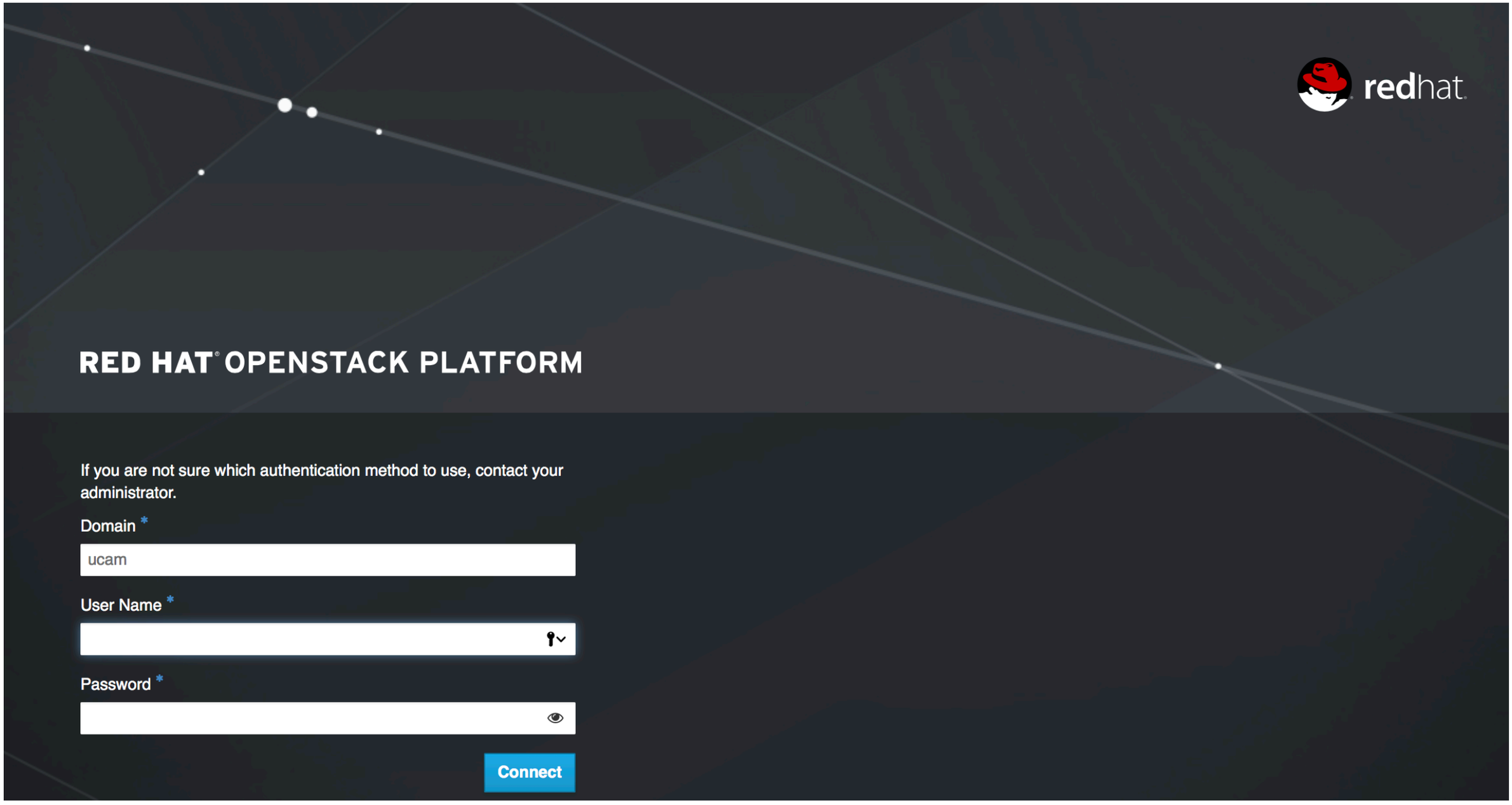
NCITA XNAT Cambridge Repository

https://ncita.xnat.radiology.medschl.cam.ac.uk/

Lorena Escudero, January 2020

UNIVERSITY OF CAMBRIDGE

0 - OPENSTACK FRAMEWORK



RED HAT OPENSTACK PLATFORM | Project | Identity | Project | Help | les44

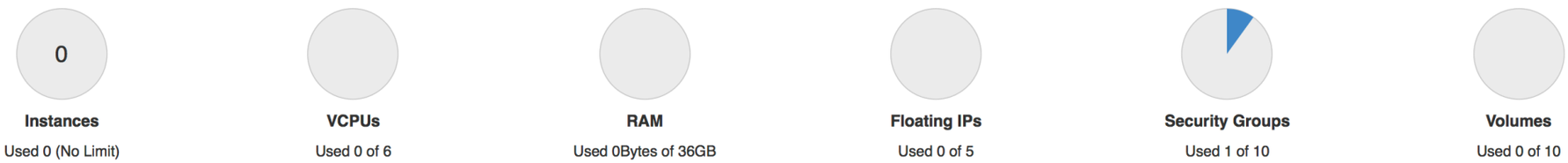
Compute | Network | Orchestration | Data Processing | Object Store

Overview | Instances | Volumes | Images | Access & Security

