Doc gestion serveur externe YunoHost

Philosophie

Comment la gestion du serveur YunoHost du LOV a été pensée

Gestion des utilisateurs

1. utilisateur YunoHost `admin` est **super administrateur** du serveur Yunohost et permet de gérer le serveur et les utilisateur/sauvegardes
2. utilisateur dédié au LOV nommé `adminlov` a été créé et toutes les données et applications doivent lui appartenir. C'est l'utilisateur **admin du lov** et est gestionnaire des données
3. Utilisateur des adhérents du LOV. Sont créés par les administrateurs du serveur
4. Lors de l'installation d'une nouvelle application sur le serveur, l'utilisateur `adminlov` doit être positionné comme **admin** de l'application.

Gestion des applications

Lors de l'installation d'une application dans YunoHost en général, il **faut** nommer un utilisateur comme "administrateur de l'aplication". pas possible de nommber un groupe.

Autant définir directement `adminlov` lors de l'instalation puis dans l'application, donner des droits à des groupes ou à des personnes. Losque le membre s'en va, les données ne sont pas perdues car ells appartiennent toujours à `adminlov`. Il suffit de "refaire un partage" aux nouveaux adhérents.

Techniquement, toutes les applications ne supportent pas d'avoir un "groupe d'utilisateur" comme "administrateur" et c'est compliqué à changer ensuite (souvent pas prévu facilement dans l'application).

gestion des adhérents de l'asso

Les adhérents qui en font la demande peuvent avoir un compte sur le serveur du LOV, il faut en faire la demande (ou automatique?)

Création compte utilisateur

Voir doc officielle sur comment faire dans YunoHost: https://yunohost.org/fr

Lors de la création:

1. utiliser le même pseudo que dans https://framateam.org/, ça permet de s'y retrouver lors de la l'AG
2. Si vous mettez votre identité réelle, elle sera visible via ce que vous publiez sur le serveur (nom et prénom). Si vous voulez un pseudonyme, mettre un prénom en pseudo et autre chose

comme nom.

Gestion des droits

Utilisateurs

Utilisateur	Description
admin	gère le serveur au global
adminlov	est admin des applis et données
adhérent X	est membre de l'asso

Groupes YunoHost de base

Groupe	Description
Visiteurs	tous les utilisateur non authentifiés
Tous les utilisateurs	tous les utilisateurs qui ont un compte sur YunoHost

Groupes ajoutés pour l'asso

Groupe	Description
conseil_administration	Membres du CA, ont des droits d'écriture et d'admin sur les applis quand possible
administrateurs	membres qui ont des droits admins sur le serveur (pas utilisé ce jour, remplacé par 'conseil_administration')

Applications installées

nom application	Description
Adminer	Gestionnaire BDD
Dokuwiki	wiki
Grav	site web test
Kanboard	kanban
Site web - dev	site web test
Site web	site web lov (site statique)
Nextcloud	fichiers + calendier + coffre fort numérique (keepass)
Redirect agenda	redirection web vers agenda
WordPress	blog

Nextcloud

Arborescence fichiers

Physiquement, les dossiers sont organisés

```
root@labovilleurbanne:~# tree /home/adminlov -d -L 2
/home/adminlov
```

```
├── Conseil administration
│   ├── Administratif
│   ├── coffre fort
│   ├── communication
│   ├── compta
│   ├── contentieux
│   ├── CR réunions et AGs
│   ├── demande sub
│   └── Suivi gros achats
├── temp
└── Vie Association
    ├── Administratif
    ├── ateliers
    ├── Boite à vrac
    ├── documentation-machines
    └── participation evenements
```

Quota espace disque

Limite fixée à 40Mo par adhérent. Pour forcer à mettre les documents dans les partages du LOV

https://docs.nextcloud.com/server/latest/user_manual/en/files/quota.html

Calendrier

Calendrier	Description
Permanances	calendier public qui liste les permanences du LOV
CA	calendrier privé pour organisation du CA

> https://labovilleurbanne.fr/agenda est un lien qui renvoit automatiquement vers le calendrier des permanences Utilisation de l'application redirect pour faire ce lien ==⇒ marche pas, il a fallu le

MDP

KeeWeb KO sur nouveau serveur, pas réussi à faire marcher:
https://github.com/jhass/nextcloud-keeweb/issues/204 ⇒ Migration sur
https://labovilleurbanne.fr/nextcloud/apps/passwords/ (ou pas)

