INSTALLATION SERVEUR Yonohost SUR KIMSUFI

- Objet : Installation d'un serveur Kimsufi en ssh pour Yunohost
- Niveau requis :
  débutant
- Commentaires : *Hébergement de services web.*
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !.
- Commentaires sur le forum : https://debian-facile.org/viewtopic.php?id=18837[1)]
- **Évolution 11/12/17** : Étant confronté au problème de faire un “su root” avec winscp (https://www.debian-fr.org/t/winscp-faire-un-su-root/70471/6), je vais reprendre ce tutoriel de façon à gérer cela au mieux en supprimant probablement la partie Mremmoteng.
- **Évolution 29/01/18**:De plus je suis entrain de passer sous openbsd.
- **Évolution 20/07/19**:Je suis passé sur un serveur chez online.net. De plus j'en ai profiter pour un louer un deuxième qui serra une plateforme d'essai dans un premier temps. La grande nouveauté est l'utilisation d'un seul outil de gestion ssh, sfps et profil de connexion au travers du logiciel bitvise client https://www.bitvise.com/ssh-client. Mais pour une première mise en place il est clair que l'utilisation de putty reste de mise. De plus je ne désespère pas de passer sous openbsd, donc ce tutoriel ne sera plus maintenu mais un autre verra le jour. Ce nouveau tutoriel est disponible ici:
  https://debian-facile.org/utilisateurs:michelw:tutos:installation-serveur-yunohost-maj

Yunohost chez Kimsufi (V1)

Ce serveur hébergé par Kimsufi supportera un serveur « lamp » et « mail » fourni par « Yunohost » en version 2.7 donc obligatoirement sur une base «Debian 8.x (Jessie)» 64bits. La gestion des paquets se fera avec les outils «APT» et avec l'éditeur «nano». Cette mise en place utilisera le protocole ssh et le logiciel client «kitty» et le programme connexe de putty; à savoir «puttygen». Ainsi que «winscp» et «notepad++» pour la mise à jour des fichiers du serveur et quelques lignes de commande. Pour mettre en œuvre une connexion en ayant changé l’utilisateur et le port par défaut avec une authentification utilisant une par clefs. Cette connexion sera également rendue accessible avec « mNremoteNG » et « keepass ».

Titre	Lien utiles
Kimsufi	https://www.kimsufi.com/fr/
Yunohost	https://yunohost.org/#/whatsyunohost_fr
Yunohost 2.7	https://forum.yunohost.org/t/en-fr-yunohost-2-7-testing/3293
Debian 8.x (Jessie) 64 bits	https://yunohost.org/#/install_on_vps_fr
Apt	https://debian-facile.org/doc:systeme:apt:clients
Nano	https://debian-facile.org/doc:editeurs:nano
Ssh	https://www.it-connect.fr/cours/comprendre-et-maitriser-ssh/https:/
Kitty	http://www.9bis.net/kitty/
Putty	https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
Winscp	https://winscp.net/eng/docs/lang:fr
Notepad++	https://notepad-plus-plus.org/fr/
mNremoteNG	https://mremoteng.org/

Keepass	http://keepass.info/
Ligne de commande	https://www.hostinger.fr/tutoriels/commandes-linux/#Etape-2-8211-Les-13-commandes-Linux-indispensables

INSTALLATION DU SERVEUR

PREMIERE CONNEXION SUR KIMSUFI

Après avoir créé un compte et loué votre serveur « Kimsufi » il s'agit maintenant de réaliser votre première connexion. A l'adresse de « kimsufi ».

Vous vous connectez avec votre mail et votre password que vous avez donnés lors de votre inscription à « kimsufi » lors de votre commande et vous installez une « Debian 8 » 64 bits.

Un message d'avertissement suit:

Vous êtes sur le point de réinstaller votre serveur avec la configuration suivante: Cette opération se traduira par la suppression de toutes les données du disque dur! Système d'exploitation Debian 8.7 stable (Jessie) (oldstable) Langue Français

Il suffit de continuer en connaissance de cause Vous recevrez à ce moment un mail qui vous donnera les paramètres du serveur suivant:

Le compte administrateur suivant a été configuré sur le serveur :

Nom d'utilisateur : root

Mot de passe : mot de passe

Sur le panneau d'accueil de votre espace kimsufi vous aurez également l'adresse Ipv4 de votre serveur:

Titre	Lien utiles
Kimsufi	https://www.kimsufi.com/fr/manager/?csid=ZTLQM#/login

PREMIERE CONNEXION EN SSH ET PARAMETRAGE DE MREMOTENG

Après avoir téléchargé dans sa dernière version et installée séparément «putty». Nous allons le paramétrer« mremoteNG» comme suit:

Et on se connecte en utilisant le mail fourni par « Kimsufi »:

Le message suivant nous avertit que la clé du serveur «ssh» n'est pas « cached in the registry », c'est-à-dire enregistrée sur notre ordinateur. Il faut valider le téléchargement de la clé pour établir la connexion en cliquant sur « Oui ».

