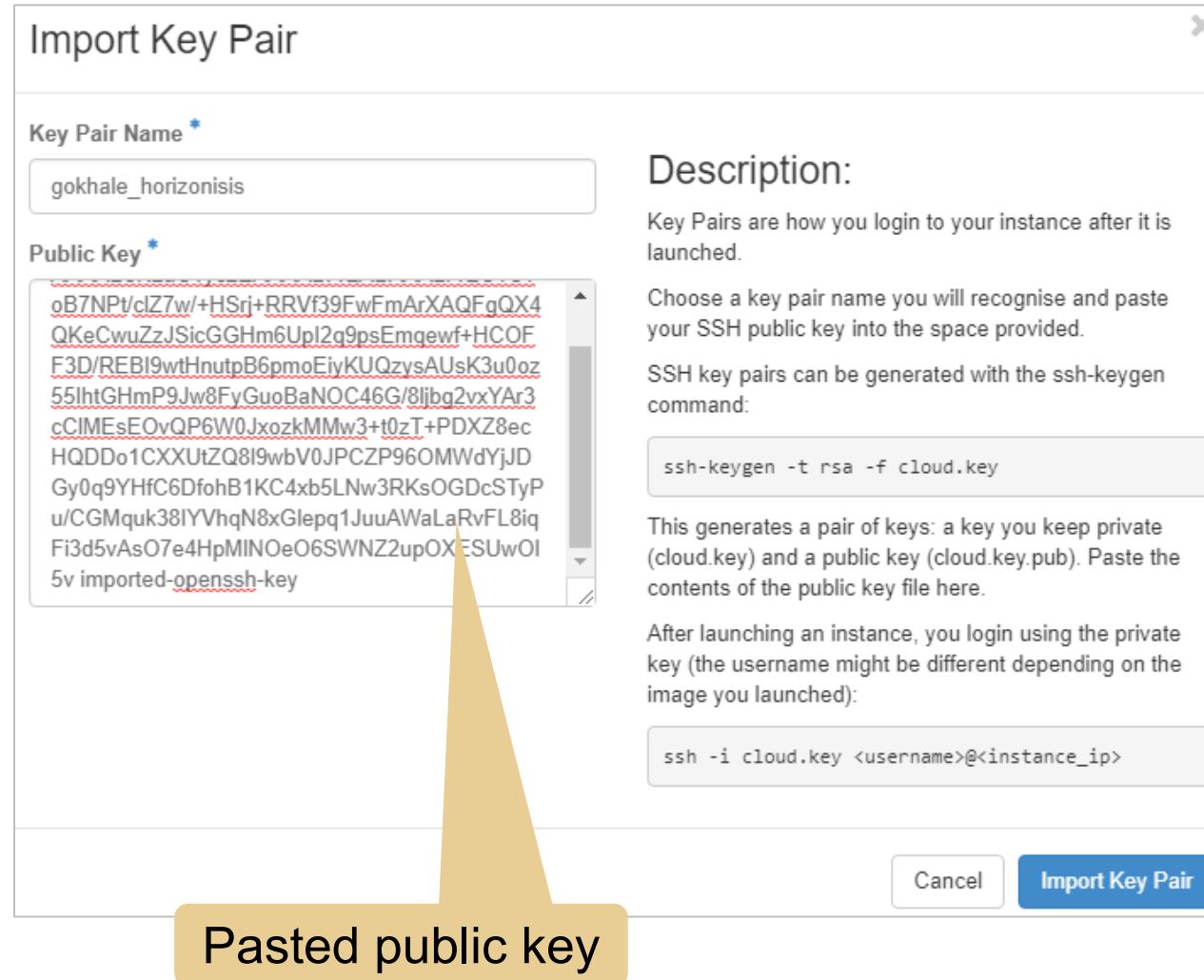
You should see output like this.

Convert .pem File to PuTTY Format, Part III

- Use some passphrase with your converted private key.
- Save your private key and public key.
- Private key is saved with a *.ppk extension.
- I suggest creating a .putty directory in your home directory and save the *.ppk file in that directory.



Setting Up Key Pairs (Import)



- If you already have an existing key pair, take the public key and paste it in the region shown.
- Assign a name.
- Click import.

Click import

Importing Key Pairs

The End

Managing a VM Instance

Managing an Instance, Part I

The screenshot shows a web browser window with the URL <https://kvm.tacc.chameleoncloud.org/project/instances/>. The page title is "Chameleon - CH-811681". The navigation menu on the left includes "Project", "API Access", "Compute" (which is expanded to show "Overview" and "Instances"), "Images", and "Key Pairs". The main content area is titled "Instances" and displays a table with 12 items. The table columns are: Instance ID (dropdown), Filter (button), Launch Instance (button), Delete Instances (button), and More Actions (dropdown). The "Instances" tab is highlighted with a blue background. A yellow callout bubble on the left points to the "Instances" tab with the text "1. Select instances tab". A yellow callout bubble on the right points to the "Launch Instance" button with the text "2. Click to launch instance".

- **Typical steps to be performed**
 1. Provide an instance name
 2. Select availability zone (just one for our cloud; AWS has multiple zones).
 3. Select how many such instances you want to execute.
 4. Select the source (image, snapshot, volume) to start instance.
 5. Select a flavor depending on your application requirements.
 6. Select network.
 7. Select security group.
 8. Associate key pair.
 9. Associate floating IP addresses.

Managing an Instance, Part II

Launch Instance

Details

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the count. Increase the Count to create multiple instances with the same settings.

Instance Name *

gokhale-demo

Description

used for demo purposes

Availability Zone

nova

Total Instances (60 Max)
22%

12 Current Usage
1 Added
47 Remaining

Count *

1

Cancel

Back

Next >

Launch Instance

1. Choose “details.”
2. Give a name to your VM.
3. Description is optional.
4. This is the only choice.
5. Set count to 1.
6. Click next

Managing an Instance, Part III

Launch Instance

Details

Source *

Flavor *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Select Boot Source

Image

Create New Volume

Yes No

Allocated

Name	Updated	Size	Type	Visibility
Select an item from Available items below				
▼ Available 133				
<input type="text"/> ubuntu18				
Name	Updated	Size	Type	Visibility
CC-Ubuntu18.04	12/30/19 5:24 PM	946.19 MB	qcow2	Public
CC-Ubuntu18.04-20190626	10/17/19 11:13 AM	4.03 GB	raw	Public
CC-Ubuntu18.04-20190627.1	10/17/19 11:13 AM	4.03 GB	raw	Public
CC-Ubuntu18.04-20190705	10/17/19 11:13 AM	4.05 GB	raw	Public
CC-Ubuntu18.04-20190708	10/17/19 11:13 AM	4.05 GB	raw	Public

1. Choose image and let New Volume be No

2. Search for Desired image (here ubuntu18)

3. I am selecting this image by clicking on this up arrow, which moves the image name up

(4) Scroll all the way down and click Next

Managing an Instance, Part IV

Launch Instance

Details

Source

Flavor *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Flavors manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
Select an item from Available items below						
▼ Available 5 Select one						
Q Click here for filters.	x					
Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
> m1.tiny	1	512 MB	1 GB	1 GB	0 GB	Yes
> m1.small	1	2 GB	20 GB	20 GB	0 GB	Yes
> m1.medium	2	4 GB	40 GB	40 GB	0 GB	Yes
> m1.large	4	8 GB	40 GB	40 GB	0 GB	Yes
> m1.xlarge	8	16 GB	40 GB	40 GB	0 GB	Yes

Cancel < Back Next > Launch Instance

(1) Select a flavor by clicking the up arrow.
I am selecting m1.small

(2) Click next

Managing an Instance, Part V

Launch Instance

Details Networks * Source Flavor Networks * Network Ports Security Groups Key Pair Configuration Server Groups Scheduler Hints Metadata

Allocated Available

Subnets Associated Shared Admin State Status

Select networks from those listed below.

Select an item from Available items below

Select at least one network

Click here for filters.

Network	Subnets Associated	Shared	Admin State	Status
CH-819381-net	CH-819381-subnet	No	Up	Active
sharednet1	sharednet1-subnet	Yes	Up	Active

(1) Select the subnet belonging to our project

(2) Click Next

< Back Next > Launch Instance

The screenshot shows the 'Launch Instance' wizard interface. The 'Networks*' tab is selected. In the 'Available' section, two networks are listed: 'CH-819381-net' and 'sharednet1'. The 'CH-819381-net' row has an upward arrow icon next to it, indicating it is selected. A callout bubble with the text '(1) Select the subnet belonging to our project' points to this row. A second callout bubble with the text '(2) Click Next' points to the 'Next >' button at the bottom right.

Managing an Instance, Part VI

Launch Instance X

Details
Source
Flavor
Networks
Network Ports
Security Groups
Key Pair
Configuration
Server Groups
Scheduler Hints
Metadata

Ports provide extra communication channels to your instances. You can select ports instead of networks or a mix of both.

