CA Recovery from Dramatic Incidents

16th EUGridPMA in Zurich

Eric Yen & Jinny Chine

Academia Sinica Grid Computing Center (ASGC)

Taipei, Taiwan

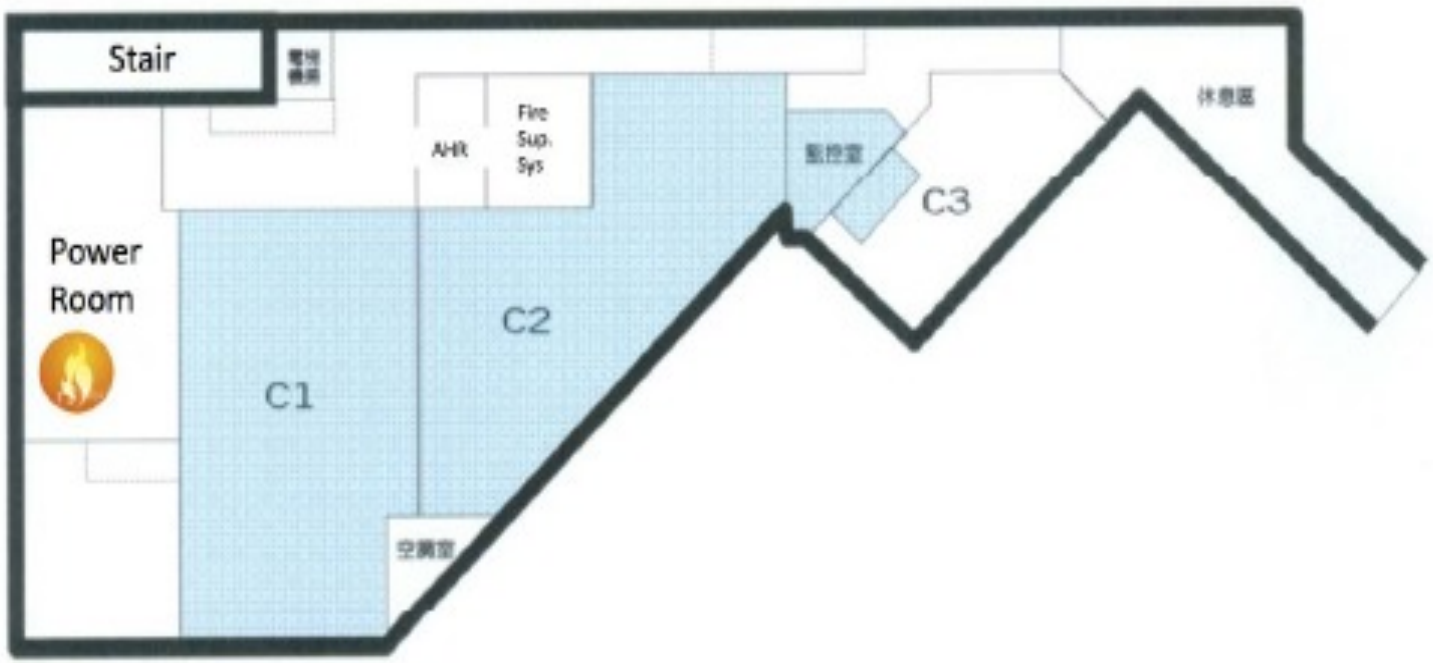
May 11, 2009

Academia Sinica Grid Computing

Motivation

- Due to UPS battery fire incident in 25 Feb. 2009, ASGCCA was out of service for 31 hours
  - Impact of CA services to emergency
  - How to reduce the impact and ensure the restoration
  - What's missing to current policy and operation procedures
- Do we have the established policy or incident response procedure for possible incident ?

Data Centre Incident @ ASGC



Event Scene Investigation

- 16:53 on 25 February (Taipei Time), fire lasted less than 3 hours:
  - SMS sent out "UPS power lost" and power generator did not start
  - Smell and visible of smoke, and fire at 2nd column of battery rack. Electric arc also viewed in the middle battery racks.
  - Fire spot (V shape) on the far-end wall, and near-end battery rack was also burned out -> fire spread to left and right within the middle battery racks, and up to the ceiling
  - But no fire burning evidence at racks in the other two ends

ASGCCA Event

- Time : 9:00 Feb-25-2009 UTC
- Event description : the unexpected accident on the part of data center at ASGC, all on-line services were shut down including ASGCCA web server.
- Root cause: UPS battery failure
- Result : ASGCCA certificate service were down. CRL did not publish in time.

Handling Process

- 9:00 Feb 25 UTC : Sent an EGEE broadcast to all ROC managers, VO managers, WLCG users, APGridPMA members, ASGCCA users
- 2:00 Feb 26 UTC : Sent an announcement to IGTF-RAT and IGTF-general lists. Try to recover ASGCCA web page
- 12:00 Feb 26 UTC: Moved ASGCCA web and CA server (offline) to another reliable place and back online after cleanup and verification.
- 16:00 Feb 26 UTC : ASGCCA web site was up. Sent the announcement to IGTF-RAT, IGTF-general and ASGCCA user lists

Basic Recovery procedure

- Evaluate the status of disaster and devise the recovery schedule
  - Share the status of CA to all related (PMA and IGTF)
  - Inform the recovery plan
- Recovery activities
  - Should be verified by audit guideline (self review first)
- Check all CA activities well and CRL will be published regularly
- Announcement of service resume: Send the final notification to IGTF-RAT, APGridPMA member, IGTF and your end entities.

Impact Analysis to CA Incident (I)

- CRL Outage
  - Any security concern ?
- Root key ruined or not ? Root key need have max security.
  - Under what circumstances, regen of root key is allowed ?
  - Auditing should be applied in a week ? Or self-audit is enough ?
- CA Services broken
  - Repository not available
  - How about private data lost ?
  - Rekey after recovery ? How about the solution in between ?
- Should be no impact to users and host/service with valid certificate, but
  - What about those certificate expires before the restoration ?

Impact Analysis to CA Incident (II)

- Services continuity Issues, what if the CA could not be recovered in 2 days ?
  - Any other CA could take over the CA services ?
  - Re-build a new CA should be always an option for the recovery plan ? --> 3 - 7 days of max CA outage would be ensured !
    - Need fast audit (both self-audit and peer review) in time
    - All certificates has to be rekeyed (revocation first).
  - Federation would help ?

Lesson Learnt

- CA services might be disrupted and will affect any single, multiple or all components.
  - HW failure, System compromised, fire incident, natural disaster, etc
- How to prepare for the risk ?
  - What should be backed up ? And how ?
    - CA server and web - ensure to be restored with a min loss of data and in min time, with exact configuration
    - Duplicate CA services
  - Prepare recovery plan accordingly
- Backup & Recovery has to be taken into account as part of minimum requirement and reviewed
- Definition of Change of CA ownership/CA termination should be in place
  - Ensure the CA's and Subscriber's keys are protected and available in accordance with this policy

IGTF-RAT

- The International Grid Trust Federation (IGTF) Risk Assessment Team (RAT) is responsible for assessing risk and setting time and deadlines for response and action for concerns and vulnerabilities.
- Email address: igtf-rat@eugridpma.org
- Members:
  - APGridPMA: Yoshio Tanaka , Jinny Chien
  - EUGridPMA: David Groep, Jens Jensen, Willy Weisz, Sajjad Asghar
  - TAGPMA: Vinod Rebello, Jim Basney, Jim Marsteller
- Public webpage
  - http://tagpma.es.net/wiki/bin/view/IGTF-RAT

Thanks for your listening

Academia Sinica Grid Computing