Project / Compute / Overview

Overview

Limit Summary



Starting point

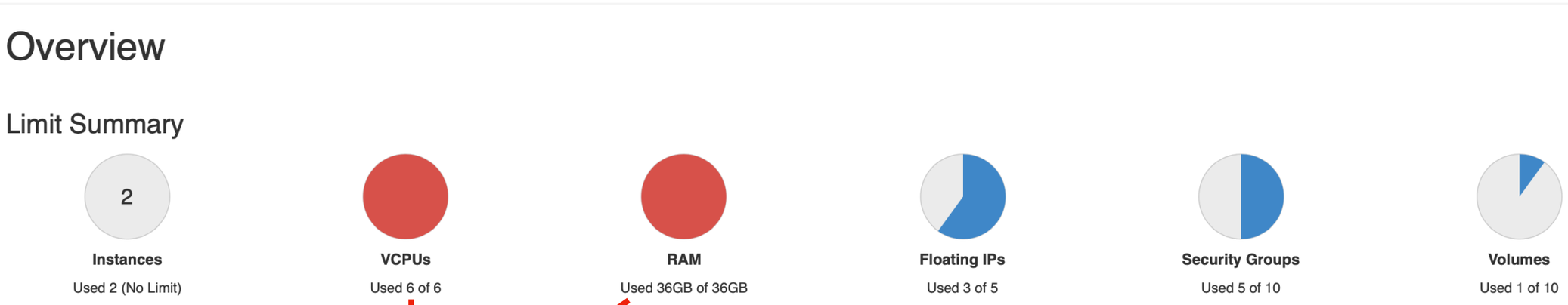
Usage Summary

Select a period of time to query its usage:

From: 2020-01-20 To: 2020-01-21 Submit The date should be in YYYY-MM-DD format.

Active Instances: 0 **Active RAM:** 0Bytes **This Period's VCPU-Hours:** 0.00 **This Period's GB-Hours:** 0.00 **This Period's RAM-Hours:** 0.00

