

CT decembre 2020

Présents:

- Histausse
- Jeltz
- ynérant
- pi-r
- Solal
- sofamaniac
- pz2891

Début : 14h06

Fin : 16h55

Resumé de l'installation des Rives

Installation finie dans le premier bâtiment (bâtiment 233), encore 2 à installer quand ils seront livrés.

Histausse remercie les membres qui se sont investis dans l'installation.

A faire rapidement

- Wifi accueil (surtout pour les Rives)
 - Autoriser 100Mo/jour/appareil en limitant le débit ;
 - Obtenir une liste des ip pour le 3D secure ;
 - Whitelist juste re2o, et au moment de la création du compte, demander une connexion gracieuse pendant 10 min
 - Comme au dessus sans dire qu'on offre 10 min de connexion
 - Le Conseil Technique envisage les 2 dernières solutions
- Centralisation des logs (les VM sont pleines !)
- Onduleurs (moins urgent) : paramétrer pour les ajouter au système de monitoring (prévenir quand les plombs ont sautés/ voir l'état de la batterie)

Sur le monitoring, Solal propose de mettre en place une page web avec le statut des services.

Proposition de cooptation de pz2891 (Paul Ziolkowski) en temps que RT

Paul se présente (par écrit, micro cassé) : il a rejoint Aurore fin octobre pour aider à résoudre les problèmes à Emilie du Châtelet. Il est en filière informatique, et gère des serveurs / sites pour son boulot, il s'est dit que ça serait cool.

Personne ne s'oppose à la cooptation.

Wifi et SSID

Actuellement, il y a 2 SSID Dual Band : Aurore et FedeRez.

Problème du 5 GHz

Problème, les clients se connectent préférentiellement au 2,4 GHz, qui propose un moins bon débit, et sature le spectre.

Le push to 5 GHz donne de bons résultats sur la majorité des clients, sauf certains chez qui ça marche très mal.

Solutions :

- 1 : Activer le push to 5 GHz sur Aurore et FedeRez et créer un Aurore-2GHz / Aurore-Legacy pour les clients qui le gèrent mal?
- 2 : Créer un SSID Aurore-5GHz soit 5 GHz only soit où on active le push to 5 GHz. Le problème du 5 GHz... c'est que certains clients loin des bornes auront de meilleurs perfs en 2,4 GHz, par conséquent un SSID 5 GHz only semble ne pas être l'idée du siècle.
- 3 : avoir un SSID optimisé dual band, et un SSID backup en 2.4 only
- 4 : Ne rien changer, et créer un 5Ghz only

Fantôme erdnaxe (qui ne sera sûrement pas dispo en vocal) :

- Le principal soucis avec le WiFi c'est les Mac qui ont un comportement cahotiquement mauvais dès qu'il y a du 2.4GHz sur un SSID. Pour moi ça fait plus sens de faire un réseau {2.4, 5}GHz "Aurore" et un réseau 5GHz-only "Aurore-5GHz" pour les gens sous Mac, il faut l'expliquer sur re2o
- SVP soyez respectueux envers les physiciens et mettez "GHz" en entier dans le SSID WiFi. Non, Aurore ne diffuse pas encore de la 5G même si ça serait super chouette.

Si les utilisateurs qui ont des problèmes ont des Mac alors partir sur la solution d'erdnaxe. Sinon partir sur la solution 3.

Tout le monde est d'accord pour dire "5GHz" plutôt que "5G"

Tester la solution 1 à la Pacaterie (et les Rives)?

Aurore et Aurore-2.4GHz.

SSID Accueil

Déployer un SSID accueil sans authentification pour permettre aux gens de s'inscrire chez Aurore.

Nom du SSID :

~~Aurore-Accueil~~

~~Aurore-Register~~

~~Accueil-Aurore~~

~~Inscription-Aurore~~

- Aurore-Inscription

Le choix du nom est déjà marqué dans les documents qui ont été envoyés au CROUS (Aurore-Inscription).

Ce SSID pourrait être dual band sans push to 5 GHz, ce qui fonctionne à peu près correctement.

Clients ne supportant pas le WPA2-Entreprise

Un certain nombre (de plus en plus) de clients ne supportent pas WPA2-Entreprise.

Solutions possibles :

- Leur permettre de se connecter à Internet sur le SSID Accueil via une auth par login/mdp sur un SSID ouvert
- Déployer un SSID de plus dédié, WPA Personnel Aurore-Personnal, avec mdp "Aurore" et portail d'authentification

Ce SSID pourrait être dual band sans "push to 5 GHz", ce qui fonctionne à peu près correctement.

Le problème concerne surtout les consoles/chromecast/enceintes (et tous les appareils connectés), mais pas les ordinateurs ou les téléphones.

Dans tous les cas, un mail général s'impose afin d'informer les adhérents sur quel SSID se connecter. L'idéal étant que la majorité des adhérents n'aient rien à changer.

Fantôme erdnaxe :

“Mouhai”, pourquoi “mouhai” ? Parce que je pense que c’est une mauvaise idée de mettre ces clients directement sur le réseau local. En pratique la plupart des périphériques sans WPA2-Enterprise sont prévus uniquement pour un réseau WiFi domestique/privé, ce qui est loin du cas d’Aurore.