Allocated

Name	IP	Admin State	Status
Select an item from Available items below			

Available 0

Name	IP	Admin State	Status
No available items			

Select ports from those listed above

? (1) Ignore this screen and click next

< Back Next > Launch Instance

Managing an Instance, Part VII

Launch Instance

Details Select the security groups to launch the instance in.

Source Allocated 1

Flavor Name Description

Networks default Default security group

Network Ports

Security Groups Available 6

Select one or more

Click here for filters.

Name	Description
Team6_Security	
ENABLE_FECBENCH	
Team3_Security	
All_Open	
Team7_Security	
ENABLE_HTTP_HTTPS	

Key Pair (1) This should automatically have been selected. If not, search for it and click up arrow

Configuration

Server Groups

Scheduler Hints

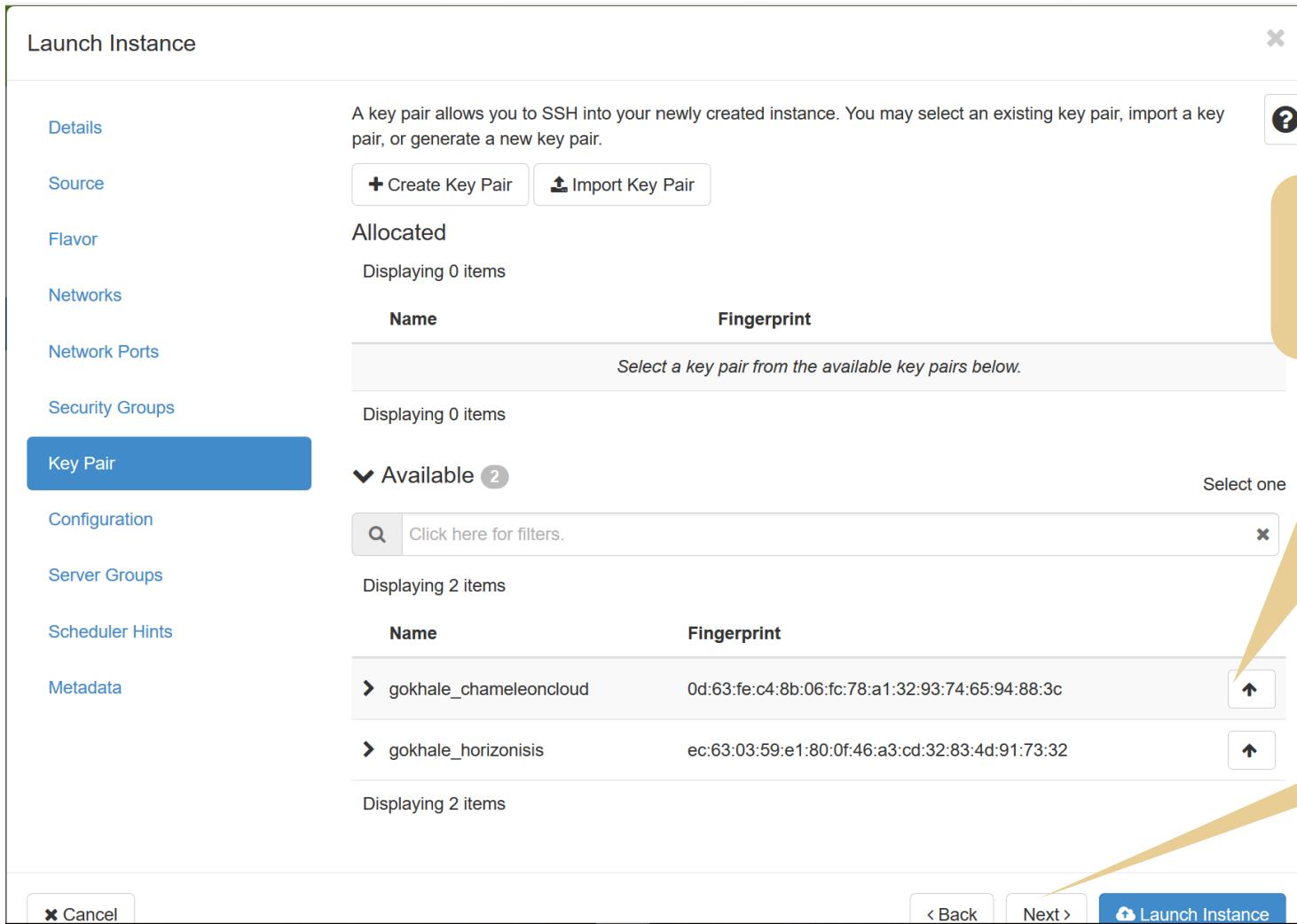
Metadata

(2) Click next

< Back Next > Launch Instance

All these are custom rules but for now we are going to not worry about these

Managing an Instance, Part VIII



(1) Select the keypair to be used and click the up arrow

(2) Click next

Managing an Instance, Part IX

The screenshot shows the 'Launch Instance' configuration interface. On the left, a sidebar lists several tabs: Details, Source, Flavor, Networks, Network Ports, Security Groups, Key Pair, Configuration (which is highlighted in blue), Server Groups, Scheduler Hints, and Metadata. The main area contains the following sections:

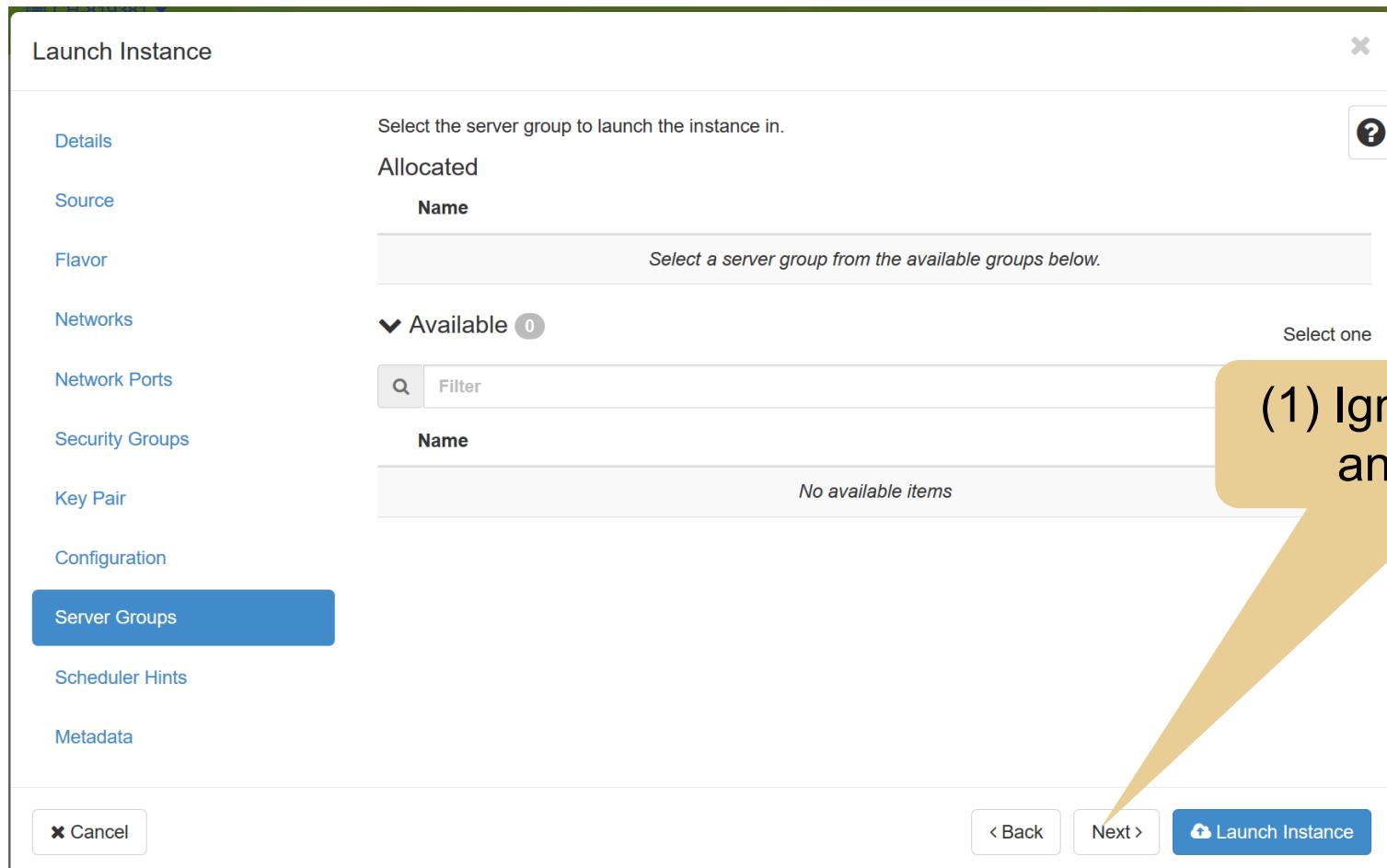
- Details:** A note states: "You can customize your instance after it has launched using the options available here. 'Customization Script' is analogous to 'User Data' in other systems." To the right is a help icon (a question mark inside a circle).
- Source:** A section titled "Load Customization Script from a file" includes a "Browse..." button which says "No file selected." Below this is a "Customization Script" editor with a note: "Content size: 0 bytes of 16.00 KB".
- Disk Partition:** Set to "Automatic".
- Configuration Drive:** An unchecked checkbox labeled "Configuration Drive".

