Notes Réunion Sécurité Grilles, Lyon 28 Janvier 2010

Jean Michel Barbet, Denis Pugnere

1 Sécurité Grille et NGI France

Présentation de l'organigramme du GIS "Institut des Grilles". Présence d'un ingénieur sécurité lié au Directeur/Gestionnaire. Groupe de travail Sécurité dans la section Opérations. Estimer les ressources pour chaque groupe de travail et écrire le mandat. Poste prévu pour l'ingénieur sécurité.

Niveau direction : relation avec le SGDN (Secrétariat Générale de la Défense Nationale, maintenant DSN Direction de la Sécurité Nationale), interaction avec les responsables sécurité des organismes participants. Faire comprendre les spécificités de la recherche.
Niveau opérations : groupe d'experts connaissant le middleware, communication sur les incidents.

Jusqu'à présent la sécurité a été un peu laissée de coté. Mais la thématique grille prend de l'importance pour tous les organismes participants. Le SGDN s'y intéresse de près.

Rappels au niveau opérations

- chaque site est responsable de sa sécurité, il existe déjà une organisation dans chaque organisme et des documents
de Politique de Sécurité, chartes, etc. En cas de non respect des préconisations venant de la grille, un site peut être exclu de la grille. Les règles grille sont assez générales et ne prennent pas le pas sur les règles en application sur le site. Le responsable sécurité du site doit établir les contacts et faire circuler l'information entre les personnes (grille et organisme)
- fredéric : vacances : absence du responsable sécurité du site ?
- sophie : qui écouter ? (préconisations provenant de canaux multiples, risque de contradictions). rolf : préconisations devraient provenir de l'organisme mais il y a des exigences spécifiques grille (transmises par Dorine). sophie : cela va audelà de contacts : il s'agit d'une chaîne fonctionnelle. Responsable organisme devrait être averti, appuyer la demande de la NGI et contrôler l'application des mesures demandées. Une NGI conserve une certaine indépendance dans ses
décisions par rapport à la grille internationale. Discussion sur la manière dont a été gérée la préconisation du SGDN concernant l'acceptation d'une classe d'utilisateurs de la grille. Rolf: Aspect grille doit être intégré au niveau IN2P3.
Thierry : Il y a un problème car cela fait deux chaines fonctionnelles distinctes.

Todo
- identifier les contacts dans les organismes (fait à l'IN2P3) et définir les chaînes fonctionnelles
- définir le partage des responsabilités et codifier les procédures opérationnelles spécifiques grille

Après la transition, il faudra prévoir de participer à certaines structures EGI, intensifier les contacts avec le CERT-RENATER et le CERT-A, participer au monitoring sécurité au niveau EGI, en explorer les possibilités au niveau NGI.
Participer aux security service challenges (SSC) mais peut-être pas à tous.

Gestion des Certificats Grille

Retrait de la hiérarchie GRID-FR : les sites seront prévenus via SA1-FR
Inclusion de GRID2-FR dans TACAR
Risk Assessment Team : contrôle les ACs. Pas d'alertes pour le moment.
Certificats robots : utilisés par des groupes de personnes ou des tâches automatiques. Expérimental pour le moment.
La CA "catch-all" va passer de la France à la Grèce. Le DN des utilisateurs va changer et sera douloureuse.

On ne sait pas si le CDD de Mirvat va être maintenu. Dans le cas contraire, Alice ne peut pas prendre en charge le travail. Rolf: les CDD doivent connaître leur situation fin janvier. Pour le moment : pas d'infos. TERENA propose des certificats personnels (uniquement pour le moment) eScience pour les Européens. Le certificat TERENA sera reconnu de base par les navigateurs. La CA émettrice sera "COMODO" et cette CE sera normalement intégrée à la distribution gLite.