Resources used



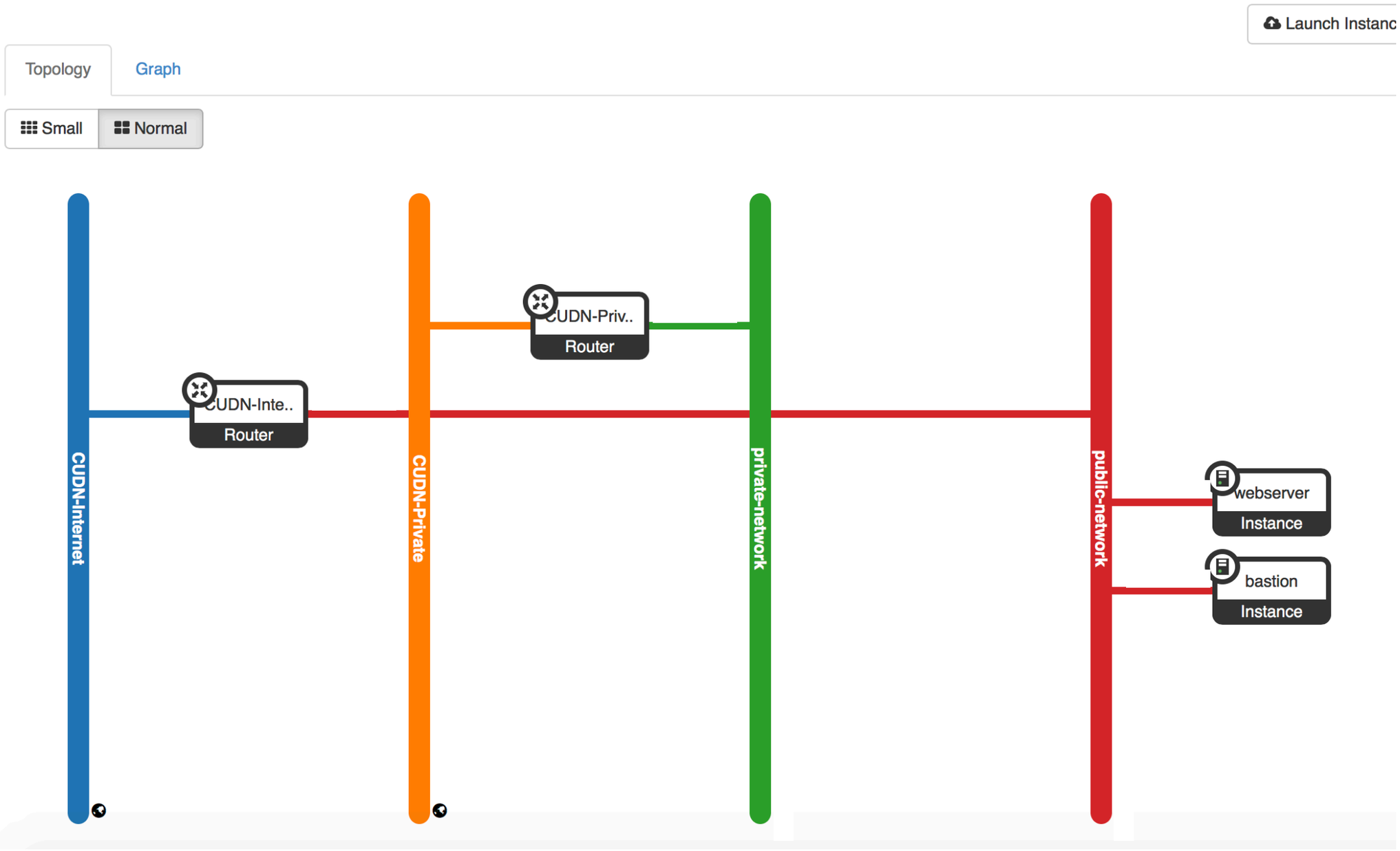
2 TB

2 VMs

1 small flavour (2VCPUs & 12 GB RAM)

1 medium flavour (4VCPUs & 24 GB RAM)

1 - NETWORK



The system is implemented such that we can’t access (SSH) directly the webserver VM, instead we need to bounce through a bastion. Both need to be in the same internal network (public-network). The webserver has a public floating IP (world-wide reachable), so routed to the CUDN-Internet.

1 - NETWORK

However, the access to the bastion is restricted to only the Cambridge Network, by specifying IP groups in the SSH rule of the external-bastion Security Group. This means it is only possible to SSH into the bastion (or ICMP) from Cambridge Network (or VPN) with a unique key pair.