At the bottom are three buttons: "< Back" (disabled), "Next >" (disabled), and "Launch Instance" (disabled).

A large orange callout bubble with a yellow arrow points from the text "(1) Ignore this screen and Click next" to the "Launch Instance" button.

(1) Ignore this screen and Click next

Managing an Instance, Part X



(1) Ignore this screen
and Click next

Managing an Instance, Part XI

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

This step allows you to add scheduler hints to your instance.

You can specify scheduler hints by moving items from the left column to the right column. In the left column there are scheduler hint definitions from the Glance Metadata Catalog. Use the "Custom" option to add scheduler hints with the key of your choice.

Available Scheduler Hints
Custom
CIM Processor Allocation Setting

Existing Scheduler Hints
No existing scheduler hints

(1) Accept the default, scroll down and Click next

Managing an Instance, Part XII

your choice.

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Available Metadata

Filter

Custom

Database Software

Runtime Environment

Web Servers

Existing Metadata

Filter

No existing metadata

Click each item to get its description here.

Cancel

< Back

Next >

Launch Instance

(1) Accept the default, and click Launch



Managing an Instance, Part XIII

The screenshot shows the Chameleon cloud management interface. The top navigation bar includes the Chameleon logo, a project dropdown (CH-819381), and a user dropdown (agokhale). The main menu has sections for Project, API Access, Compute (selected), and Overview. The Compute section is expanded to show Instances, Images, Key Pairs, Server Groups, Volumes, and Network. The Instances section is selected and displays a table of instances. The table columns are: Instance Name, Image Name, IP Address, Flavor, Key Pair, Status, Availability Zone, Task, Power State, Time since created, and Actions. One instance, "gokhale-dem0", is highlighted with a yellow background. Its details are: Image Name - CC-Ubuntu18.04, IP Address - 10.212.96.7, Flavor - m1.small, Key Pair - gokhale_chameleoncloud, Status - Build, Availability Zone - nova, Task - Spawning (highlighted with a blue bar), Power State - No State, and Time since created - 0 minutes. An action button "Associate Floating IP" is shown next to it. A yellow callout bubble points to the "Spawning" status in the Task column.

	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
	gokhale-dem0	CC-Ubuntu18.04	10.212.96.7	m1.small	gokhale_chameleoncloud	Build	nova	Spawning	No State	0 minutes	<button>Associate Floating IP</button>

Shows the status

Managing an Instance, Part XIV

The screenshot shows the Chameleon cloud management interface. The top navigation bar includes the Chameleon logo, a dropdown for 'Project' (set to 'CH-819381'), and a user account for 'agokhale'. The main menu on the left has sections for 'Project', 'API Access', 'Compute' (selected), 'Overview', 'Instances' (selected), 'Images', 'Key Pairs', 'Server Groups', 'Volumes' (with a right-pointing arrow), 'Network' (with a right-pointing arrow), and 'Identity' (with a right-pointing arrow). The 'Instances' page displays a table with one item:

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
<input type="checkbox"/>	gokhale-demo	CC-Ubuntu18.04	10.212.96.7	m1.small	gokhale_chameleoncloud	Active	nova	None	Running	2 minutes	Create Snapshot

Two callout boxes with yellow arrows point to specific elements: one points to the instance name 'gokhale-demo' with the text 'Click on the name to see details of the VM', and another points to the 'Power State' column showing 'Running' with the text 'Status should change to Running'.

Managing an Instance, Part XV

The screenshot shows the Chameleon cloud management interface. The top navigation bar includes the Chameleon logo, a dropdown menu for 'CH-819381', and links for 'Project', 'API Access', and 'Compute'. Under 'Compute', there are dropdowns for 'Project' and 'Compute', with 'Compute' being selected. Below this, the 'Instances' tab is highlighted. The main content area displays the details for a VM named 'gokhale-demo'. The VM's name is shown in the title bar and the main heading. The 'Overview' tab is selected, showing the following details:

Name	gokhale-demo
Description	for demo purposes
ID	d6fe2257-2727-4259-8cc3-aa0fd60d358f
Status	Active
Locked	False
Availability Zone	nova
Created	Jan. 8, 2020, 11:20 p.m.
Time Since Created	5 minutes

Below the overview, the 'Specs' section lists the VM's specifications:

Flavor Name	m1.small
Flavor ID	2
RAM	2GB
VCPUs	1 VCPU
Disk	20GB

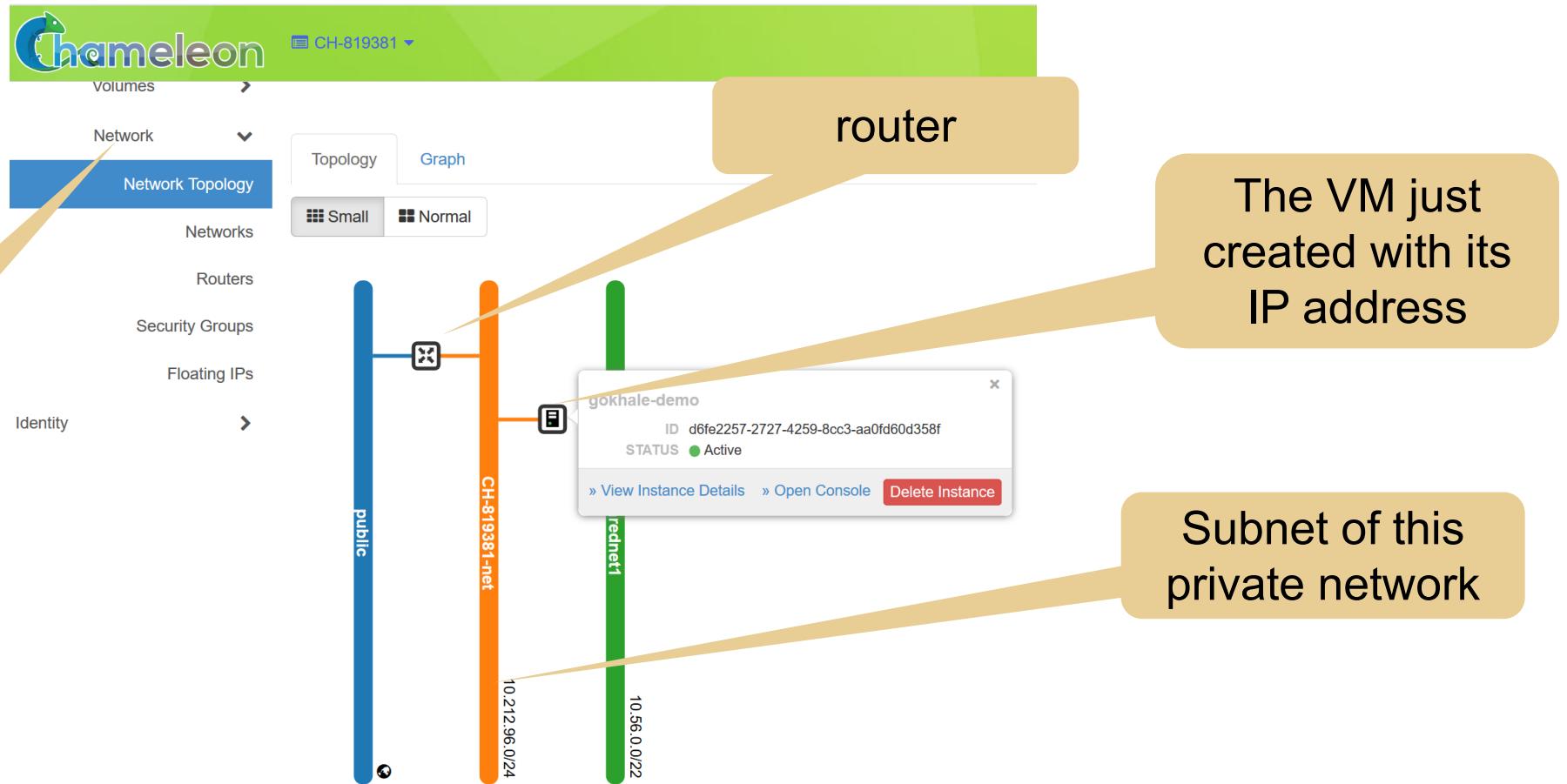
At the bottom, the IP address 'Ch-819381-Net' is listed as 10.212.96.7, with a note indicating it is a private IP.

Name and specification
of the VM

Private IP address

- Can I reach this VM remotely?
- No, but why?