Quelques rappels

Utilisateur : protéger sa clé privé, si perte, prévenir les Autorités d'Enregistrement (Alice)

Statistiques sur le nombre de certificats personnels ou serveurs GRID-FR et GRID2-FR. Les certificats GRID2-Fr ont presque totalement remplacé les GRID-FR. Le nombre de révocations reste faible et concerne essentiellement les certificats personnels.

Durée des certificats : 1 an max imposé par l'Europe (en rapport avec la complexité de la clé).
Possibilité de faire descendre les AEs dans les laboratoires : les pré-requis ne sont pas les mêmes que pour CNRS, nécessite de refaire la procédure d'agrément.

La Sécurité dans la stratégie de la NGI

La NGI CSIRT doit investiguer les ressources non dédiées à la grille.
Permettre aux autres partenaires de la Grille de relier une adresse IP à un site.
Serveur Pakiti central géré par l'OSCT : ne voit que des adresses IP. Demande de l'OSCT : associer le nom du site avec des plages d'adresses IP. Cette connaissance existe au CC pour l'IN2P3, mais pas pour tous les sites EGEE.

Site France-Grille : espace sécurité : que souhaite-on mettre dans cet espace ?
Fred : les contacts de sécurité
JC : les derniers patchs
Espace accès privé ou public ?
Sophie: partie publique pour la communication, partie privée pour les membres du groupe.
Contenu : howtos, informations
Yannick: les parties privées sont exclues de l'indexation par des moteurs de recherche. Il faut donc limiter la partie privée à ce qui requiert effectivement une protection.
Sophie: que chacun puisse ajouter une information intéressante (mais nécessite validation ?)
JC: Utiliser le site pour distribuer des informations et éviter que tous les sites fassent les mêmes recherches au même moment.

Security Challenges :
SSC organisés par OSCT, 3 jusqu'à présent. Rappel de la procédure de gestion d'incident vue par l'OSCT.
Avant le SSCx, seuls les T1 avaient été inclus dans les SSC. Il s'avère que l'exercice a été plus difficile pour les T2.
L'exercice consistait à bannir un utilisateur sans affecter la VO et à suivre la procédure de gestion d'incident.
Thierry : Est-ce que EGEE envoie des retours à l'envoi des messages ? Lors de l'exercice, ces retours ont manqués.
Eric : Il n'y a pas eu de phase d'analyse permettant de remonter des informations sur des échecs de banissement.
Pierre : Est-ce que l'on est prévenu d'un banissement (à part si on regarde les CRLs) et surtour, est-ce que l'on est prévenu de la fin d'un banissement ?
Eric: Le banissement par le site est une procédure d'urgence, par la suite c'est la VO qui bani un utilisateur mais l'information circule difficilement.
Thierry : Qui avertit l'autorité de certification ?
Benoit: Tout ceci doit faire l'objet d'une procédure à suivre. Normalement c'est la personne de l'OSCT qui gère l'incident qui doit s'occuper de cela. Lors des derniers incidents, j'ai prévenu : Thierry (IN2P3),

RENATER, la VO, le CSIRT régional CNRS, etc.
Rolf: Il est prévu explicitement (procédure) d'informer le resp.de la VO si la nature de l'incident l'exige.
Dorine: Outre la VO, la CA, l'utilisateur concerné, il fallait penser à contacter le responsable de l'UI.
Juan Carlos : Il faut un modèle pour le contenu des messages
Rolf: le modèle existe, il suffit de mettre le lien dans la zone sécurité sur le site de la NGI.
Yannick: le mécanisme actuel est trop verbeux pour les incidents classiques où la grille n'est en fait pas réellement ciblée mais pas assez dynamique s'il s'agit réellement d'une attaque conçue pour récupérer des certificats vivants et lancer immédiatement des travaux sur plein de sites distants.
Dorine: C'est l'objet de cette réunion de détecter les insuffisances du modèle actuel et proposer des améliorations.
Rolf: La présence des contacts sécurité dans la GOC-DB permet effectivement de s'adresser très rapidement à tous les sites.
JM: la rapidité des mécanismes d'alertes est bien mais la majorité des sites n'a pas les moyens d'avoir une personne disponible 24h/24.
Fred: Avoir des mécanismes permettant d'intervenir rapidement sur les éléments centraux tels les WMS au cas où ces élements sont eux-mêmes corrompus (corruption de nombreux proxies d'utilisateurs).
Pierre: Sortir immédiatement le WMS de production.
JC: l'IN2P3 a les moyens de couper le réseau si urgence.
David: Est-ce pertinent de donner le contact d'une autre personne pouvant intervenir.
Eric: On ne peut pas couper instantanément. Des temps de latence existent : mise à jour des CRLs, temps de validité d'un proxy. Une coupure d'accès au niveau du service VOMS semble assez efficace.
Pierre: Est-ce qu'il y a groupe qui recherche activement les vulnérabilités ? (sophie: Le groupe de Linda ?)
Rolf: le financement de ce groupe n'est pas assuré dans EGI.
Techniques de "foresics"
JM: Partager la connaissance technique nécessaire.
Dorine: organiser le partage d'expérience.