Manage Security Group Rules: external-bastion

+ Add Rule | Delete Rules

	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
☐	Egress	IPv4	Any	Any	0.0.0.0/0	-	Delete Rule
☐	Egress	IPv6	Any	Any	::/0	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	172.24.0.0/14	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	172.16.0.0/13	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	172.28.0.0/15	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	172.30.0.0/16	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	10.128.0.0/9	-	Delete Rule
☐	Ingress	IPv4	TCP	22 (SSH)	172.24.0.0/14	-	Delete Rule
☐	Ingress	IPv4	TCP	22 (SSH)	172.16.0.0/13	-	Delete Rule
☐	Ingress	IPv4	TCP	22 (SSH)	10.128.0.0/9	-	Delete Rule
☐	Ingress	IPv4	TCP	22 (SSH)	172.30.0.0/16	-	Delete Rule
☐	Ingress	IPv4	TCP	22 (SSH)	172.28.0.0/15	-	Delete Rule

These properties make UDN-wide private addresses ideal for client-only devices, such as end-user devices, including those on the University Wireless Service (captive portal [UniOfCam] and eduroam).

The ranges currently in use are:

Range	Comments / use
10.128.0.0/9	Institutional allocations. Changed status from *Reserved* in September 2015.
172.16.0.0/13	Institutional allocations, including University Telephone Network
172.24.0.0/14	
172.28.0.0/15	
172.30.0.0/16	Management networks used by the UDN, University Wireless, etc.

1 - NETWORK

Manage Security Group Rules: external-webserver

+ Add Rule | Delete Rules

	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
☐	Egress	IPv6	Any	Any	::/0	-	Delete Rule
☐	Egress	IPv4	Any	Any	0.0.0.0/0	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	172.30.0.0/16	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	172.28.0.0/15	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	10.128.0.0/9	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	172.16.0.0/13	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	172.24.0.0/14	-	Delete Rule
☐	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0	-	Delete Rule
☐	Ingress	IPv4	TCP	443 (HTTPS)	0.0.0.0/0	-	Delete Rule

Displaying 9 items

HTTP is allowed from everywhere though in the external SG, so that the site is reachable from anywhere

2 - INSTANCES

Using Ubuntu 18.04. LTS (Bionic Beaver) from bionic-server-cloudimg-amd64

There is another Ubuntu option available: 16.04 (Xenial Xerus)

bastion

Overview | Log | Console | Action Log

Name	bastion
ID	
Status	Active
Availability Zone	nova-1-wcdc
Created	21 Jan 2020, 5:34 p.m.
Time Since Created	17 hours, 50 minutes

Specs

Flavour Name	C1.vss.small
Flavour ID	
RAM	12GB
VCPUs	2 VCPU
Disk	30GB

webserver

Overview | Log | Console | Action Log

Name	webserver
ID	
Status	Active
Availability Zone	nova-1-wcdc
Created	21 Jan 2020, 5:47 p.m.
Time Since Created	17 hours, 47 minutes

Specs

Flavour Name	C1.vss.medium
Flavour ID	
RAM	24GB
VCPUs	4 VCPU
Disk	60GB

3 - XNAT

https://github.com/ncita-repository/WP3_infrastructure/blob/master/docs/XNAT_StepByStepInstall.md

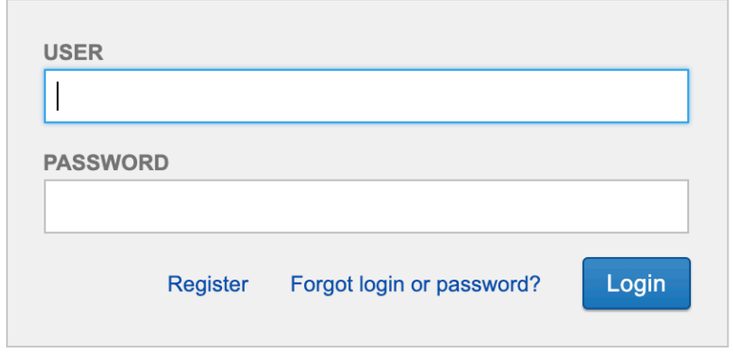
Package	Version	Comment
Ubuntu	18.04.1 LTS (Bionic Beaver)	GNU/Linux 4.15.0-38-generic x86_64
Java (openjdk)	1.8.0_232	Via apt (openjdk-8-jre-headless)
PostgreSQL	10	https://www.postgresql.org/download/linux/debian/
Tomcat	7.0.99	Via apt
XNAT	1.7.6	bitbucket

https://ncita.xnat.radiology.medschl.cam.ac.uk/

Welcome to the **NCITA XNAT of the University of Cambridge**!