Managing an Instance, Part XVI



- Our VM is in a private network with a certain subnet address
- We need some way to reach it via the router using network address translation (provided by floating IP addresses)
 - See network refresher slides towards the end

Managing an Instance, Part XVII

(1) Go back to the Compute tab and see instances

(2) Using the pulldown menu, select “Associate Floating IP”

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
gokhale-demo	CC-Ubuntu18.04	10.212.96.7	m1.small	gokhale_chameleoncloud	Active	nova	None	Running	10 minutes	<button>Create Snapshot</button>

- Associate a floating IP address, which is a public IP address reachable from outside

Managing an Instance, Part XVIII

Manage Floating IP Associations

IP Address *

Select an IP address

Select the IP address you wish to associate with the selected instance or port.

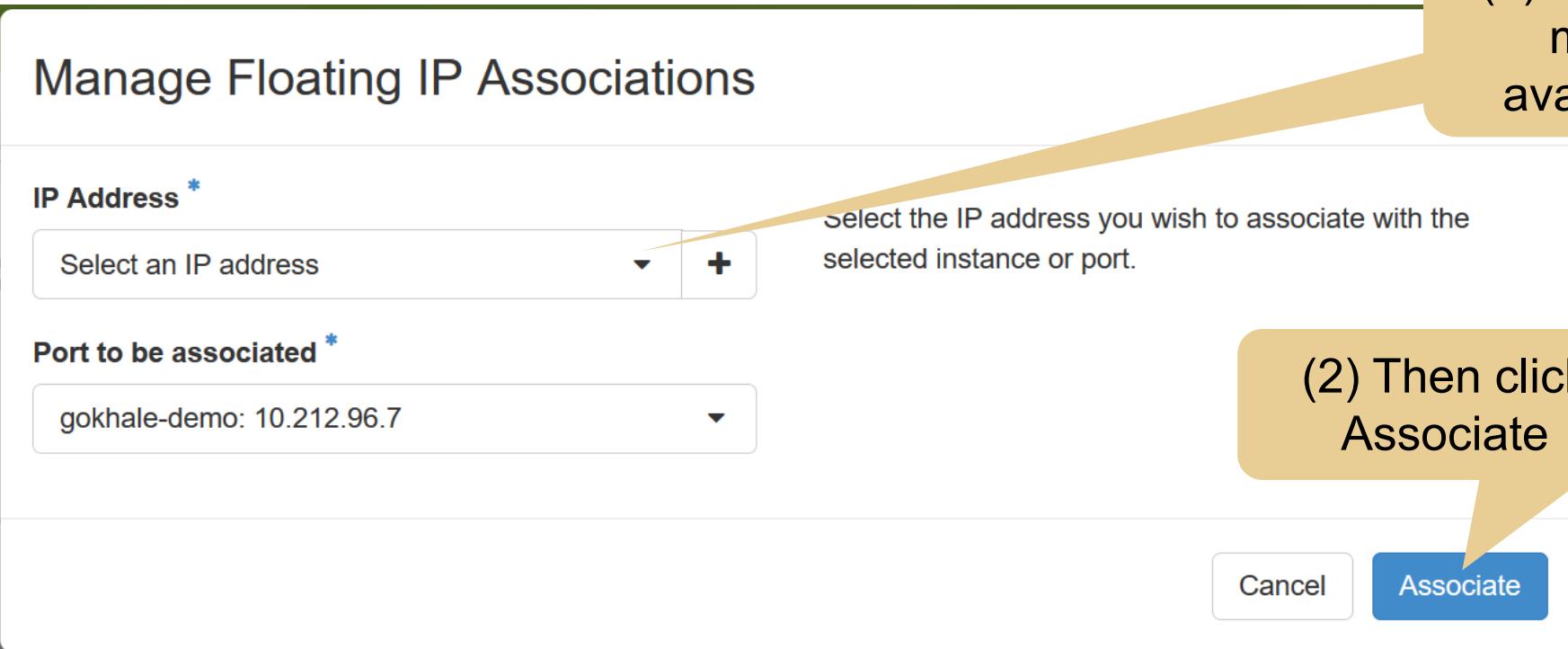
Port to be associated *

gokhale-demo: 10.212.96.7

(1) Using the pulldown menu, select an available IP address

(2) Then click Associate

Cancel Associate



- Shows the actual process of associating a floating IP address

Managing an Instance, Part XIX

CH-819381 ▾ agokhale ▾

Project API Access Compute Overview Instances

Instances Images Key Pairs Server Groups Volumes Network

Displaying 1 item

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
gokhale-dem	CC-Ubuntu1 8.04	10.212.96.7 Floating IPs: 129.114.25.5	m1.small	gokhale_chameleoncloud	Active	nova	None	Running	13 minutes	Create Snapshot ▾

Notice the floating IP

- Now your VM is reachable from outside because it now has a public IP address
 - Note that this is a temporary IP address available to us until our instance is still running unless we disassociate the IP manually or terminate the VM

Managing an Instance, Part XX

The screenshot shows the Chameleon cloud management interface. At the top, there's a navigation bar with the Chameleon logo, a dropdown menu 'CH-819381 ▾', and a breadcrumb path 'Project / Compute / Instances / gokhale-demo'. Below the navigation is a sidebar with 'API Access' and a 'Compute' dropdown set to 'Compute'. The main content area is titled 'gokhale-demo'. On the left, a sidebar has 'Overview' and 'Instances' selected (highlighted in blue). Other options include 'Images', 'Key Pairs', 'Server Groups', 'Volumes', 'Network', and 'Identity'. The main content area has tabs for 'Overview', 'Interfaces', 'Log', 'Console', and 'Action Log', with 'Overview' selected. The 'Overview' section displays instance details:

Name	gokhale-demo
Description	for demo purposes
ID	d5fe2257-2727-4259-8cc3-aa0fd60d358f
Status	Active
Locked	False
Availability Zone	nova
Created	Jan. 8, 2020, 11:20 p.m.
Time Since Created	14 minutes

Below this is a 'Specs' section:

Flavor Name	m1.small
Flavor ID	2
RAM	2GB
VCPUs	1 VCPU
Disk	20GB

Under 'IP Addresses', it shows 'Ch-819381-Net' with IP addresses '10.212.96.7, 129.114.25.5'. Under 'Security Groups', it shows a 'default' group with the rule 'ALLOW IPv4 22/tcp from 0.0.0.0/0'.

A yellow callout bubble points to the floating IP address '129.114.25.5' with the text 'Notice the floating IP'.

- Another view of the instance details with floating IP

Managing an Instance, Part XXI

The screenshot shows the Chameleon web interface with the following details:

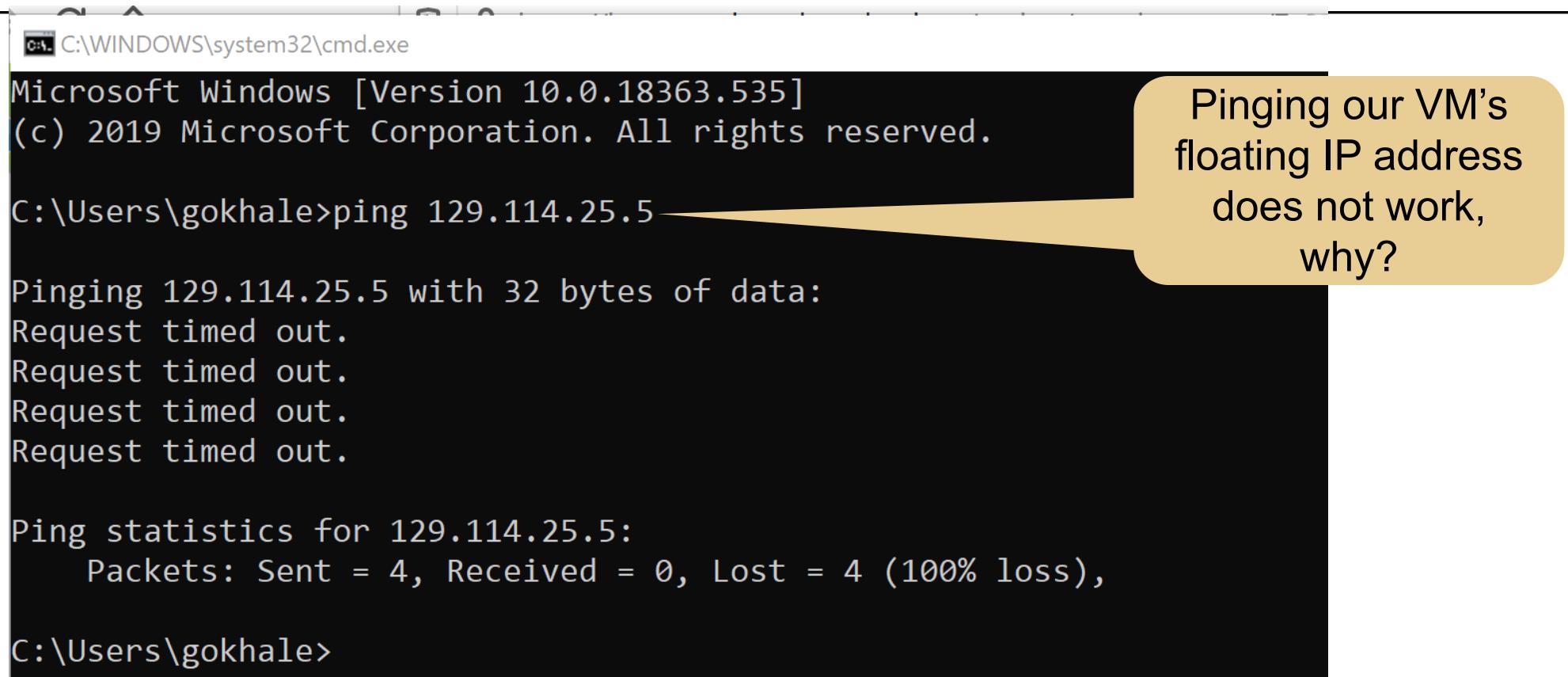
- Header:** CH-819381, agokhale
- Sidebar:** Project, API Access, Compute, Volumes, Network (Network Topology, Networks, Routers, Security Groups, Floating IPs - highlighted in blue)
- Breadcrumbs:** Project / Network / Floating IPs
- Search/Filter:** Floating IP Address = ▾, Filter, Allocate IP To Project, Release Floating IPs
- Data Table:** Displaying 40 items. Columns: IP Address, Description, Mapped Fixed IP Address ▾, Pool, Status, Actions. One row is highlighted: IP Address 129.114.25.5, Description gokhale-demo, Mapped Fixed IP Address 10.212.96.7, Pool public, Status Active, Actions Disassociate ▾.

