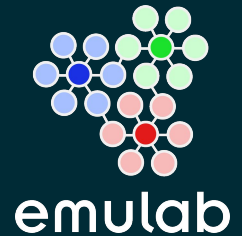


# Infrastructure For Building Cyber Experimentation Testbeds

Robert Ricci  
August 2017



# Diversity in Environments for Cyber Experimentation

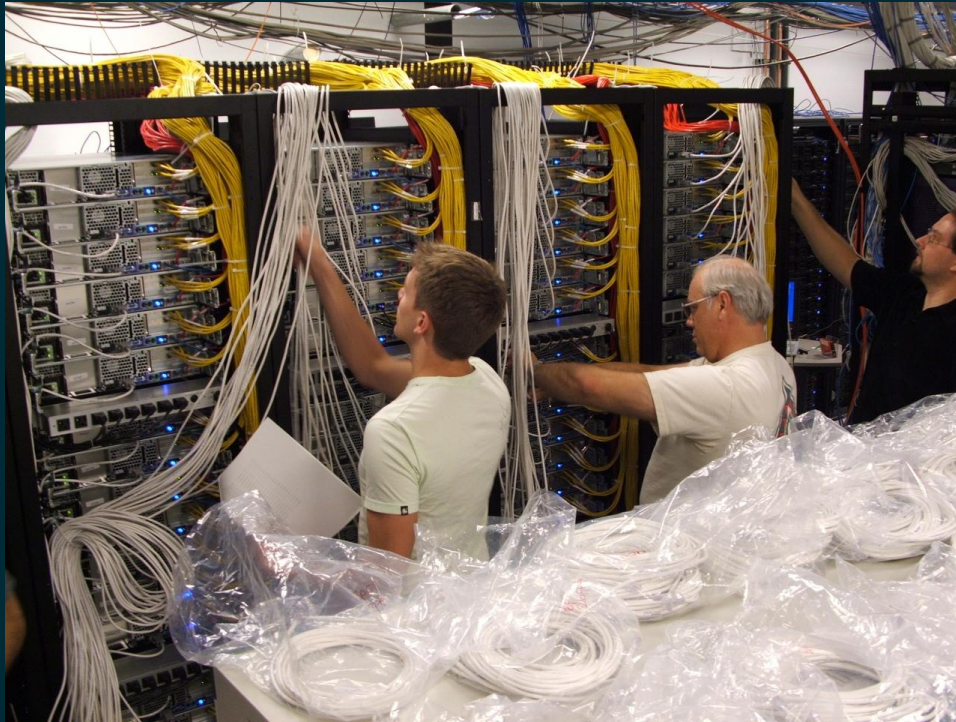


# Dimensions of Diversity

- Level of control
- Level of isolation
- Operating systems
- Application software
- Attack/defense tools
- Types of hardware
- Specialized devices
- Network technologies
- Network topology
- Storage
- User community
- Disciplines
- Ease of use
- User interface
- Dataset control
- Access policies
- User participation
- Red / blue teams
- Workflows
- ...

# Building New Cyber-Experimentation Infrastructure

# Building a Testbed Is Hard





# Building a Testbed is Expensive



# Building a New Testbed is Risky





A Proposed Solution:

**Build infrastructure for  
building infrastructure**

“Meta Infrastructure”



