# Compte rendu CT octobre 2020

## Participants

- leo
- elkmaennchen
- yberreby
  - intéressé par Ansible
- Chibrac
- Erdnaxe
- Ÿnerant
- Histausse
- Solal
- Jeltz
- Esum
- (Hachino)

## Cooptations en tant que RTs

1. Leopold
   - script de provisioning avec Mikachu
   - secrétariat
   - intéressé par la gestion/réseau, moins par l'installation de nouveaux services
2. Jeltz
   - centralisation des logs
   - intéressé par la sécurité divers
3. Ÿnerant
   - rejoint quand il a aménagé
   - installation de bornes
   - a installé camelot
   - intéressé par l'installation de services
   - développe un logiciel de streaming
     - réécriture Python → Go
     - avec Erdnaxe

Tous les membres du Conseil Technique présents sont d'accord avec les propositions de cooptation.
Ils auront peu de nouvelles responsabilités, mais doivent réagir en cas d'urgence (mais pas encore arrivé cette année).

## Bornes à la Pacaterie et raccordement à Fleming

**2020-10-10** Installation fibre GS <-> Fleming
Il s'agit d'une liaison 10Gbit/s au village 3

Locaux à Fleming (village 3):

- local Flemnet
- local rangement sous-sol
- local baie Crous sous-sol
- local bureaux Crous avec brassage de village

Coeur de réseau au village 2 : pas réussi à le relier en 10Gbit/s, fallback en 1Gbit/s : problème de distance. La liaison a tenu 10min, pas plus.

On peut avoir 10Gbit/s dans un local (pour les services), mais le reste est relié en 1Gbit/s.

Les vieilles bornes de la Pacaterie sont de mauvaise qualité. Bientôt plus supportées par le contrôleur unifi. Il restait des bornes de réserve, elles ont été installées à la Pacaterie.

Pour Fleming : pas eu le temps. Impossible de changer toutes les bornes (pas assez). Changement à prévoir dans les années à venir.

Locaux de la Pacaterie à ranger (+ local nord : serrure cassée).

Le contrôleur Unifi Pacaterie un peu à plat pour des raisons obscures.

–> Que fait-on des anciennes bornes ?
Elles n'ont plus de support mural (utilisé par nouvelles bornes).

- Essai de revente (~20/30 bornes) ?
- Les proposer aux adhérents qui ont une mauvaise réception Wi-Fi ? Problèmes d'alimentation ? Comme routeur Wi-Fi perso avec OpenWRT ?
    - Manipulation proposée via un tuto pour les adhérents (voire projet apprenti). Pas une priorité.
    - Page wiki Cr@ns existe.
- Voir à les proposer via Frnog ?
- Ebay: se vend 10 euros l'unité.

- Attention; certaines sont peut-être abimées (moisissure, …).

## Bornes à Emilie du Châtelet

Combien sont inutilisées ?

Bornes à re-poser, mais pas nouveau, la pose est complexe avec les clefs que le CROUS ne prête pas.

Personne habitant à EdC ne l'a fait.

À voir plus tard.

## Sécurité

En premier, tiering LDAP (administration + adhérents).

Formation des administrateurs (mots de passe forts).
Ajout de clefs SSH pour l'administration.

Créer divers groupes.

Ménage dans les comptes (notamment les non adhérents).

VLANs

Moyen d'accès de backup (Freebox de backup au Cr@ns, forfait 4G, …).

Yggdrasil peut tomber ?

Rézel devient FAI ? Route depuis Télécom.

Mdp root VS compte Aurore.

Clef SSH hardcodée.

Clef root en cas de problème.

Résumé :

- Serveur LDAP indépendant pour l'administration
- Clefs SSH dans le LDAP
- Protocole en cas de problème réseau/LDAP
- Feuille de route pour les droits "propres"
- Segmentation du réseau

Changement des statuts potentiels à effectuer pour les privilèges.

Privilèges sur quelques machines pour les apprentis ?

## Retour sur le script de provisioning

Utilisation du script actuel avec switchs du modèle actuel (plus chers) VS nouveau script avec autres modèles (moins chers).

Actuellement :

- Lecture depuis re2o ;
- Génération configuration lisible par les switchs;
- Envoi la configuration aux switchs;
- Les switchs n'arrivent pas à se connecter au Radius;
- Problèmes de droits (superuser Django requis pour API).

Le switch a t-il besoin de rebooter/reloader ? Reboot requis d'un switch.
–> Contrainte Chibrac: pas de reboot ! un enfer si reboot requis à chaque brassage à GS.