Mises à jour sécurité et la pratique

Eplucher les sites CERTA et US-CERT pour étudier les avis de sécurité.
Précautions :
- RPMs signés et contrôle du md5sum
- Tests (complets) sur machines hors production
- Vérifier le redémarrage du démon ou de la machine et tester les principales fonctionalités
Confiance à accorder aux repositories DAG,rpmforge, etc.
Se limiter aux mises à jour de sécurité ?
Recomplier à partir du source RPM. Parfois nécessaire pour ajouter des patches, supporter KVM, compatibilité avec SELinux, bénéficier de versions non encore disponibles avec SL.
Utilisation de quattor : prend du temps de préparation mais revert facile. On essaye de limiter le nombre d'OS
supportés.
Temps de déploiement de l'ordre d'une semaine.
Si un reboot est nécessaire, c'est délicat sur la grille selon le type de noeud. Sur les worker nodes, cela aboutit à une perte de production. Un mécanisme de job suspend/resume serait bienvenu.
Yannick: cela nécessite la programmation de points de reprise.
Fred: Avec des machines virtuelles cela pourrait marcher, du moins avec certains protocoles.
La synchronisation (rsync) des repositories locaux et pour 7 OS avec les repositories SL prend plusieurs heures.
Mais les signatures md5sum ne sont pas vérifiées, de plus Quattor ignore les signatures. La compromission
d'un serveur mirroir SL peut potentiellement aboutir à compremettre toute la grille. Avoir un mirroir français bien sécurisé ? Qui gèrerait cela ?
Recompilation : avoir un système de build (ETICS ?, Koji ?) pour recompiler au niveau français.
Que déclarer à EGEE si on doit rebooter des noeuds ? Rolf: Au moins les expériences LHC acceptent qu'un site soit indisponible pour cette raison.

Dorine: faut-il avoir un cluster de test pour tester les mises à jour ?
Discussion sur l'automatisation des mises à jour ou sur un outil permettant d'être averti si des mises à jour sont
à faire avec Quattor.
Fred: Avec Quattor on se comporte plus comme un fournisseur de distributions dans la mesure ou il apporte
également les mises à jour.
Yannick: Existe-t'il des moyens de tout mutualiser dans un serveur Quattor unique ?
Actuellement les sites sont avertis des mises à jour disponibles via les templates Quattor par la liste quattor. Faut-il ajouter un système de diffusion via flux RSS ou news ?
JC: Pour les alertes comme celle récente concernant le noyau, Il faut informer les sites qu'il y a un problème mais que la solution n'est pas prête.
Dorine: Etes-vous intéressé pour avoir accès au serveur Pakiti qui contrôle la mise à jour des sites ?
Guillaume: plutôt nous informer s'il y a un problème.
JC, Eric: Le test de version de RPM n'est pas toujours pertinent (exemple l'application de mesures de maîtrise de la
vulnérabilité)

Gestion des droits et Argus

Avec la grille il est nécessaire de pouvoir appliquer des politiques de sécurité différentes provenant de plusieurs
sources. Un modèle de gestion centralisée de l'antentification et de l'autorisation est souhaitable.
Il existe deux suites d'outils :
a) SCAsuite : SCAS, LCAS, LCMAPS, Glexec
b) Argus (ex.authz) : PAP,PIP,OH,PEP,PDP
SCAS est développé par Nikef et EGEE prône Argus.