On arrive alors sur un «shell». Pour cette première connexion on ne fera surtout pas de mise à jour du sytème avec le traditionnel:

```
apt update && apt upgrade
```

de manière à être sûr de ne pas changer de version de « debian ». Nous allons donc ouvrir le fichier « sources.list » pour forcer les mises à jours pour rester sur la version « jessie ». Ceci peut se faire avec nano mais nous choisirons « winscp ».

Titre	Lien
MremoteNG	https://mremoteng.org/

PARAMETRAGE DE WINSCP

Après avoir installé et lancer «winscp» nous allons dans un premier temps le paramétrer en adaptant trois paramètres dans le menu préférence de «winscp».

On choisi «notepad++» comme éditeur par défaut après l'avoir installé.

Et on choisi également de mettre comme client ssh, «putty». On affiche aussi les fichiers cachés.

Titre	Lien
Winscp	https://winscp.net/eng/download.php
Paramétrage winscp	https://github.com/recalbox/recalbox-os/wiki/acces-via-WinSCP-(FR)

VERIFICATION DU FICHIER « sources.list » WINSCP

On se connecte à notre serveur avec les paramètres suivants en acceptant la clef proposée et en enregistrant éventuellement le mot de passe.

On se déplace vers /etc/apt et en cliquant sur le fichier «sources.list» on obtient le fichier suivant:

sources.list

```
#deb http://debian.mirrors.ovh.net/debian/ jessie main
#deb-src http://debian.mirrors.ovh.net/debian/ jessie main

deb http://security.debian.org/ jessie/updates main
deb-src http://security.debian.org/ jessie/updates main

# jessie-updates, previously known as 'volatile'
deb http://debian.mirrors.ovh.net/debian/ jessie-updates main
deb-src http://debian.mirrors.ovh.net/debian/ jessie-updates main

# jessie-backports, previously on backports.debian.org
deb http://debian.mirrors.ovh.net/debian/ jessie-backports main
deb-src http://debian.mirrors.ovh.net/debian/ jessie-backports main

deb http://debian.mirrors.ovh.net/debian/ jessie main contrib non-free
deb-src http://debian.mirrors.ovh.net/debian/ jessie main contrib non-
free
```

que l'on compare à celui donné avec le lien de debian facile. On vérifie à ce moment que toutes les sources sont liées à jessie donc en aucun cas on ne pourra faire de mise à jour vers une autre version involontairement. Pour la mise à jour on peut alors faire un:

```
apt update && apt upgrade
```

Et on vérifie la version

```
cat /etc/debian_version
```

On obtient:

retour de la commande

```
8.9
```

Donc la mise à jour c'est bien effectuée puisque la version de départ installée sur « Kimsuffi » était la 8.7

Titre	Lien
Syntaxe sources.list	https://debian-facile.org/doc:systeme:apt:sources.list?s[]=sources&s[]=list&s[]=jessie#sourceslist-pour-debian-oldstable-jessie
Sources.list pour jessie	https://debian-facile.org/doc:systeme:apt:sources.list:jessie

UTILISATEUR NON PRIVILEGIE

On va d'abords créer un groupe de manière à éventuellement changer rapidement le nom de l’utilisateur qui lui seul aura accès à la connexion «ssh».

Attention à la fin de ce paragraphe vous n'aurez plus d'accès direct en « superutilisateur »

```
addgroup schtroumpf
```

On créé un utilisateur et son mot de passe: mdp

```
adduser schtroumpfette
```

On ajoute cet utilisateur existant dans le groupe existant.

```
adduser schtroumpfette schtroumpf
```

Avec winscp on ouvre /etc/ssh/sshd_config pour permettre l'accès ssh au groupe schtroumpf. Repérez la ligne avec « allowGroup », si elle n'y est pas ajoutez là à la fin du fichier.

```
allowgroups schtroumpf
```

Après être connecté en « root » il faut créer un répertoire «.ssh» dans «/home/ schtroumpfette»

```
mkdir .ssh
```

