WLCG et grille EGI : Continuité de service

Eléments de discussion.
Merci à tous ceux qui ont apporté leur contribution

Jean-Michel BARBET, Laboratoire SUBATECH, Nantes

Plan

- De quoi parle t'on ?
- Les différents éléments qui entrent en jeu
- Réponses au sondage
- Points techniques
- Conclusion

WLCG Operations service levels [1]

	Maximum delay in responding to operational problems		Average availability on an annual basis
	Prime time	Other periods	
End user analysis facilities	2 hours	72 hours	95 %
Other services	12 hours	72 hours	95 %

Max.indisponibilité 5% = 438 heures / an soit 18 jours et 6 heures

- Quelle disponibilité annuelle constatée pour les sites FR ?
- Est-ce prévu de demander plus (stockage) ?

Les éléments en jeu

- Expertise, humain
- Services EGI (stockage, CE, SE, BDII,…)
- Services sous-jacents (Auth, NFS, httpd, tomcat, SGBD)
- Système exploitation, dimensionnement
- Couche abstraction (hyperviseurs, cloud,...)
- Réseau et services associés (DNS, NTP, ...)
- Matériel
- Infrastructure

Les menaces

- Sinistres
- Pannes matérielles
- Pannes logicielles
- Dépassement de capacité
- Intrusion, piratage, DoS, sabotage
- Erreur humaine
- Compétences indisponibles

Les mesures pour contrer le risque

- Sinistres : répartition dans des locaux distants, alarmes incendie, détecteurs de fuite liquides, para-foudres,…
- Pannes matérielles : redondance, spare, contrats de maintenance, détection
- Pannes logicielles : log des actions, plateformes de test, réversibilité, réinstallation automatique
- Dépassements de capacité : surveillance, nettoyage

Les mesures pour contrer le risque

- Intrusion : diminution de la surface d'attaque, correctifs, détection, capacité de réaction
- Erreur humaine : formation, surveillance mutuelle, attitude « zen » (éviter de travailler sous pression)
- Indisponibilité des compétences : prévision, formation, partage des informations, procédures

Résultats de l'enquête

- Personnel et organisation : procédures partagées (au sein du site, entre sites,…) logbooks et suivi des modifications, couverture des compétences toute l'année
- Utilisation d'outils de déploiement : homogénéité des configurations, réinstallation automatique
- Réseau de management (IPMI?)
- Surveillance, détection des problèmes et alertes (nagios, envoi de SMS?)

Résultats de l'enquête

- Résilience des infrastructures réseau : technologie VSS : coeur de réseau réparti et redondant ?
- Résilience du stockage : technologies RAID pour système et données
- Matériel : pouvoir compter sur le SAV du fournisseur
- Fragilité de certaines briques logicielles (mal maintenues)
- Protection et disponibilité de l'alimentation électrique : onduleur(s), groupe électrogène de secours

Points de vigilence

- Points de vigilence remontés par l'enquête :
  - Le facteur humain est très important
  - Le réseau et la fiabilité des liens externes
  - La climatisation

Autres points techniques

- Redondance, duplication, fermes de services
  - Quels services s'y prêtent ?
  - Utilisation d'alias DNS « dynamiques »
  - La redondance dans le réseau
- Identification de SPOFS
  - Ex : Storage « head-node »
  - ARGUS ?

Discussion

Références

[1] WLCG Memorandum of Understanding (MoU)
http://wlcg.web.cern.ch/collaboration/mou