Script actuel : envoi de conf (via REST/TFTP/FTP/...), diff automatique et reload (mais pas reboot).
La version pour les nouveaux switchs reboote !

Utilisation de `config restore` dans la nouvelle configuration.

`ansible-network` (nul d'après Erdnaxe). Python `napalm` (à voir).

Pas de reboot là où on a du brassage (ie GS). Aux Rives, c'est pas important.

API 16.0.5 a introduit le `config restore` (calcule la diff et applique). API 16.0.2 dispose d'un embryon d'API partiel (assignation VLAN à des ports, ...).
Une possibilité serait un système hybride qui utilise l'API si possible et sinon passe par `scp + reboot`.

Possibilité de calculer la diff via SSH (avec `paramiko` p.ex.).
Fichier de config contextuel -> il faudrait faire un parser propre du langage de configuration (voir ce qui est utilisé en interne ?).

## Les Rives pour novembre

Les Rives: Résidence en 3 bâtiments (réouverture suite à des innondations).
Aurore sera seul à fournir internet: c'est une épreuve vis-à-vis du CROUS.

Tengué (DSI Crous Versailles): demande opérationnel en novembre.
Requis: faire les courses (rapidement)

- serveur de backup

- serveur main

Installation possible sans être aux Rives

Installation sur place assez simple (câbles pour bornes déjà fournis par le Crous).

Problème: il faut un uplink. Demander à l'UPS. Méré (UPS) ne sait pas (pour l'uplink et les baies) car le CROUS ne discute pas avec lui.
–> Solution de repli si pas la fibre ? Discuter avec Tengué: condition non-négociable ?
Le Crous a des fibres mais ne veut pas partager.

Envoyer un mail à Tengé : opérationnel seulement si fibre présente.

Envisagé : un ou plusieurs pont(s) Wi-Fi pour aller jusqu'aux Rives, mais pas idéal (est-ce seulement envisageable techniquement ?).

Y a-t-il des gens motivés pour faire l'installation (pas très compliqué, voire ennuyeux, mais formateur) ? Recrutement d'apprentis ?

Provisioning plus important que les Rives.

Commandes:

- serveurs
- cartes réseau 10Gbit/s
- optiques (1G, 10G)
- jarretières
- jarretières optiques
- bornes (commande en cours)
- quanta (2 commandés, un 3ème serait requis pour un vrai spare — moins urgent cependant)

Script `cloud-init` du Cr@ns: super rapide et efficace pour création de masse.

Histausse et Chibrac: gestion des optiques
Otthorn: achats un peu repoussés, mais en cours

Cr@ns: achète serveur + bornes (car choix des switchs moins chers).

Gen9 + carte 10G.

Histausse: pas envie de mettre un Gen8 en serveur principal d'une résidence. Beaucoup de problèmes rencontrés.

## Discussion sur l'infrastructure actuelle

Actuellement :

Rives: Gen9/10G + Gen8/Backup
Pacat: Gen10 + Gen7/Backup + Gen10/Merlin/Services
EdC: Gen10/Main + Gen8/Backup
GS: Gen9/Main + Gen8/Backup

Serveurs backups: ne font rien

Déplacer backups sur le virtualiseur principal d'une autre résidence.
Libérerait un Gen7 et 4 Gen8 (dont 1 en mauvais état).
Gen7: peu de disques.
1 Gen8: plus d'iLO et reboot pas auto.

Suggestion :

- Gen7 + Gen8 en mauvais état: cluster de test avec avec VMs de test.
- 1 Gen8 : logs + serveurs critiques
- 2 Gen8 : cluster avec Merlin
- Achat d'un serveur pour les rives.

Viviane (Gen8) traîne encore (ventilo + connecteurs USB en mauvais état), mais fonctionne.
Serveur de backup append-only ?

- Potentiellement utilisable ? Mais fiabilité non-garantie ?
- Serveur pour backups du NAS ?
- Veille sur leboncoin pour des offres intéressantes ?

Quelles permutations de résidence fait-on ? Rajout de résidences (complexe si permutation circulaire → beaucoup de déplacements de VMs) ?

Possibilité de cycles plus "courts" ? EdC <-> GS (pas pour l'instant, on a pas la RAM pour GS). Les reste plus tard (quand on aura les Rives) :

- Pacat -> Rives
- Rives -> Fleming
- Fleming -> Pacat

32G de RAM requis pour les hyperviseurs de réseau (main + failover).

