Fermilab

Computing Division

Lessons Learned

Build Service

Version 0.1
July 18, 2014

DocDB #

PREPARED BY:
Steve Jones

<Official copy is maintained electronically – printed copy may be obsolete>

Lessons Learned Approvals

Name	Signature	Date

Table of Contents

1. ATTENDEES 1

2. FEEDBACK RECEIVED 1

A. PROJECT TEAM FEEDBACK 1

B. USER FEEDBACK 1

3. WHAT WAS DONE WELL 3

4. WHAT COULD HAVE BEEN DONE BETTER 3

1. Attendees

ATTENDEE NAME	ROLE
Glenn Cooper	Technical Lead/Architect
Steve Jones	Project Manager
Patrick Gartung	Developer
Seth Graham	Developer
Marc Mengel	Developer
Ed Simmonds	Assistant Technical Lead

2. Feedback Received

A. Project Team Feedback

NAME / ROLE	COMMENT	PHASE
Teamwork		
Steve Jones	The team worked together extremely well. There was good communications, cooperation and feedback between team members in developing requirements, testing and setting up the Jenkins Build Service. The planning was realistic and based on the availability of the resources supporting the project.	All
<Topic>		
<Topic>		
<Topic>		

B. User Feedback

NAME / ROLE	COMMENT	PHASE
Copy Parts of Jobs		
Lynn Garren	Develop a means add credentials to the job to allow parts of the job to be copied. Team agrees and is working on this. Looking into how to manage credentials. Send x509 cert with job suggested by Marc Mengel. May need to have space on master for artifacts (1-2 TB) which is simple- move master or start slave on your node when you need one.	Post Go Live

NAME / ROLE	COMMENT	PHASE
Security		
Adam Lyon	Improved security needs to be added. This was a known risk. From Adam: “With my laptop connected as a slave, anyone logged into Jenkins can then run commands on it. And those commands can do anything, including writing and deleting files in my home area. Is there a way to run the slave in some restricted mode so that it can only read/write files in its workspace? And perhaps turn off or restrict access to the direct Groovy prompt. Can we immediately restrict the Jenkins web server to on-Fermilab-site access? So you'll need VPN for use offsite (sorry Brett). Then we can figure out something more sensible.” Brett Viren: “Definitely run the slave in a dedicated, unprivileged account. And, thanks, this reminds me I need to request such an account here. We have talked about access controls in the past. My understanding that only "a few" (order 1) people from any experiment or project be able to initiate jobs (or set up their triggers). I can't remember if there was further segmentation possible so that they could only initiate jobs on certain slaves, but that would be welcome. I'm for adding access control, but I would be very unhappy with a VPN. Simply limiting access to FNAL networks doesn't solve any problem, it just somewhat shrinks it and it would hugely reduce functionality for anyone not on such networks. I'm glad to see that there are plans for https+password and/or certificate-based access control. I think that's a much better solution.” The team is continuing to evaluate and address this issue. Steps taken so far: • Redirecting to https. • Have a host certificate • Can use anonymous access to see status, download tar files (if any)	Post Go Live

3. What Was Done Well

WHAT WAS DONE WELL	PHASE
1. Teamwork (see above)	All
2.	

4. What Could Have Been Done Better

WHAT COULD HAVE BEEN DONE BETTER	PHASE
1.	
2.	
3.	