Secure Multiparty Computation Sprint 3

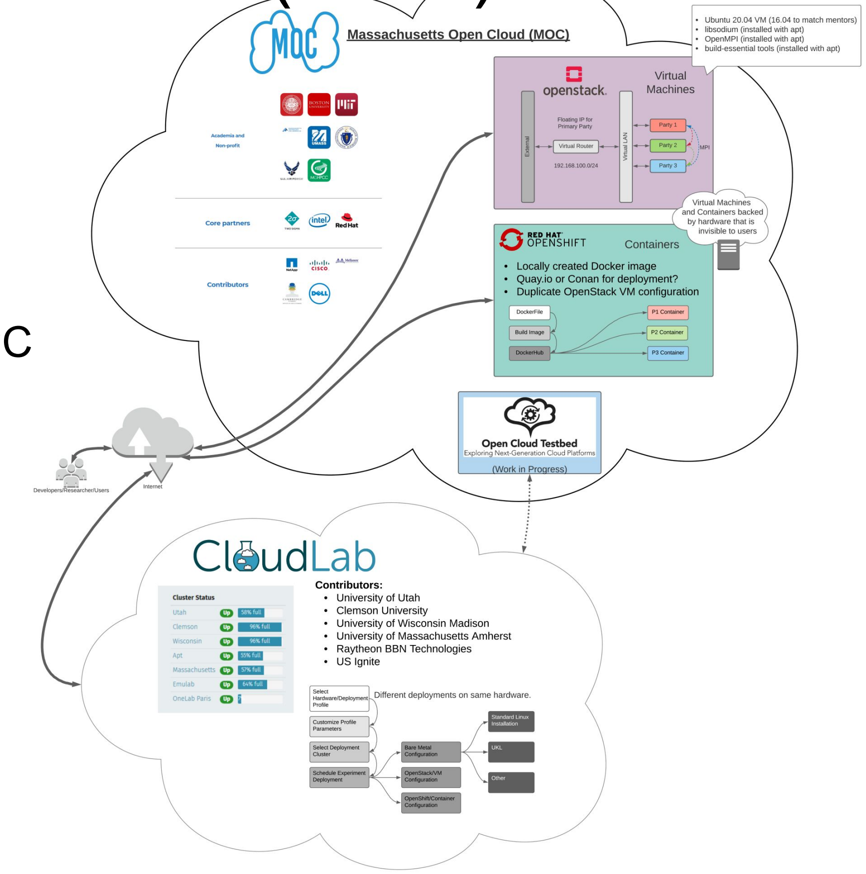
Developer | Hasnain Abdur Rehman| hasnain@bu.edu
Developer | Pierre-François Wolfe | pwolfe@bu.edu
Developer | Samyak Jain | samyakj@bu.edu
Developer | Suli Hu | sulihu@bu.edu
Developer | Yufeng Lin | yflin@bu.edu
Mentor/Client | John Liagouris | liagos@bu.edu
Mentor/Client | Vasiliki Kalavri | vkalavri@bu.edu
Subject-Matter Expert | Mayank Varia | varia@bu.edu

Presentation Outline

- Project Recap
- Project Goals & Sprint 3 Stories/Tasks
- Work Accomplished & Information Learned
  - Cloudlab/Bare-Metal Progress
  - Geni-Scripts & Bare-Metal results
  - Docker progress
- Project Organization Assessment (Burndown)
- Sprint 4 goals (Mentor priorities)

Recap of Multi-Party Computation (MPC)

- MPC enables...
  - Shared Computation on Private Data
  - Protects the Privacy of Data
  - Mutually Agreed Computation
- Our mentors…
  - Are using three party Secret Sharing MPC
  - Perform Relational Queries with MPC
  - Keep all parts secure vs. splitting into secure and insecure steps
- Our mission…
  - Profile this new MPC library
  - Identify bottlenecks
  - Compare deployment scenarios and find the best performance


Massachusetts Open Cloud (MOC)
Academia and Non-profit
Core partners
Contributors
openstack.
Virtual Machines
External
Floating IP for Primary Party
Virtual Router
192.168.100.0/24
Virtual LAN
Party 1
Party 2
Party 3
MPI
Virtual Machines and Containers backed by hardware that is invisible to users
RED HAT OPENSHIFT
Containers
DockerFile
Build Image
DockerHub
P1 Container
P2 Container
P3 Container
Open Cloud Testbed
Exploring Next-Generation Cloud Platforms
(Work in Progress)
Developers/Researcher/Users
Internet
CloudLab
Select Hardware/Deployment Profile
Customize Profile Parameters
Select Deployment Cluster
Schedule Experiment Deployment
Bare Metal Configuration
OpenStack/VM Configuration
OpenShift/Container Configuration
Standard Linux Installation
UKL
Other