Look under Network-Floating IP tab for the mapping

Notice the mapping

- View of the mapping maintained by the system

Managing an Instance, Part XXII



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.18363.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\gokhale>ping 129.114.25.5
Pinging 129.114.25.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 129.114.25.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\gokhale>
```

Pinging our VM's floating IP address does not work, why?

- Let us try to reach our VM by pinging it
- Open a cmd shell (on Windows) or bash shell on Mac and issue a ping to the floating IP address of your VM

Managing an Instance, Part XXIII

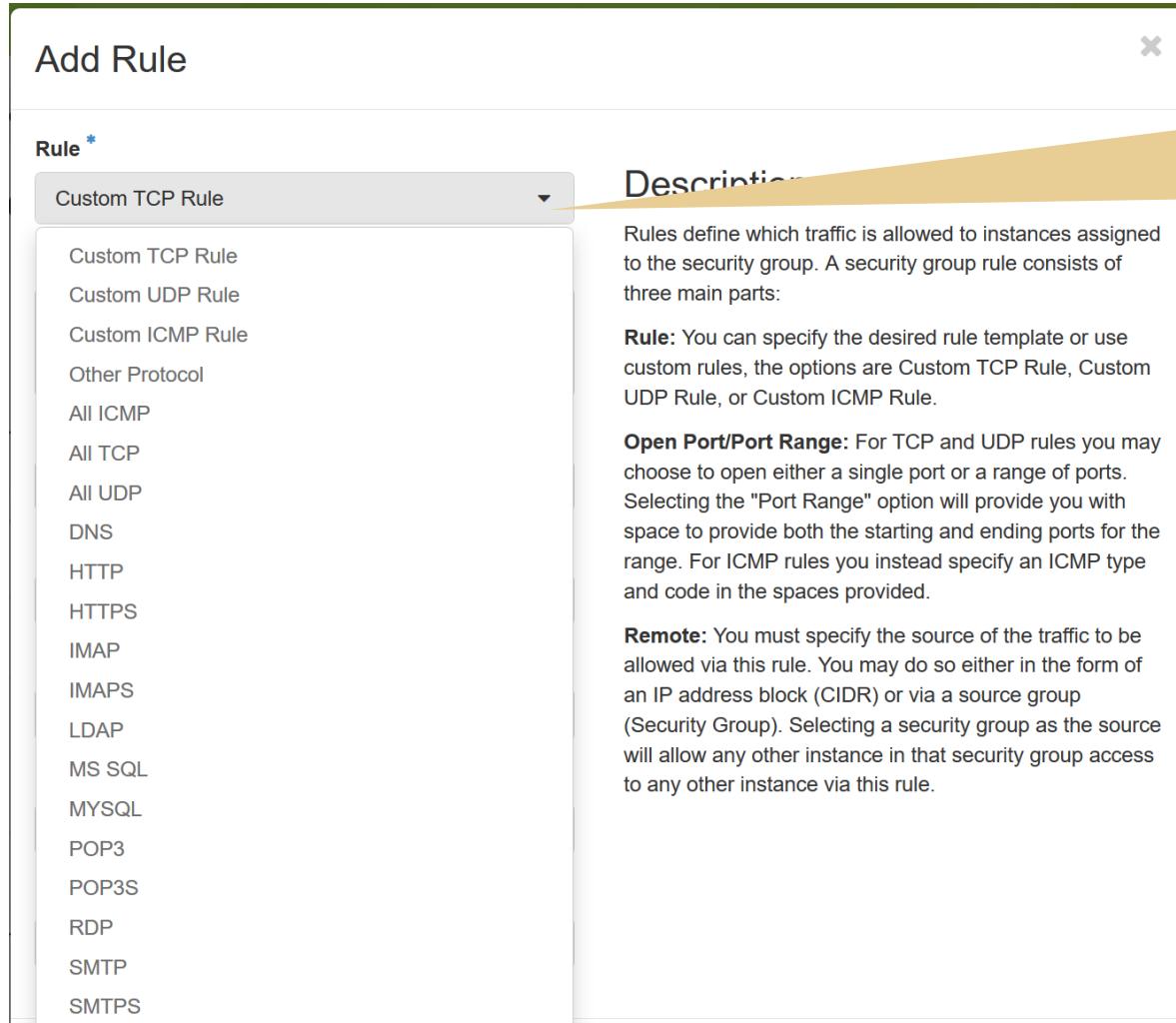
The screenshot shows the Chameleon cloud management interface. The left sidebar has a navigation menu with items like Project, API Access, Compute, Volumes, Network, Network Topology, Networks, Routers, Security Groups (which is selected and highlighted in blue), Floating IPs, and Identity. The main content area shows the 'Manage Security Group Rules' page for the 'default' security group. The URL in the browser bar is 'Project / Network / Security Groups / Manage Security Group Rule...'. The page displays a table with 5 items, each representing a security rule. The columns are: Direction, Ether Type, IP Protocol, Port Range, Remote IP Prefix, Remote Security Group, Description, and Actions. The rules listed are:

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

A yellow speech bubble with a black outline points to the '+ Add Rule' button at the top right of the table, containing the text 'Click to add a new rule to allow ping'.

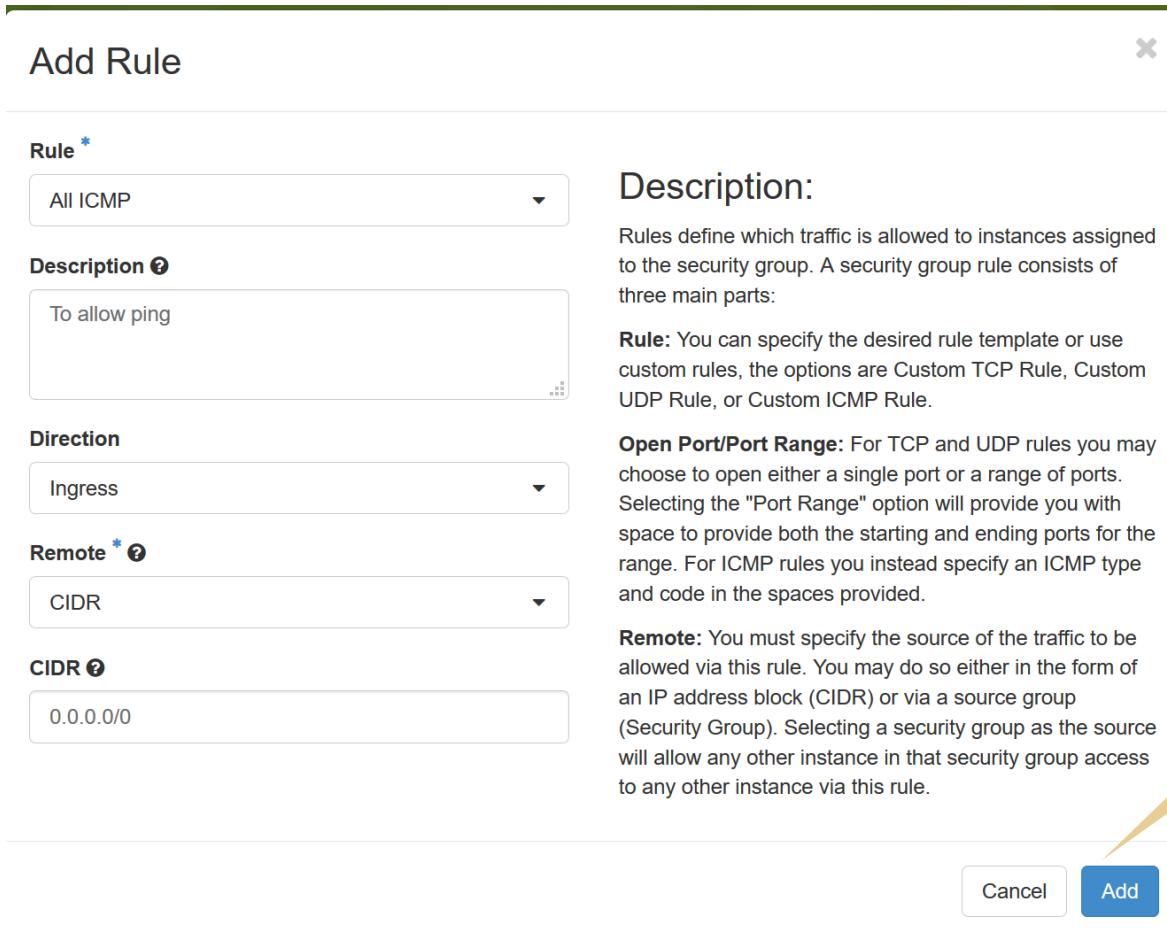
- The “default” security group did not allow incoming ping requests (which is supported by ICMP protocol)

Managing an Instance, Part XXIV



Use the pulldown menu and select “All ICMP”. We could have used “Custom ICMP” also

Managing an Instance, Part XXV



The pop up window should look like this. We add some description to the rule. Then click on the Add button

Managing an Instance, Part XXVI

The screenshot shows the Chameleon cloud management interface. The top navigation bar includes the Chameleon logo, project ID CH-819381, and user agokhale. The left sidebar has sections for Project, API Access, Compute, Volumes, Network (selected), Network Topology, Networks, Routers, Security Groups (selected), Floating IPs, and Identity. The main content area shows the 'Manage Security Group Rules' page for the 'default' security group. It displays six rules:

Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Action
Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
Egress	IPv6	Any	Any	::/0	-	-	Delete Rule
Ingress	IPv4	Any	Any	-	default	-	Delete Rule
Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	To allow ping	Delete Rule
Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-	-	Delete Rule
Ingress	IPv6	Any	Any	-	default	-	Delete Rule

A large orange callout bubble with the text 'Newly added rule' points to the last row of the table, which represents the most recently added rule.

Managing an Instance, Part XXVII