On va également changer le groupe et le propriétaire de ce dossier « .ssh »

```
chown schtroumpfette:schtroumpf .ssh
```

Puis mettre les droits sur « .ssh » pour que le répertoire ne soit accessible que pour notre utilisateur

```
chmod 700 .ssh
```

On vérifie les droits avec la commande:

```
ls -a -l
```

Qui renvoie

retour de la commande

```
drwx------  schtroumpfette schtroumpf
```

Et cela correspond bien au codage recherché car 700=rwx Puis finalement on relance le service

```
service sshd restart
```

Connectez-vous alors avec le compte « schtroumpfette » et cela fonctionnera. Pour récupérer les pleins pouvoirs, utiliser la commande « su », et le mot de passe root seras alors demandé. Après cela il faut paramétrer un nouveau compte avec le nouvel utilisateur sous « winscp » et « mRemoteNG ».

Ci-dessous l'exemple avec « mRemoteNG ».

Vous pouvez encore augmenter la sécurité avec « MaxStartups » par exemple.

Titre	Lien
Ajouter un groupe	https://debian-facile.org/doc:systeme:groupadd?s[]=addgroup
Ajouter un utilisateur	https://debian-facile.org/doc:systeme:adduser
Ajouter un utilisateur à un groupe existant	https://debian-facile.org/doc:systeme:adduser
Utilisation de AllowGroup	http://www.tuto-linux.com/tutoriel/acces-ssh-securise/
Création d'un utilisateur	https://www.papygeek.com/linux/authentification-ssh-par-cle/
Chown et chmod	http://www.leshirondellesdunet.com/chmod-et-chown
Commande ls	https://debian-facile.org/doc:systeme:ls
Redémarrer le service ssh	http://www.tuto-linux.com/tutoriel/acces-ssh-securise/
Accès ssh MaxStartups	http://linux-attitude.fr/post/bloquer-lacces-dun-serveur-ssh
Enlever authentification root	http://forum.ubuntu-fr.org/viewtopic.php?id=383526

CHANGEMENT DE PORT

Changer le numéro de port car il est balayé par les robots. Avec « nano » aller sous «/etc/ssh/» et éditez le fichier« sshd_config ».

```
nano sshd_config
```

puis à la ligne

sshd_config

```
Port 22
```

Remplacez le numéro du port en évitant ceux recommandez par wikipédia, attention le pavé numérique n'est pas actif avec « nano »

```
Port nnnn
```

Sauvegader le fichier en tapant la touche « Ctrl » et la touche « o » puis valider par la touche « Entrée ». Et enfin confirmer la sortie de « nano » en appuyant « Ctrl » et la touche « x » Il faut maintenant relancer le service ou deamon ssh. Pour cela on se connecte avec « mRemoteNG » puis on tape la commande suivante

```
service sshd restart
```

Après cela il faut sous «mRemoteNG» et «winscp» paramétrer un nouveau compte avec le nouveau port. Ci-dessous l'exemple avec « winscp ». Après un avertissement au démarage vous pourrez vous

connecter avec le nouveau port.

Titre	Lien
Changement numéro de port	https://www.hostinger.fr/tutoriels/changer-ports-ssh-vps/
Ports recommandés	https://fr.wikipedia.org/wiki/Liste_de_ports_logiciels

AUTHENTIFICATION PAR CLEFS

Il faut d'abord créer un fichier « authorized_keys »qui contiendra la clef public. Pour cela après s'être logué et pris l'identité « root » avec la commande « su » on va se déplacer dans: /home/schtroumpfette/.ssh puis dans ce dossier on créé un fichier « authorized_keys »

```
touch authorized_keys
```

On va maintenant générer la paire de clef pour cela on utilise « key generator »

On va mettre une « passphrase » avec éventuellment un commentaire permettant de la retrouver avec une taille de 4096. Puis on va sauver ces clefs dans leur fichier respectif « public_key.txt » et « private_key.ppk » Copier la clef publique en ayant ouvert un fichier avec «notepad++» puis en collant cette clef sur une seule ligne dans le fichier « authorized_keys » sur le serveur. Pour cela il faut éditer le fichier.

```
nano authorized_keys
```

avec un clique droit de la souris le clef est collée. Sauvegader le fichier en tapant la touche « Ctrl » et la touche « o » puis valider par la touche « Entrée ». Et enfin confirmer la sortie de « nano » en appuyant « Ctrl » et la touche « x ». Vérifiez votre fichier « /etc/ssh/sshd_config ». Après avoir pris l'identité « root » et vous être déplacé dans le bon dossier éditer le fichier « sshd_config »

```
nano sshd_config
```

