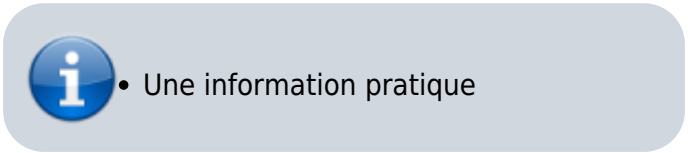
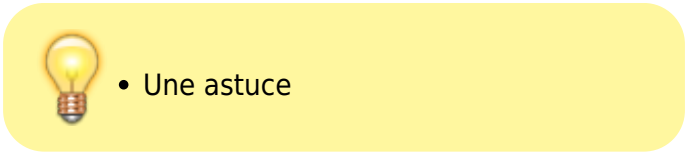
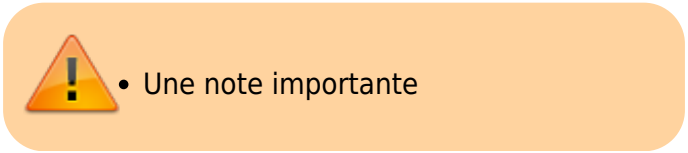
GUIDE UTILISATEUR

Voici un petit guide de prise en main rapide pour les utilisateurs. La syntaxe suivante est utilisée pour :

- ***une définition informatique*** (provenant du jargonf informatique)
- `une commande unix à taper dans un terminal`
- un chemin pour atteindre une fonction dans KerHost
- **une action importante**
- Le terme générique **votre_domaine** utilisé dans ce guide correspond au nom de domaine de votre serveur qui vous héberge.
- Les termes génériques **votre_nom_de_connexion / votre_mot_de_passe** font référence à vos identifiants utilisateur de **votre_domaine**.
- Le terme PORTAIL ⇒ correspond à l'url du portail du serveur après authentification, à savoir http://www.**votre_domaine**.







1-Votre compte utilisateur

Vous venez de faire une demande de création de compte et c'est chose faite ! Votre compte vient d'être ouvert avec les identifiants que vous avez indiqués dans le formulaire d'inscription. Votre compte principal sur farmserv est avant tout un compte ***unix*** [1)]. Chaque compte est accessible en ***SSH*** [2)]. Une connexion SSH vous permet d'accéder à votre espace disque (***home directory*** [3)]) en ligne de commande, et d'interagir directement sur le serveur comme si vous y étiez. C'est la façon la plus rapide de manipuler votre espace de stockage. Pour vous connecter, vous devez taper dans un ***terminal*** [4)] la commande suivante :

```
ssh votre_nom_de_connexion@votre_domaine
```

Si vous êtes sous Windows ou Mac et que vous ne disposez pas d'un terminal, vous pouvez utiliser le terminal intégré à l'interface de gestion en passant par PORTAIL ⇒ Mon compte ⇒ Ma boîte à outils ⇒ Accéder au terminal votre_domaine.

Attention !!! Depuis la version **5.0** de **farmserv** (et si l'option a été activée), il n'est plus possible de se connecter directement en SSH sans avoir fait **valider son adresse IP** dans son interface de gestion mon. Par contre, il est possible d'utiliser le service terminal.

Par défaut, votre home directory contient à la création de votre compte 4 répertoires : **Maildir**, **nextcloud**, **sauvegardes** et **www** :

- **Maildir** est le répertoire où sont stockés vos mail. À manipuler en connaissance de cause !
- **nextcloud** est le répertoire qui vous permet de stocker/partager n'importe quel type de documents. C'est votre répertoire Cloud. Il n'est pas directement accessible ou modifiable en FTP/SSH. Seul NextCLoud peut y accéder.
- **sauvegardes** est le répertoire où vous allez pouvoir à partir de l'interface de gestion réaliser et stocker automatiquement certaines sauvegardes importantes.
- **www** est le répertoire qui permet de stocker vos sites web perso.

Vous pouvez ajouter, supprimer et modifier répertoires et fichiers à votre guise dans votre home directory, mais :

Il est important de ne pas **supprimer** ces 4 répertoires et de ne surtout **rien faire dans le répertoire Maildir** qui est géré exclusivement par le serveur de mail et **nextcloud** que seul NextCloud peut modifier lui même !

Votre adresse mail principale (dite adresse canonique) est composée de la sorte : **votre_nom_de_connexion@votre_domaine** Vous pouvez consulter les informations de votre profil ici : PORTAIL ⇒ Mon compte ⇒ Mon profil et l'éditer ici : PORTAIL ⇒ Mon compte ⇒ Modifier mon profil. Si vous le souhaitez, vous pouvez apposer à votre profil une **photo** (avatar) pour le **trombinoscope** des utilisateurs qui sera visible sur le PORTAIL et PORTAIL ⇒ Mon compte.

2-Le portail

Pour accéder globalement aux ressources de **KerHost**, il suffit de se connecter sur le portail http://www.**votre_domaine**. Vous aurez accès à l'intégralité des services, ainsi que l'interface de gestion de votre compte utilisateur. Elle permet par exemple d'accéder à vos informations

personnelles, à activer vos services web, à administrer vos sites web perso,... et plein d'autres choses.

Si vous êtes **déclaré comme administrateur du système KerHost**, alors le portail vous donne accès en plus à l'interface d'administration.

3-HTTP ou HTTPS ?

Tous les services web proposés sur KerHost sont accessibles avec le protocole de sécurisation ***HTTPS*** [5]. Cela veut dire que vous pouvez atteindre un service de deux façons :

- En **http**, protocole standard qui ne nécessite aucun certificat de sécurité. Les données qui transitent entre le serveur et votre navigateur circulent en clair sur le réseau.
- En **https**, protocole qui permet de crypter les données à l'aide d'un certificat de sécurité SSL rendant difficilement W analysable le réseau.

La gestion du serveur permet aux administrateurs d'autoriser les deux **protocoles** mais aussi de forcer les services exclusivement sur le https ! Donc il se peut que le http de certains (ou tous !) services soit désactivé.

Utiliser le protocole https nécessite d'accepter le ***certificat*** si **Let'sEncrypt** n'est pas utilisé [6]. Pour savoir si votre instance utilise des **certificats de sécurité certifiés Let's Encrypt**, il suffit de regarder l'état du **cadenas** qui se trouve dans la **barre de saisie de l'URL** du service. Si il est **vert**, le certificat est **certifié**, sinon, c'est qu'il est **auto-signé**. Si le certificat est **auto signé**, vous devez autoriser ce certificat pour chaque service manuellement. La pénibilité de la gestion des certificats non certifiés dépend essentiellement du navigateur utilisé. Certains navigateurs vous demanderont systématiquement de confirmer à chaque fois le certificat et d'autre non.

Pour Firefox, vous obtiendrez un message lors de la première connexion à un service https vous indiquant que Cette connexion n'est pas certifiée (elle ne l'est pas en effet, mais seulement aux yeux des instances de certification). Cliquez sur Je comprends les risques et sur Ajouter une exception... Attendez 5 secondes, vérifiez que la case Conserver cette exception de façon permanente soit bien cochée et cliquez sur Confirmer l'exception de sécurité. Voilà. Maintenant vous pouvez naviguer sur le serveur en toute sécurité. Les échanges de données entre votre ordinateur et le serveur seront cryptés.

Pour Google Chrome (sous linux), vous pouvez lancer l'application avec la ligne de commande `google-chrome-beta –ignore-certificate-errors` à partir d'un terminal (ou alors créer un petit script bash que vous pouvez placer dans /usr/bin/) afin de ne pas être importuné par les messages d'alerte.

Le fait d'**accepter un certificat de sécurité** non certifié par un organisme agréé ne change en rien sa **fiabilité**. Cela veut juste dire qu'il n'est pas certifié !

4-Mon profil

Vous pouvez consulter votre profil utilisateur à partir de PORTAIL ⇒ Mon compte ⇒ Mon profil. Vous y trouverez les **informations générales** (les infos saisies lors de la création de votre compte à partir du formulaire d'inscription), **informations entité** (l'entité dont vous dépendez) et les informations d'administration système (si vous êtes administrateur ou non du serveur).
Vous pouvez modifier une partie des informations générales (PORTAIL ⇒ Mon compte ⇒ Modifier mon profil) :

- Adresse postal
- Code postal
- Ville de domiciliation
- Votre pays de résidence
- Votre téléphone
- Votre email de secours (qui sert par exemple à réinitialiser votre mot de passe)
- Photo de trombinoscope (voir trombinoscope)

5-Votre boîte mail

Chaque utilisateur dispose automatiquement d'une boîte ***mail*** [7] (de type ***IMAP*** [8] pour le serveur de réception et de type ***SMTP*** [9] pour le serveur d'envois).
Votre adresse canonique est : **votre_nom_de_connexion@votre_domaine**
Votre adresse principale est : **alias_mail_que_vous_avez_choisi_a_l_inscription@votre_domaine**
Vous avez 2 possibilités pour consulter votre boîte mail :

1. Utiliser le service ***webmail*** [10] RoundCube (http://mail.**votre_domaine**/ ou PORTAIL).
2. Utiliser un logiciel de mail indépendant.