```
C:\Users\gokhale>  
C:\Users\gokhale>ping 129.114.25.5  
  
Pinging 129.114.25.5 with 32 bytes of data:  
Reply from 129.114.25.5: bytes=32 time=36ms TTL=49  
Reply from 129.114.25.5: bytes=32 time=36ms TTL=49  
Reply from 129.114.25.5: bytes=32 time=36ms TTL=49  
  
Ping statistics for 129.114.25.5:  
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 36ms, Maximum = 36ms, Average = 36ms  
Control-C
```

Pinging our VM's floating IP address now works

- It now works because of the ICMP rule we added

Managing a VM Instance

The End

Security and Access Control

Security and Access Control, Part I

The screenshot shows the Chameleon cloud management interface. The top navigation bar includes the Chameleon logo, a project dropdown (CH-819381), and a user dropdown (agokhale). The left sidebar has a 'Project' section with a dropdown arrow, followed by 'API Access', 'Compute' (with a dropdown arrow), 'Volumes' (with a dropdown arrow), 'Network' (with a dropdown arrow), 'Network Topology', 'Networks', 'Routers', 'Security Groups' (which is highlighted in blue), 'Floating IPs', and 'Identity'. The main content area is titled 'Security Groups' and displays a table of existing security groups. The table has columns for Name, Security Group ID, Description, and Actions. There are four items listed:

Name	Security Group ID	Description	Actions
All_Open	ded43f3c-09a8-42b9-a3a9-08970bdc99eb		Manage Rules ▾
ENABLE_FECBENCH	4e07c105-745e-4e70-a97f-0a3c451961be		Manage Rules ▾
ENABLE_HTTP_HTTPS	e6e44931-b44f-4211-8d7d-5c7ca25b5a6a		Manage Rules ▾
default	7e09e9fd-4971-49bb-bd55-9aa2fa149b16	Default security group	Manage Rules

Below the table, it says 'Displaying 4 items'.

- Go to the Network -> Security Groups tab which shows existing groups
- Recall that our VM was allocated to the “default” security group
- Click on the “Manage Rules” tab

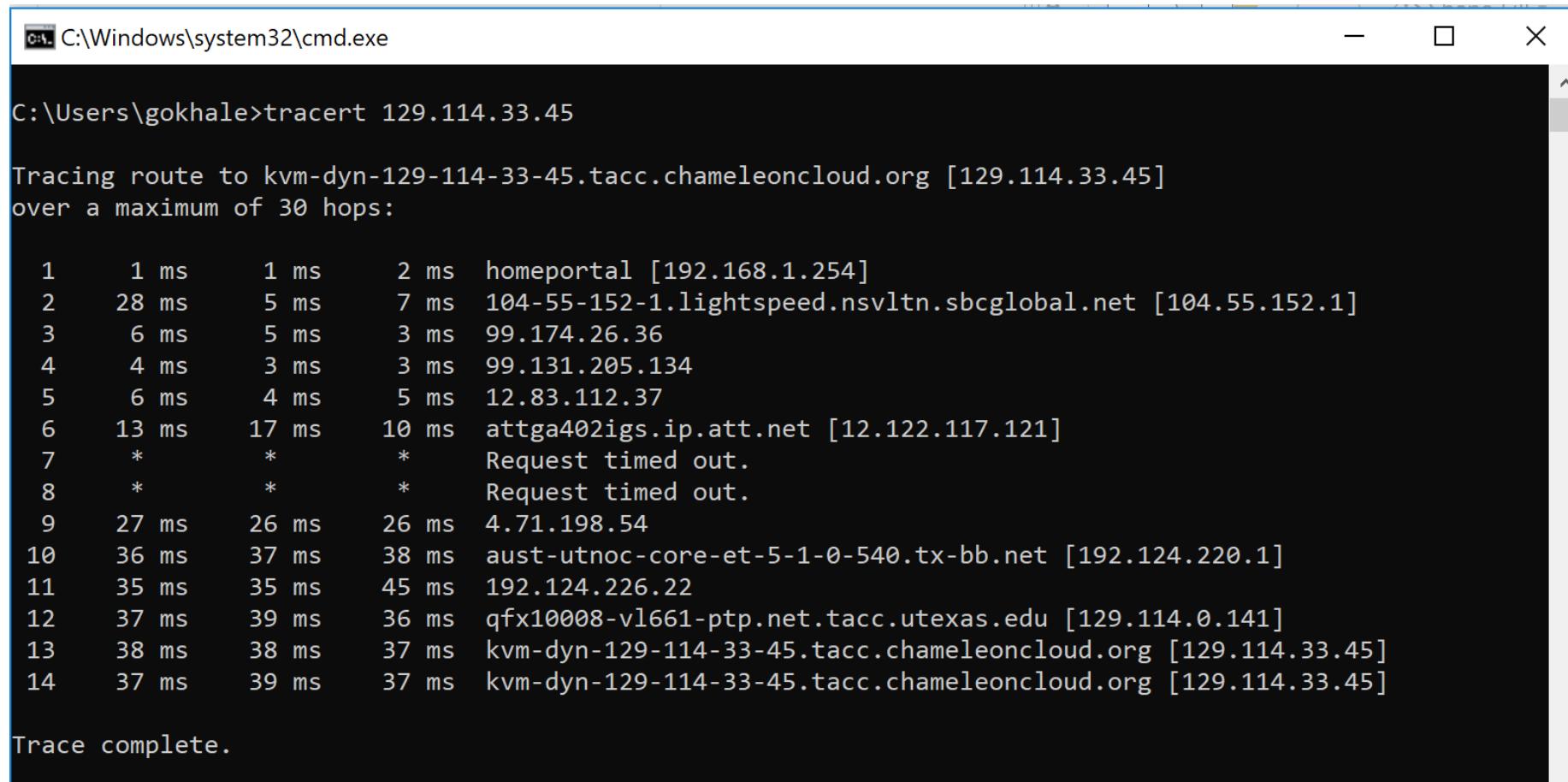
Security and Access Control, Part II

The screenshot shows the Chameleon cloud management interface. The left sidebar has sections for Project, API Access, Compute, Volumes, Network (Network Topology, Networks, Routers), Security Groups (selected), Floating IPs, and Identity. The main area is titled "Manage Security Group Rules: default (7e09e9fd-4971-49bb-bd55-9aa2fa149b16)". It displays a table of security rules:

Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
Egress	IPv6	Any	Any	::/0	-	-	Delete Rule
Ingress	IPv4	Any	Any	-	default	-	Delete Rule
Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	To allow ping	Delete Rule
Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-	-	Delete Rule
Ingress	IPv6	Any	Any	-	default	-	Delete Rule

- Take a look at the allowed traffic in and out of the private network of the cloud (managed by router)
- Only egress (outgoing) traffic is allowed for IPv4 and IPv6
- Notice that we had added ICMP previously and so ping works
 - Internet Control Message Protocol (ICMP) is a protocol at the same layer as IP protocol and is used for applications like ping, traceroute, etc

Security and Access Control, Part III



C:\Windows\system32\cmd.exe