This is a repository of imaging data of radiological images for cancer research. This repository is for anonymised data only and for research use only. Patient-identifiable data should never be uploaded to this server or any clinical decisions made on the basis of information contained here.

If you have any questions or problems, please contact us at ncita.xnat.ucam@gmail.com



3 - XNAT & chrony

As we know now, we need to install chrony to handle time differences in the VM clock when the VM is restarted, which can be tiny, but still makes the user session to constantly expire

From the XNAT-discussion Google group:

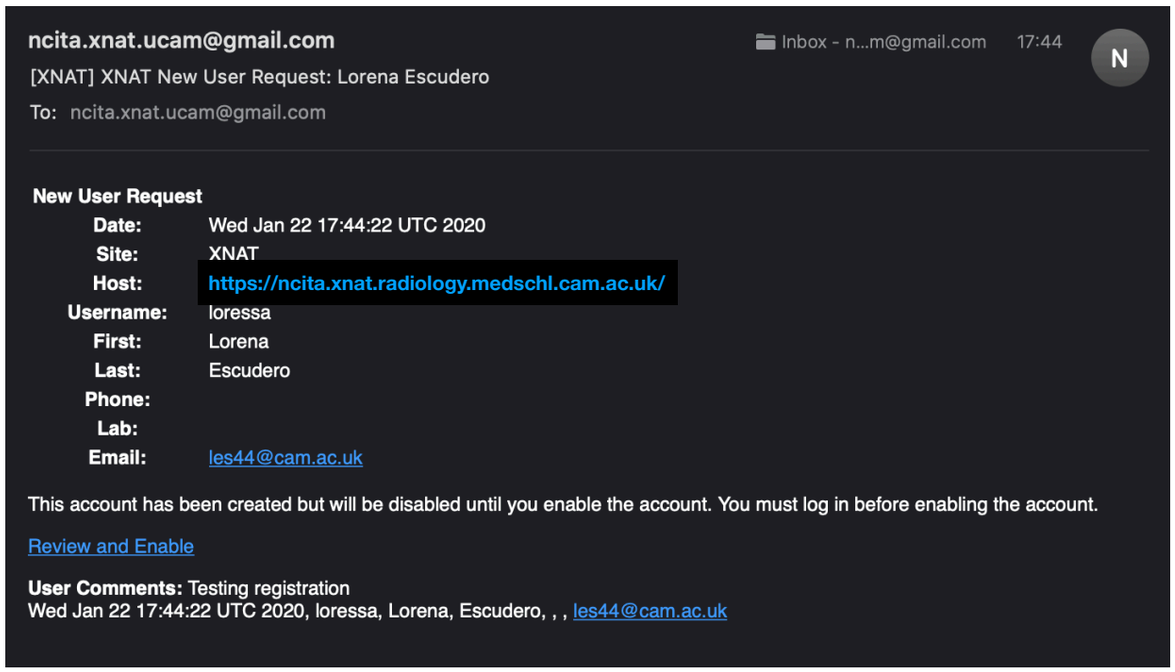
https://groups.google.com/forum/#!searchin/xnat_discussion/session$20timeout%7Csort:date/xnat_discussion/4k73efu-8eo/lUxnefLuDAAJ

