Secure Multiparty Computation
Sprint 2

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

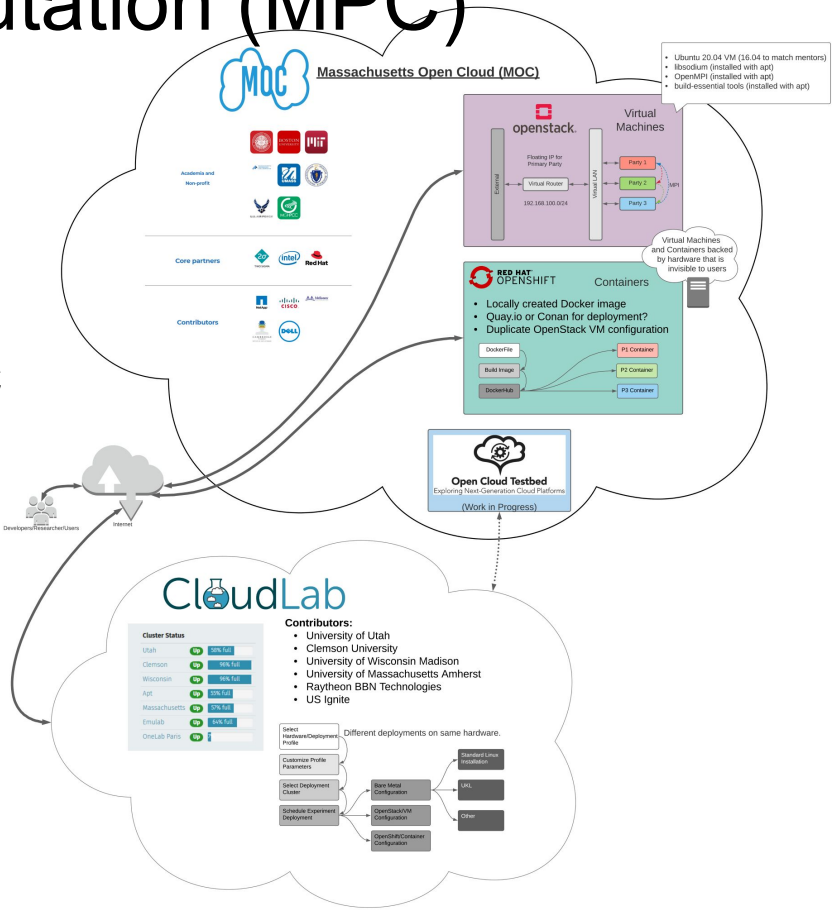
BOSTON UNIVERSITY

Presentation Outline

- Project Recap
- Project Goals & Sprint 2 Stories/Tasks
- Work Accomplished & Information Learned
  - Mentor MPC result recreation
  - Profiling Tools exploration (C, and MPI)
  - OpenShift Container deployment progress
  - CloudLab bare metal deployment progress
- Project Organization Assessment (Burndown)
- Sprint 3 goals (Mentor priorities)

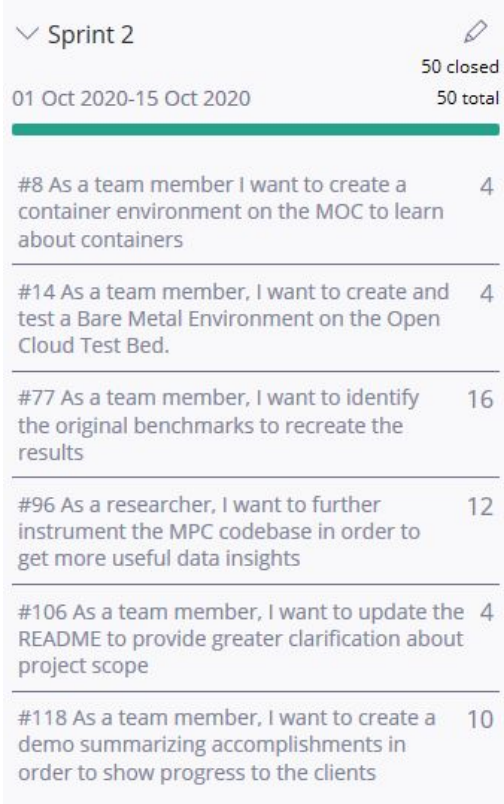
Recap of Multi-Party Computation (MPC)