- Ubuntu 20.04 VM (16.04 to match mentors)
- libsodium (installed with apt)
- OpenMPI (installed with apt)
- build-essential tools (installed with apt)

- Locally created Docker image
- Quay.io or Conan for deployment?
- Duplicate OpenStack VM configuration

Cluster Status

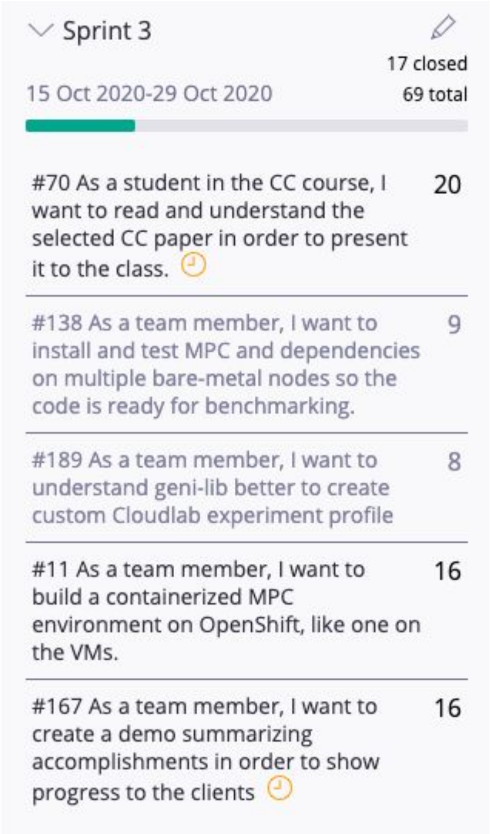
Utah	Up	58% full
Clemson	Up	96% full
Wisconsin	Up	96% full
Apt	Up	55% full
Massachusetts	Up	57% full
Emulab	Up	64% full
OneLab Paris	Up	7

Contributors:
- University of Utah
- Clemson University
- University of Wisconsin Madison
- University of Massachusetts Amherst
- Raytheon BBN Technologies
- US Ignite

Different deployments on same hardware.

Project Goals & Sprint 3 Stories/Tasks

- VMs -
  - Improve existing instrumentation (delayed)
  - Explore tracing and profiling outputs from Score-p (delayed)
- Containers -
  - MPC test on single-container deployment (runs but debugging)
  - MPC test on multi-container deployment (waiting for single-container debug)
- Bare Metal -
  - MPC test on multi-bare-metal deployment (runs)
  - Initial data for exp-exchange collected, plotted
  - Challenges: Need to test on different profile deployment on bare metal
- Other -
  - Preparation for paper presentation (progress made, final revisions remain)



Sprint 3

15 Oct 2020-29 Oct 2020

17 closed
69 total

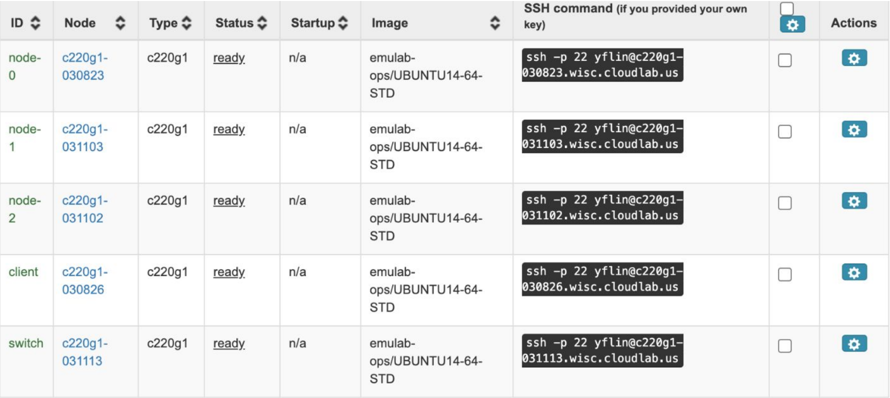
#70 As a student in the CC course, I want to read and understand the selected CC paper in order to present it to the class.	20
#138 As a team member, I want to install and test MPC and dependencies on multiple bare-metal nodes so the code is ready for benchmarking.	9
#189 As a team member, I want to understand geni-lib better to create custom Cloudlab experiment profile	8
#11 As a team member, I want to build a containerized MPC environment on OpenShift, like one on the VMs.	16
#167 As a team member, I want to create a demo summarizing accomplishments in order to show progress to the clients	16

