OSG Security Team

OSG Staff Retreat

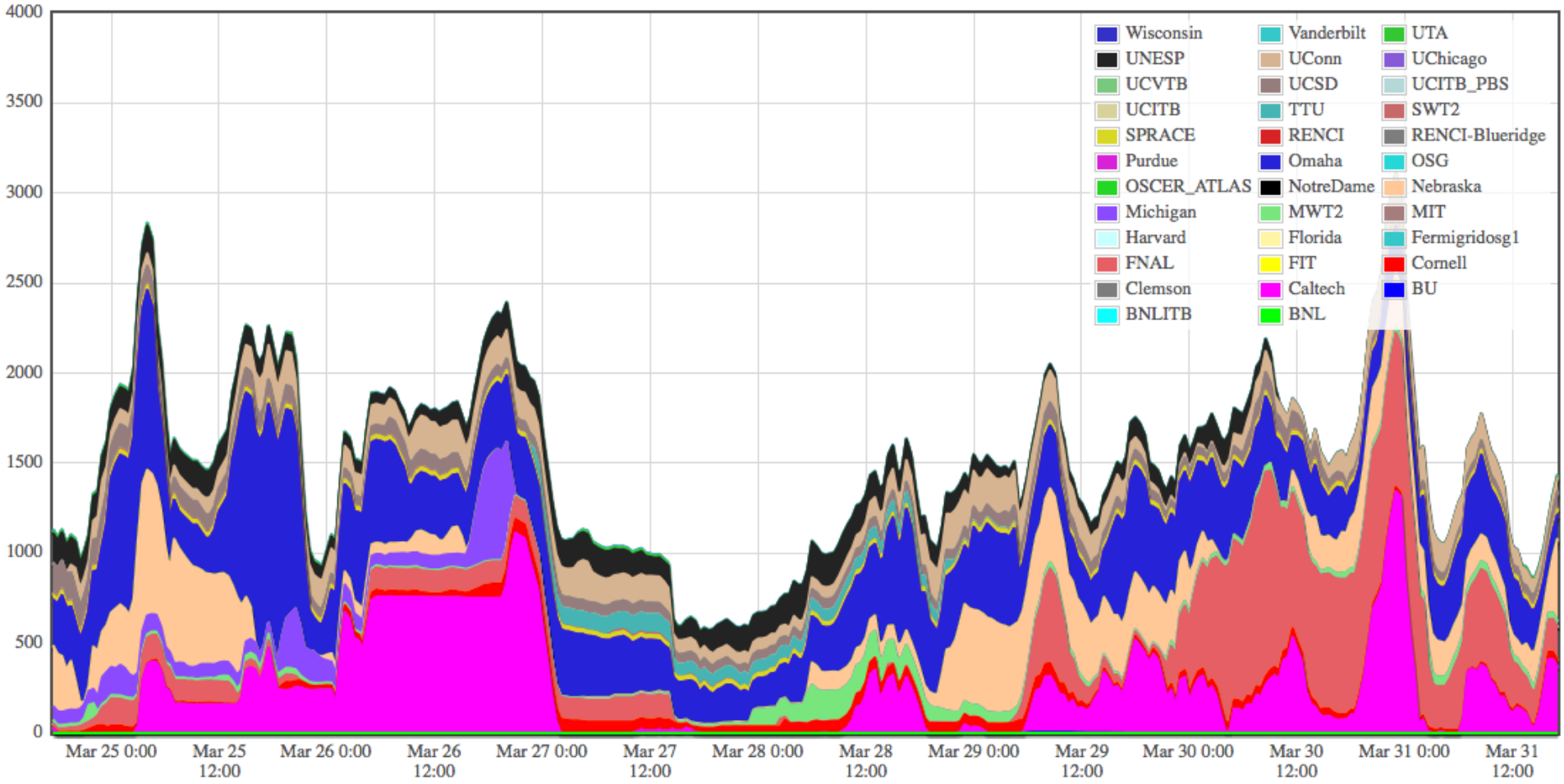
May 18-19

Wisconsin, Madison

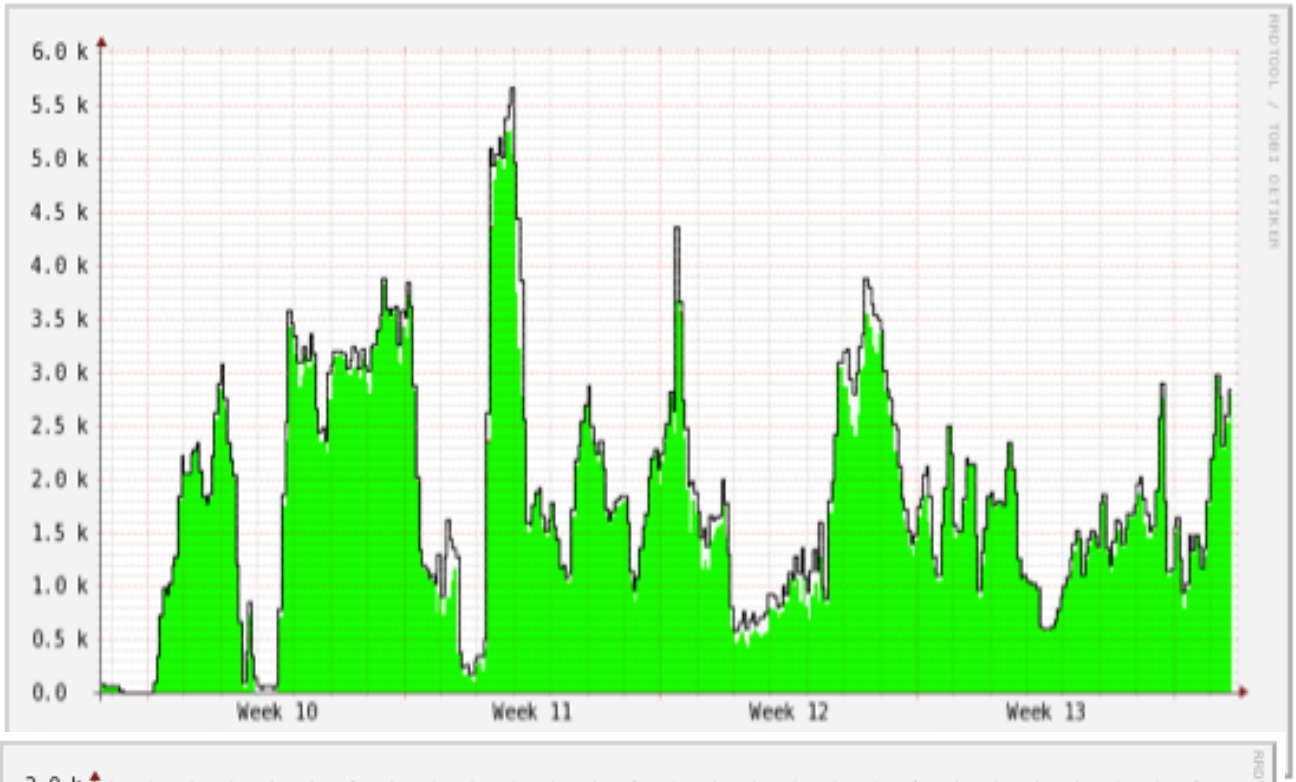
A review of the last year Accomplishments May 2014-May 2015

- Traceability project
  - Ability to send user jobs without the end user certificates while maintaining the user traceability.
  - Made a risk assessment of the existing system, proved that we can still trace jobs to users even without the user certificates
  - FNAL accepted our findings and they started allowing jobs from HCC, GLOW and XSEDE.
    - With GLOW we only allow jobs coming from CHTC-managed submit nodes.