La solution plus propre serait de donner des références/vendre des routeurs aux gens pour qu’ils aient leur propre sous-réseau avec tous leurs périphériques non protégés. On n’a pas envie d’avoir 36000 chromecast publiques.

Après si vous continuez avec votre solution de WPA2-Perso, des gens se feront un plaisir d’utiliser Aurore comme terrain de jeu pour hacker de l’IoT en masse :p

Les routeurs permettraient aussi de résoudre les problèmes de couverture à Emilie du Châtelet.

Le détail concernant les routeurs (location / achat) est laissé au Conseil d’Administration). Mais le partage de compte devient plus compliqué à contrôler. À voir selon la portée des routeurs (même si le problème persiste pour les colocations).

Personne ne s’oppose à ce que soient achetés quelques routeurs pour tester.

Wiki-JS

- Instance déployée sur wikijs.adm.auro.re (<http://wikijs.adm.auro.re>) sur odin (<https://wikijs.auro.re>) (<https://wikijs.auro.re>)
- Backend adapté ?
- Quelle structure ?
- Quels accès ?
 - Wiki réservé uniquement aux membres actifs ou à une partie publique ?
- Stockage :
 - Activation du stockage Git ?
 - Accessible uniquement au CT, de préférence reste en lecture seule, pour débogage uniquement pour récupérer l’historique.
 - Activation du stockage local ? (En plus du stockage BDD)
 - Backup du wiki sur un serveur externe ? (via SFTP)

Il y a un salon matrix dédié au Wiki.

sofamaniac et Jeltz se proposent pour transférer des pages sur le nouveau wiki.

Toutes les données personnelles dans administratif (**avec accès authentifié**).

AuroreBox

→ ~~Fantôme erdnaxe : cette section devrait être liée au WPA2-Perso~~

C'est cher. On n'a pas assez de trésorerie et de motivation. Le faire avec ViaRézo ?

Proposer une box a la location a edc?

On va peut-être quitter Emilie Du Châtelet d'ici 2023-2024 lors de la rénovation.

Revente / location de petits routeurs / laisser les gens l'acheter sur Amazon.

Les mails

- On dépend actuellement du Crans pour les listes de diffusion d'Aurore (ca.aurore@lists.crans.org (mailto:ca.aurore@lists.crans.org), support.aurore@lists.crans.org (mailto:support.aurore@lists.crans.org), tech.aurore@lists.crans.org (mailto:tech.aurore@lists.crans.org)). Elles marchent bien. Le besoin de s'en détacher est le gain d'autonomie.
- Des mails persos (ou pro) en @auro.re pour tous les adhérents, c'est vachement cool aussi.
 - D'un point de vue technique, il est essentiel d'avoir plusieurs serveurs de mails, dont un qui n'est pas hébergé à Aurore (sur le serveur à OVH par exemple). **Jamais, une fois le service mis en production, un mail ne doit être perdu.**

Fantôme erdnaxe :

C'est vraiment génial d'offrir un service de messagerie in-house. Quelques retours avec l'expérience au crans :

- Mettez les mails en opt-in, sinon vous en aurez beaucoup de comptes et vous aurez des problèmes de comptes piratés qui vont spammer.
- Surtout ne faites pas de pré-traitement sur les messages reçus, mettez les antispams/filtres en opt-in. C'est beaucoup trop chiant les providers de mails qui décident de supprimer des mails sans l'accord de l'user.
- Au Crans on a un MX en fibre, un MX en ADSL et un MX chez OVH. En pratique je coinche sur l'utilité du MX en ADSL... Vous devriez juste avoir un MX chez OVH de secours et ça serait pleinement suffisant.
- C'est bien d'avoir des MX de secours, mais vérifiez aussi que vous avez des slaves DNS chez OVH pour éviter d'imiter ce que faisait la DSI de l'ENS l'an dernier. Pas de nom de domaine = mails perdus.
- Quoi que vous fassiez, vous aurez sûrement un uptime plus grand que la DSI de l'ENS et un meilleur service (car le filtre Renater est VIOLENT).

Les backups

Fantôme erdnaxe : on a déployé BorgBackup au Crans et c'est SUPER CHOUETTE. 5 étoiles, recommande à 100%, passez d'excellentes vacances, le petit déjeuné était parfait, rien à redire.

<https://www.borgbackup.org/> (<https://www.borgbackup.org/>)

Pas de **vrai** appendonly :

<https://borgbackup.readthedocs.io/en/stable/usage/notes.html?highlight=appendonly#append-only-mode> (<https://borgbackup.readthedocs.io/en/stable/usage/notes.html?highlight=append%20only#append-only-mode>)

Clusters

- Stockage?
 - avoir un NAS ?
 - glusterFS ?

RAM OVH

2 incidents en 2 mois. Proxmox réduit la qté de RAM des VM pour son propre fonctionnement et ça casse tout parfois (balloning).

Plan proposé:

- Récupérer le serveur des Rives
- Mettre le cluster en place
- Racheter du stockage pour les serveurs
- Migrer des services
- Regarder sur Horus s'il y a de la RAM pour mettre les mails dessus