Change of Plans

- Challenges
  - Time spent on paper presentation
  - MOC downtime
  - CloudLab reservation challenges
  - Docker debugging
  - Team time conflicts this sprint (travel, exams, ...)
- Adjustment
  - Focus on running exp-exchange
    - Bare-metal on CloudLab → geni scripts
    - Containers → Local tests → Docker debugging

CloudLab/Bare-Metal Progress

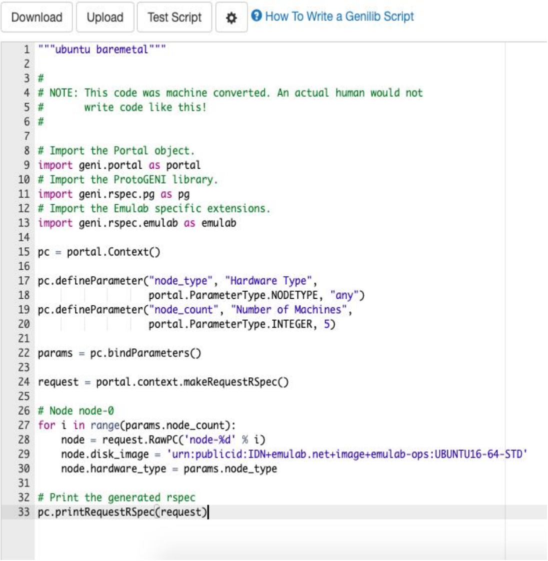
- Specify new testing profile/environment
- Install dependencies needed for multi-nodes MPI
- Identify different testing environment
- Resolve communication between multi-nodes
- Test MPI functionality
- Run exp-exchange



ID	Node	Type	Status	Startup	Image	SSH command (if you provided your own key)	□	Actions
node-0	c220g1-030823	c220g1	ready	n/a	emulab-ops/UBUNTU14-64-STD	`ssh -p 22 yflin@c220g1-030823.wisc.cloudlab.us`	□	⚙
node-1	c220g1-031103	c220g1	ready	n/a	emulab-ops/UBUNTU14-64-STD	`ssh -p 22 yflin@c220g1-031103.wisc.cloudlab.us`	□	⚙
node-2	c220g1-031102	c220g1	ready	n/a	emulab-ops/UBUNTU14-64-STD	`ssh -p 22 yflin@c220g1-031102.wisc.cloudlab.us`	□	⚙
client	c220g1-030826	c220g1	ready	n/a	emulab-ops/UBUNTU14-64-STD	`ssh -p 22 yflin@c220g1-030826.wisc.cloudlab.us`	□	⚙
switch	c220g1-031113	c220g1	ready	n/a	emulab-ops/UBUNTU14-64-STD	`ssh -p 22 yflin@c220g1-031113.wisc.cloudlab.us`	□	⚙