CloudLab



# The Problem with Cloud Research

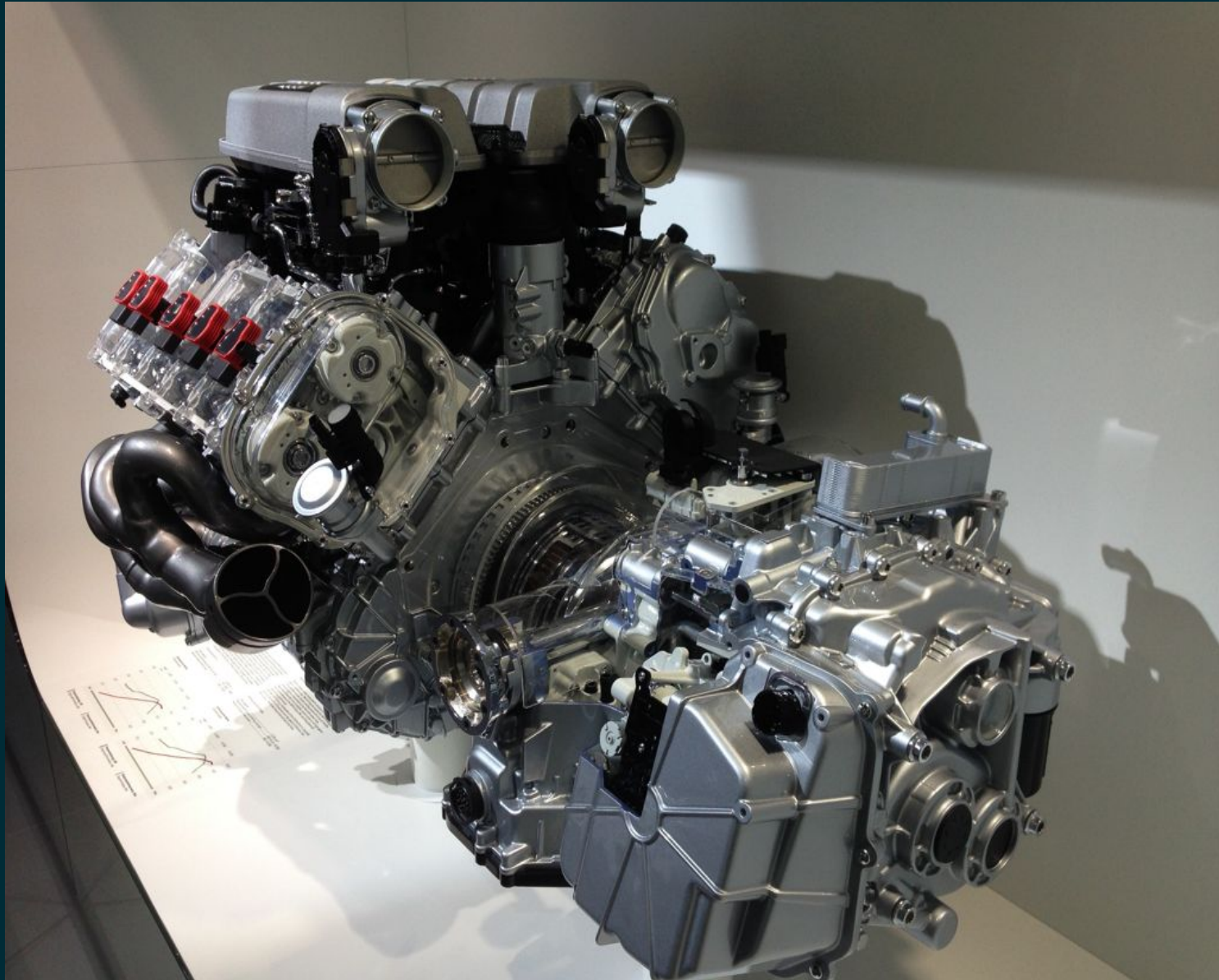


# The CloudLab Vision

- A “meta-cloud” for building clouds
- Build your own cloud on our hardware resources
- Run any cloud software
- Control and visibility all the way to the bare metal
- “Sliceable” for multiple, isolated experiments at once

With CloudLab, it's as easy to get *an entire cloud* as it is to get a VM *in* a cloud