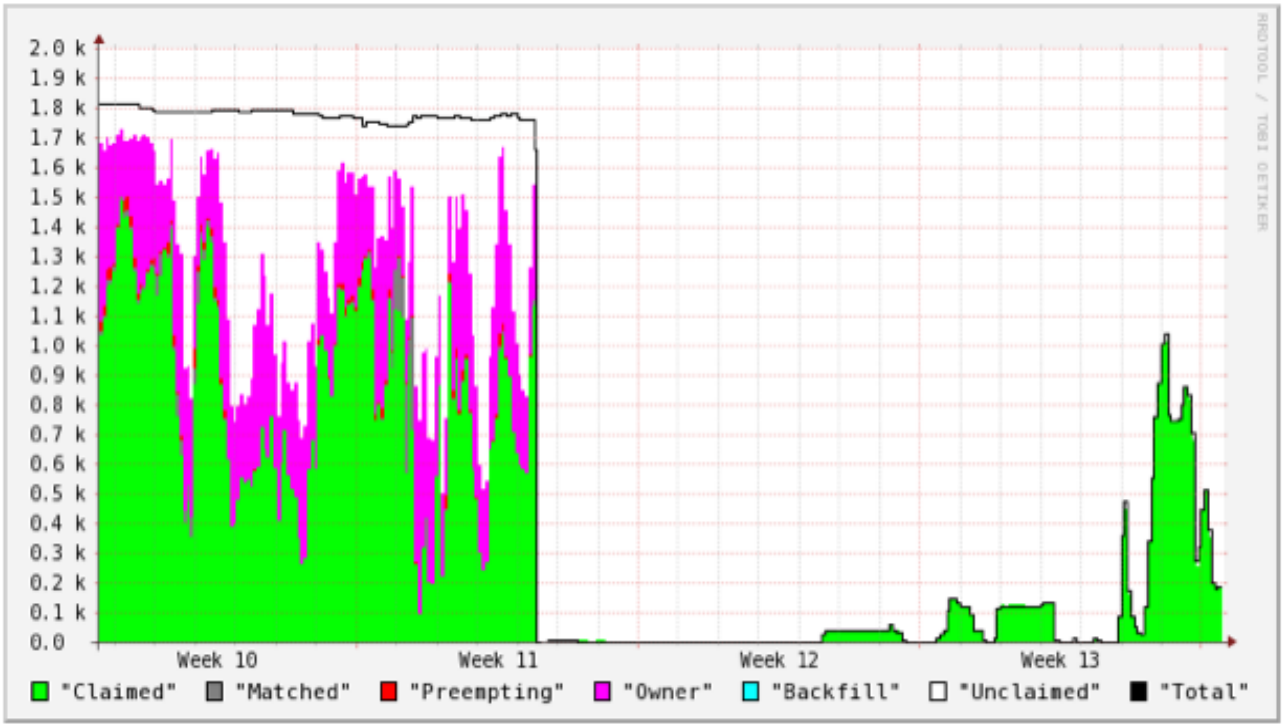
Glow VO Job Stats



- Number of Glideins from Glow running on all OSG sites.
- The dark salmon color is FNAL, not SWT2.
- The number of jobs running on FNAL increasing



Glow Glideins at all OSG sites during the last month



Glow Glideins at FNAL during the last month

Disregard data before week11.
We started on FNAL at week 11
FNAL providing a significant amount of Glideins for Glow

Accomplishments

- Created an identity roadmap for after our contract with DigiCert expires.
  - What would happen to OSG stakeholders if we stop to provide certificates?
  - Can we get certificates somewhere other than DigiCert?
  - Created a short-term roadmap, **OSG-doc-1185,**
- As a result of the roadmap, we started experimenting with CILogon HSM service

Accomplishments

- CILogon OSG Pilot Project
  - Collaborated with GOC staff to complete a prototype service, which we completed by June.
  - Very successful experience
  - Wrote an MOU and sought collaboration with XSEDE

Accomplishments: Operational Security

- Very busy year with serious vulnerabilities.
- Heartbleed, Poodle, PerfSonar, xrootd, bash, HTCondor and dCache vulnerabilities to name a few
- Bitcoin mining incidents on EGI made us launch a project on awareness
  - Contacted all VO managers and asked them to emphasize to their users that these activities are not allowed on OSG
  - Audited the VOs:
    - Whether they have an AUP and their users sign and understand the AUP
    - We tested by selecting a random user and checking if they signed the AUP.
    - Results were promising, all the VOs were doing their job.
    - All heavy-usage VOs successfully passed our audit: Alice, Atlas, CMS, STAR, CDF, Nanohub, DZero, GlueX, LBNE, Nova, Minos, Mars, Mu2e, OSG, HCC, Glow.
    - We had some issues with smaller VOs such as: GPN, Geant. Given the small amount of activity from these VOs, we are very satisfied with our findings. https://twiki.grid.iu.edu/bin/view/Security/VOAUPSurvey