On se débarasse aussi des réplicats LDAP de backup (pour ne pas en avoir 2 par résidence, pas utile, on configure les services pour utiliser le serveur de l'autre résidence).

Il faudra bien propager les bons VLANs aux bons endroits.

RAM achetée pour avoir >=32G partout.

Résumé :

- Achat Gen9 360P? (32G RAM) pour rives + carte 10G — reconditionné
  - copier la conf de `marki`, ou trouver mieux (pas forcément nécessaire)
  - Chibrac regarde

Consultation du configurateur Bargain hardware (choix des barettes de RAM, carte RAID, ...)

Demande d'avis à Erdnaxe pour comparer les processeurs (générations ? performances ?). Il y aurait moyen de diminuer pas mal le prix.

## Information des adhérents

Quel protocole en cas de maintenance ? Par mail à tous les utilisateurs concernés ?

Datadog viarezo -> fait par des centraliens, discussions ?

Au Cr@ns, page de statut (à la pagerduty) à destination des adhérents, pas de l'administration.

Système de communication peu pratique et insuffisant.
On change rien pour l'instant, mais les mails arriveront plus tard + status page en projet latent.

## Point sur la coopération avec Wifirst à George-Sand

Depuis l'installation d'Aurore à GS, WiFirst installé aussi. Pas mal de boulot (brassage, changements re2o, ...). WiFirst n'a pas déployé SmartCampus via bornes couloir, mais en in-wall dans les chambres.

Mais seulement 2 prises dans les chambres: 1 pour les FAIs et 1 "directe".

Si quelqu'un veut être raccordé à Aurore, il faut débrancher la borne in-wall qui utilise la prise "directe".
Le Crous râle car couverture SmartCampus a diminué.

Aurore n'a pas la liste des bornes placées chez les gens, donc dépend de la bonne foi des adhérents.

Liste partielle obtenue récemment, seule 17 des 27 sont chez Aurore actuellement. Les autres sont débranchés pour des raisons quelconques.

Aurore a envoyé aux utilisateurs en leur demandant de rebrancher.

Wifirst fournit parfois du filaire (selon le bâtiment).

Solutions techniquement envisageables: dédoubleur au niveau de la baie de brassage (1 cable 1G -> 2 cables 100M), mais sans doute nécessité d'installer un injecteur PoE chez les adhérents (pas forcément requis, à voir).
Achat de quelques boîtiers de test.

Autre option: accord avec Wifirst pour propagation du VLAN filaire adh Aurore via leurs switchs. (peu probable que wifirst accepte, mais on peut proposer). Requiert un paiement du Crous car presta WiFirst, donc assez peu probable.

Convention Crous <-> Wifirst <-> Aurore : Aurore ne doit pas interférer avec SmartCampus (mais très flou, et n'est sans doute pas applicable à cette situation).

Le Crous/Wifirst ne justifie pas l'installation de bornes dans les chambres.

D'après certains textes juridiques glannés sur Legifrance / jurisprudence : il semble que les adhérents aient droit de débrancher les bornes WiFi si elles sont installés chez eux sans le consementement explicite. Il serait de mauvais ton de la part d'Aurore d'utiliser ce genre d'arguement qui souhaite garder des relations cordiales avec le CROUS.

Réunion bureau a été effectuée. Qu'est-ce qu'on fait maintenant si un adhérent a une borne Wi-Fi ?

Quelques adhérents ont envoyé des mails au Crous pour se plaindre de WiFirst. Pas de réponse du Crous.

Dédoubleur 1G pas possible car Ethernet Gigabit utilise les 8 ports, et Fast Ethernet en utilise que 4.

La possibilité de fournirs aux adhérents un template mail aller discuter avec le CROUS du problème des bornes directement plutot que de discuter avec nous, qui n'avons pas le pouvoir de prendre cette décision.

## Protocole pour éviter les coupures

Vérifier que le backup fonctionne.

Plus pertinent sinon.

## Discussions Wiki

Wiki pas accueillant (pages orphelines, pas à jour, ...).
ACL mal faites (sous pages accessibles quand pages pas accessibles).
Très incomplet.
Thème de base pas très joli.

Quitte à refactoriser, pourquoi ne pas changer de moteur.

Wiki aurore supporte très mal les outils d'accessibilité (pages mal rédigées ET moteur de wiki mauvais)

Accessibilité ?

Contenu automatique (Ansible) ?

Ajout de graphiques ?