Pour l'utilisation du webmail, il vous suffit de vous connecter avec **votre_nom_de_connexion** et **votre_mot_de_passe**, tout simplement. Si vous décidez d'utiliser un logiciel de mail indépendant (thunderbird, OutLook, Mail...), alors vous allez avoir besoin des paramètres suivants pour configurer votre compte :

Adresse email :
alias_mail_que_vous_avez_choisi_a_l_inscription@votre_domaine
Serveur IMAP : **votre_domaine**
Port : **993**
Login : **votre_nom_de_connexion**
Password : **votre_mot_de_passe**
Sécurité de la connexion : **SSL/TLS**
Méthode d'authentification : **mot de passe normal**
Serveur SMTP : **votre_domaine**
Port : **587**
Authentification : **votre_nom_de_connexion**
Password : **votre_mot_de_passe**
Sécurité de la connexion : STARTTLS
Méthode d'authentification : **mot de passe normal**

Les logiciels de mail détectent en général assez bien les **paramètres de configuration** à partir de votre **adresse email** (**KerHost** propose un fichier d'auto configuration sur le domaine principal). Mais il se peut que ça foire dans certains cas. Il est donc **important** de bien vérifier les paramètres qu'il a détecté, surtout **Thunderbird** !

Vous pouvez retrouver toutes ces informations de paramétrage de votre messagerie sur PORTAIL ⇒ Mon compte ⇒ Mon mail ⇒ Paramètres/Sauvegarde de ma boîte mail .
Si l'instance utilise Let'sEncrypt pour la gestion des certificats de sécurité, alors il n'y a rien à faire. En revanche si elle utilise des certificats auto signés, vous allez être obligé d'accepter (seulement la première fois, rassurez-vous !) les deux certificats de sécurité (imap et smtp) lors du paramétrage (ou à la réception/envoi des premiers mails).

RECOMMANDATION : On utilise en général le webmail de façon **nomade** (voyage, vacances, travail...) et un logiciel de mail de façon **sédentaire** (maison, ou sur smartphone/tablette). Il est beaucoup plus utile d'utiliser un logiciel de mail chez soi pour les raisons suivantes :

- **Rapidité**. Un webmail est une interface web qui se charge via internet et qui prend beaucoup plus de temps à charger alors qu'un logiciel de mail se lance quasi instantanément.
- **Plus d'options**. Un logiciel de mail vous proposera bien plus d'outils pour gérer vos mails qu'un webmail.
- **Utilisation offline**. Un logiciel de mail permet de consulter vos anciens mails sans avoir à être connecté à internet, ce qui n'est pas le cas du webmail.

Pensez aux alias mail ! N'utilisez surtout pas votre adresse canonique **votre_nom_de_connexion@votre_domaine**, c'est une aberration !

En cas de dysfonctionnement grave de votre boîte mail (mauvaise utilisation de Ferchmail ou Procmail) ou tout simplement pour repartir de zéro, vous pouvez réinitialiser votre répertoire Maildir pour revenir à son état initial. Pour cela : PORTAIL ⇒ Mon compte ⇒ Mon mail ⇒ Réinitialiser ma boîte mail . **Attention !!! Cela efface tous les mails** et c'est irréversible. Il est conseillé de faire une sauvegarde avant.

La taille maximum des messages en **envois** et en **réception** est de **10Mo**. Le mail est un outils de communication, pas d'échange de fichier. Pour cela il est préférable d'utiliser le service de partage.

5.1-Les alias mail

Alias mail

Vous pouvez vous ajouter des alias mail supplémentaires pour votre ***adresse canonique*** [11]. Ce sont des variantes du nom de votre adresse mail principale. La gestion des alias passe par PORTAIL ⇒ Mon compte ⇒ Mon mail ⇒ Gérer mes alias mail . Un alias mail est toujours rattaché à votre adresse canonique (**votre_nom_de_connexion@votre_domaine**). Tout mail envoyé sur un alias mail atterrira forcément sur votre adresse canonique.
Concrètement, pourquoi utiliser des alias mail ?

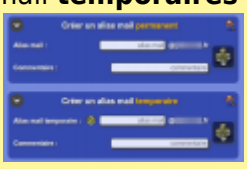
- Ne pas diffuser votre adresse canonique (lutter contre le SPAM donc)
- Disposer de variantes pour différents domaines d'utilisation

Attention ! Votre adresse canonique ne peut pas être modifiée. Elle est liée **intrinsèquement** à votre **nom de connexion utilisateur** (**login**) qui ne peut pas être modifié également. Il est donc impératif de bien comprendre qu'un alias mail est **quasi indispensable**. Si vous diffusez votre adresse canonique d'une quelconque façon, alors considérez de suite cet acte comme **suicidaire** pour celle-ci !
Notez qu'il n'est pas possible de choisir un nom d'alias mail existant déjà dans la base de données.

RECOMMANDATION : Se **créer** un alias mail est **la première chose à faire** avant d'utiliser votre boîte mail, tout simplement pour préserver votre adresse canonique (**votre_nom_de_connexion@votre_domaine**). Le SPAM est un vrai fléau qu'il faut combattre intelligemment. Votre adresse canonique ne pourra pas être modifiée alors qu'un alias mail oui. Il peut même être supprimé et remplacé par un autre à tout instant. Donc, il ne faut pas utiliser votre adresse canonique !
Voici un exemple d'utilisation des alias mail pour un utilisateur (nous prendrons l'utilisateur Raoul DUGENOUX dépendant du domaine youpla.org pour cet exemple) :

- **adresse canonique** : *raoul@youpla.org* (ne communiquera jamais cette adresse !)
- **alias mail principale** : *raoul.dugenoux@youpla.org* (adresse qu'il transmettra à son cercle privé de connaissances)
- **mail dit “pourriel”** : *raoul.poubelle@youpla.org* (adresse qu'il transmettra pour laisser des commentaires sur les forums, ou alors faire un achat sur des sites marchands)
- **alias mail pour le travail** : *raoul.maxiprout@youpla.org* (adresse qu'il transmettra uniquement avec les gens en relation avec sa boîte de travail ®MaxiProut)
- ...

Et ainsi de suite... Le jour où un alias mail pose problème (trop de spam), hop suffit de le supprimer !
Vous pouvez même pousser à l’**extrême** l'utilisation des alias en vous créant un alias mail à chaque fois que vous avez besoin d'une adresse “pourriel” (inscription...) et le supprimer tout de suite après !

Vous pouvez également générer des alias mail **temporaires** qui seront automatiquement détruits à minuit. 

Dans **thunderbird**, il est très facile de gérer simultanément plusieurs alias mail à partir de votre adresse canonique. Vous configurez normalement votre adresse canonique, et ensuite, vous allez dans :

- Édition ⇒ Paramètres des comptes
- Sélectionnez le premier niveau de votre adresse canonique et cliquez sur le bouton Gérer les identités
- Cliquez sur Ajouter pour ajouter un alias mail
- Configurer le compte
- Répéter autant que vous avez d'alias mail

Maintenant, vous disposez lors de la création d'un nouveau message du choix de l'adresse mail dans le menu expéditeur.

alias2.png

Partage

Le **partage** d'alias mail permet si vous le souhaitez de rendre accessible tous les mails à destination d'un de vos alias mail à un autre utilisateur de **votre_domaine**. Cela est pratique notamment pour les associations. Exemple concret :
Une entité de type **ASSOS** dispose de 3 comptes utilisateurs. Un compte par membre du bureau (président, trésorier et secrétaire). Le président dispose d'un **alias mail** sur son compte principal comme adresse de contact de son association. Il pense que ça serait bien que le trésorier puisse recevoir les mails qui arrivent sur cette adresse (alias mail) de contact, ainsi que le secrétaire. Il se rend sur son interface de gestion d'alias mail (PORTAIL ⇒ Mon compte ⇒ Mon mail ⇒ Gérer mes alias mail) et ajoute les **logins** des utilisateurs avec qui il veut partager son alias mail en cliquant sur en face de l'alias mail. Les autres utilisateurs recevront dès lors les mails arrivant sur cet alias mail directement sur leurs boîtes mail principales.
Pour supprimer un partage d'alias, il suffit de cliquer sur la croix à côté de l'avatar du partage