Accomplishments: Operational Security

- Received a request from WLCG to implement/ install a central bannign service.
  - After reviewing, we decided to reject the request
  - Most our sites accept jobs without end user certs,
  - Even if we had a banning service, we cannot ban any users because there is no user certs
  - We can ban select few pilot credentials, but it is very rare to have pilot certs compromised.
  - With our current direction to get rid of certs or make them transparent, banning service will not be useful to us.

Accomplishments: Operational Security

- Did an incident drill with HT-Condor CE. Thanks to Nebraska for their support. Nothing major to report
- We will also do an incident drill with OASIS service last week of May.
- Finished all the security controls except for the Campus Grids.
  - We met with Dave Champion later at All hands meeting and did a verbal assessment.
  - We also agreed to do a real incident drill with OSG Connect. Looking forward to it.

Future Projects: OSG Certificate Service

- After our successful prototype, we started the OSG Certificate Service officially in December
- Main project hub is at https://twiki.grid.iu.edu/bin/view/Security/OSGCATransitionToCILogonHSM
- Phases:
  - Planning, Development, Testing, IGTF Accreditation, Deployment, and Transition

OSG Certificate Service

- Completed the Planning and Development phases ahead of the schedule
- Currently in Testing Phase, which should end by 6/30/2015.
- After Testing completes, we will send a report to OSG Managament in mid-July.

Testing Phase

	Testers	Status
CA Functionality	Kevin, Neha	Done. No Issues.
OSG Software	Brian Lin, Garhan, Horst, Neha, Suchandra, Xin	70% Done. Expected completion date - 05/31/15
OSG Services	Alain D., DCSO (@FNAL) , Jeff, Mat, Neha, Scott, Suchandra	Just started
VO Software	CMS - CRAB (Eric V.) WMAgent (Krista, Seangchen) ATLAS - John H.	Cannot test until CA makes it in to IGTF bundle
Fermilab-owned Services	TBD	Not started

Issues found so far

- Changes required to OSG Software

HTCondor CE

Add following to /etc/condor-ce/condor_mapfile

GSI "^\/DC\=org\/DC\=opensciencegrid\/O=Open Science Grid\/OU\=Services\/CN\=(host\/)?([A-Za-z0-9.\-]*)$" \2@daemon.opensciencegrid.org

vo-client

/etc/grid-security/vomsdir/[VO]/*.lsc file/s will need to have DNs for new host/service and CA cert

- Policy/Procedure

Issue: CA software upgrade on Apr 21 resulted in certificates issued with 1 day lifetime

Cause: integer overflow in some new MyProxy code that wasn't tested for long-lived certificates

Remedy: Create a change management process between CILogon and OSG

IGTF Accreditation

- Encouraged by our progress, we sped up our process and decided to go for our accreditation in May 27th. We originally planned around October TAGPMA meeting.
- It is an important undertaking and has been our top priority.
- Spent lots of effort to make sure we can pass it on our first try with no issues.
- Typically this is a 6-9 months end-end process. We decided in April, so it is a bit ambitious to seek accreditation in May given we have never done this before.

OSG Certificate Service: Going forward

- As soon as testing ends, we will write a report for OSG management.
  - Identify all changes to OSG policy and procedures.
  - Continue answering to IGTF queries.
- After we receive our Accreditation in the summer,
  - Immediately start testing CMS and Atlas services
  - We could not test them because some of the CMS and Atlas services such as VOMS Admin does not have an ITB version that accepts an unaccredited CA.
  - VO representatives decided to wait until we receive accreditation.