```
C:\Users\gokhale>tracert 129.114.33.45

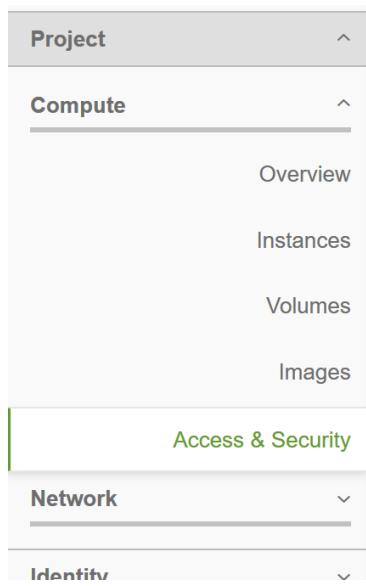
Tracing route to kvm-dyn-129-114-33-45.tacc.chameleoncloud.org [129.114.33.45]
over a maximum of 30 hops:

 1   1 ms    1 ms    2 ms  homeportal [192.168.1.254]
 2   28 ms   5 ms    7 ms  104-55-152-1.lightspeed.nsvltn.sbcglobal.net [104.55.152.1]
 3   6 ms    5 ms    3 ms  99.174.26.36
 4   4 ms    3 ms    3 ms  99.131.205.134
 5   6 ms    4 ms    5 ms  12.83.112.37
 6   13 ms   17 ms   10 ms  attga402igs.ip.att.net [12.122.117.121]
 7   *        *        *      Request timed out.
 8   *        *        *      Request timed out.
 9   27 ms   26 ms   26 ms  4.71.198.54
10   36 ms   37 ms   38 ms  aust-utnoc-core-et-5-1-0-540.tx-bb.net [192.124.220.1]
11   35 ms   35 ms   45 ms  192.124.226.22
12   37 ms   39 ms   36 ms  qfx10008-vl661-ptp.net.tacc.utexas.edu [129.114.0.141]
13   38 ms   38 ms   37 ms  kvm-dyn-129-114-33-45.tacc.chameleoncloud.org [129.114.33.45]
14   37 ms   39 ms   37 ms  kvm-dyn-129-114-33-45.tacc.chameleoncloud.org [129.114.33.45]