Mappage

Le **mappage** est comme un alias mail, sauf qu'on fait directement **transiter** les mails d'un utilisateur vers un autre utilisateur. L'alias mail devient alors un **login** que l'on associe à un autre **login**.
Exemple concret :
Une entité de type **ASSOS** dispose de 4 comptes utilisateurs. Un compte par membre du bureau (président, trésorier et secrétaire) plus un compte générique pour l'association qui appartient en réalité au président (il a deux comptes utilisateurs donc). Le président de l'association en a marre de jongler en permanence entre sa boîte mail et celle de l'association. Il peut alors mapper la boîte mail du compte générique sur celle de son compte. Ainsi tous les mails du compte générique arriveront sur sa boîte mail de président. Pour cela, il doit se connecter avec le login du compte générique sur PORTAIL ⇒ Mon compte ⇒ Mon mail ⇒ Gérer mes alias mail ⇒ Mapper ma boîte mail vers un autre compte utilisateur et saisir le login de son compte de président. C'est tout. Dès lors, les mails arrivant

sur le compte générique sont déplacés (pas copiés, mais déplacés, cela veut dire qu'ils ne sont plus consultables sur la boîte mail du compte générique de l'association) sur la boîte mail du président.

5.2-Fetchmail

Fetchmail est un outil unix qui vient s'intercaler entre le serveur de mail et votre boîte mail et qui permet d'associer d'autres boîtes mail que vous possédez (gmail, orange, free, hotmail, yahoo...) et de rapatrier automatiquement leurs contenus à intervalles réguliers sur votre adresse canonique. Vous n'aurez donc plus par la suite à gérer ces boîtes mail. C'est votre adresse principale qui s'en occupera. L'association de ces boîtes mail externes passe par PORTAIL ⇒ Mon compte ⇒ Mon mail ⇒ Gérer mes boîtes mail externes . Les champs suivants sont requis pour ajouter un compte :

- Adresse email du compte
- Prestataire (choisir autre s'il n'est pas présent dans la liste)
- Si autre, serveur de réception
- Si autre, protocole utilisé (pop ou imap)
- Si autre, utilisation du protocole SSL (oui ou non)
- Nom de connexion (login)
- Mot de passe (password)

Référez-vous à l'aide en ligne pour plus d'informations sur son utilisation.

Les **informations** de ces comptes mail externes sont stockées dans un fichier **.fetchmailrc** qui se trouve à la racine de votre **home directory**.

Attention !!! Dans le cas d'un compte email de type POP3, l'intégralité de la boîte de réception sera rapatriée et supprimée du serveur original !!!

mon_fetchmail.png

5.3-Procmail

Procmail est également un outil unix qui vient s'intercaler entre le serveur de mail et votre boîte mail et qui permet d'appliquer des actions automatiques sur celle-ci comme classer (structurer) votre boîte mail directement sur le serveur (et non sur votre client mail comme peut le faire thunderbird avec les règles). La gestion des règles **Procmail** se fait dans : `PORTAIL ⇒ Mon compte ⇒ Mon mail ⇒ Gérer le classement automatique de ma boîte mail et mon répondeur`. **Procmail** permet :

- d'**ajouter/supprimer** des **répertoires** dans votre **Maildir**

- Créer des **règles** de **classement automatique** sur les critères de **titre**, **destinataire** et **corps** du message
- Ajouter des **règles** de **transfert automatique** vers une autre **adresse mail**
- d'activer le **classement automatique des SPAMS** dans le dossier **junk**
- d'activer la suppression automatique du SPAMS qui obtiennent des scores supérieur à **12**
- d'ajouter un **répondeur automatique** en cas d'absence
- d'**exclure** des adresses email/domaines avec possibilité de **réponse** automatique
- de **réinitialiser** toutes vos règles si ça ne marche plus !

Référez-vous à l'aide en ligne pour plus d'informations sur son utilisation.

Les **informations** de ces règles sont stockées dans un fichier **.procmailrc** qui se trouve à la racine de votre **home directory**. Il est tout à fait possible de modifier celui-ci en **ssh** si vous voulez peaufiner les réglages, à condition bien sur de savoir ce que vous faites !

Manipulez cet outil avec précaution et lisez bien les instructions. Une mauvaise manipulation peut vite rendre inutilisable votre boîte mail, voire le serveur de mail !

mon_procmail.png

6-FTP

Un des moyens les plus simples pour accéder à votre espace de stockage est d'utiliser le protocole ***FTP*** [12)]. Ce protocole permet à l'aide d'un logiciel dédié (il en existe plein) d'accéder à distance à votre **home directory** pour réaliser des manipulations sur vos répertoires et fichiers. Les paramètres pour établir une connexion FTP avec le serveur sont :

- **Serveur FTP** : *ftp.votre_domaine*
- **Port** : *21*
- **Nom de connexion** : *votre_nom_de_connexion*
- **Mot de passe** : *votre_mot_de_passe*

7-Messagerie instantanée JABBER

Ce service remplace l'utilisation de Skype, Wat'sApp et compagnie. Vous disposez d'un compte JABBER (***XMPP*** [13]) pour la ***messagerie instantanée*** [14]. Les login/password sont ceux de votre adresse mail (login : **votre_nom_de_connexion@votre_domaine**). C'est tout ce dont vous avez besoin pour paramétrer votre logiciel de messagerie instantanée. La connexion est sécurisée ***SSL***[15]. Vous devez donc accepter le certificat lors de la première connexion si celui-ci est auto-signé. Vous devez disposer d'un client JABBER. Pour les utilisateurs linux/ubuntu, il existe le superbe Dino, Empathy, Gajim ou bien encore Thunderbird (qui intègre une messagerie instantanée). Sous Android, Conversations fera l'affaire. Et pour pouvoir entrer en contact avec les autres utilisateurs, vous devez les ajouter à partir de votre logiciel client en entrant leurs adresses mail (pour les utilisateurs de l'instance) ou un identifiant JABBER. JABBER ne se limite pas aux utilisateurs de **votre_domaine**. Vous pouvez ajouter des contacts provenant d'autres serveurs JABBER. La visioconférence avec webcam, appels vocaux ou transferts de fichiers dépendent de votre client utilisé. Empathy supporte les trois sans problème. Il est toutefois conseillé d'utiliser le même client des deux côtés.

8-Sites web perso

En tant qu'utilisateur, vous bénéficiez d'un nombre illimité d'hébergement de sites web personnels sur le serveur. C'est une des fonctions essentiellement recherchée par les utilisateurs .La gestion des sites perso se fait ici : PORTAIL ⇒ Mon compte ⇒ Mes sites web.

Les actions possible sur chaque site web perso sont :

- **activer/désactiver** le site
- **éditer** les options du site
- faire une **sauvegarde** du site (+base de donnée)
- voir le fichier log en **accès**
- voir le fichier log des erreurs
- **accéder** directement au site
- connaître l'**état** du certificat (http, https, auto-signé ou certifié Let'sEncrypt)
- **supprimer** le site

Les options dans la gestion des sites web perso sont :

- **faire une demande** de site web en précisant le nom de sous domaine désiré
- **Activer/désactiver** son compte **MySQL/PhpMyAdmin**
- **Modifier** le **mot de passe** de son compte **MySQL/PhpMyAdmin**
- **Récupérer** son **mot de passe MySQL/PhpMyadmin** par mail

La politique de **validation** des **sites web perso** dépend de votre instance. Par défaut, elle doit correspondre à la **charte** que vous devez lire avant de faire votre demande. Si votre demande ne colle pas avec la **charte** ou le type de votre

adhésions, il y a de forte chance qu'elle soit **refusée**.

Les possibilités de configuration d'un site web perso sont :

- Le choix du protocole à utiliser (http, http/https ou https avec certificat auto-signé ou Let'sEncrypt si proposé par l'instance)
- Gestion du **.htaccess** perso
- Activer le **mod_rewrite**
- Utilisation et déploiement d'un **SPI** (Site Web pré-Installé)
- Configurer la **base de données**
- Gestion des statistiques du site avec Matomo
- Gestion de l'indexation des moteurs de recherches
- Gestion des droits d'accès du répertoire d'installation
- léguer son site web perso à un autre utilisateur

Qu'est ce que un .htaccess ? Un **.htaccess** est un fichier que l'on place dans le répertoire d'installation d'un site web et qui permet d'en restreindre l'accès. C'est un système d'authentification propre à apache. Cela permet entre autre de :

- restreindre/autoriser l'accès à un répertoire
- obliger une authentification (couplé en général avec un fichier .htpasswd)
- ...