DEPLOYMENT PHASE	LEAD	DURATION	START	END
	Altunay	61 days	10/9/15	1/1/16
Update/Execute Communication Plan	Clemmie	1 day	10/9/15	10/9/15
Distribute new IGTF bundle to OSG stakeholders	Padmanabhan	10 days	10/12/15	10/23/15
Wait for first wave VOs to deploy new IGTF bundle	Altunay	20 days	10/26/15	11/20/15
Cutover system from ITB to Production	Hayashi (Possible change?)	2 days	11/23/15	11/24/15
Propagate the new user DNs automatically to VOMS admins, service owners	Sharma	20 days	11/25/15	12/22/15
Complete implementing the changes to OSG Process and Policies	Gross, Teige	5 days	12/23/15	12/29/15
Update the SLA with CILogon	Teige, Hayashi, Basney	3 days	12/30/15	1/1/16

TRANSITION PHASE	LEAD	DURATION	START	END
	Sharma, Altunay	**65 days**	**1/4/16**	4/1/16
Transition first wave of VOs	Sharma, Gross	20 days	1/4/16	1/29/16
Management Review - Continue Transition?	Altunay, OSG-ET	5 days	2/1/16	2/5/16
Transition second wave of VOs	Sharma, Gross	20 days	2/8/16	3/4/16
Transition all remaining VOs	Sharma, Gross	20 days	3/7/16	4/1/16

- Biggest bottleneck is IGTF accreditation.
- Deployment and Transition can significantly move up if we can gain accreditation before October

Other Future Projects

- Mitigation for the security weaknesses in Traceability project
- Accessing storage without user certs
  - Either no user certs, or
  - Make the certificates completely transparent to the user

User separation in pilots without user-managed certificates

- A security mitigation to the traceability project.
  - The security risk is that user code can modify pilot logs and access pilot's proxy. Our ability to trace a user is under risk. We always knew about the risk, but promised to deal with it later once a few VOs get onboard.
  - We need to run users' jobs in a separate account, with no access to pilot logs
  - Users still does NOT have to have a certificate,
- Simplest solution:
  - User still does NOT need a certificate. We will create a proxy for her on the fly.
  - All users run under the same account, only the pilot runs under a separate account
  - Make a new lcmaps plugin that adds a fixed suffix to the pilot's Linux user name, e.g. "cmsprod" becomes "cmsprod_user"
  - Include a command that creates a new delegated proxy on pilot's proxy and invokes glexec to trigger the new plugin and run use code under separate user name
  - Change pilot jobs to invoke the new command
  - Require system administrators to create the extra login when they create the login for the pilot

User Separation

- Although the first solution is simple, it has limitations:
  - Sites have to be very careful to make sure there is no storage in common between jobs
    - Especially have to make sure there is no writable home directory for the account that user jobs run in
  - It is possible for different users sharing a pilot to interfere with each other

Separating users from each other

- For this case we propose a slightly more complex option:
  - Use the same new lcmaps plugin, and include some unique user identification string in the DN of the pilot-created proxy
  - Instead of mapping always to a known other user, add a GUMS feature to recognize new DN and to assign each user to a separate user id from a pool
  - Site administrators will need to configure GUMS and create the pool of user accounts
  - Pilot needs to pass user identification but will then work with either this solution or the simpler one

Higher level alternative for full X.509 cert compatibility

- A limitation of both proposed solutions is that they don't allow access control to persistent storage for subgroups of users
  - Most such storage systems require a pre-registered X.509 cert
- For this case we propose a higher level alternative:
  - Before submitting to the pilot system, create a genuine certificate with CILogon but hide them from the user
  - Authenticate user with Shibboleth federation
  - Register the DN of created certificate in VOMS
  - No change needed to grid infrastructure
  - A limitation is that the Shibboleth command line tools require support for a protocol that few federated sites offer as of yet
  - A workaround is to ask the user to authenticate by web annually and automatically store their certificate/key in a MyProxy server

Higher level alternative for full X.509 cert compatibility

- FIFE experiments are very interested in this solution
- Entertaining the idea of having the “FIFE Connect”
- Another motivation is FNAL is debating whether they should stop the KCA Certificate service used by FIFE experiments.
  - This change will force the FNAL to consider a FIFE Connect type solution instead.