Centre Réseau & Informatique Commun

A Mmes & MM. les utilisateurs du Système d'Informations

CNRS Grenoble − Polygone Scientifique

Grenoble, décembre 2023

Rapport d'activités 2023

Contexte général

L'année 2023 a démarré dans un contexte de crise Cyber, qui a impacté à moindre échelle les unités du Campus, mais qui a sollicité grandement l'équipe auprès d'unités relevant de l'hébergement du partenaire attaqué.

De nombreux chantiers sur le Campus ont eu des incidences évoquées plus en détail plus loin.

D'un point de vue ressources humaines, suite au départ d'un agent en fin 2022 (Laurent Neiger), le service a fonctionné à effectifs restreints au premier semestre 2023, et l'ASR des services de la délégation (Grégory Arnéodo) est venu en renfort pour faciliter la continuité de service. A partir de mai 2023, un nouvel arrivant (Guillaume Gielly) est venu compléter l'équipe, ainsi qu'une stagiaire (Malika Mebrouk) sur un sujet qu'elle poursuit en tant qu'apprentie sur l'année 2024. Enfin, le responsable de la cellule (Dominique Fournier) s'est vu confié le rôle de responsable de la Sécurité des Systèmes d'Information à compter de septembre 2023.

Ainsi la cellule CRIC fonctionne actuellement avec 2,5 ETPT + 1 apprenti sur les missions actuelles plus une nouvelle mission régionale de coordination de la sécurité.

La suite de ce bilan décrit dans le détail les aspects techniques et organisationnels mis en œuvre en 2023

Activités liées aux Systèmes

Plateforme de messagerie Zimbra

Il était prévu de migrer notre plateforme Zimbra en version 10, cependant ce projet est repoussé à 2024 du fait de contraintes techniques liées au système d'exploitation qui devrait aussi être mis à jour. L'ensemble de ces 2 mises à jour a donc été reprogrammé sur 2024.

La messagerie a évolué avec la mise en place de la fonctionnalité de certification des emails par SPF/DKIM. Ces deux fonctions permettent de limiter l'usurpation d'identité de

nos utilisateurs. Cela implique néanmoins des contraintes : il faut que les mails soient envoyés par nos serveurs sinon ils peuvent être considérés comme spam par les correspondants.

Mise à jour des systèmes et serveurs

Nous avons mis à jour l'ensemble du parc des serveurs (50 machines physiques ou virtuelle) afin d'être protégés des dernières failles de sécurité.

Cela permet aussi de voir apparaître de nouvelles fonctionnalités et de nouveaux usages :

- Edition collaborative sur l'offre de service Cloud (NexCloud)
- Sauvegarde historisée permettant la restauration d'un fichier (précédemment restauration de l'ensemble de la VM)

Tous les serveurs hébergés sur Debian sont maintenant en version Bookworm, la dernière version stable de cette plateforme.

Infrastructure de virtualisation

Nous avons rationalisé la gestion des stockages de nos infrastructures de virtualisation. Il est maintenant possible de déployer une nouvelle machine en quelques minutes, et de la supprimer en quelques secondes. Cette réactivité, associée au déploiement de « templates » permet de déployer des nouvelles machines préconfigurées sous Debian pour des actions ponctuelles.

Une nouvelle infrastructure Kubernetes, de type containerisation, qui fait l'objet du sujet de master de notre apprentie, a été déployée en 2023. La partie sécurisation est en cours de réalisation et la plateforme sera ouverte aux utilisateurs à partir d'avril 2024. Ce nouvel environnement permet d'héberger des services (applications web) à la demande des utilisateurs et de gérer les montées en charge des ressources allouées de manière dynamique. L'aspect sécurité est indispensable, car ces applications ayant vocation à être utilisées par un grand nombre de personnes, doivent être cloisonnées pour éviter une diffusion non désirée. Ainsi, une application ne pourra communiquer avec lnternet qu'au travers de filtres et elle ne pourra pas accéder aux données des autres applications.

Activités liées au Réseau

Connexion de Eurofidai

Eurofidai est un laboratoire situé sur le Campus de Saint Martin d'Hères. Son bâtiment d'hébergement est géré par les services techniques du CNRS. Il devenait nécessaire de mettre en place un pilotage à distance des équipements de GTC (Gestion Technique Centralisée. Nous en avons profité pour activer la téléphonie Xivo pour ce laboratoire (10 postes connectés sur la solution ToiP du Campus).

Projet UpAlim

Le projet UpAlim concerne l'installation d'un transformateur électrique pour le LNCMI qui est implanté sur notre Campus. Nous avons travaillé sur plusieurs mois avec le laboratoire et les prestataires concernés afin de construire l'architecture réseau qui permet de piloter cet outil.

Activités liées à la Sécurité

Plusieurs chantiers liés à la sécurité ont été conduits.

Crise Cyber touchant un partenaire universitaire

La cellule a été fortement impliquée et impactée par un incident grave de sécurité des SI chez l'un de nos partenaires qui a engendré un arrêt/dégradation d'activité au sein de plus de dix unités mixtes du site Alpes. Cet incident a nécessité de mettre en place des procédures d'urgence, a généré de nombreuses réunions en coordination avec l'ensemble des établissements partenaires concernés, avec les instances nationales du CNRS (RSSI, FSD) et auprès des directeurs d'unité concernées et leur équipe SSI.

Durcissement de Debian

Le premier chantier est consacré au durcissement du système d'exploitation Debian que nous utilisons principalement sur nos serveurs. Ce durcissement est nécessaire suite aux nombreuses attaques intervenues en 2023 et aux recommandations de l'ANSSI qui s'en sont suivies. Il a été déployé sur les nouveaux services activés en 2023 (6 nouveaux services) et sera aussi mis en place sur les services installés antérieurement (35 services concernés).

Analyse des logs

Nous réalisons quotidiennement des analyses des logs issus de nos systèmes afin de détecter des comportements anormaux. Depuis le début de l'année 2023, nous avons conçu une nouvelle méthode d'analyse innovante (déclenchement d'alerte sur logs inconnus) qui nous permet une proactivité dans ce domaine. Cette solution sera présentée aux Journées Réseaux de l'enseignement et de la recherche, qui se tiendront à Rennes en fin 2024.

Activités liées aux développements d'applications

Application visiteurs

Nous avons fait également évoluer l'application visiteurs, cette année, avec un nouveau module qui permet aux visiteurs (dans le cadre de certaines manifestations) d'enregistrer directement les informations les concernant. Ainsi, le valideur n'a plus qu'à confirmer ces informations sans avoir à les saisir.

Autres

Participation au groupe national pour le déploiement d'une offre visioconférence BBB

Accompagnement de l'arrivée d'un agent (G. Gielly) en FSEP sur missions Campus (2ème trimestre 2023)