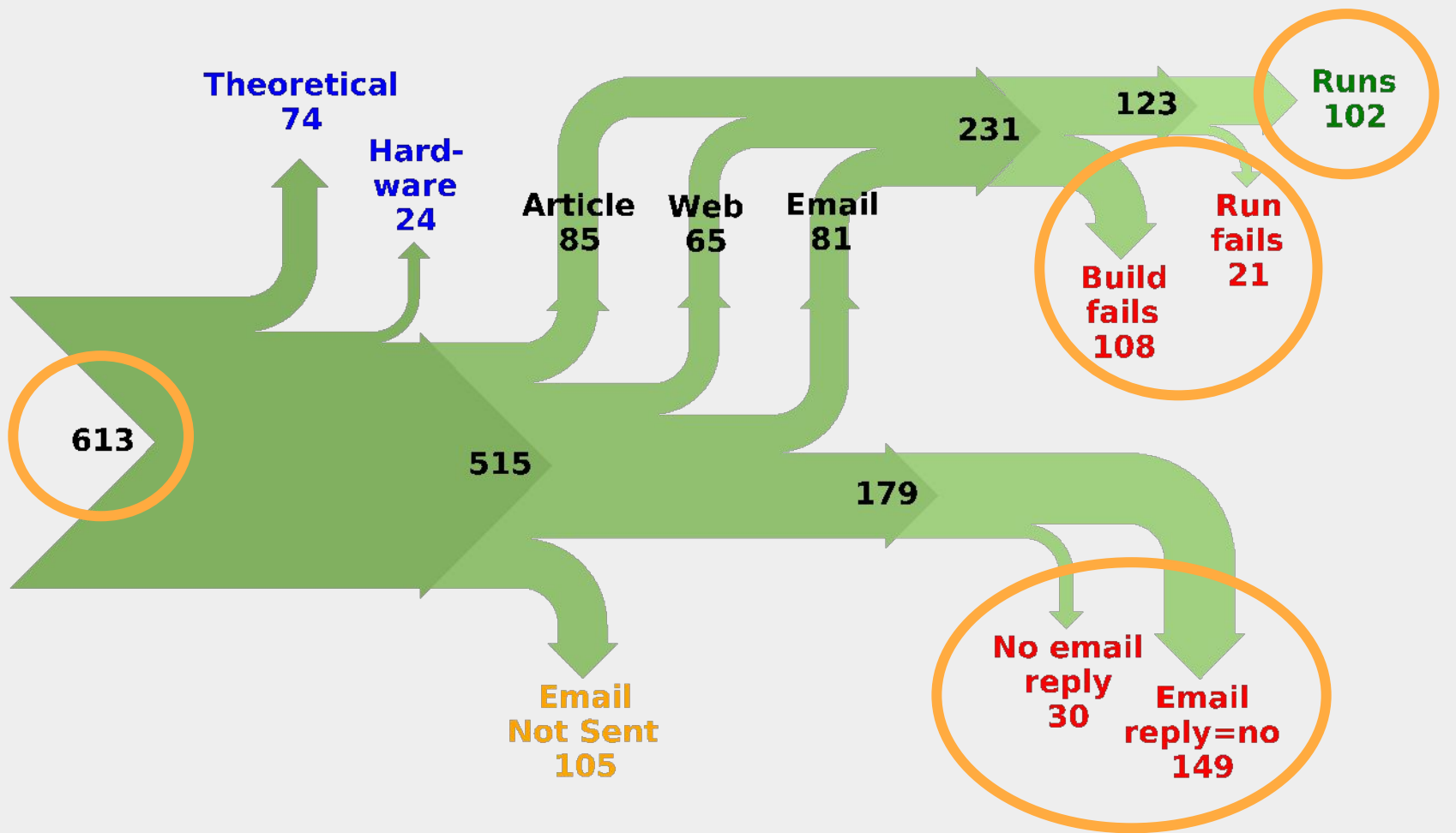
# Building on Each Other's Work







# The Difficulty of Reproducing Papers



From Collberg et al. - <http://reproducibility.cs.arizona.edu/>

A Proposed Solution:

**Make it easy to encapsulate  
everything about an  
experimental environment**

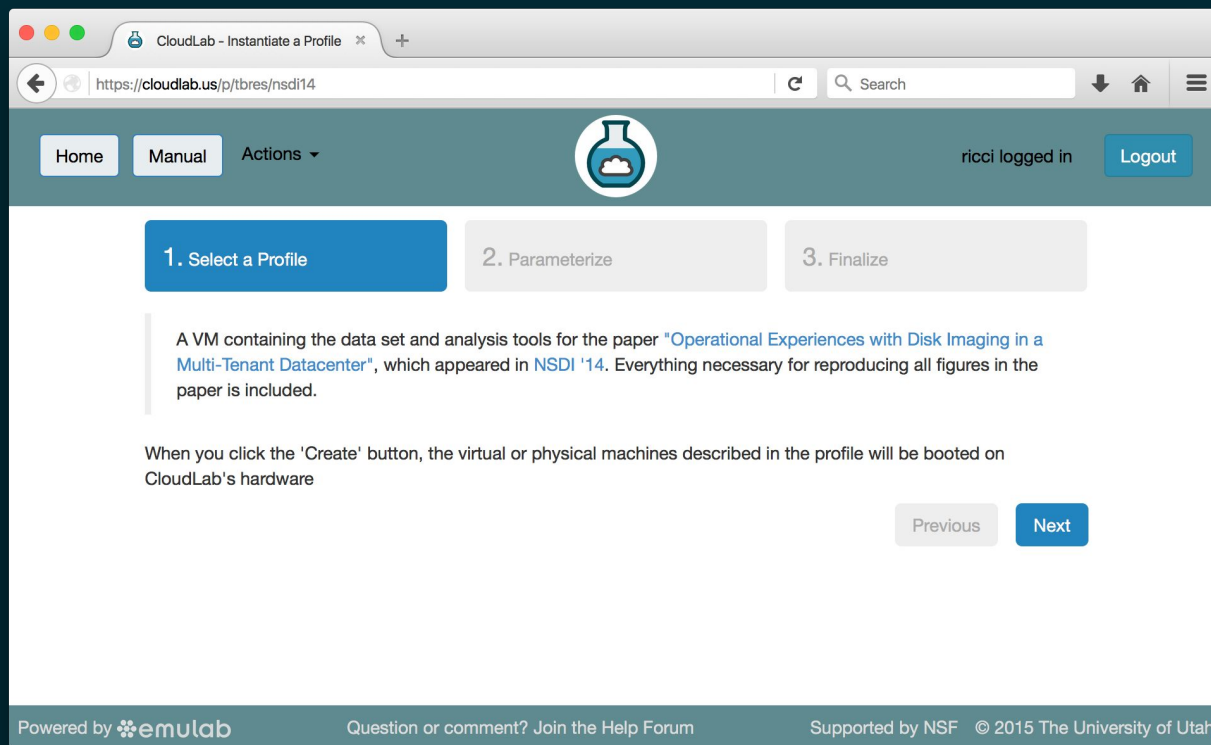
# An Example of The Solution: Profiles





# Profile URLs

<https://cloudlab.us/p/tbres/nsdi14>



# What a Profile Contains

**Name**

controller

**Node Type**

Other...

raw

**Hardware Type**

(any)

**Disk Image**

Other...

urn:publicid:IDN+utah.cloudlab.us+im

version

☐ Disable MAC Learning (For OVS Images Only)☐ Publicly Routable IP**Icon**

(any)