Vérifier que la ligne « PubkeyAuthentication » soit bien à « yes », sinon ajouter là ou modifiez là : PubkeyAuthentication yes On modifie les droits en lecture et écriture juste pour le propriétaire du fichier « authorized_keys » en étant dans le répertoire « .ssh » de stroupfette

```
chmod 600 authorized_keys
```

On va également changer le groupe et le propriétaire du fichier « authorized_keys »

```
chown schtroumpfette:schtroumpf authorized_keys
```

Et on relance le service

```
service sshd restart
```

Titre	Lien

Authentification par clef	https://www.papygeek.com/linux/authentification-ssh-par-cle/
Authentification par clef	http://www.woueb.net/2011/09/13/authentification-ssh-cle-publique-windows/
Gestion de son dossier home	http://www.tuto-linux.com/tutoriel/acces-ssh-securise/
Déplacement dans l'arborescence	https://www.hostinger.fr/tutoriels/commandes-linux/#Etape-2-8211-Les-13-commandes-Linux-indispensables
Nano	https://korben.info/utiliser-nano.html
Key generator	https://wwhttps://www.chiark.greenend.org.uk/~sgtatham/putty/latest.htmlw.chiark.greenend.org.uk/~sgtatham/putty/latest.html

PARAMETRAGE DE PUTTY

« NremoteNG » utilise « putty » pour faire l'authentification par clef. C'est pourquoi nous allons d'abord paramétrer « putty » comme suit.

Sans oublier de sauvegarder la session. En cliquant sur son nom à ce moment on peut se connecter par clefs!

Mais il faudra se souvenir de la passphrase à la première connexion

Titre	Lien
Clef avec putty	https://www.howtoforge.com/ssh_key_based_logins_putty
Forme de le clef	https://www.howtoforge.com/how-to-configure-ssh-keys-authentication-with-putty-and-linux-server-in-5-quick-steps
Clef avec putty autre lien	https://mediatemple.net/community/products/dv/204644740/using-ssh-keys-on-your-server

PARAMETRAGE DE MREMOTENG

Mais il faudra se souvenir de la passphrase à la première connexion

Titre	Lien
Configuration NremotNG	http://technotes.khitrenovich.com/opening-ssh-aws-hosted-linux-servers-mremoteng/

PARAMETRAGE DE WINSCP

En suivant les étapes ci-dessous on fera le paramétrage de « winscp » pour avoir l'accès au seerveur

par clefs.

Il faudra se souvenir de la passphrase!

La connexion sera alors disponible dans à l'accueil de « winscp »

Titre	Lien
Authentification par clef et paramétrage winscp	https://www.oceanet-technology.com/blog/authentification-ssh-paire-de-cles-priveepublique/

PARAMETRAGE DE KEEPASS

Ici la passphrase sera enregistrée. Vous n'aurez plus à vous en souvenir

Il s'agit ici d'automatiser la connexion. Mais attention en cas de vol de vos clefs vos accès serons perdus. Ceci est donc à mettre en place à vos risques et périls. Il est d'usage pour ce faire d'utiliser « pageant ». Pour ma part j'utilise au quotidien « keepass » qui sera utilisé pour lancer la session « putty ». A l'aide plugin « keeagent » qui permet d'appeler les clefs en se servant de la session créée sous « putty ». Après avoir installé « keepass» et son plugin « keeagent » on fait le paramétrage suivant:

Mais il faudra se souvenir de la passphrase à la première connexion

Titre	Lien
Automatisation	https://eric.bugnet.fr/keepass-putty-connexion-automatique/
Keepass et keeagent	http://keepass.info/plugins.html#keeagent
Putty en ligne de commande	http://marc.terrier.free.fr/docputty/chapter03.html#utilisation-de-putty-en-ligne-de-commande
Keeagent	http://lechnology.com/software/keeagent/

SUPPRESSION DE LA CONNEXION ROOT

Cette étape est inutile puisque seul les utilisateurs de «allowgroups» peuvent se connecter en ssh.