- 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



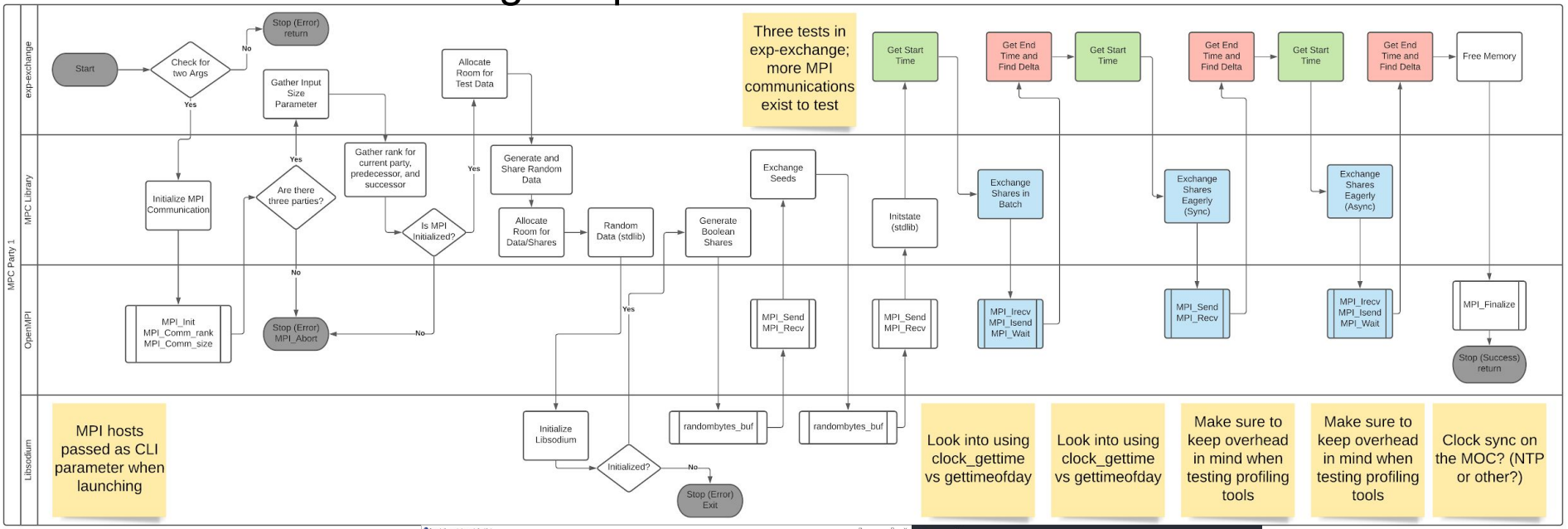
Project Goals & Sprint 2 Stories/Tasks

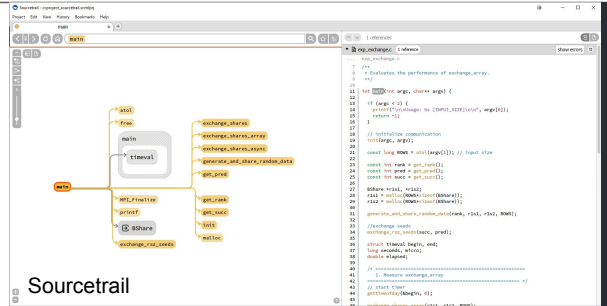
- Understand and recreate original test
  - Perform on working VM environment
  - Analyze new vs old results
- Continue efforts to prepare containers to support MPC codebase
- Continue efforts to prepare bare metal deployment for MPC codebase
- Clarify scope/focus with mentors and refine project plan
- Explore additional code instrumentation and profiling/benchmarking tools