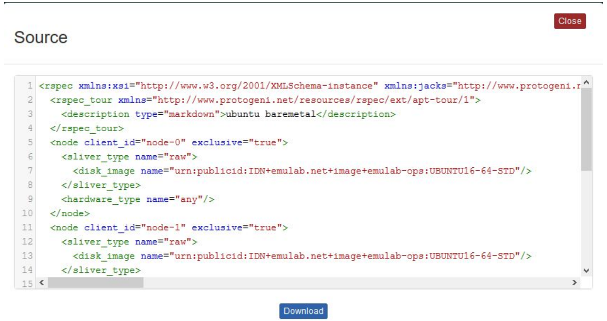
Custom CloudLab Experiments

- CloudLab Options
  - “Jacks” GUI
  - Hand crafted GENI RSpec (XML)
  - geni-lib → RSpec
- geni-lib script
  - Generates RSpec files with Python script
  - Much more readable
- Some Parameters
  - Number, type of nodes
  - Size of nodes
  - Type of link between nodes
  - Physical hardware



```python
"""ubuntu baremetal"""

#
# NOTE: This code was machine converted. An actual human would not
#       write code like this!
#

# Import the Portal object.
import geni.portal as portal
# Import the ProtoGENI library.
import geni.rspec.pg as pg
# Import the Emulab specific extensions.
import geni.rspec.emulab as emulab

pc = portal.Context()

pc.defineParameter("node_type", "Hardware Type",
                   portal.ParameterType.NODETYPE, "any")
pc.defineParameter("node_count", "Number of Machines",
                   portal.ParameterType.INTEGER, 5)

params = pc.bindParameters()

request = portal.context.makeRequestRSpec()

# Node node-0
for i in range(params.node_count):
    node = request.RawPC('node-%d' % i)
    node.disk_image = 'urn:publicid:IDN+emulab.net+image+emulab-ops:UBUNTU16-64-STD'
    node.hardware_type = params.node_type

# Print the generated rspec
pc.printRequestRSpec(request)
```

Custom Cloudlab Profile (geni-lib script)



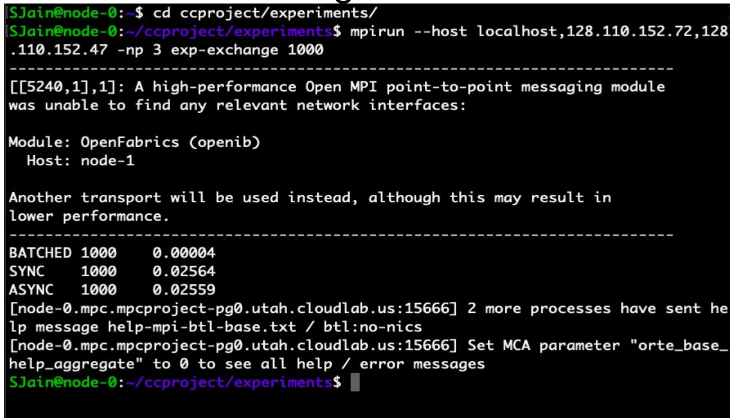
```xml
<rspec xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:jacks="http://www.protogeni.r
  <rspec_tour xmlns="http://www.protogeni.net/resources/rspec/ext/apt-tour/1">
    <description type="markdown">ubuntu baremetal</description>
  </rspec_tour>
  <node client_id="node-0" exclusive="true">
    <sliver_type name="raw">
      <disk_image name="urn:publicid:IDN+emulab.net+image+emulab-ops:UBUNTU16-64-STD"/>
    </sliver_type>
    <hardware_type name="any"/>
  </node>
  <node client_id="node-1" exclusive="true">
    <sliver_type name="raw">
      <disk_image name="urn:publicid:IDN+emulab.net+image+emulab-ops:UBUNTU16-64-STD"/>
    </sliver_type>
```

Generated RSpec

Some Bare-Metal Results

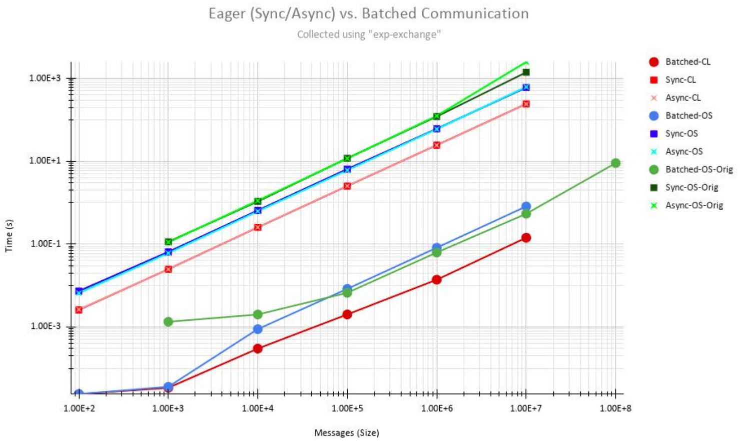
- Cloudlab resources weren’t available
  - Started new experiment on ARM based m400 nodes (only available nodes)
  - Used ‘centos-n-bare-metal’ profile as reference
  - Changed geni script to run with Ubuntu 16.04 OS
- Exp-exchange test
  - MPI batched, MPI eager (sync, async)
- Bare Metal tests faster than VMs
  - Due to ARM (on bare metal) vs x86 (on VMs)??
- Notes:
  - Sent huge traffic over shared control network on Cloudlab
  - Will create own LAN system to avoid this