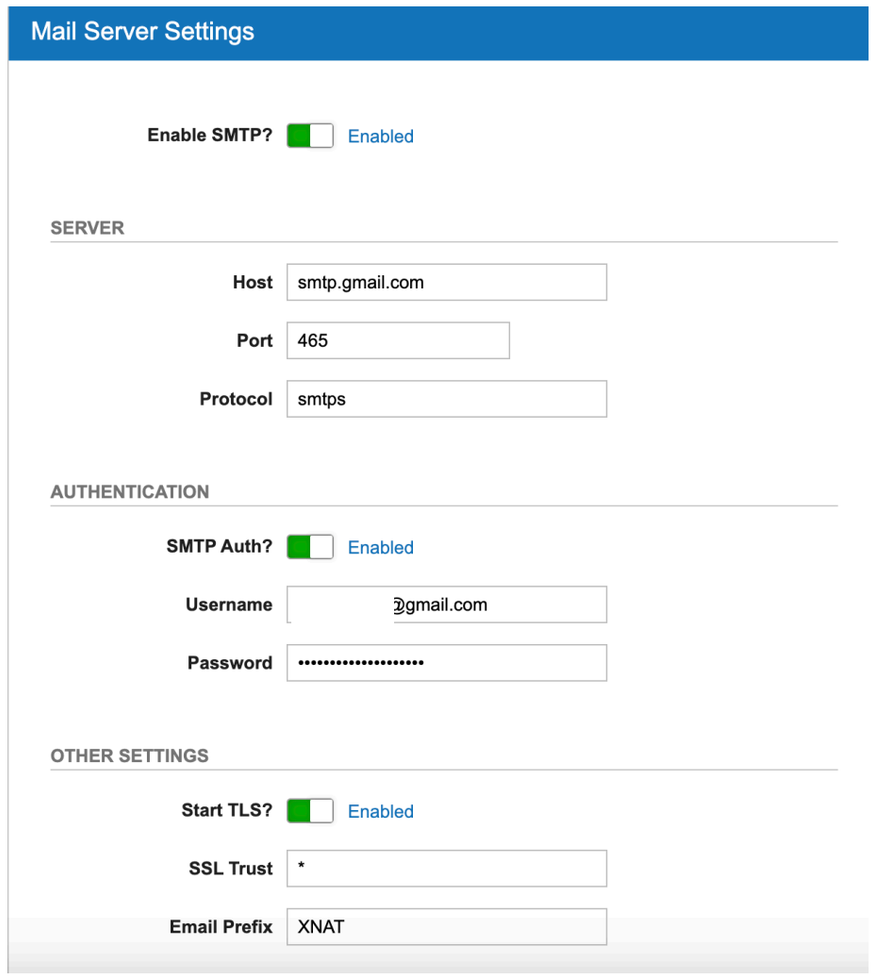
```
sudo -i
apt-get install chrony
systemctl stop chrony.service
mv /etc/chrony/chrony.conf /etc/chrony/chrony.conf.bak
wget -O /etc/chrony/chrony.conf https://bitbucket.org/rherrick/xnat-vagrant/raw/
09295f0527a26981efec3fb8b570dc37b1f8531f/templates/chrony.conf.tmpl
systemctl start chrony.service
timedatectl set-timezone Europe/London
systemctl stop chrony.service
chronyd -q
systemctl start chrony.service
```