BOSTON UNIVERSITY

Test Focus - Exchange Experiments





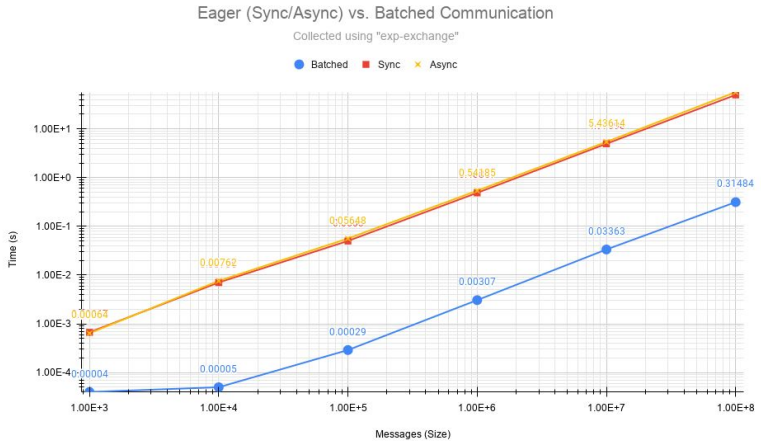
Boston University CS & ECE

BOSTON UNIVERSITY

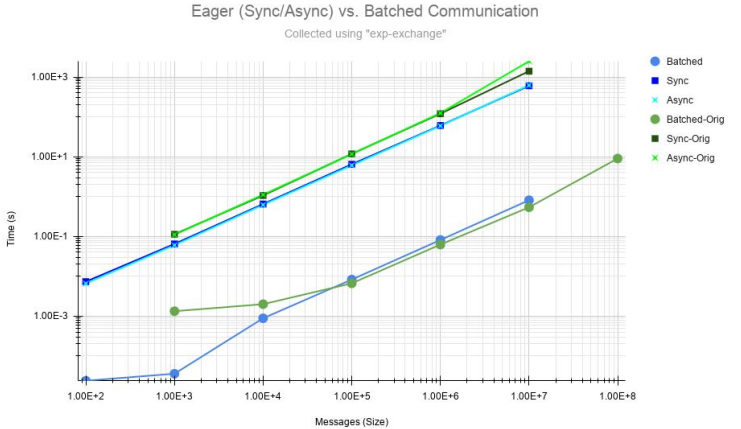
Mentor MPC Result Recreation

- Exp-exchange test
  - MPI batch (async)
  - MPI eager (sync)
  - MPI eager (async)
- All Tests (Local, Orig VM, New VM)
  - VMs similar performance
  - Local test (slightly) faster
  - Same trend with message size
- Notes:
  - Improve instrumentation (i.e. consider clock used, data output)
  - More data points to probe MPI behavior

Local Desktop Single Node Test

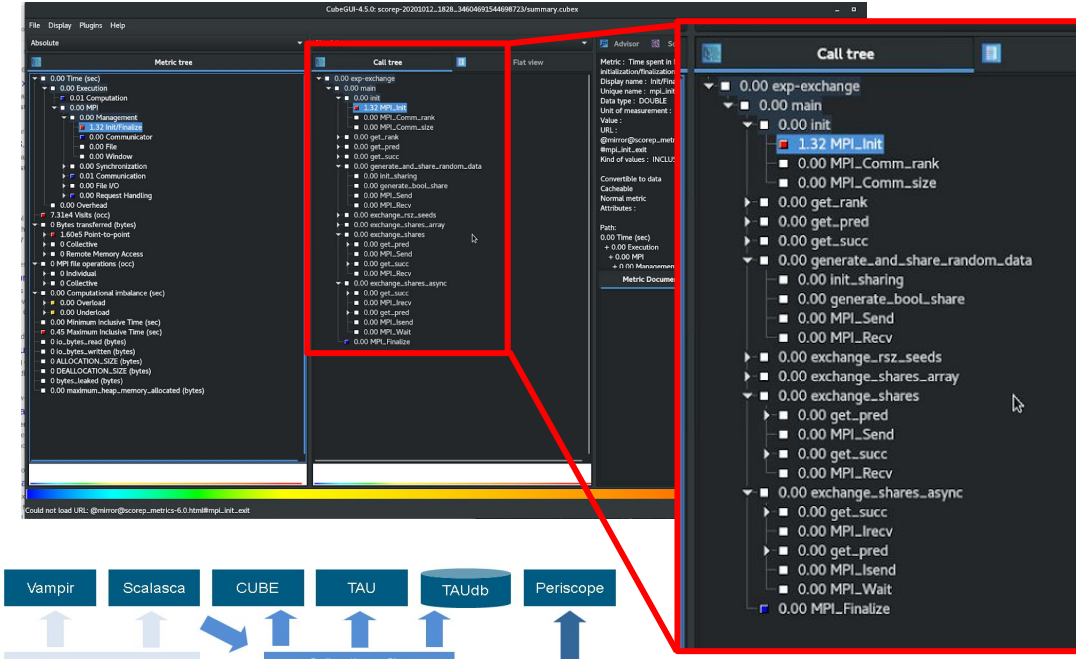


Mentor MOC VM Test vs New MOC VM Test



Profiling Tools Exploration

- Performance Analysis
  - Tracing: Event History (often with timeline)
  - Profiling: Aggregated runtime statistics
- Gotcha's
  - Be wary of overhead…
- Challenge
  - Lots of different tools to consider/explore...



*.cubex profile data in Scalasca

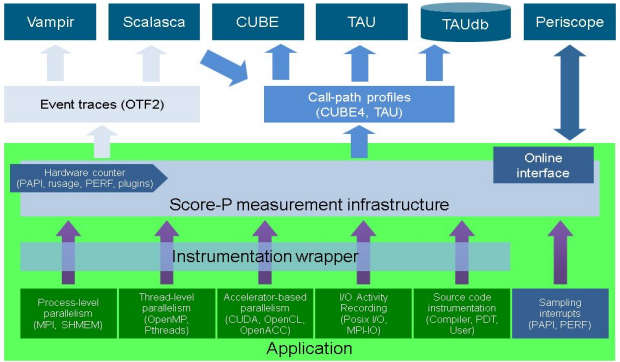


Image source: http://scorepci.pages.jsc.fz-juelich.de/scorep-pipelines/docs/scorep-6.0/html/index.html

BOSTON UNIVERSITY

OpenShift Deployment Progress

In the previous sprint:

- Tried using OpenShift Web Console / CLI to deploy our C-based-application.
- Failed, because the ‘builder images’ that use OpenShift s2i to deploy applications directly from the SCM are only available for **web applications.**
- Decided to use ‘Conan’
  - A C/C++ package manager that also works as a ‘builder image’
  - Feed the C code and builder image to OpenShift s2i, Openshift makes the deployment right away!
  - Conan accelerates C/C++ applications in Openshift.

BOSTON UNIVERSITY

OpenShift Deployment Progress

In this sprint:

- Generated Conan Builder image
  - Includes Conan, Gcc, make, etc.
- Deployed a sample application on OpenShift, created using OpenShift s2i and Conan builder image.
- **Problem**: Size of Container is huge ~300 to 400 Mbs, while application is just in kb's. -- much of space is still being occupied by things not used by application

OpenShift Deployment Progress

In this sprint:

- Rollback:-
  - Create a Dockerfile for a container that contains the specified **linux, gcc, code.**
  - Instantiate this container, open bash, install dependencies, compile the source code and libraries to **obtain executable binaries.**
  - Download the binaries off of the container.
  - Instantiate another linux container, without gcc and other unneeded libraries. Copy executable binaries into it, using the dockerfile.
  - And we have a light-weight container running our application.

CloudLab Bare Metal Deployment Progress

1.Single-bare-metal profile selection & Parameterization.

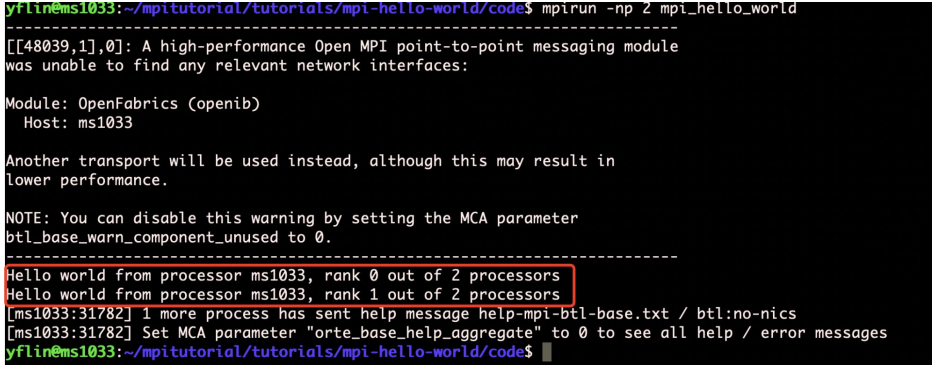
2.Provisioning the profile.

3.Connect node with SSH.

4.Install dependencies required for test code.

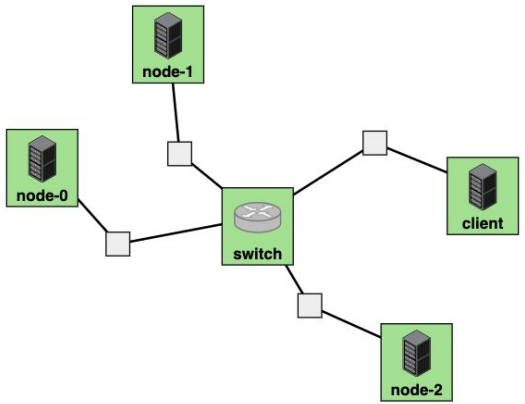
5.Tested basic MPI functionality on single-bare-metal node.

6. Future work expected: More MPI communications tested between nodes.



BOSTON UNIVERSITY

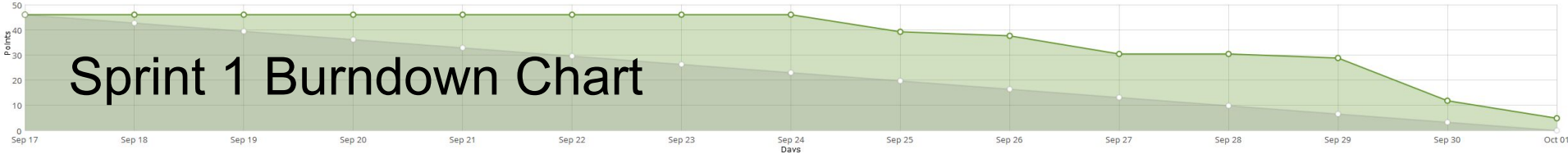
Multi-bare-metal Deployment Progress

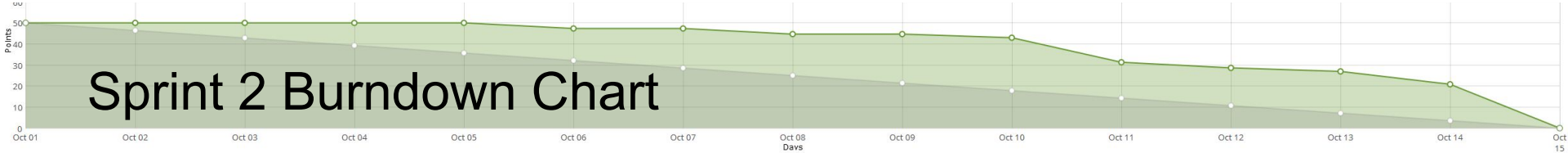


Topology View | List View | Manifest | Graphs

ID	Node	Type	Status	Startup	Image	SSH command (if you provided your own key)
node-0	hp067	xl170	ready	n/a	emulab-ops/UBUNTU14-64-STD	ssh -p 22 Suli@hp067.utah.cloudlab.us
node-1	hp056	xl170	ready	n/a	emulab-ops/UBUNTU14-64-STD	ssh -p 22 Suli@hp056.utah.cloudlab.us
node-2	hp055	xl170	ready	n/a	emulab-ops/UBUNTU14-64-STD	ssh -p 22 Suli@hp055.utah.cloudlab.us
client	hp072	xl170	ready	n/a	emulab-ops/UBUNTU14-64-STD	ssh -p 22 Suli@hp072.utah.cloudlab.us
switch	hp041	xl170	ready	n/a	emulab-ops/UBUNTU14-64-STD	ssh -p 22 Suli@hp041.utah.cloudlab.us

```
finiband_verbs/uverbs3
libibverbs: Warning: no userspace device-specific driver found for /sys/class/in
finiband_verbs/uverbs2
libibverbs: Warning: no userspace device-specific driver found for /sys/class/in
finiband_verbs/uverbs1
libibverbs: Warning: no userspace device-specific driver found for /sys/class/in
finiband_verbs/uverbs0
Hello world from processor node-0.bmtest4.mpcproject-pg0.utah.cloudlab.us, rank
0 out of 3 processors
Hello world from processor node-0.bmtest4.mpcproject-pg0.utah.cloudlab.us, rank
1 out of 3 processors
Hello world from processor node-0.bmtest4.mpcproject-pg0.utah.cloudlab.us, rank
2 out of 3 processors
[node-0.bmtest4.mpcproject-pg0.utah.cloudlab.us:19600] 2 more processes have sen
t help message help-mpi-btl-base.txt / btl:no-nics
[node-0.bmtest4.mpcproject-pg0.utah.cloudlab.us:19600] Set MCA parameter "orte_b
ase_help_aggregate" to 0 to see all help / error messages
Suli@node-0:~/mpitutorial/tutorials/mpi-hello-world/code$
```





- Observations:
  - Apparent Sprint 2 burndown delay
    - Team backlog grooming not shown
    - Formal planning poker session 10/3 not shown
  - Still need to work on the habit of updating tasks as they progress
  - The MPI and Profiling stories changed which delayed progress
  - Realized that some stories should be split and moved to backlog
  - More improvement is needed but the planning poker did help planning
  - The mentors were pleased with the replicated tests

BOSTON UNIVERSITY

Sprint 3 - 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 perform an initial MPC test on containers in order to progress towards reproducing the exp-exchange test with this deployment approach.
- Bare Metal -
  - As a team member, I want to perform an initial MPC test on multiple bare metal nodes in order to progress towards reproducing the exp-exchange test with this deployment approach
  - As a team member, I want to work on recreating OpenStack and OpenShift environments on bare metal nodes for more comparable test results

Thank you

...any questions?

BOSTON UNIVERSITY