**Install Tarball****URL:**

http://www.emulab.net/download

**Install Path:**

/tmp

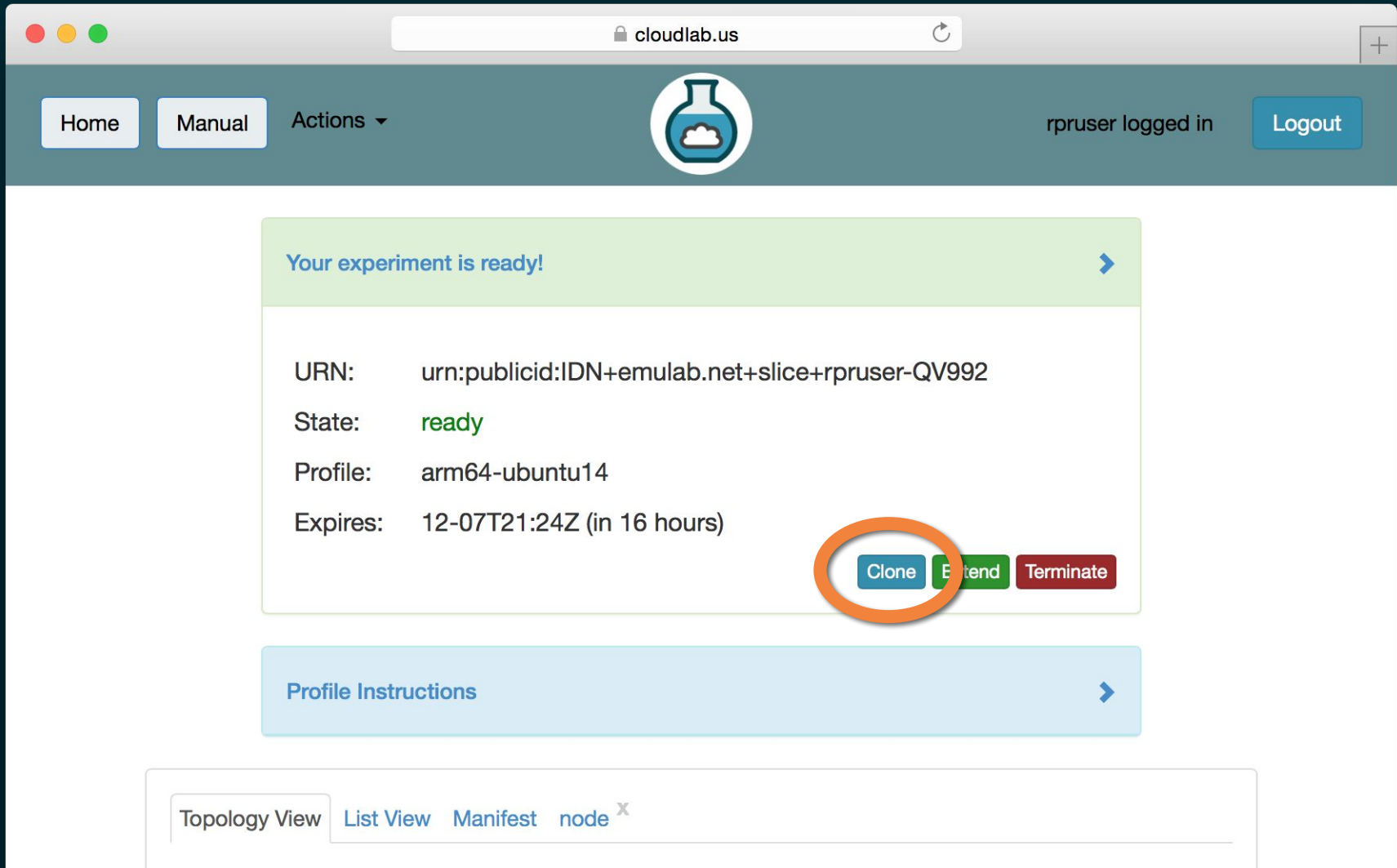
Remove

**Execute Command****Command:**

sudo mkdir -p /root/setup &amp;&amp; su

```
graph LR; subgraph Site1 [Site 1]; controller; networkmanager; compute1[compute-1]; compute2[compute-2]; compute3[compute-3]; end; subgraph Site2 [Site 2]; compute_s2_1[compute-s2-1]; compute_s2_2[compute-s2-2]; compute_s2_3[compute-s2-3]; end; hub(( )); controller --- hub; networkmanager --- hub; compute1 --- hub; compute2 --- hub; compute3 --- hub; compute_s2_1 --- hub; compute_s2_2 --- hub; compute_s2_3 --- hub;
```

# Copy an Existing Profile



The screenshot shows the CloudLab web interface. The browser address bar displays "cloudlab.us". The navigation bar includes "Home", "Manual", and "Actions" (with a dropdown arrow). The user "rpruser" is logged in, with a "Logout" button. A green notification box states "Your experiment is ready!" with a right-pointing arrow. Below this, the experiment details are listed: URN: urn:publicid:IDN+emulab.net+slice+rpruser-QV992, State: ready, Profile: arm64-ubuntu14, and Expires: 12-07T21:24Z (in 16 hours). At the bottom of this box are three buttons: "Clone" (blue), "Extend" (green), and "Terminate" (red). The "Clone" button is circled in orange. Below the notification box is a blue box labeled "Profile Instructions" with a right-pointing arrow. At the bottom of the page, there is a tabbed interface with "Topology View" selected, and other tabs for "List View", "Manifest", and "node" (with a close icon).

cloudlab.us

Home Manual Actions

rpruser logged in Logout

Your experiment is ready! >

URN: urn:publicid:IDN+emulab.net+slice+rpruser-QV992

State: ready

Profile: arm64-ubuntu14

Expires: 12-07T21:24Z (in 16 hours)

Clone Extend Terminate

Profile Instructions >

Topology View List View Manifest node<sup>x</sup>

# Use a GUI

cloudlab.us

## Topology Editor

Tidy View Delete All

☐ Custom Type

**Hardware Type**

(any)

☐ Custom Hardware

**Disk Image**

Ubuntu 12.04 LTS 64-bit

☐ Custom Disk Image

**Install Scripts** Add

• URL:

ex: http://example.com/mystuff.tar

```
graph TD; CC[cloud-controller] --- Hub(( )); NN[name-node] --- Hub; W1[worker-1] --- Hub; W5[worker-5] --- Hub; Unlabeled[ ] --- Hub
```

The diagram illustrates a network topology with a central hub connected to five nodes. The nodes are labeled: cloud-controller, name-node, worker-1, worker-5, and an unlabeled node. The cloud-controller node is highlighted with a green border.