- https://forum.chatons.org/t/a-propos-de-la-categorie-gestionnaire-de-mots-de-passe/684/3
- https://forum.chatons.org/t/bitwarden-le-serveur-depend-dun-logiciel-proprietaire/1531/10
- https://github.com/awesome-selfhosted/awesome-selfhosted#password-managers
- https://apps.nextcloud.com/apps/passman
- https://apps.nextcloud.com/apps/passwords
- Vaulwarden YunoHost
    - https://github.com/dani-garcia/vaultwarden

DokuWiki

Ajouter sidebar: https://www.dokuwiki.org/config:sidebar Authoriser le html: Permettre l'utilisation de code HTML dans les pages

Migration vers nouveau serveur

Tests fait au préalable via modifications de 'fichier hosts' puis fait sur le fournisseur DNS Gandi quand ok

bascule IPs

- Changer TTL DNS puis IP
  - TTL DNS 3600 (1h au lieu de 3h)
- Basculer de serveur
  - ancienne IP serveur: 51.15.217.89
  - nouvelle IP: 167.235.31.8
- Ajout ipv6 au passage via enregistrement AAAA

Sites inspirants:

- https://wiki.pcet.link/accueil?do=index
- https://wiki.apprentilab.cnam.fr/wiki:config?s[]=dokuwiki
  - https://wiki.apprentilab.cnam.fr/doku.php?do=index
  - https://wiki.apprentilab.cnam.fr/fab:machines:brodeuse_numerique
- https://wiki.lereset.org/start?do=index
- https://wiki.fuz.re/doku.php?id=projets:datapaulette&do=index

Documentation DokuWiki - https://docs.framasoft.org/fr/dokuwiki/ - https://wiki.picasoft.net/doku.php?id=asso:tuto:wiki&s[]=dokuwiki

Gestion email

Constat

Après instalation d'une application qui a besoin d'envoyer des mails, je n'ai rien reçu... Après recherche, le serveur du LOV n'envoie pas de mail, tout est délégué à Gandi pour le mail.

Piste pour que serveu r puisse envoyer du mail: https://forum.yunohost.org/t/permettre-aux-apps-denvoyer-du-mail-meme-si-le-serveur-de-mail-principal-est-ailleurs/10941/24

Sécurisation

Lutte contre le spam mail : Doc gandi en français ou en anglais

Il faut utiliser les trois protocoles:

- DKIM
- Enregistrement SPF
- DMARC

Au passage:

- Bascule sur “Gandi Live DNS”, nouvelle infra DNS
  - Permet de versionner la conf DNS automatiquement
  - Etre à jour côté Gandi ?
- Activation DKIM
  - Fait dans interface web Gandi
  - Ajout clée DKIM proposée par la conf YunoHost
    - `mail._domainkey 3600 IN TXT "v=DKIM1; h=sha256; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDWZBbH5pLdpYYPAMo+O7ZUVEi/7irHzz9BkUeBqu+Jhbh1g1WSB5p/hmouoPtBr8yNlxAn5FTQYIiqCUEsusP1VTvhMYj0wr7pjUq0zYHbu8CKZLlBQ51370dOHUSXSiKQylCZStJ0rpwjHDbqr+0a4umyQdEesbpWmtlTD2zGfwIDAQAB"`
- Modif SPF
  - avant: `@ 10800 IN TXT "v=spf1 include:_mailcust.gandi.net ?all"`
  - après: `@ 10800 IN TXT "v=spf1 a mx include:_mailcust.gandi.net ~all"`
    - Ajout champs a et mx pour autoriser les IP du serveurs à envoyer des mails en plus des serveurs gandi
    - Passage à `~all` pour durcir la configuration (voir https://en.wikipedia.org/wiki/Sender_Policy_Framework#Qualifiers et les RFC)
- Ajout enregistrement proposé par YunoHost, pas certain de l’utilité
  - `@ 3600 IN CAA 128 issue "letsencrypt.org"`

Sources: - https://easydmarc.com/blog/how-to-optimize-spf-record/ -

Outils pour tester la conf DNS: - https://mxtoolbox.com/SuperTool.aspx?action=mx%3alabovilleurbanne.fr&run=toolpage# - https://easydmarc.com/tools/domain-scanner?domain=labovilleurbanne.fr

Gandi

Création d’une équipe en plus que l’utilisateur du LOV et invitation envoyée à Gofannon pour avoir un “compte de secours” au cas où.

sources administration

- https://yunohost.org/en/admin_guide
- https://yunohost.org/fr/groups_and_permissions
- https://yunohost.org/fr/admin_interface
- https://moulinette.readthedocs.io/en/latest/ldap.html
- shcéma ?
    - Users groups and permissions