Vous ne pourrez plus vous connecter avec la session «root» directement. Dans le fichier de

configuration avec « nano » aller sous «/etc/ssh/» et éditez le fichier« sshd_config » ajoutez ou dé-commenter les lignes :

```
nano sshd_config
```

sshd_config

```
PermitRootLogin no
```

Et on relance le service

```
service sshd restart
```

Titre	Lien
Enlever authentification root	http://forum.ubuntu-fr.org/viewtopic.php?id=383526

SUPRESSION DE L'ACCES PAR MOT DE PASSE

Retirer cette authentification ne vous permettra plus de vous connecter avec votre mot de passe, et

 vous ne pourrez que vous connecter que depuis l'utilisateur non privilégié

sur le port que vous avez défini et avec les clefs et lui seul! Réfléchissez bien avant de faire ça! Dans le fichier de configuration avec « nano » aller sous «/etc/ssh/» et éditez le fichier« sshd_config » ajoutez ou décommenter les lignes :

```
nano sshd_config
```

sshd_config

```
PasswordAuthentication no
```

Et on relance le service

```
service sshd restart
```

Titre	Lien
Enlever authentification par passe	http://support.netissime.com/Knowledgebase/Article/View/96/8/desactiver-lacces-root-via-ssh-sur-votre-serveur-linux

INTEGRATION DE WINSCP DANS MREMOTENG

Il s'agit simplement de mettre un raccourci dans «mremoteng» pour lancer «winscp»

Avec les paramètres suivants:

```
Nom affiché: WinSCP

Nom du fichier: C:\Program Files (x86)\WinSCP\WinSCP.exe

Arguments: scp://%Username%:%Password%@%Hostname%/
```

Maintenant avec cette session vous aurez accès à «winscp» directement à partir de «mremoteng».

Titre	Lien
Winscp mremotemg	https://github.com/mRemoteNG/mRemoteNG/wiki/Common-External-Tool-Configurations

INSTALLATION DU YUNOHOST

SUPPRESSION DE BIND

Sous «Kimsufi» le serveur de noms «bind» est installé par défaut et il rentre en conflits avec «dnsmasq» qui lui est utilisé pour «yunohost». En va consulter la liste des paquets installés.

```
dpkg --list
```

«Bind» est présent ici:

```
bind9
bind9-host
bind9utils
```

On va donc supprimer ces paquets.

```
apt-get autoremove bind9
```

Titre	Lien
Lister les paquets installés	https://www.it-connect.fr/lister-tous-les-paquets-installes-sous-linux/
Supprimer un paquet	https://doc.ubuntu-fr.org/apt-get

DNS BOOKMYNAME

Si vous avez acheté un nom chez bookmyname. Nous allons le configurer pour que votre «instance «yunohost» soit accessible sur le web.

On écrit le fichier «dns»

On choisi les serveurs «dns»

Titre	Lien
Bookmyname	https://www.bookmyname.com/

SCRIPT YUNO

Installez git

```
apt-get install git dialog
```

Clonez le dépôt du script d'installation de YunoHost

```
git clone https://github.com/YunoHost/install_script /tmp/install_script
```

Lancez le script d'installation

```
cd /tmp/install_script && ./install_yunohost
```

Au bout d'un certain temps il vous est demandé de faire la post-installation:

Durant cette post-installation on vous demande votre nom de domaine et le mot de passe administrateur de «yunohost»:

retour de la commande

```
Domaine principal : votredo.maine
Nouveau mot de passe d'administration : (mot de passe pour la connexion
web)
Confirmez : nouveau mot de passe d'administration :
Succès ! L'annuaire LDAP a été initialisé
ip NNN.NNN.NNN.NNN
Succès ! La configuration a été mise à jour pour le service « ssl »
Succès ! L'autorité de certification locale a été créée.
Succès ! La configuration a été mise à jour pour le service « nsswitch
»
Succès ! Installation avec succès d'un certificat auto-signé pour le
domaine votredo.maine !
Succès ! Le domaine a été créé
Attention : You are inside a container and hostname cannot easily be
changed
Succès ! La configuration de SSOwat a été générée
Succès ! Le domaine principal a été modifié
```

```
Succès ! Le mot de passe d'administration a été modifié
Succès ! Le pare-feu a été rechargé
Succès ! La liste d’applications yunohost a été récupérée
update-rc.d: error: no runlevel symlinks to modify, aborting!
Attention : Le fichier de configuration « /etc/default/glances » est
désormais géré par le service glances.
Succès ! La configuration a été mise à jour pour le service « glances »
Attention : Le fichier de configuration « /etc/nslcd.conf » est
désormais géré par le service nslcd.
Succès ! La configuration a été mise à jour pour le service « nslcd »
Attention : Le fichier de configuration «
/etc/metronome/metronome.cfg.lua » est désormais géré par le service
metronome.
Succès ! La configuration a été mise à jour pour le service « metronome
»
Attention : Le fichier de configuration « /etc/postfix/master.cf » est
désormais géré par le service postfix.
Attention : Le fichier de configuration « /etc/postfix/main.cf » est
désormais géré par le service postfix.
Succès ! La configuration a été mise à jour pour le service « postfix »
Succès ! La configuration a été mise à jour pour le service « rspamd »
Succès ! La configuration a été mise à jour pour le service « nginx »
Attention : Le fichier de configuration « /etc/rmilter.conf » est
désormais géré par le service rmilter.
Succès ! La configuration a été mise à jour pour le service « rmilter »
Attention : Le fichier de configuration « /etc/default/dnsmasq » est
désormais géré par le service dnsmasq.
Attention : Le fichier de configuration « /etc/dnsmasq.conf » est
désormais géré par le service dnsmasq.
Succès ! La configuration a été mise à jour pour le service « dnsmasq »
Attention : Le fichier de configuration « /etc/fail2ban/jail.conf » est
désormais géré par le service fail2ban.
Succès ! La configuration a été mise à jour pour le service « fail2ban
»
Attention : Le fichier de configuration « /etc/mysql/my.cnf » est
désormais géré par le service mysql.
Succès ! La configuration a été mise à jour pour le service « mysql »
Attention : Le fichier de configuration « /etc/avahi/avahi-daemon.conf
» est désormais géré par le service avahi-daemon.
Succès ! La configuration a été mise à jour pour le service « avahi-
daemon »
Attention : Le fichier de configuration « /etc/dovecot/dovecot.conf »
est désormais géré par le service dovecot.
Succès ! La configuration a été mise à jour pour le service « dovecot »
Succès ! La configuration a été mise à jour pour le service « slapd »
Succès ! YunoHost a été configuré
Success !

Installation logs are located in /var/log/yunohost-installation.log
```

Il reste maintenant à paramétrer les certificats «https» fournis par «let's encrypt».

Titre	Lien
Script	https://yunohost.org/#/install_manually_fr

CERTIFICAT LET'S ENCRYPT

Tapez simplement la commande suivante pour installer les certificats.

```
yunohost domain cert-install
```

Et voici le retour

retour de la commande

```
Succès ! La configuration de SSOwat a été générée
Succès ! Installation avec succès d’un certificat Let’s Encrypt pour le
domaine votredo.maine !
root@ns:/tmp/install_script#
```

En allant sur votre navigateur préféré et en tapant votre nom de domaine:

```
votredo.maine
```

Vous allez être rediriger vers la page de démarrage de «yunohost»

retour de la commande

```
https://votredo.maine/yunohost/admin/#/login
```

Titre	Lien
Letsencrypt	https://yunohost.org/#/certmanager_fr

INSTALLATION DES UTILISATEURS

Avant d'installer une application, déclarer un utilisateur. Pour sécuriser vos applications je vous conseil d'en déclarer un différent pour chaque applications. Attention ces utilisateurs seront administrateur de votre application. Pour le mettre en place il suffit d'aller dans la rubrique utilisateur et de l'ajouter par défaut dans «yunohost» tous les utilisateurs créés ont accès à toutes las applications.

Pour nexcloud:

Tous les utilisateurs créés dans «yunohost» apparaitront dans les contacts mais seul le premier sera administrateur pour «nextcloud». Vous pourrez enlevez ceux que vous

souhaitez supprimer avec votre compte administrateur et vous ne pourrez alors plus vous connecter avec ceux-ci. Mais un utilisateur créé dans «nextcloud» pourra toujours envoyer un mail car ils restent visibles dans «contact»

N'oubliez pas de changer les paramètres de sécurité dans: Administration - Sécurité - Politique des mots de passe

.

Titre	Lien
Panneau de l'interface web	https://yunohost.org/#/admin_fr

INSTALLATION DES APPLICATIONS

Il suffit de choisir une application dans la liste et de l'installer en répondant aux questions posées et éventuellement en la choisissant comme application par défaut auquel cas vous arriverez directement sur celle-ci en tapant votre nom de domaine. Attention à bien attendre la fin de l'installation avant de commencer une autre opération. Puis précisez bien les utilisateurs qui auront accès à l'application car par défaut tous les utilisateurs enregistrés dans «yunohost» ont accès aux applications installées.

Titre	Lien
Applications officielles	https://yunohost.org/#/apps_fr
Applications fonctionnelles	https://yunohost.org/#/apps_in_progress_fr

1)

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !