

# 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

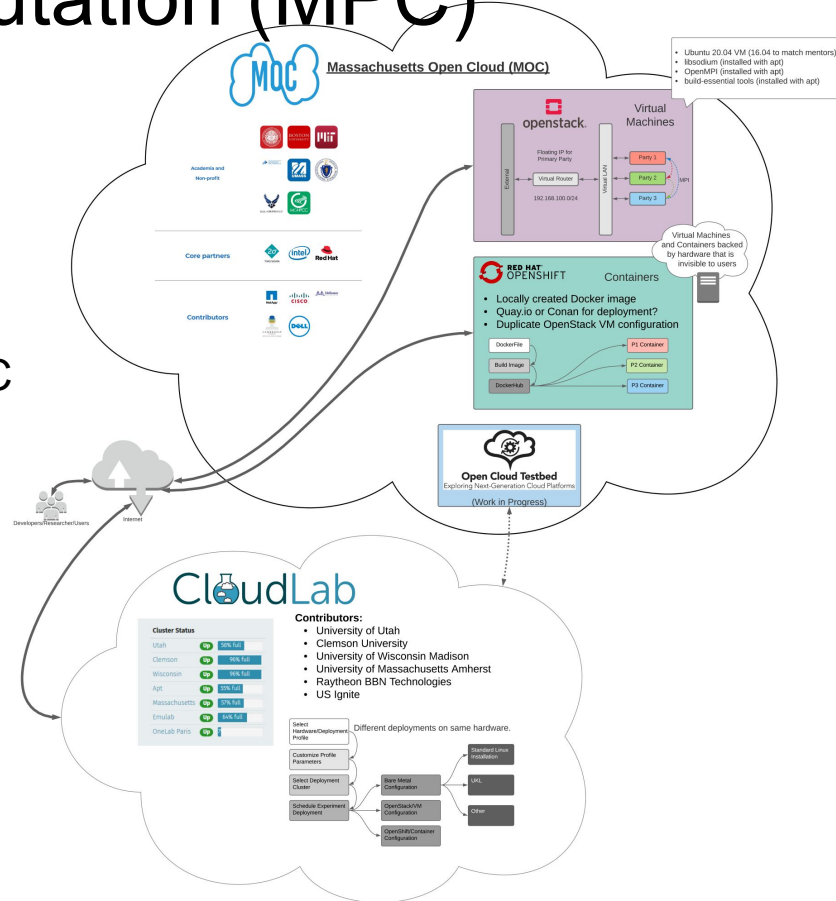
# Presentation Outline

- 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

Boston University CS & ECE



# 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

## ▼ Sprint 2



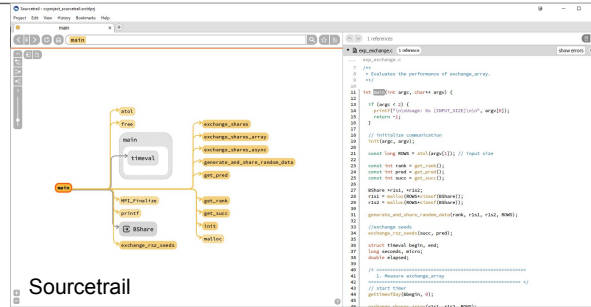
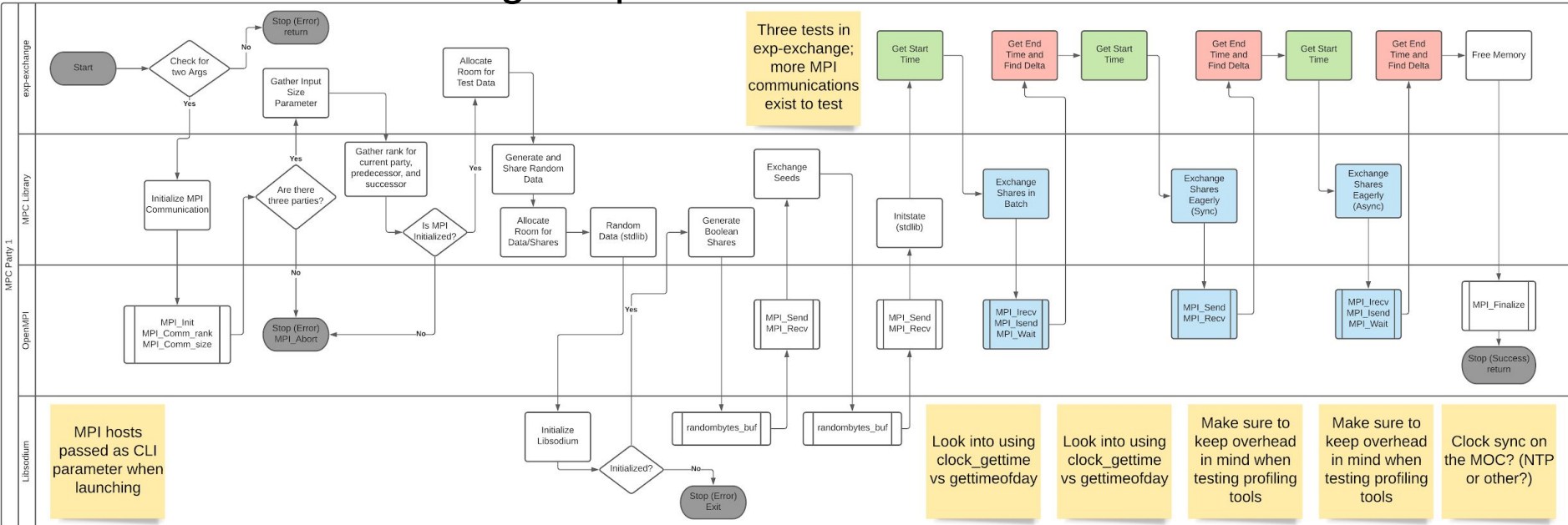
50 closed

01 Oct 2020-15 Oct 2020

50 total

#8 As a team member I want to create a container environment on the MOC to learn about containers	4
#14 As a team member, I want to create and test a Bare Metal Environment on the Open Cloud Test Bed.	4
#77 As a team member, I want to identify the original benchmarks to recreate the results	16
#96 As a researcher, I want to further instrument the MPC codebase in order to get more useful data insights	12
#106 As a team member, I want to update the README to provide greater clarification about project scope	4
#118 As a team member, I want to create a demo summarizing accomplishments in order to show progress to the clients	10

## Test Focus - Exchange Experiments



```

40  /*
41      1. Measure exchange_array
42      =====
43      // start timer
44      gettimeofday(&begin, 0);
45
46      exchange_shares_array(r1s1, r1s2, ROWS);
47
48      // stop timer
49      gettimeofday(&end, 0);
50      seconds = end.tv_sec - begin.tv_sec;
51      micro = end.tv_usec - begin.tv_usec;
52      elapsed = seconds + micro*1e-6;
53
54      if (rank == 0) {
55          printf("BATCHED\t%d\t%.5f\n", ROWS, elapsed);
56      }
57  */

```

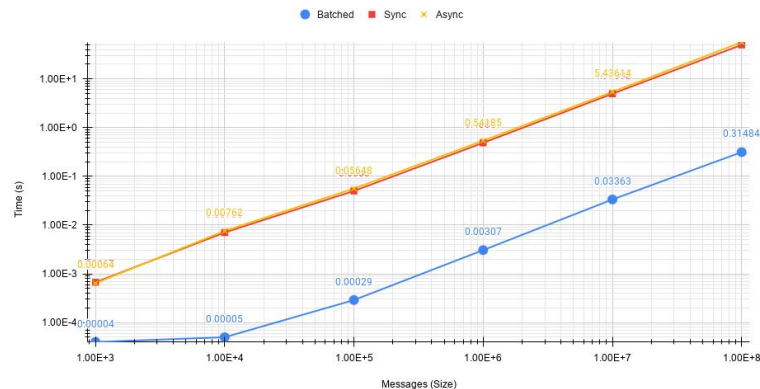
## Mentor MPC Result Recreation

- 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

Eager (Sync/Async) vs. Batched Communication

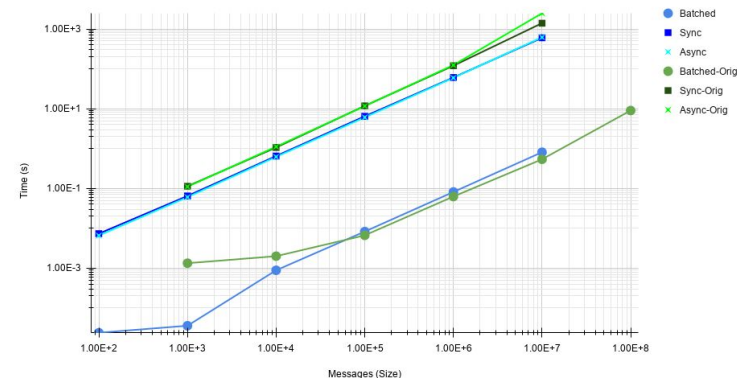
Collected using "exp-exchange"



## Mentor MOC VM Test vs New MOC VM Test

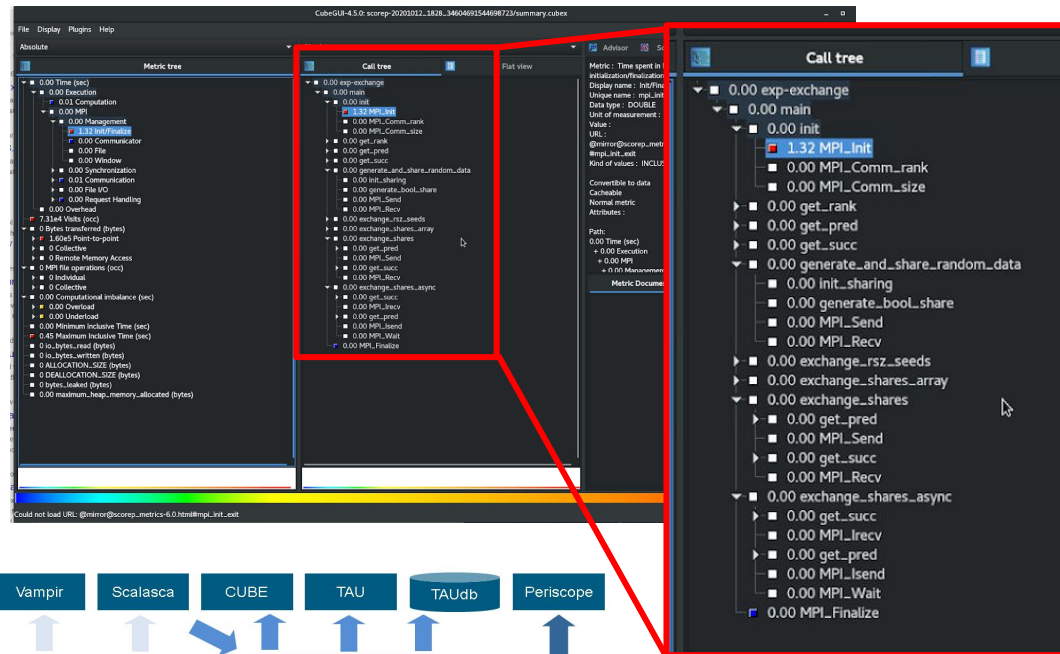
Eager (Sync/Async) vs. Batched Communication

Collected using "exp-exchange"

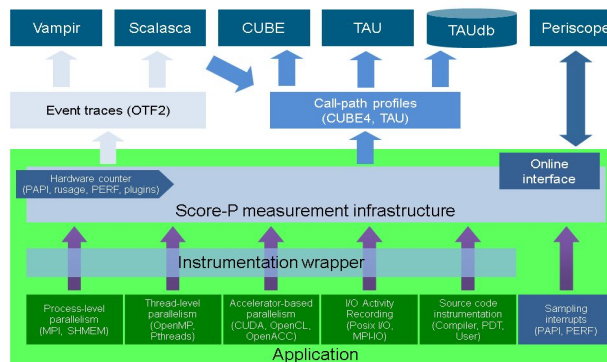


# Profiling Tools Exploration

- 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



# 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.





# 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.

The screenshot shows the CloudLab web interface. On the left, under 'Default Profiles +', the 'Single-bare-metal' profile is selected. Below it, under 'Other Profiles -', are 'spark-bare-metal', 'centos-n-bare-metal', '4-Bare-Metal-Ubuntu\_1604 dcsc-boulder', and 'five-bare-metal'. On the right, the details for 'Single-bare-metal' are displayed:

Created By:	fzhan
Project:	SuperPages
Latest Version:	0
Last Updated:	2016-04-19 13:03:46
Description:	A single bare-metal node for experiment

```
yflin@ms1033:~/mpitutorial/tutorials/mpi-hello-world/code$ mpirun -np 2 mpi_hello_world
[[48039,1],0]: A high-performance Open MPI point-to-point messaging module
was unable to find any relevant network interfaces:

Module: OpenFabrics (openib)
Host: ms1033

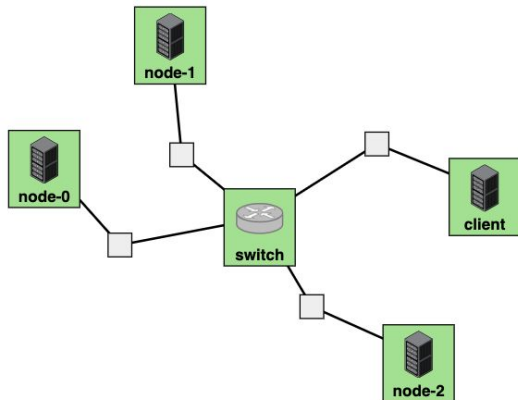
Another transport will be used instead, although this may result in
lower performance.

NOTE: You can disable this warning by setting the MCA parameter
btl_base_warn_component_unused to 0.

-----
Hello world from processor ms1033, rank 0 out of 2 processors
Hello world from processor ms1033, rank 1 out of 2 processors
[ms1033:31782] 1 more process has sent help message help-mpi-btl-base.txt / btl:no-nics
[ms1033:31782] Set MCA parameter "orte_base_help_aggregate" to 0 to see all help / error messages
yflin@ms1033:~/mpitutorial/tutorials/mpi-hello-world/code$
```



# 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	<code>ssh -p 22 Suli@hp067.utah.cloudlab.us</code>
node-1	hp056	xl170	ready	n/a	emulab-ops/UBUNTU14-64-STD	<code>ssh -p 22 Suli@hp056.utah.cloudlab.us</code>
node-2	hp055	xl170	ready	n/a	emulab-ops/UBUNTU14-64-STD	<code>ssh -p 22 Suli@hp055.utah.cloudlab.us</code>
client	hp072	xl170	ready	n/a	emulab-ops/UBUNTU14-64-STD	<code>ssh -p 22 Suli@hp072.utah.cloudlab.us</code>
switch	hp041	xl170	ready	n/a	emulab-ops/UBUNTU14-64-STD	<code>ssh -p 22 Suli@hp041.utah.cloudlab.us</code>

```

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

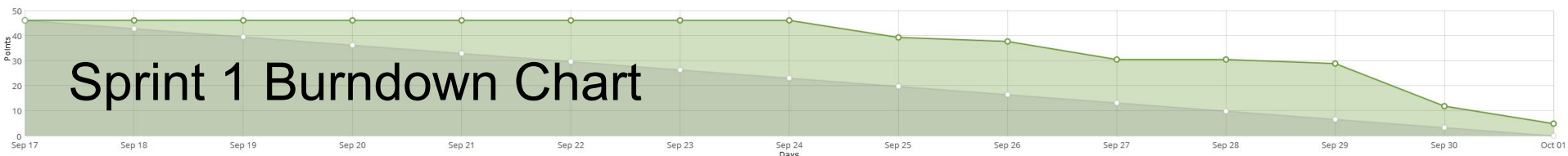
```

```

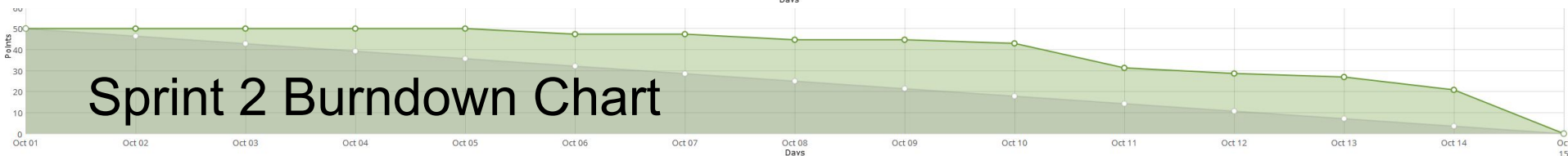
[node-0.bmtest4.mpcproject-pg0.utah.cloudlab.us:19600] 2 more processes have sen
t help message help-mpi-btl-base.txt / btl:no-nics
[node-0.bmtest4.mpcproject-pg0.utah.cloudlab.us:19600] Set MCA parameter "orte_b
ase_help_aggregate" to 0 to see all help / error messages
Suli@node-0:~/mpitutorial/tutorials/mpi-hello-world/code$

```

## Sprint 1 Burndown Chart



## Sprint 2 Burndown Chart



- 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



## 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?