Trace complete.
```

- Trace route to the IP address shows a path that was found

Security and Access Control, Part IV



Manage Security Group Rules: default (16407bob-6713-4c85-aa3c-c689fe51da5c)

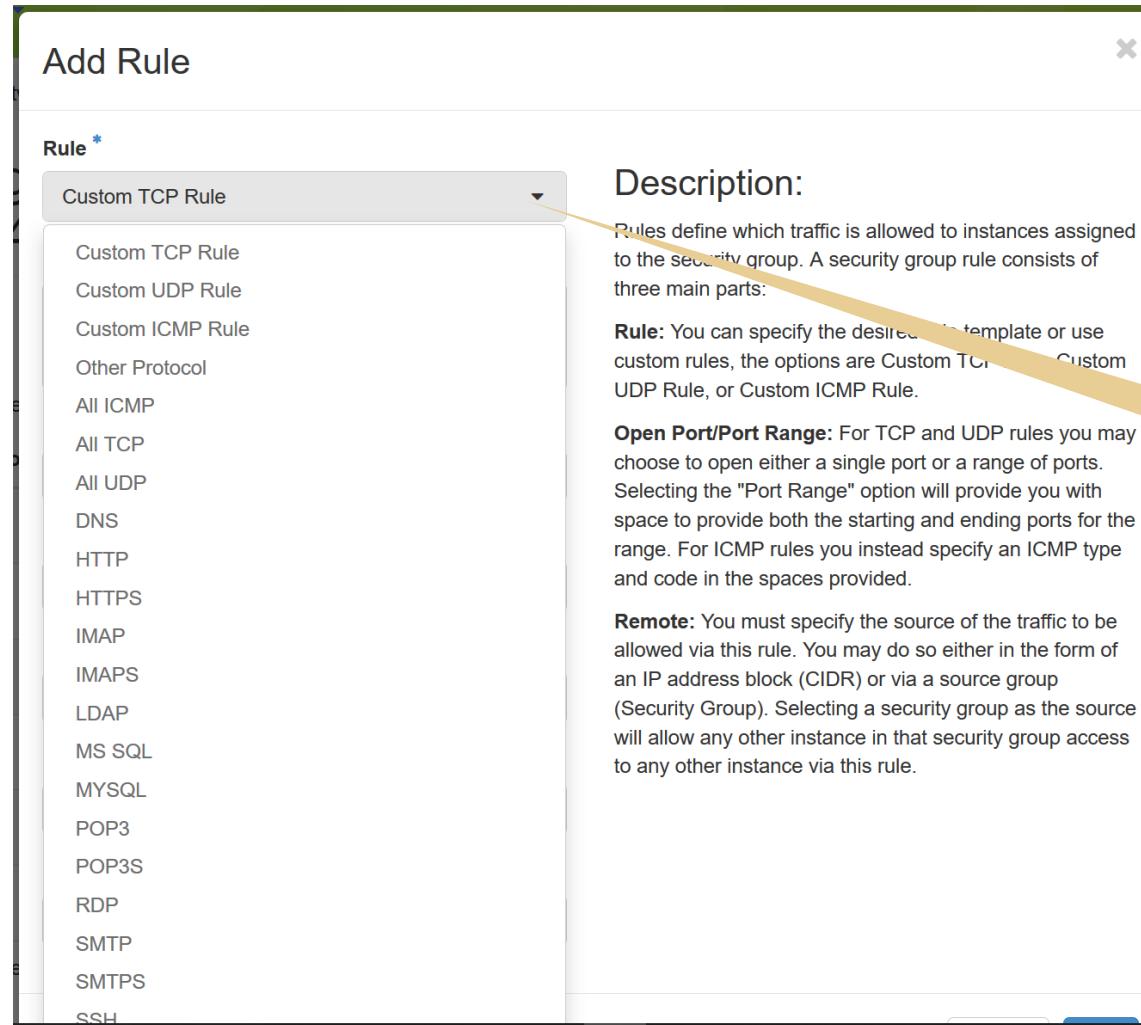
<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
<input type="checkbox"/>	Egress	IPv6	Any	Any	::/0	-	<button>Delete Rule</button>
<input type="checkbox"/>	Egress	IPv4	Any	Any	0.0.0.0/0	-	<button>Delete Rule</button>
<input type="checkbox"/>	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	<button>Delete Rule</button>

Displaying 3 items

- If you want to allow additional traffic, click Add Rule
- Usually we let default remain the minimal
- We then add special rules in their own security groups
- We then let a VM inherit multiple rules
- This way we do not clutter a single group with large number of rules

New rules can
be added this
way

Security and Access Control, Part V



- Select the whatever custom rule you need and click Add

Use this
pulldown menu

Security and Access Control, Part VI

Add Rule

Rule *

Description

Remote *

CIDR

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.

Cancel Add

- Say I want to allow HTTPS traffic

Click add.

Security and Access Control, Part VII

The screenshot shows the Chameleon cloud provider's web interface. The top navigation bar includes the Chameleon logo, a dropdown for 'Project' (set to 'CH-819381'), and a user profile for 'agokhale'. The main menu on the left has sections for Project, API Access, Compute, Volumes, Network (with sub-options like Network Topology, Networks, and Routers), Security Groups (which is currently selected and highlighted in blue), and Floating IPs. The Network section also shows 'Displaying 2 items'. The central content area is titled 'Manage Security Group Rules: ENABLE_HTTPS (e6e44931-b44f-4211-8d7d-5c7ca25b5a6a)'. It contains two table rows representing security rules:

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
<input type="checkbox"/>	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0	-	-	<button>Delete Rule</button>
<input type="checkbox"/>	Ingress	IPv4	TCP	443 (HTTPS)	0.0.0.0/0	-	-	<button>Delete Rule</button>

- Notice how we allow incoming HTTP and HTTPS traffic in this special security group
- VMs can inherit multiple groups

Security and Access Control

The End

Combining Security Groups

Associating Multiple Security Groups

- The “default” security group rules may provide only the bare minimum firewall rules.
 - There is no reason to keep adding more rules to the default because any VM using the default will have all those firewall rules enabled, and hence may be vulnerable to security attacks
- A better approach is to create separate security groups for specific purposes.
- Your VM can then be made to use a combination of groups as needed by simply combining the groups.
 - This can be done at the time of VM creation, or
 - Updated later on when it is desired to add a new set of rules

Defining Custom Security Groups

The screenshot shows the Chameleon web interface with the following details:

- Header:** Chameleon logo, Project dropdown (CH-819381), User dropdown (agokhale).
- Breadcrumbs:** Project / Network / Security Groups.
- Left Sidebar:** API Access, Compute, Volumes, Network (Network Topology, Networks, Routers, Security Groups, Floating IPs, Identity).
- Title:** Security Groups.
- Search & Buttons:** Filter, Create Security Group, Delete Security Groups.
- Data Table:** Displays 4 items.

Name	Security Group ID	Description	Actions
All_Open	ded43f3c-09a8-42b9-a3a9-08970bdc99eb		Manage Rules
ENABLE_FECBENCH	4e07c105-745e-4e70-a97f-0a3c451961be		Manage Rules
ENABLE_HTTP_HTTPS	e6e44931-b44f-4211-8d7d-5c7ca25b5a6a		Manage Rules
default	7e09e9fd-4971-49bb-bd55-9aa2fa149b16	Default security group	Manage Rules
- Bottom:** Displaying 4 items.

Adding Custom Security Groups

Select the instance which you want to modify

Use this pulldown menu and select "Edit Security Groups"

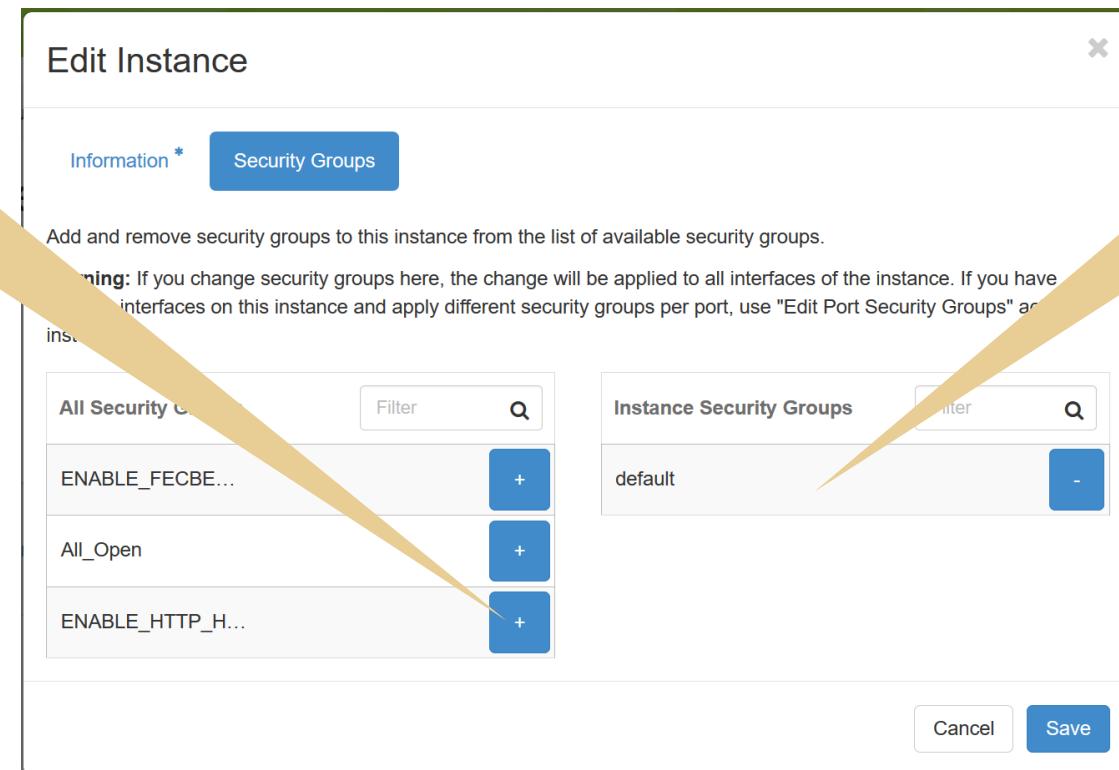
The screenshot shows the Chameleon cloud interface. On the left, a sidebar menu includes Compute (Overview, Instances, Images, Key Pairs, Server Groups, Volumes, Network, Identity), API Access, and a dropdown for CH-819381. The Instances tab is selected. The main area displays a table titled 'Instances' with one item: 'gokhale-dem0'. The table columns are: Instance Name, Image Name, IP Address, Flavor, Key Pair, Status, Availability Zone, Task, Power State, Time since created, and Actions. The Actions column for 'gokhale-dem0' contains a dropdown menu with options: Create Snapshot, Disassociate Floating IP, Attach Interface, Detach Interface, Edit Instance, Attach Volume, Detach Volume, Update Metadata, Edit Security Groups (which is highlighted in red), Edit Port Security Groups, Console, View Log, and Pause Instance.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
gokhale-dem0	CC-Ubuntu1 8.04	10.212.96.7 129.114.25.5	Floating IPs: m1.small	gokhale_chameleoncloud	Active	nova	None	Running	6 days, 1 hour	<ul style="list-style-type: none">Create SnapshotDisassociate Floating IPAttach InterfaceDetach InterfaceEdit InstanceAttach VolumeDetach VolumeUpdate MetadataEdit Security GroupsEdit Port Security GroupsConsoleView LogPause Instance

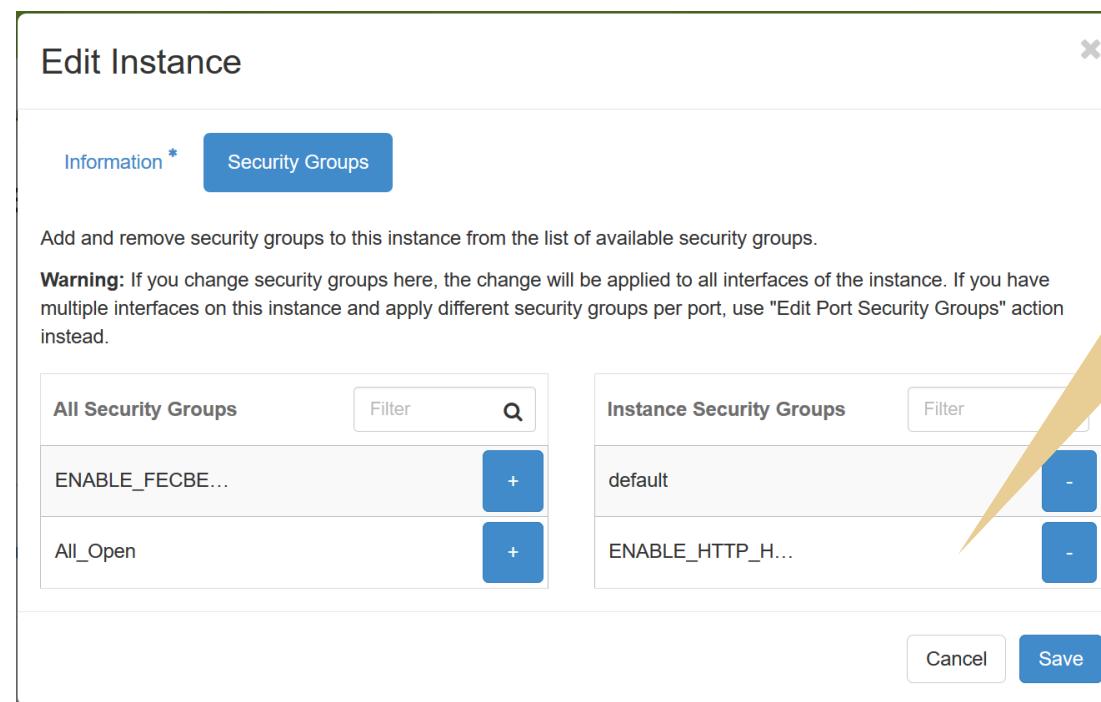
Adding Custom Security Groups

Click on the + to add that security group to your instance and click Save

Existing security group our VM belongs to



Adding Custom Security Groups



Inherited security group

Combining Security Groups

The End

VM Instance Cleanup

Cleanup

Select the instance you want to terminate

Either use this button or use the pulldown menu and select “delete instance”

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
<input checked="" type="checkbox"/> gokhale-dem	CC-Ubuntu18.04	10.212.96.7 129.114.25.5	m1.small	gokhale_chameleoncloud	Active	nova	None	Running	6 days, 1 hour	<button>Create Snapshot</button> Disassociate Floating IP Attach Interface Detach Interface Edit Instance Attach Volume Detach Volume Update Metadata Edit Security Groups Edit Port Security Groups Console View Log Pause Instance Suspend Instance Shelve Instance Resize Instance Lock Instance Soft Reboot Instance Hard Reboot Instance

Terminating an instance should automatically first disassociate the floating IP so there is no need for separate steps

VM Instance Cleanup

The End