Présentation Argus (Emmanuel)

PAP : administrer un ensemble de politiques d'authentification et d'autorisation
PDP : évaluation des politique pour un crédential donné : donne la décision
PEP : lieu où l'on met en application la décision

Installation de PAP sur une machine, description et exemple d'utilisation de pap-admin.
Installation de PDP, configuration, exemple.
Installation de PEPD, configuration, exemple.
Ports utilisés (1 en écoute et 1 pour l'administration par service): 8150,8151,8152,8153,8154,8155
Démarrer PAP avant PDP. Temps d'initialisation au redamarrage : 5mn
Tests avec PEP-Cli.

Test : installation d'un worker-node avec gLexec. En cours (problèmes d'installation)
Note: Argus n'est pas encore intégré sur le CREAM-CE.

Sophie: quelles différences avec SCAS ?
Dorine: Règles dans Argus ont une capacité d'expression suppérieure
Pierre : SCAS est identique à ce que l'on trouve actuellement sur un LCG-CE. Il semble que cela soit plus finement défini dans Argus.
Dorine: Argus n'est pas encore adopté largement.
Sophie: quels services peuvent utiliser Argus actuellement ?
Rolf: Actuellement les mêmes services peuvent utiliser SCAS ou Argus mais le nombre de noeuds gérables par Argus va augmenter. Il est prévu également que d'autres middlewares (ARC) utilisent Argus.
Eric: Ce sont des webservices, est-ce qu'ils tiennent bien la charge ?
Rolf: Avantage Argus : permet de construire une hiérarchie de politiques de sécurité avec héritage et de

gérer des exceptions
à chaque niveau.
Eric: Possibilité que ces hiérarchies soient des PAP tournant sur des sites différents

Retour sur le Service Challenge SSCx

Logiciels de détection d'intrusion (système)
Qui utilise Tripwire ? David : a abandonné car trop de travail pour intégrer les changements consécutifs aux mises à jour.
Autre ? Benoit : SAMHAIM+YUL, Thierry : AIDE
Choix Tripwire Vs Samhaim :
a) tripwire pas bien supporté sur les platesformes
b) suivre les modifs faites par les autres sys admins
Le problème est la maintenance de la base de signatures et le réglage pour éliminer les parties variables.
Pierrre: Au CC on configure le middleware pour que les parties variables soient dans /var. Cela coûte pas mal de temps. On pourrait aller jusqu'à mettre les partitions /bin /opt en read-only.
David: Comment exploiter le résultat d'un netstat sur un CE (trop verbeux)
Dorine: Est-ce que vous déployez des outils anti-rootkit ?
Guillaume : utilisation de "rootkit" de nagios.
Fred: le "rootkit" est simplement la détection de quelques rootkits célèbre interfacé avec un plugin nagios. chkrootkit est obsolète.

Questions/Conclusion

Pascale: Est-ce que EXTRA peut apporter quelque chose ?
Fred: Est-ce qu'un outil comme Nessus peut apporter quelques chose ?
Benoit: Nessus est libre mais pas adapté à la grille
Sophie: l'UREC avait fait un travail sur les plugins Nessus.
JM: Quid d'une démarche d'analyse de risque classique ?
Sophie: les administrateurs de sites grille peuvent bénéficier des formations existentes au niveau CNRS.
Dorine: Le JSVG a déjà construit une liste de risques
Discussion: intégration de l'analyse de risques grille avec l'élaboration de la PSSI su laboratoire.