MPC running on Bare Metal



```
SJain@node-0:~$ cd ccproject/experiments/
SJain@node-0:~/ccproject/experiments$ mpirun --host localhost,128.110.152.72,128
.110.152.47 -np 3 exp-exchange 1000
--------------------------------------------------------------------------
[[5240,1],1]: A high-performance Open MPI point-to-point messaging module
was unable to find any relevant network interfaces:

Module: OpenFabrics (openib)
  Host: node-1

Another transport will be used instead, although this may result in
lower performance.
--------------------------------------------------------------------------
BATCHED 1000     0.00004
SYNC    1000     0.02564
ASYNC   1000     0.02559
[node-0.mpc.mpcproject-pg0.utah.cloudlab.us:15666] 2 more processes have sent he
lp message help-mpi-btl-base.txt / btl:no-nics
[node-0.mpc.mpcproject-pg0.utah.cloudlab.us:15666] Set MCA parameter "orte_base_
help_aggregate" to 0 to see all help / error messages
SJain@node-0:~/ccproject/experiments$
```

Mentor MOC VM vs Our VM vs Bare Metal



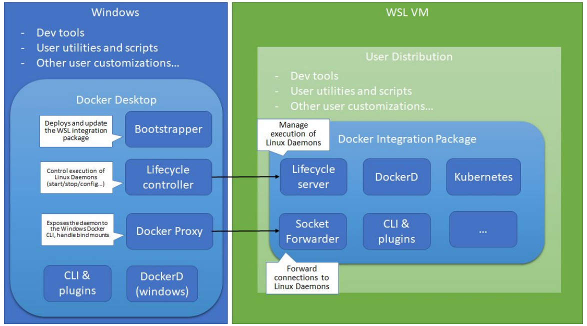
Docker as a Stepping Stone to OpenShift

- Plan for Testing
  - Local single-container MPC test
  - Local multi-container MPC test
  - Some type of more automated grouping
    - Local Kubernetes?
  - Deploy to OpenShift
- Execution of Plan
  - Discovered Interesting Docker Features
  - Worked around some OpenMPI issues
  - Still debugging/evaluating some messages from OpenMPI

Local Docker Setup

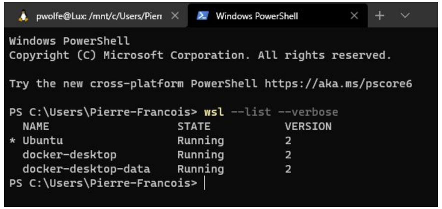
- Previously on Windows 10
  - Non-Pro → Docker Toolbox (deprecated)
  - Pro → Docker Desktop (using Hyper-V)
- Now on Windows 10
  - Anyone → Docker Desktop (WSL2)

Docker in WSL2


Windows
- Dev tools
- User utilities and scripts
- Other user customizations...
Docker Desktop
Deploys and update the WSL integration package
Bootstrapper
Control execution of Linux Daemons (start/stop/config...)
Lifecycle controller
Exposes the daemon to the Windows Docker CLI, handle bind mounts
Docker Proxy
CLI & plugins
DockerD (windows)
WSL VM
User Distribution
- Dev tools
- User utilities and scripts
- Other user customizations...
Manage execution of Linux Daemons
Docker Integration Package
Lifecycle server
DockerD
Kubernetes
Socket Forwarder
CLI & plugins
...
Forward connections to Linux Daemons

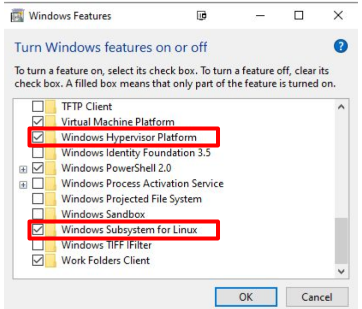
Image/reference: https://code.visualstudio.com/blogs/2020/03/02/docker-in-wsl2