# Write Code

```
#!/usr/bin/env python
"""An example of constructing a profile with a single physical
host. Instructions: Wait for the profile instance to start,
and then log in to the VM via the ssh port specified below.
"""

import geni.rspec.pg as rspec
import geni.portal as portal

# Create the Portal context.
rspec = portal.context.makeRequestRSpec()

# Create a raw machine and add it to the RSpec.
node = rspec.RawPC("node")

# Print the RSpec to the enclosing page.
portal.context.printRequestRSpec()
```

# A More Complex Profile

```
# Describe the parameter(s) this profile script can accept.
pc.defineParameter( "n", "Number of VMs", portal.ParameterType.INTEGER, 1)

# Retrieve the values the user specifies during instantiation.
params = pc.bindParameters()

# Check parameter validity.
if params.n < 1 or params.n > 8:
    pc.reportError(
        portal.ParameterError(
            "You must choose at least 1 and no more than 8 VMs.))

for i in range( params.n ):
    # Create a raw node and add it to the RSpec.
    node = rspec.RawPC( "node" + str( i ) )
```

# Demo

<https://www.cloudlab.us/p/emulab-ops/OpenStack>

Home

Manual



Sign Up

### Login

**Username**

ricci

**Password**

.....

Forgot Password?

Geni User?

Login



## 1. Select a Profile

## 2. Parameterize

## 3. Finalize

**Selected Profile:** OpenStack

A highly-configurable OpenStack instance with a controller, network manager, and one or more compute nodes (potentially at multiple sites). This profile runs x86 or ARM64 nodes. It sets up OpenStack Kilo or Juno on Ubuntu 15.04 or 14.10, and configures all OpenStack services, pulls in some VM disk images, and creates basic networks accessible via floating IPs. You'll be able to create instances and access them over the Internet in just a few minutes. When you click the Instantiate button, you'll be presented with a list of parameters that you can change to control what your OpenStack instance will look like; **carefully** read the parameter documentation to understand the various features available to you!

[Copy Profile](#)[Show Profile](#)[Change Profile](#)[Previous](#)[Next](#)



CloudLab - Instantiate a Profile

Select a Profile

Use Classic Picker

✕

Search

Recent -

OpenStack

System

arm64-ubuntu15-10 CloudLab

two-site-demo flux

two-nodes utahstud

geni-lib-ramcloud-test utahstud

CloudLab -

arm64-ubuntu15-10

Tutorial-OpenStack

ARM64OpenStack-Tutorial

Example

Hadoop\_skollu0

ShrutiSaumya\_Profile

rogile

profile-1

OpenStack

★ Add to Favorites

Created By:

johnsond

Project:

System

Latest Version:

26

Last Updated:

2016-02-25 16:21:27

Description:

This profile provides a highly-configurable OpenStack instance with a controller, network manager, and one or more compute nodes (potentially at multiple Cloudlab sites). This profile runs x86 or ARM64 nodes. It sets up OpenStack Liberty, Kilo, or Juno (on Ubuntu 15.10, 15.04, or 14.10) according to your choice, and configures all OpenStack services, pulls in some VM disk images, and creates basic networks accessible via floating IPs. You'll be able to create instances


ctl

cp-1

nm

Select Profile

Cancel

Powered by emulab

Question or comment? Join the Help Forum

Supported by NSF © 2015 The University of Utah


30

CloudLab - Instantiate a Profile

Home

Manual

Actions ▾



ricci1 logged in 

Logout

1. Select a Profile

2. Parameterize

3. Finalize

**Selected Profile:** OpenStack

A highly-configurable OpenStack instance with a controller, network manager, and one or more compute nodes (potentially at multiple sites). This profile runs x86 or ARM64 nodes. It sets up OpenStack Kilo or Juno on Ubuntu 15.04 or 14.10, and configures all OpenStack services, pulls in some VM disk images, and creates basic networks accessible via floating IPs. You'll be able to create instances and access them over the Internet in just a few minutes. When you click the Instantiate button, you'll be presented with a list of parameters that you can change to control what your OpenStack instance will look like; **carefully** read the parameter documentation to understand the various features available to you!


Copy Profile

Show Profile

Change Profile

Previous

Next


Powered by  emulab

Question or comment? Join the Help Forum

Supported by NSF © 2015 The University of Utah

CloudLab - Instantiate a Profile

HomeManualActions



ricci1 logged inLogout

1. Select a Profile2. Parameterize3. Finalize

Please review the selections below and then click Finish.