If the session still expires, remember to clean cookies in your browser

3 - XNAT - SMTP

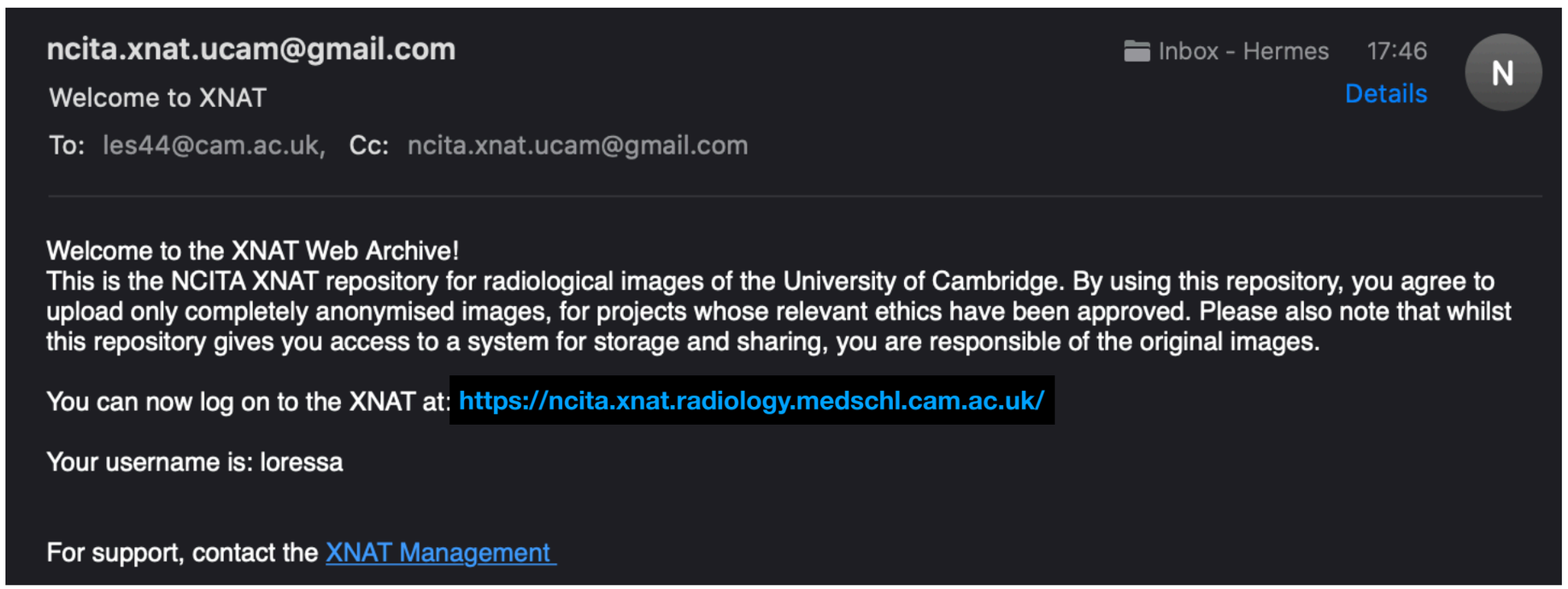
I created a dedicated email address: ncita.xnat.ucam@gmail.com





Email worked with Gmail and this settings the first time! Hooray!

I added some “disclaimer text” to the registration email (updated now to include also text in site description)



4 - TLS/SSL

1) **Got a human-friendly domain name registered as ncita.xnat.radiology.medschl.cam.ac.uk**

2) **TLS/SSL certificate with Let's Encrypt (zero-cost certificate)**

https://letsencrypt.org

https://certbot.eff.org/lets-encrypt/ubuntubionic-nginx.html

```
~$ sudo apt-get update
~$ sudo apt-get install software-properties-common
~$ sudo add-apt-repository universe
~$ sudo add-apt-repository ppa:certbot/certbot
~$ sudo apt-get update
~$ sudo apt-get install certbot python-certbot-nginx
~$ sudo emacs -nw /etc/nginx/sites-available/xnat
        Add:
             > server_name ncita.xnat.radiology.medschl.cam.ac.uk;
        inside the server{} block
~$ sudo certbot --nginx

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/ncita.xnat.radiology.medschl.cam.ac.uk/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/ncita.xnat.radiology.medschl.cam.ac.uk/privkey.pem
   Your cert will expire on 2020-05-06. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
```

5 - Storage

Cloud storage offers two options:

- **Block Storage (Cinder)**
- **Object Storage (Swift)**

Block Storage provides a traditional block storage device -like a hard drive- over the network.

/dev/vdc is the new disk -> Now we can create a filesystem and mount it

```
root@webserver:/opt/tomcat7# lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda     252:0    0   60G  0 disk
├─vda1  252:1    0 59.9G  0 part /
├─vda14 252:14   0    4M  0 part
└─vda15 252:15   0  106M  0 part /boot/efi
vdb     252:16   0    2G  0 disk [SWAP]
vdc     252:32   0    2T  0 disk
└─vdc1  252:33   0    2T  0 part
```

```
sudo mount  /dev/vdc1 /storage
```

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/vdc1       2.0T  2.1G  2.0T   1% /storage
```

Then make a symbolic link between /data/xnat and /var/storage/xnat