Décision : changement d'engine. Installation par Solal (priorité < aux mails).

Page : https://codimd.auro.re/ad2AwnRNRrKZgmLMB0cI3w#
(https://codimd.auro.re/ad2AwnRNRrKZgmLMB0cI3w#).

## Présentation de Gitea

Service de "forge logicielle" (sic). Alternative Gitlab/Github/Bitbucket.

Jusqu'à récemment, dépendant du Gitlab Fédérez.
Stockage sur NAS (dataset ZFS partagé en NFS, monté sur une VM sur Merlin).

Connexion via le LDAP. Pas de mailer configuré.

Problèmes:

- dépôts mirrorés, mais pas migrés;
- bugs légers sur les webhooks;
- mails du LDAP mal importés ( `nom@localhost` , pas le mail du LDAP).

Authentification pour des comptes ? SAML/OAuth/OpenID pour authentification tierce ?

Drone/Jenkins pour la CI git ?

ViaRezo: OAuth pratique
Rezel: KeyCloak

SSO pour partager l'authentification entre les services

Certains services ne doivent pas être accessibles aux non adhérents, d'autres si ?

Attention au webmail, qui doit avoir accès au mot de passe (ou un plugin Dovecot pour oauth ?).

Si des dérives sont observées, on pourra toujours prendre des mesures.

Tâche Phabricator pour OAuth pour CodiMD/Gitea/…

Peut diminuer l'intérêt des services pour les adhérent, puisqu'il faut pas être adhérent pour accéder aux services. Ca pourrait faire découvrir les services à d'autres personnes.

Ajout manuel par un administrateur sur le service. C'est un peu du "copinage" avec les RT. A minima, il faut annoncer publiquement qu'on peut créer un compte.

Système de parainage ? Envisageable ?

Création d'un salon Matrix pour discuter de l'authentification partagée par Otthorn.

## Projet mail, discussion sur l'infrastructure choisie

Salon de discussion Matrix + CodiMD.

Otthorn: tests sur son VPS + spécifications.

1 seul serveur avec Dovecot + Postfix (MX).
Déploiement de DKIM + greylisting.
Réservation de plein de comptes tq `abuse@auro.re` , … (utilisation d'alias re2o).

Quelle architecture pour les MX (fiabilité, …) ?

Sandwitching ? Faire le MX le + prioritaire "faux" pour embêter les spammers ?

Un MX relais chez OVH qui forwarde sur le MX "principal" en interne ?

Stockage des messages: sur NAS ? ou directement dans la VM ?

- les mettre sur le NAS simplifie les backups
- mais spof

**consensus:** plutôt sur le NAS

Support POP3 ? nécessaire ? utile ?

- fortement privilégier IMAP (au moins inciter les adhérents)

Automatisation DKIM ? re2o ? durée d'expiration ?

**Aside:** merlin est presque plein, il faut rajouter des disques

**Aside:** quelle architecture pour le cluster de proxmox ? stockage des VMs sur un NAS ou copie entre les hyperviseurs ? Regarder GlusterFS (conseillé par chirac). Regarder technologies mises en place par Amazon/Netflix (mais peut-être un peu lourd).

## Installation de Caradoc

Achat sur Leboncoin.

Il s'avère que caradoc > perceval (c'est pas cohérent avec le lore).

Pour les backups du NAS: send/receive ZFS pour synchroniser les 2 (en plus des snapshots).

Backups: chiffrées, authentifiées, append-only, dédupliquées, incrémentales.

Solutions : borg, backuppc, backups Proxmox, restic, bacula, rsnapshot, duplicity, …

Otthorn: partirait sur Borg

On peut créer un salon Matrix.

Qu'est-ce qu'on veut sauvegarder (bases de données postgres, re2o, mails, nextcloud, logs, …) ?

## SoftEtherVPN OVH

Pont horus <-> reste du réseau.
Actuellement bridge SoftEther.

Attention, L2 SoftEther -> L3 WireGuard.

Déplacement des endpoints VPN.

## Questions diverses

Quand est-ce qu'on mange ?

Pourquoi le numéro de téléphone est-il obligatoire dans re2o ?
Dossier personnel des administrateurs (téléphone, mail, …) ? Signature d'une charte des membres actifs ?
Définition rigoureuse de "membre actif" ? Faire un RI spécial CT ?

Séminaires

Liquide disparu ? C'est n'importe quoi. On a pas de caisse à GS.
Inventaire du liquide + des cartes bleues des comptes Aurore