Profile:OpenStack

Name:Optional

Cluster:

Please Select

Please Select

Cloudlab Utah

Cloudlab Wisconsin

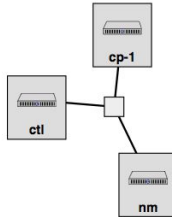
Cloudlab Clemson

Federated Clusters


Emulab

APT Utah

IG UtahDDC



PreviousFinish


Powered by emulab

Question or comment? Join the Help Forum

Supported by NSF © 2015 The University of Utah

CloudLab - Instantiate a Profile

HomeManualActions ▾



ricci1 logged inLogout

1. Select a Profile2. Parameterize3. Finalize

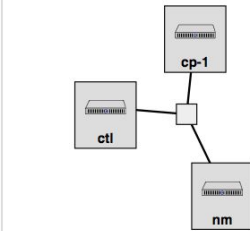
Please review the selections below and then click Finish.

Profile:OpenStack

Name:Optional


Cluster:Please Select ▾

Check Cluster Status



Previous

Finish

Powered by emulab

Question or comment? Join the Help Forum

Supported by NSF © 2015 The University of Utah


33

CloudLab - Experiment Status

Home

Manual

Actions ▾



ricci1 logged in

Logout

Please wait while we get your experiment ready

Name: ricci1-QV6643

State: booting

Profile: [Tutorial-OpenStack](#)

Created: Jun 10 2015 12:43 PM

Expires: Jun 11 2015 4:43 AM (in 16 hours)

Sliver

Copy

Extend

Terminate


Profile Instructions

Topology View

List View

Manifest

ID	Node	SSH command (if you provided your own key)	Actions
ctl	ms0503	<code>ssh -p 22 ricci1@ms0503.utah.cloudlab.us</code>	
nm	ms0520	<code>ssh -p 22 ricci1@ms0520.utah.cloudlab.us</code>	
cp1	ms0512	<code>ssh -p 22 ricci1@ms0512.utah.cloudlab.us</code>	

Powered by emulab


Question or comment? Join the Help Forum

Supported by NSF © 2014 The University of Utah



CloudLab - Experiment Status

HomeManualActions



ricci1 logged inLogout

Your experiment is ready!

Name:ricci1-QV10477

State:ready

Profile:OpenStack

Created:Nov 5 2015 11:14 AM

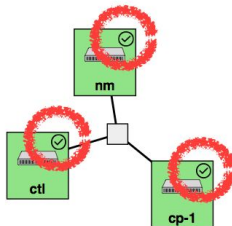
Expires:Nov 6 2015 3:14 AM (in 16 hours)

Sliver

CopyExtendTerminate

Profile Instructions

Topology ViewList ViewManifest



# ubuntu<sup>®</sup> OpenStack Dashboard

## Log In

User Name

admin

Password

.....



Sign In

## Admin

## System

Overview

Hypervisors

Host Aggregates

Instances

Flavors

Images

Networks

Routers

Defaults

System Information

## Identity

## Hypervisor Summary

**VCPU Usage**  
Used 0 of 24**Memory Usage**  
Used 1.5GB of  
188.9GB**Disk Usage**  
Used 0Bytes of  
327GB

Hypervisor

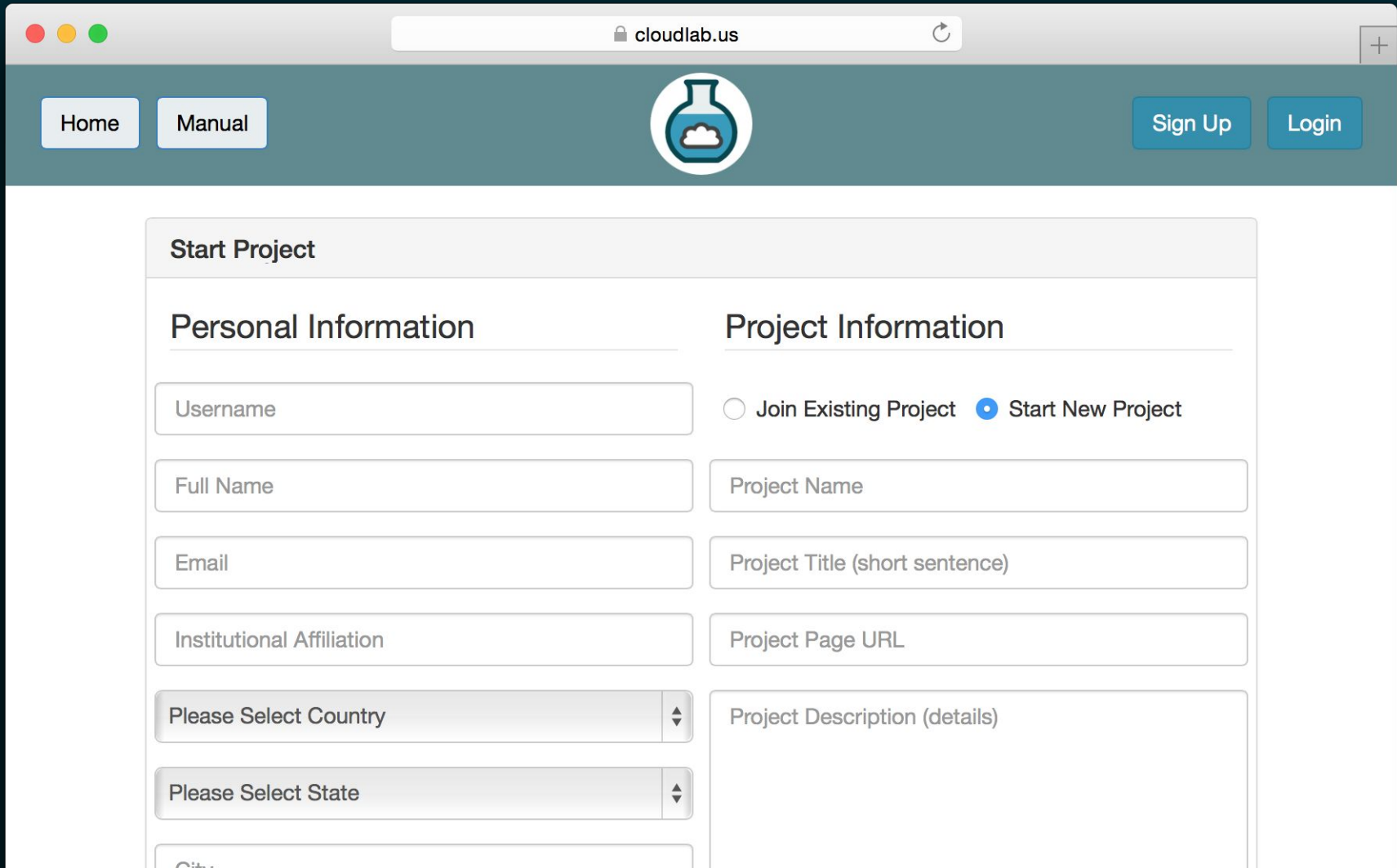
Compute Host

## Hypervisors

Hostname	Type	VCPUs (used)	VCPUs (total)	RAM (used)	RAM (total)	Storage (used)	Storage (total)	Instances
compute2.ricci-qv1031.emulab-net.utah.cloudlab.us	QEMU	0	8	512MB	63GB	0Bytes	109GB	0
compute3.ricci-qv1031.emulab-net.utah.cloudlab.us	QEMU	0	8	512MB	63GB	0Bytes	109GB	0
compute1.ricci-qv1031.emulab-net.utah.cloudlab.us	QEMU	0	8	512MB	63GB	0Bytes	109GB	0

Displaying 3 items

# Sign Up At CloudLab.us



The screenshot shows a web browser window with the address bar displaying "cloudlab.us". The page has a teal header with navigation links "Home" and "Manual" on the left, a logo in the center, and "Sign Up" and "Login" buttons on the right. The main content area is titled "Start Project" and is divided into two columns: "Personal Information" and "Project Information".

**Start Project**

**Personal Information**

Username

Full Name

Email

Institutional Affiliation

Please Select Country

Please Select State

City

**Project Information**

☐ Join Existing Project ☒ Start New Project

Project Name

Project Title (short sentence)

Project Page URL

Project Description (details)

# Thoughts for Future Cyberinfrastructure

- **Build flexible platforms, and testbeds on top**
  - Like the cloud, but lower level and security-focused
  - Use economies of scale
  - Reduce risk -> encourage more diversity
- **Capture entire environments**
  - Cyber experiments are often messy
  - Often require a known-good state
  - Encourage collaboration and building on each other's work



# CloudLab