WSL Distros & Versions



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Pierre-Francois> wsl --list --verbose
  NAME                   STATE           VERSION
* Ubuntu                 Running         2
  docker-desktop         Running         2
  docker-desktop-data    Running         2
PS C:\Users\Pierre-Francois> |
```

1. Features

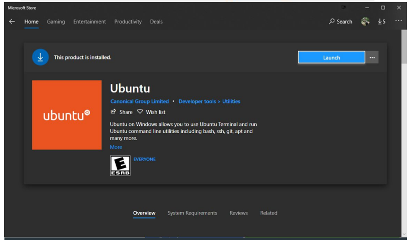


Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☐ TFTP Client
- ☑ Virtual Machine Platform
- ☑ Windows Hypervisor Platform
- ☐ Windows Identity Foundation 3.5
- ☑ Windows PowerShell 2.0
- ☐ Windows Process Activation Service
- ☐ Windows Projected File System
- ☐ Windows Sandbox
- ☑ Windows Subsystem for Linux
- ☐ Windows TIFF IFilter
- ☑ Work Folders Client

2. Linux



This product is installed.

Ubuntu

Canonical Group Limited • Developer tools > Utilities

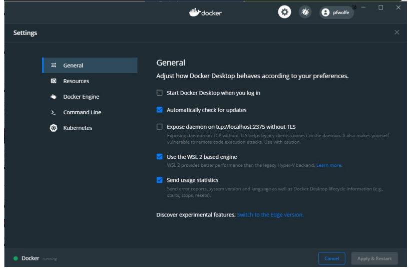
Share Wish list

Ubuntu on Windows allows you to use Ubuntu Terminal and run Ubuntu command line utilities including bash, ssh, git, apt and many more.

More

EVERYONE

3. Docker



General

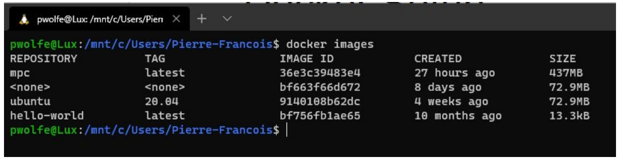
Adjust how Docker Desktop behaves according to your preferences.

- ☐ Start Docker Desktop when you log in
- ☑ Automatically check for updates
- ☐ Expose daemon on tcp://localhost:2375 without TLS
  Exposing daemon on TCP without TLS helps legacy clients connect to the daemon. It also makes yourself vulnerable to remote code execution attacks. Use with caution.
- ☑ Use the WSL 2 based engine
  WSL 2 provides better performance than the legacy Hyper-V backend. Learn more.
- ☑ Send usage statistics
  Send error reports, system version and language as well as Docker Desktop lifecycle information (e.g., starts, stops, resets).

Discover experimental features. Switch to the Edge version.

● Docker running

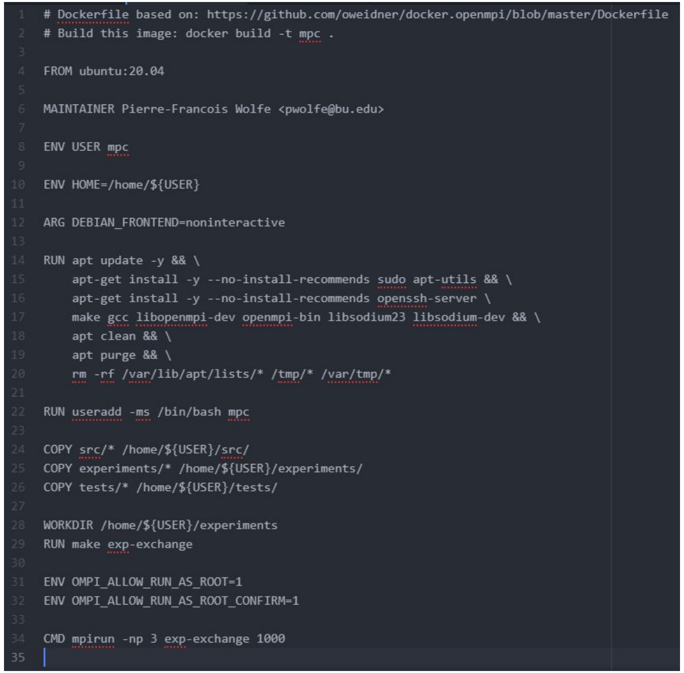
4. Terminal



```
pwolfe@Lux:/mnt/c/Users/Pierre-Francois$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
mpc                 latest              36e3c39483e4        27 hours ago        437MB
<none>              <none>              bf663f66d672        8 days ago          72.9MB
ubuntu              20.04               9140108b62dc        4 weeks ago         72.9MB
hello-world         latest              bf756fb1ae65        10 months ago       13.3kB
pwolfe@Lux:/mnt/c/Users/Pierre-Francois$ |
```

Dockerfile with MPC Dependencies

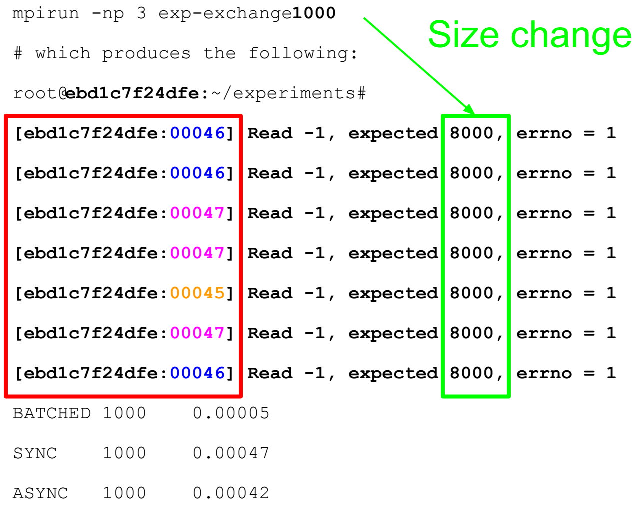
- Interactive testing
- Dockerfile creation
  - Reference MPI Dockerfile
  - Insights from interactive Docker
- OpenMPI
  - Prevents running as root
  - Solution 1:
    - --allow-run-as-root
  - Solution 2: (per: https://github.com/open-mpi/ompi/pull/5597)
    - OMPI_ALLOW_RUN_AS_ROOT=1
    - OMPI_ALLOW_RUN_AS_ROOT_CONFIRM=1
- Future Steps:
  - We already minimize RUN commands
  - Multi-stage build to copy only needed binaries: see https://docs.docker.com/develop/develop-images/multistage-build/



```
# Dockerfile based on: https://github.com/oweidner/docker.openmpi/blob/master/Dockerfile
# Build this image: docker build -t mpc .

FROM ubuntu:20.04

MAINTAINER Pierre-Francois Wolfe <pwolfe@bu.edu>

ENV USER mpc

ENV HOME=/home/${USER}

ARG DEBIAN_FRONTEND=noninteractive

RUN apt update -y && \
    apt-get install -y --no-install-recommends sudo apt-utils && \
    apt-get install -y --no-install-recommends openssh-server \
    make gcc libopenmpi-dev openmpi-bin libsodium23 libsodium-dev && \
    apt clean && \
    apt purge && \
    rm -rf /var/lib/apt/lists/* /tmp/* /var/tmp/*

RUN useradd -ms /bin/bash mpc

COPY src/* /home/${USER}/src/
COPY experiments/* /home/${USER}/experiments/
COPY tests/* /home/${USER}/tests/

WORKDIR /home/${USER}/experiments
RUN make exp-exchange

ENV OMPI_ALLOW_RUN_AS_ROOT=1
ENV OMPI_ALLOW_RUN_AS_ROOT_CONFIRM=1

CMD mpirun -np 3 exp-exchange 1000

```

MPC in Docker Container Debugging...

- Running tests.sh → OK
- Running exp-exchange
  - Issue with size greater than 505… ex: with 1000
  - Cryptic message…
- Determine source…
  - Some clues but overall meaning still unclear



```
mpirun -np 3 exp-exchange1000
# which produces the following:
root@ebd1c7f24dfe:~/experiments#
[ebd1c7f24dfe:00046] Read -1, expected 8000, errno = 1
[ebd1c7f24dfe:00046] Read -1, expected 8000, errno = 1
[ebd1c7f24dfe:00047] Read -1, expected 8000, errno = 1
[ebd1c7f24dfe:00047] Read -1, expected 8000, errno = 1
[ebd1c7f24dfe:00045] Read -1, expected 8000, errno = 1
[ebd1c7f24dfe:00047] Read -1, expected 8000, errno = 1
[ebd1c7f24dfe:00046] Read -1, expected 8000, errno = 1
BATCHED 1000     0.00005
SYNC     1000     0.00047
ASYNC    1000     0.00042
```

Size changes value

[Hostname:PID]

Debugging Technique

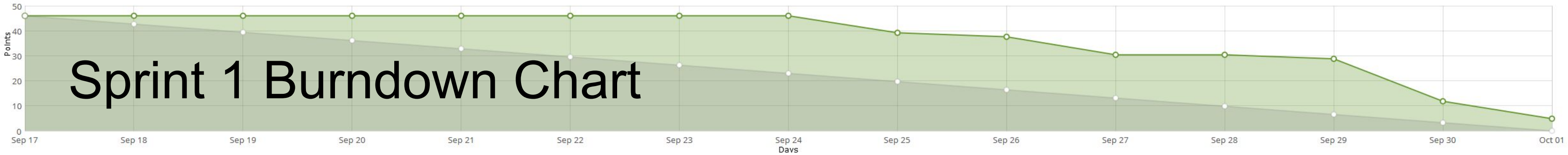
Rank 0 → main party
Rank 1,2 → parties 2,3

- Code snippet entry point
  - Modify rank to attach to specific process
  - pid will print
- Attach with GDB using pid
- Change val i to continue
- Step through program
- Identify functions:
  - generate_and_share_random_data
  - exchange_rsz_seeds
  - exchange_shares_array
- MPI_Send/MPI_Recv pairs
  - 4, 1, and 2 respectively

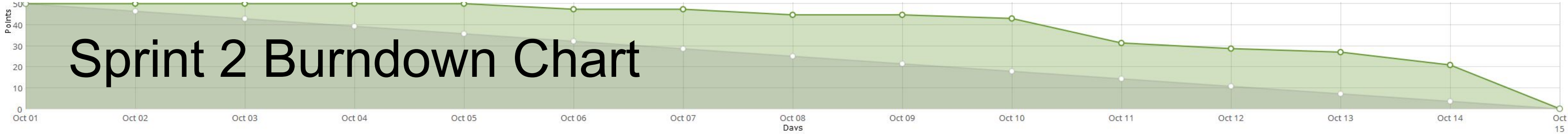
```
# From: https://www.open-mpi.org/faq/?category=debugging

If (rank == 0) {

    volatile int i = 0;

    char hostname[256];

    gethostname(hostname, sizeof(hostname));

    printf("PID %d on %s ready for attach\n", getpid(), hostname);

    fflush(stdout);

    while (0 == i)

        sleep(5);

}
```

Changing rank to inspect different parties → message appears when the MPI_Recv is evaluated..

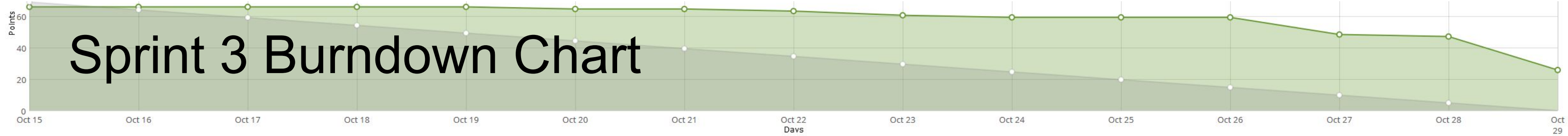
Sprint Demo



Sprint 1 Burndown Chart



Sprint 2 Burndown Chart



Sprint 3 Burndown Chart

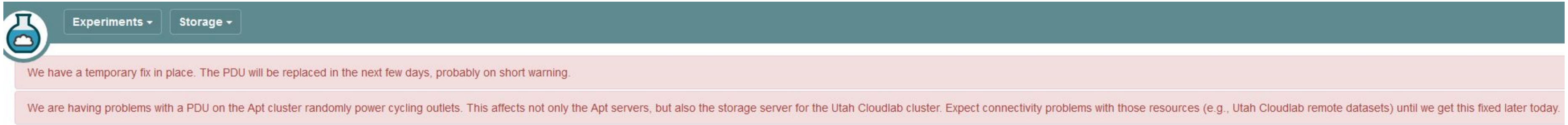
Sprint 4 - Some Known Stories

- VMs -
  - As a researcher, I want to improve the existing test instrumentation in order to more easily collect extra data samples, especially for large message sizes.
  - As a team member, I want to further explore the tracing and profiling outputs from Score-p to determine how to best assess performance.
- Containers -
  - As a team member, I want to fix issues with OpenMPI when running exp-exchange in docker to move closer to a local multi-container test and OpenShift deployment.
- Bare Metal -
  - As a team member, I want to make some improvements to my geni-lib script in order to refine my test environment and be able to capture more exp-exchange data runs
  - As a team member, I want to employ my geni-lib insights to create custom environments for testing OpenStack and OpenShift on CloudLab

Thank you

...any questions?

Backup Slides



We have a temporary fix in place. The PDU will be replaced in the next few days, probably on short warning.

We are having problems with a PDU on the Apt cluster randomly power cycling outlets. This affects not only the Apt servers, but also the storage server for the Utah Cloudlab cluster. Expect connectivity problems with those resources (e.g., Utah Cloudlab remote datasets) until we get this fixed later today.

It seems there is an ongoing issue with CloudLab