Qu'est ce qu'une base de données ? Une base de données est un ensemble de variables qu'un site web dynamique a besoin pour fonctionner. Ces bases de données sont stockées sur le serveur et gérées par ***MySQL*** [16]. Si vous souhaitez utiliser un site web dynamique (comme un SPI par exemple) alors il vous faut un compte MySQL que vous pourrez configurer avec PhpMyAdmin. L'interface de PhpMyAdmin est utilisable à cette adresse : https://php.**votre_domaine**/. Pour activer votre compte MySQL/PhpMyAdmin, vous devez choisir un mot de passe. Ce mot de passe **ne peut pas être le même que votre mot de passe utilisateur unix** pour des raisons évidentes de **sécurité**. Autant il est facile de garantir la sécurité du mot de passe unix, autant ce n'est pas possible pour le compte MySql étant donné que celui-ci peut apparaître en clair dans certains fichiers conf de vos sites web perso.
Pour plus d'informations, veuillez consulter l'aide en ligne.

KerHost vous offre la possibilité de consulter individuellement les fichiers d'activité (**log**) de vos sites web perso. Ils sont aux nombre de deux par site web perso :

- **access-votre_sous_domaine.log** (vous informe de chaque accès à votre site)
- **error-votre_sous_domaine.log** (vous informe des erreurs rencontrées par le serveur web)

Ces fichiers log sont situés dans home_directory ⇒ www ⇒ log. Cette fonction est très pratique pour visualiser les requêtes qui sont faites sur vos sites ou encore connaître les causes d'une erreur. Si vous souhaitez voir en temps réel dans un terminal les connexions à votre site web perso, vous pouvez utiliser cette commande après avoir établi une connexion ssh :

`tail -f www/log/access-votre_sous_domaine.log |ccze` (ou `tail -f www/log/error-votre_sous_domaine.log |ccze` pour voir les erreurs)
D'autre part, ces fichiers log peuvent vite devenir volumineux et compliqués à afficher sur l'interface de gesion. Il est donc fortement conseillé de les **supprimer** régulièrement.

Les SPI

Qu'est ce que les SPI ? Les **SPI** sont des applications web développées par des tiers et que KerHost intègre en tant que déploiement semi-automatique pour les sites web perso des utilisateurs. En choisissant un **SPI**, l'utilisateur s'affranchit d'une installation parfois compliquée et fastidieuse en FTP ou SSH. La liste des **SPI** disponible par défaut est ici.

Exemple

Voici un exemple concret pour créer un site web perso à partir d'un SPI :
Je souhaite créer un site web perso, de type **blog** plus exactement, mais je sais pas comment m'y prendre. Et c'est pas forcément facile, de créer un blog quand on n'y comprend pas grand chose en informatique. Heureusement, **farmserv** vas vous simplifier la tâche. D'abord, vous devez activer votre **site web perso**, c'est-à-dire préparer l'**espace** de stockage qui va héberger votre site et faire en sorte que celui-ci soit disponible sur **internet**. Ce **stockage** (ou répertoire d'installation) est réalisé dans votre home directory, et plus exactement dans le répertoire www (**/home/votre_login/www/votre_site_web**). Pour cela, vous devez dans un premier temps trouver un **nom** à votre site. Plus exactement un nom de **sous-domaine**. Il y a déjà le nom de domaine de votre site (on prendra l'exemple **tralala.org**) qui est le serveur auquel vous avez adhéré et que vous connaissez. Votre site web perso aura donc comme adresse **quelque_chose.tralala.org**. Ce **quelque_chose**, c'est votre sous domaine. Vous devez bien l'identifier, ce nom de sous domaine doit refléter votre site web perso. Il doit être court, simple et facile à retenir. Un seul mot (mais vous pouvez utiliser le tiret "**-**") ne comportant que des chiffres et des lettres. Vous l'avez trouvé, super. On va dire que vous voulez comme sous-domaine **youpla**, ce qui nous donnera au final l'adresse suivante pour votre site web perso : **http://youpla.tralala.org**. Maintenant que vous avez choisi le nom de votre sous domaine, il faut le réserver et le valider. Pour cela, connectez-vous sur le portail de votre serveur PORTAIL ⇒ Mon compte ⇒ Mes sites web et ajoutez le nom de votre domaine dans le champ Ajouter un site web perso et validez :
mon_swp01.png Vous devez ensuite donner un rapide descriptif de votre site web afin de s'assurer que votre demande soit en adéquation avec votre type d'adhésion) et valider la charte d'utilisation :
mon_swp02.png Maintenant vous devez attendre qu'un **administrateur valide** votre demande de réservation. Cela ne se fait pas automatiquement. L'administrateur doit s'assurer que ce nom de sous domaine soit bien valide et disponible et doit l'enregistrer auprès du **serveur DNS** de **votre_domaine**. Vous êtes ensuite redirigé vers la liste de vos sites web perso :
mon_swp03.png Vous remarquerez que toutes les actions pour ce site sont **grisées**. Vous ne pouvez rien faire tant que celui-ci n'est pas validé par un administrateur. Attendez donc que celui-ci soit validé. Vous recevrez par mail une **confirmation** de validation (ou non). Revenez sur cette page ou rechargez-la et vous devriez voir le site actif :

mon_swp04.png Vous avez maintenant **8 actions possibles** pour ce site web :

1. **Interrupteur ON/OFF** : permet de **désactiver/activer** le site d'internet
2. **Bouton crayon** : permet de **paramétrer** le site
3. **Bouton disquette** : permet de lancer une **sauvegarde** du site
4. **Bouton PQ vert** : permet de visualiser les **logs d'accès** du site
5. **Bouton PQ rouge** : permet de visualiser les **logs d'erreurs** du site
6. **Bouton planète/souris** : permet de se **rendre** sur le site
7. **Bouton cadenas** : détermine si le site est **sécurisé** par un certificat de sécurité
8. **Bouton poubelle** : permet de **supprimer** le site

Cliquez sur le bouton 6 (planète/souris) pour vous rendre sur le site et vérifier qu'il est bien actif. Vous devriez avoir une page en construction :
mon_swp05.png Si ce n'est pas le cas et que vous obtenez un message d'erreur de type **404 not found**, c'est que la propagation DNS n'as pas eu le temps de se faire. Attendez un peu et revenez dessus. Normalement c'est assez rapide.
Voilà, votre espace web est disponible. Il ne reste plus qu'à y mettre du contenu. Mais vous n'êtes pas un programmeur de site, donc vous ne savez pas comment faire un blog. Heureusement, il existe plein de solutions clés en main vous permettant de gérer facilement différents types de sites web. On appelle cela un CMS. Pour faire simple, des gens développent des **structures** (squelettes) de sites dans différents types de catégories selon les besoins des utilisateurs et qu'ils mettent gracieusement à disposition sur internet. En général l'installation de ces structures n'est pas évidente pour le commun des mortels et nécessite quelques connaissances informatique (ftp, droit d'accès sur les fichiers, décompression d'archive…). Et c'est là que farmserv intervient. En un clic de souris, vous allez pouvoir choisir un type de **CMS** (**SPI** donc) parmi une liste correspondant à votre souhait et le déployer sur votre site. Mais, avant d'aller plus loin, il y a un petit truc en plus à intégrer : **la base de données**. La base de données, c'est un espace de stockage particulier où l'on va stocker toutes les données de contenu de votre CMS. Elle est indépendante dans son fonctionnement du site web mais elle y est étroitement liée. Sur farmserv, les bases de données sont gérées par **MySQL**, et pour qu'un utilisateur puisse gérer des bases de donnée MySQL, il lui faut activer son compte MySQL/PhpMyAdmin. Ce service est indépendant de votre compte utilisateur pour des raisons de sécurité. Donc, avant d'aller plus loin, il faut activer votre compte MySQL/PhpMyAdmin si ce n'est pas encore fait. Pour cela, revenez sur la liste de vos sites web perso et activez votre compte MySQL/PhpMyAdmin en saisissant un mot de passe différent de votre compte utilisateur (c'est important pour des raisons de sécurité) :
mon_swp06.png Si vous ne savez pas quoi utiliser comme mot de passe robuste, alors cliquez sur le bouton bleu avec deux flèches pour en **générer** un automatiquement (vous pouvez le faire jusqu'à en trouver un qui vous convienne). Confirmez-le et validez. Voilà, votre compte est activé. Vous recevrez un mail de notification.
Passons maintenant à la configuration du site. Il est actif, mais vide. Nous voulons y déployer un blog. Dans la liste de vos sites, cliquez sur le **crayon** (1) pour rentrer dans le paramétrage de celui-ci. La page qui s'ouvre offre beaucoup d'options. Nous allons nous concentrer sur le déploiement du SPI. Descendez dans la page pour arriver à la section **Configuration Site Pré Installé** :
mon_swp07.png Pour le moment, aucun spi installé, tout comme la base de donnée. Il vous faut choisir votre SPI. Pour cela, vous avez une page qui va vous le permettre. Cliquez sur **Descriptifs et versions des SPI disponibles**
mon_swp08.png Un nouvel onglet s'ouvre avec le descriptif complet de tous les SPI mis à disposition :

- le nom du SPI (CMS, solution…)
- sa version
- sa catégorie (type, genre de CMS)

- son descriptif
- son lien pour accéder au site officiel du site de développement de celui-ci
- un bouton permettant de faire une demande de mise à jour de celui-ci si la version disponible est obsolète

Vous devez rechercher dans la liste le SPI qui doit correspondre le plus avec ce que vous recherchez. Un blog est de type **publication**. Il va falloir donc regarder dans la **catégorie** publication. Il y en a plusieurs. À vous de voir. Dans cet exemple, nous allons choisir **WordPress** qui reste le **CMS** le plus connu et le plus facile d'utilisation dans le domaine de la publication. Fermez cette page et retournez dans les paramètres du site. Vous allez dans **Type de site dynamique (SPI)** sélectionnez WordPress dans le menu, et validez. Notez qu'il n'y a rien à faire côté base de données à moins que vous souhaitiez la configurer manuellement. Si le SPI a besoin d'une base de données (ce qui est le cas le plus souvent), elle sera automatiquement créée. Vous recevez normalement un mail de confirmation avec les élément clés de la configuration de votre site:
mon_swp09.png À ce niveau, votre **SPI** est **actif** et **déployé**, mais pas encore **configuré**. Vous êtes redirigé vers une page vous invitant à lancer le **paramétrage** de votre SPI. Et oui, il va falloir fournir à votre SPI quelques informations. En général, il faut :

- paramétrer l'accès à la base de données (serveur, login, password, nom de la base)
- créer le compte administrateur du SPI pour pouvoir vous connecter à votre site

mon_swp10.png Gardez bien cette page sous les yeux et cliquez sur **Procéder à la configuration**. Vous êtes redirigé vers votre site web, qui n'est plus en construction mais en attente de **paramétrage**. Suivez pas à pas les instructions données juste avant. Si tout va bien, votre site est **opérationnel**.

Redirection

Vous avez déjà un **nom de domaine** et vous aimeriez bien que votre site web perso hébergé sur votre**instance** pointe sur celui-ci ? C'est possible. Voila comment procéder. Prenons l'exemple d'un utilisateur **toto** qui dispose déjà :

- d'un site web perso **toto.farmserv.org**
- d'un nom de domaine **www.toto.com** enregistré chez le régistar **OVH**

Toto veut que son site web perso **toto.farmserv.org** hébergé sur **farmserv.org** soit accessible à partir de **www.toto.com**.
Cela ce passe au niveau du **registar** et non de **farmserv.org**. Il va falloir donc modifier la **zone DNS** de **toto.com** pour que ce domaine soit redirigé vers **toto.farmserv.org**. Il y a deux façons de rediriger un domaine :

- la redirection **visible**, **www.toto.com** se transforme en l'url cible **toto.farmserv.org**. Cette transformation sera visible dans la barre d'adresse du navigateur internet.
- la redirection **invisible**, **www.toto.com** reste inchangé dans la barre d'adresse du navigateur internet mais le contenu de la page est celui de l'url cible **toto.farmserv.org**.

Si vous voulez absolument que **toto.farmserv.org** n'apparaisse pas, il faut donc choisir la redirection **invisible**.

ATTENTION !!! Il y a un inconvénient majeur à la redirection invisible, le **certificat de sécurité certifié**. Si toto.farmserv.org tourne avec un certificat de sécurité certifié Let'sEncrypt, vous aurez un gros problème car celui-ci sera valide uniquement pour **toto.farmserv.org** et ne sera donc pas identifié comme fiable pour **www.toto.com**. Toto devra alors gérer son propre certificat par ses propres moyens.

Voici la procédure pour faire une redirection chez **OVH** :
https://docs.ovh.com/fr/domains/redirection-nom-de-domaine/ Si vous n'êtes pas chez OVH, en règle général vous devrez modifier votre zone DNS de la façon suivante :
invisible

www IN A 213.186.33.5 ⇐ Adresse IP du serveur de redirection de votre Registar (içi celui d'OVH)
www 60 IN TXT "t|Toto web site" ⇐ Vous pouvez renseigner un Titre
www 60 IN TXT "2|http:*toto.farmserv.org/*" ⇐ *L'adresse de redirection*
www 60 IN TXT "k|youpla" ⇐ Vous pouvez renseigner des mots clés

visible

www IN A 213.186.33.5 ⇐ Adresse IP du serveur de redirection de votre Registar (içi celui d'OVH)
***www 60 IN TXT "4|http:*toto.farmserv.org/"** ⇐ L'adresse de redirection

---

9-Les services web

KerHost et **votre_domaine** vous proposent une suite de services alternatifs afin de vous **dégoogliser** un maximum !

- Blog (remplace Google Blogger)
- Partage (remplace Google Doc, DropBox...)
- Rss (remplace Google News)
- Stasperso (remplace Google Analitics)
- Lists (remplace Google Groupes)
- Recherche (remplace Google Search)
- Émulateur terminal
- Sondage (remplace Doodle)
- Wiki
- Sync
- Ntp
- Proxy
- VPN
- Newsletter
- Doc et Calc (remplace Google doc)

9.1-Blog

Le blog (propulsé par Wordpress) est un site d'informations sur la vie associative du serveur. C'est un espace d'échange entre les utilisateurs afin de partager un certain nombre d'informations en tout genre (articles, tutos...). Chaque utilisateur peut être rédacteur et proposer des articles. Les articles écrits **ne sont pas modérés** et sont **immédiatement mis en ligne**, et **sont accessibles à tout le monde**. Pour accéder à ce service, http://blog.**votre_domaine**/ ou PORTAIL . mon_services.png

9.2-Partage

Ce service (propulsé par NextCloud) propose une solution de **stockage/partage** en ligne. Cette interface permet de contrôler votre stockage disque d'où que vous soyez. Voici une liste non exhaustive des possibilités de ce service :

- Structuration de votre espace disque (du répertoire nextcloud de votre home directory plus exactement)
- ajout/modification/suppression de documents (texte, image, audio, vidéo, pdf...)
- partage de ces fichiers en interne (avec les membres de **votre_domaine**) ou en externe (avec tout le monde)
- gestionnaire de contacts compatible ***CardDAV*** [17)]
- gestionnaire d'agenda compatible ***CalDAV*** [18)]
- accès possible de votre espace disque par ***WebDAV*** [19)] (montage distant sur un ordinateur)
- gestionnaire de bookmark
- travail collaboratif sur document texte (type OpenOffice)
- visionneuse photo
- player audio
- gestionnaire d'activité
- lecteur de flux RSS intégré
- ...

Il est possible de partager son agenda, ses contacts et bookmark pour faire de la synchro sur plusieurs ordinateurs. NextCloud et compatible thunderbird et android, ce qui permet de s'affranchir totalement des services de google. Il existe également un client (linux, windows et mac) de synchronisation permettant de faire une **réplication** automatique entre un **répertoire local** de votre ordinateur et le **répertoire nextcloud de votre home directory**, ainsi qu'une application Android/IOS. Il n'y a pas besoin d'activer ce service car il est lié à votre compte unix. Ce service est donc directement disponible pour tout nouvel utilisateur. Pour accéder à ce service, https://partage.**votre_domaine**/ ou par le PORTAIL .

Tous les utilisateurs d'une même **entité** disposent d'un **groupe** au nom de l'entité dans NextCloud. Ainsi, le partage entre utilisateurs d'une même entité peut se faire directement avec le **nom du groupe**.

nextcloud.png

9.3-Rss

Le service ***RSS*** [20)] vous propose de suivre d'où vous voulez, vos flux RSS préférés. Il s'agit d'un agrégateur qui vous fait une synthèse à intervalles réguliers de la parutions de nouveaux articles de vos sites internet préférés. C'est très pratique pour suivre d'un seul coup d'œil l'actualité de plusieurs sites. tinyrss.png

---

9.4-Statsperso

Le service **statsperso** (propulsé par ~~Piwik~~ Matomo) est un service de statistique web. Il permet d'obtenir des informations très précises sur la fréquentation d'un site web perso. C'est un outil fort pratique si l'on veut analyser l'audience de son site web. En plus d'afficher en temps réel les données, il permet également de vous envoyer des rapports par mail (journalier, hebdomadaire ou mensuel) au format html ou pdf des éléments suivants :

- Récapitulatif des visites
- Visites par fuseau horaire du serveur
- Visites par fuseau horaire local
- Visites par Jour de la Semaine
- Résolutions d'écran
- Navigateurs du visiteur
- Version du navigateur
- Navigateurs par famille
- Liste de Plugins
- Normal / Écran large
- Systèmes d'exploitation
- Configuration globale des visiteurs
- Famille de systèmes d'exploitation
- Mobile vs Fixe
- Langage du navigateur
- Code langue
- Actions - Métriques principales
- URL de la page
- Pages d'entrée
- Pages de sortie
- Titres des pages
- Titres de la page d'entrée
- Titres de la page de sortie
- Liens sortant
- Téléchargements
- Content Name
- Content Piece
- Catégories d'événement
- Actions de l'événement

- Noms d’événement
- Types d'affluents
- Tous les référents
- Mots-clés
- Sites web
- Moteurs de recherche
- Campagnes
- Réseau sociaux
- Objectifs
- Visites par conversion
- Jours par conversion
- Pays
- Continent
- Région
- Ville
- Variables personnalisées
- Durée des visites
- Pages par visite
- Visites par numéro de visite
- Visites par jour depuis la dernière visite
- Visites retour
- FAI
- Type du périphérique
- Marque du périphérique
- Modèle du périphérique
- Familles de système d'exploitation
- Versions de système d'exploitation
- Familles de navigateurs
- Versions du navigateur

Pour **activer les statistiques d'un site web perso**, il faut passer par les préférences de votre site : PORTAIL ⇒ Mon compte ⇒ Mes sites web ⇒ Liste de mes sites web perso (sous-domaine) ⇒ Paramétrer ce site web perso ⇒ Paramètres Analyses et Statistiques ⇒ Activée pour ce site web perso . Ensuite vous pouvez accéder et configurer les statistiques sur le service.

Pour **créer l’envoi d'un rapport automatique**, connectez-vous au service, sélectionnez votre site web perso, cliquez en haut à gauche sur votre identifiant, et choisissez Rapports e-mail. Ensuite cliquez sur **Planifier un rapport** et remplissez le formulaire en choisissant vos options.

matomo.png

9.5-Lists

Lists est un gestionnaire de ***listes de diffusion*** [21)] propulsé par mailman. Le principe d'une liste de diffusion est de pouvoir diffuser massivement de l'information via l'outil mail à partir d'un seul point. Les listes de diffusion sont ouvertes à tout le monde, même aux gens qui n'ont pas d'adresse mail sur **votre_domaine**.

L'**ajout/suppression** d'une liste de diffusion passe par PORTAIL ⇒ Mon compte ⇒ Mes listes de diffusion . La **gestion** d'une liste de diffusion, elle, passe par http://lists.**votre_domaine**/admin/nom_de_la_liste. L'**abonnement** à une liste de diffusion passe par http://lists.**votre_domaine**/listinfo/nom_de_la_liste. L'adresse d'une liste de diffusion est toujours de la forme : **nom_de_la_liste@lists.votre_domaine**.

La demande d'une liste de diffusion doit être **justifiée**. Elle doit être en adéquation avec votre type d'adhésion. Elle sera ensuite **validée** ou non par un administrateur. Si par exemple vous avez une adhésion SOLO est que vous demandez une liste de diffusion pour gérer une association, elle vous sera refusé.

Les listes de diffusion sont par défaut **publique** à la création. Cela veut dire que n'importe qui peut consulter la liste des listes de diffusion hébergées sur le serveur. Il est donc très fortement conseillé de les rendre **privées** (invisible) et de communiquer manuellement leurs existences aux intéressés. Pour cela rendez-vous dans la partie **admin** de votre liste et ensuite allez dans Options de confidentialité→Afficher cette liste lorsqu'on demande les listes hébergées par cette machine ? et cocher **Non**. Cela permettra de limiter le SPAM.
La gestion de votre liste de diffusion est importante et il ne s'agit pas de faire n'importe quoi avec. Une liste mal configurée peut poser de gros problème de sécurité au serveur de mail. Déterminez bien la politique d'abonnement, la taille d'envoi pour chaque email... Il y a beaucoup de paramètres à prendre en compte et c'est un outils assez complexe à maîtriser.
En cas de **mauvaise** configuration (envoi massif de spam par exemple), l'équipe admin se donne le droit de **désactiver/supprimer** la liste de diffusion posant problème sur le champ (vous en serez averti bien entendu !)

mailman.png

9.6-Recherche

Recherche est le moteur de recherche indépendant de **votre_domaine** afin de vous affranchir du traçage de Google. Il est propulsé par **SearX**. Il s'agit plus exactement d'un méta-moteur de recherche. Il agit comme un proxy entre vous et les moteurs de recherche (Google, bing, Qwant, Wikipedia...), vous rendant totalement anonyme.

Ce service est disponible pour tout le monde, même pour les gens ne faisant pas partie de l'instance. Pour accéder à ce service, https://recherche.**votre_domaine**/ ou PORTAIL .

searx.pngsearx3.png

9.7-Émulateur terminal

L'émulateur de ***terminal*** [22)] vous permet d'obtenir une console directement à partir de votre navigateur. Pratique si votre OS n'en dispose pas nativement, comme Windows (MacOsX en dispose un, si si, regardez bien !). Le terminal est fort pratique pour débloquer certaines situations en ligne de commande, comme changer par exemple les droits d'accès à un fichier, mais il nécessite quelques connaissances au monde unix.

Ce service est disponible via PORTAIL ⇒ Mon compte ⇒ Ma boîe à outils ⇒ Accéder au terminal **votre_domaine**. Cet outil est **obligatoirement** sécurisé **https** et vous devez accepter le certificat de sécurité **SSL** pour pouvoir l'utiliser si celui-ci est auto-signé.

shellinabox.png

9.8-Sondage

Le service de **sondage** (propulsé par Framadate) et un service équivalent à Doodle, qui vous propose de créer deux types de catégories de sondages :

- Sondage classique (vous sélectionnez vos questions à proposer)
- Sondage spécial date (vous sélectionnez vos dates à proposer)

Une fois un sondage créé, vous recevez un email contenant :

- Le lien de gestion/consultation
- Le lien à transmettre aux participants

Il est possible de définir une date limite de participation.

La création d'un sondage est **exclusivement réservée aux utilisateurs de votre_domaine** et ne nécessite **aucune activation du service**. Il vous sera donc demandé de vous authentifier. En revanche, tout le monde peut participer aux sondages à partir du lien de participation.

Pour accéder à ce service, http://sondage.**votre_domaine**/ ou PORTAIL .

framadate.png

9.9-Wiki

Le wiki (propulsé par DokuWiki) est une base de connaissance sur le serveur de **votre_domaine**. Il est réservé exclusivement aux utilisateurs de **votre_domaine**. Ce service permet à l'administrateur et aux utilisateurs d'alimenter en documentations (tutos...) l'utilisation du serveur. C'est en quelque sorte un guide utilisateur comme celui-ci mais avancé et alimenté par la communauté de **votre_domaine**.

Ce service **n'est pas activable**. Tout utilisateur y est directement inscrit. Pour y accéder : http://wiki.**votre_domain**.

9.10-Sync

Sync est un serveur de synchronisation dédié à l'utilisation de Firefox. Il permet de pouvoir synchroniser plusieurs profils de Firefox sans avoir à utiliser celui qui est proposé nativement par Mozilla. Sync propose de :

- synchroniser vos marques page
- vos mots de passe
- votre historique de navigation
- vos préférences
- vos onglets

Pour utiliser sync il vous suffit de lancer l'assistant Sync dans votre Firefox et de vous créer votre compte avec votre adresse mail. Vous devez sélectionner le serveur de syncho manuellement en choisissant cette adresse : https://sync.**votre_domaine**/token/1.0/sync/1.5/ dans la variable `identity.sync.tokenserver.uri` de la page `about:config`.

Sync est exclusivement accesible en HTTPS, donc si le serveur travaille avec des certificats **auto-signés**, vous devez dans un premier temps **visiter le site** https://sync.**votre_domaine**/ une première fois avec Firefox pour accepter le certificat de sécurité. Si le serveur propose des certificats **Let'sEncrypt**, alors cette manipulation n'est pas utile.

9.11-Serveur de temps

Le serveur de temps NTP proposé permet de garder l'horloge interne de votre ordinateur toujours à la bonne heure en se calant sur celle du serveur.

Le paramétrage de l'horloge de votre ordinateur dépend de l'OS que vous utilisez. L'adresse à utiliser est : ntp.**votre_domaine**.

9.12-Proxy

Est mis à votre disposition un serveur ***proxy*** [23)] vous permettant de naviguer anonymement sur internet. Principe de fonctionnement :

- Vous configurez directement votre connexion réseau (ou indirectement votre application) pour utiliser le serveur proxy.
- Quand votre ordinateur veut joindre un serveur externe (navigation internet par exemple), celui-ci fait sa requête au serveur proxy, qui va traiter la demande
- Le serveur proxy contacte le serveur demandé
- Le serveur demandé répond au proxy
- Le proxy vous relaie la réponse du serveur demandé à votre ordinateur

Vous l'aurez compris, le proxy est un intermédiaire qui vous rend anonyme aux yeux du serveur demandé. C'est une façon de mettre des bâtons dans les roues à d'éventuels traçages sur internet. Le proxy peut être utilisé pour différents protocoles :

- http/https (80/443)
- ftp (21)

- gopher (70)
- wais (210)
- unregistred ports (1025-65535)
- http-mgmt (280)
- gss-http (488)
- filemaker (591)
- multiling http (777)
- ...

Pour l'utiliser, vous devez utiliser les paramètres suivants dans votre navigateur ou dans votre connexion internet:

- **Serveur** :proxy.**votre_domaine**
- **Port** : *3128*
- **Login** : *nom_de_connexion*
- **Password** *votre_mot_de_passe*

Utiliser un proxy peut ralentir votre navigation. Vous ajoutez un intermédiaire sur lequel vous allez faire transiter votre trafic réseau. Selon la charge du serveur proxy, cela peut occasionner des ralentissements à l'utilisation. A n'utiliser qu'en cas d'anonymisation justifiée. Notez également qu'utiliser un proxy ne vous garantit aucune sécurité. Tout ce qui rentre et sort entre le proxy et votre ordinateur n'est pas sécurisé ni crypté. Il est donc tout à fait possible pour un organisme de flicage d'intercepter le contenu de ce trafic. Si vous voulez une connexion sécurisé, il faut alors utiliser le VPN.

Le fait que vous utilisiez le proxy ne vous dédouane pas de la responsabilité de vos actes sur internet ! **Le proxy vous rend uniquement anonyme des ressources demandées**. En cas de délit, l'administrateur est légalement responsable de l'utilisation du proxy. La procédure d'authentification de ce service, qui permet d'en réserver l'accès aux seuls utilisateurs de **votre_domaine**, laisse toutefois une trace des utilisations successives (log), pouvant être officialisée en cas de litige. Il est donc inutile de considérer cet outil comme un bouclier à une activité douteuse !

9.13-VPN

Le ***VPN*** [24)] est un outil similaire au proxy à la différence essentiel qu'il est entièrement **sécurisé** et **inviolable**. Ce qui n'est pas du tout le cas du proxy. Le VPN ne s'applique que sur la configuration de votre carte réseau et n'est donc pas paramétrable au niveau logiciel. C'est une modification de votre

connexion internet. Le VPN n'agit pas comme un ***routeur*** [25]. Comment cela fonctionne-t-il ?

- Vous modifiez votre connexion réseau (méthode qui défère selon votre OS)
- Vous établissez une connexion avec le VPN
- Tout ce qui sort de votre ordinateur est physiquement relié au VPN et entre en connexion directe avec celui-ci, d'une manière sécurisée et chiffrée.

Le VPN est le protocole ultime de sécurisation en matière de lutte contre le flicage internet (NSA, ANSSI, RG...). Tout ce qui transite entre votre ordinateur et le VPN est inviolable. C'est aussi une excellente solution pour contourner les restrictions de certains réseaux (universités, certains pays, etc...).
Son utilisation n'est pas très compliquée. Elle dépend surtout de votre système d'exploitation. Vous devez dans un premier temps récupérer l'**archive** de configuration (certificat et fichiers conf) en fonction de votre **OS**, et ensuite vous authentifier avec votre **nom_de_connexion/mot_de_passe** utilisateur.

Pour utiliser le VPN, vous devez dans un premier temps télécharger l'archive qui contiendra tout ce qu'il faut pour que votre ordinateur puisse se connecter au VPN. Pour cela, dirigez vous sur PORTAIL ⇒ Mon compte ⇒ Mes services ⇒ Autres services . Téléchargez le fichier **openvpn-gnu-linux.zip** si vous êtes sur une ditribution linux, macosx ou androïd, ou **openvpn-windows.zip** si vous êtes sous windows. Décompactez l'archive. Vous obtenez un répertoire **gnu-linux** ou **windows** qui contient les fichiers suivants :

- ca.crt (le certificat de sécurité du serveur)
- client.conf (votre fichier de configuration)
- ta.key
- update-resolve.sh (seulement pour gnu-linux)

Maintenant vous devez importez le fichier client.conf dans votre gestionnaire VPN. Cela dépend bien évidement de votre OS. voici la manipulation sous Ubuntu :

- Commencez par installer les paquets suivant : `sudo apt-get install openvpn network-manager-openvpn`
- Cliquez en haut à droite sur connexion réseau (les deux flèches en sens inverse)
- Connexions VPN ⇒ Configurer le VPN...
- Cliquez Importer
- Sélectionnez votre fichier de configuration **client.conf**
- Choisissez un nom de la connexion (vpn-**votre_domaine** par exemple)
- Saisissez votre login et mot de passe utilisateur
- Cliquez Enregistrer...
- Cliquez sur Fermer

Voilà pour la partie configuration. Maintenant pour utiliser le VPN, il vous suffit de cliquer en haut à droite sur connexion réseau (les deux flèches en sens inverse) ⇒ Connexions VPN ⇒ Sélectionner le nom de la connexion que vous avez donné dans la configuration. Si tout se passe bien, au bout de quelques secondes vous

devez obtenir un message vous signalant que vous êtes bien connecté au VPN. Votre ordinateur est maintenant physiquement routé par le VPN. Quand vous ne voulez plus utiliser le VPN, cliquer en haut à droite sur connexion réseau (le deux flèches en sens inverse) ⇒ Connexions VPN ⇒ Déconnecter le VPN.

Tout comme l'utilisation du proxy, le fait que vous utilisiez le VPN ne vous dédouane pas de la responsabilité de vos actes sur internet ! **Le VPN vous garantit une transaction sécurisée entre le serveur et votre ordinateur, c'est tout**. En cas de délit, l'administrateur est légalement responsable de l'utilisation du VPN. La procédure d'authentification de ce service, qui permet d'en réserver l'accès aux seuls utilisateurs de votre domaine, laisse toutefois une trace des utilisations successives (log), pouvant être officialisée en cas de litige. Il est donc inutile de considérer cet outil comme un bouclier à une activité douteuse !

9.14-Newsletter

La **newsletter** (ou lettre d'information, et une liste de diffusion provenant directement du service **lists**), permet à l'administrateur, mais aussi aux utilisateurs de communiquer entre eux via cette liste de diffusion. En général, elle est surtout utilisée par l'administrateur pour prévenir la communauté de l'activité du serveur (nouveauté, mise à jour, nouveaux articles sur le blog et le wiki, maintenance du serveur...)
Par défaut, tout nouvel utilisateur y est directement abonné. Toutefois, il lui est possible de se désabonner via PORTAIL ⇒ Mon compte ⇒ Mes services web ⇒ Autres services ⇒ Abonnement Newsletter **votre_domaine**.

L'adresse mail de la newsletter est : **newsletter-votre_domaine@lists.votre_domaine**

10-Gérer votre entité

Vous pouvez à partir de PORTAIL ⇒ Mon compte ⇒ Mon entité obtenir les informations concernant votre entité. Si vous n'êtes pas le responsable de votre entité, vous pouvez :

- Obtenir le récapitulatif de votre entité
- Obtenir la liste des utilisateurs de votre entité
- Faire une demande de résiliation de votre compte utilisateur

Si vous êtes le responsable, vous pouvez :

- Obtenir le récapitulatif de votre entité
- Obtenir la liste des utilisateurs de votre entité
- Faire une demande de résiliation de votre compte utilisateur
- Faire une demande de résiliation d'un compte utilisateur de votre entité
- Ajouter un compte utilisateur à cette entité
- Changer la formule d'adhésion de votre entité
- Léguer votre responsabilité
- Résilier votre entité
- Gérer le quota disque de votre entité
- Modifier votre adresse mail de contact de responsable d'entité

Vous pouvez en temps que responsable **modifier votre formule d'adhésion**. Le changement de formule n'est pas immédiat. Un administrateur traitera votre demande et la validera (ou non). Votre demande doit être justifiée. C'est-à-dire qu'elle doit être en rapport avec votre nouvelle situation. Seules les situations suivantes sont acceptées (par défaut, selon les règles établies par votre mode associatif) :

- SOLO vers DUO
- SOLO vers ASSOS
- SOLO vers FAMILLE
- DUO vers FAMILLE
- DUO vers ASSOS

L'inverse est possible à condition que le nombre de comptes utilisateurs diminue en conséquence. Un réajustement (au prorata de l'année en cours) du montant de votre cotisation est alors effectué lors de votre prochain renouvellement.
Vous pouvez également **léguer votre responsabilité** à un autre membre de votre entité. Ainsi, vous lui donnez les droits de la gestion de votre entité et vous en perdez le contrôle ! Cette procédure n'est pas irréversible. Si vous voulez récupérer cette responsabilité, il vous faudra la demander à celui ou celle à qui vous l'avez léguée. Cette procédure est immédiate et s'applique tout de suite. Vous devrez donc vous reconnecter tout de suite après pour prendre en compte le nouveau changement.
Seul le responsable de l'entité peut faire une demande de résiliation d'adhésion. Cette procédure n'est pas immédiate et est traitée par un administrateur.

La résiliation d'une entité entraîne la suppression de tous les comptes utilisateurs qui y sont rattachés !

Enfin, toujours en tant que responsable d'entité, vous pouvez modifier votre quota disque.

11-Gérer vos cotisations

PORTAIL ⇒ Mon compte ⇒ Mes cotisations permet si vous n'êtes pas responsable de votre entité de :

- Obtenir le récapitulatif de votre cotisation actuelle

- Lister l'état de toutes les cotisations de votre entité

Et si vous êtes le responsable :

- Obtenir le récapitulatif de votre cotisation actuelle
- Lister l'état de toutes les cotisations de votre entité
- Pré valider votre prochaine cotisation
- Télécharger une attestation de règlement/don

La pré validation de votre cotisation est importante. Elle permet de garantir la pérennité du serveur. C'est un acte de responsabilisation qui vous engage à amorcer le processus de règlement de votre adhésion après l'appel à cotisation annuelle en cours. Ainsi en pré validant votre cotisation, il ne vous reste plus qu'à faire parvenir votre règlement au trésorier de **votre_domaine**. De plus, la pré validation facilite le travail de ce dernier, en insérant automatiquement une écriture dans la comptabilité qui n'a plus qu'à être pointée à la réception du règlement..

12-Quota disque

Vous pouvez à tout moment consulter le niveau de votre quota disque. Pour cela, il suffit d'aller dans PORTAIL ⇒ Mon compte ⇒ Ma boîte à outils ⇒ Gérer l'espace disque de mon entité. Vous pourrez alors voir en détail la répartition de votre espace disque, aux niveaux :

- utilisateurs
- global (entité)

En cas de dépassement, vous êtes directement informé par l'état du voyant (rouge). Si vous êtes le responsable de votre entité, alors il vous est possible d'augmenter votre espace disque par tranche de 1Go supplémentaire (10 Go maximum autorisé en plus et selon les disponibilités du serveur). Le prix du Giga supplémentaire est par défaut de 0.10€/mois. Votre prochaine cotisation est donc automatiquement ré évaluée en début d'année.

La page quota disque peut prendre un certain temps à s'afficher selon le nombre plus ou moins important de fichiers compris dans les home directory des utilisateurs de votre entité !
Tous les mois (le **28** exactement), un processus automatique vérifie le quota de chaque entité. En cas de dépassement, le responsable de l'entité reçoit une alerte par mail l'invitant à régler le problème.

13-Bug tracking

Le **Bug Tracking** est un module de KerHost vous permettant de **référencer tout type de bug rencontré sur le serveur** (services, site web perso...), de façon à ouvrir un ticket que l'administrateur pourra suivre et corriger. Un certain nombre de renseignements est demandé pour déterminer le bug en question :

- Date de déclaration
- Produit (sous domaine qui pose problème)
- Url qui déclenche le bug
- La reproductibilité
- L'impact
- La priorité
- La plate forme
- L'OS
- la version de l'OS
- Navigateur utilisé
- La version du navigateur
- La version du produit utilisé
- L'intitulé du bug
- La reconstitution
- Une information complémentaire
- Ajout d'une capture d'écran

Une fois votre bug déclaré, l'administrateur peut apporter des solutions et régler ou non le problème en commentant à chaque fois les étapes d'amélioration. Il peut également transmettre le ticket à l'équipe de **KerHost** si cela concerne un problème de l'interface. Vous pouvez à tout moment suivre les étapes de résolution. Quand un bug est résolu, le ticket est alors clôturé par l'administrateur.

Plus vous **donnez** d'informations sur la nature du bug et plus cela sera facile pour l'administrateur de le résoudre ! N'hésitez pas à utiliser cet outil. C'est une plate forme de gestion interne très utile pour vous et l'administrateur.

14-Sauvegardes

Il y a deux types de sauvegardes gérées par le serveur :

- Les sauvegardes automatiques
- Vos sauvegardes

Les sauvegardes automatiques sont automatiquement exécutées à intervalle régulier par le serveur. Elles comprennent :

- sauvegarde journalière des bases de données MySQL (services et sites web perso)

- sauvegarde journalière des boîtes au lettre utilisateur (Maildir)
- sauvegarde hebdomadaire des home directory
- sauvegarde hebdomadaire du système

Elles sont cryptées et stockées sur le serveur de sauvegarde défini par l'administrateur. Elles ne sont pas directement accessibles aux utilisateurs mais peuvent être réclamées à tout moment à l'administrateur. Ces sauvegardes sont essentiellement réalisées dans le but d'une restauration rapide en cas de crash du serveur. Toutefois elles peuvent servir à récupérer des données malencontreusement supprimées par un utilisateur.

Vos sauvegardes elles sont réalisées et déclenchées manuellement par vous. À tout moment, vous pouvez décider de sauvegarder les éléments suivants :

- boîtes mail
- sites web perso comprenant le répertoire d'installation et la base de donnée
- Archive de configuration OpenVPN
- Home directory

Vos **sauvegardes** sont stockées dans le répertoire **sauvegardes** de votre **home directory**. Elles sont déclenchées via l'interface de gestion, et sont disponibles par cette même interface ou via une connexion ssh/ftp.

Pour accéder aux sauvegardes via l'interface de gestion : PORTAIL ⇒ Mon compte ⇒ Ma boîte à outils ⇒ Mon centre de sauvegardes/restauration.
À partir du centre de restauration/sauvegarde, vous pouvez :

- Lister vos sauvegardes avec les actions suivantes : **téléchargement**, **restauration** et **suppression**.
- Sauvegarder vos home directory en incluant ou non sa boîte mail (MailDir)
- Sauvegarder votre boîte mail (MailDir)
- Sauvegarder un de vos site web perso en incluant ou non sa base de données.
- Supprimer toutes vos sauvegardes d'un coup
- Restaurer une sauvegarde automatique de son home directory
- Restaurer une sauvegarde automatique de sa boîte mail
- Restaurer une sauvegarde automatique d'une base de données

15-SSH

Les **administrateurs** peuvent décider d'**interdire** la connexion directe aux utilisateurs en **SSH** en bloquant toutes les adresses ip pour des raisons de **sécurité** (et c'est fortement conseillé !). Si c'est le cas, pour pouvoir quand même accéder à votre **Home Directory** en **SSH**, vous avez la possibilité de **valider** et d'**autoriser temporairement** votre adresse ip pour vous connecter. Pour cela, rendez-vous dans : PORTAIL ⇒ Mon compte ⇒ Ma boîte à outils ⇒ Gérer mon accès SSH.
mon_ssh.png Normalement votre **adresse ip publique** (l'adresse ip de votre router/box) est **automatiquement détectée**. Pour vous en assurer, allez sur cette adresse et vérifiez/reportez

l'adresse ip affichée. Cliquez sur **ajouter**, et vous avez ensuite la possibilité de vous connecter en **ssh** pour une période définie par défaut de **2 heures**.

Une manière plus simple d'accéder au serveur **SSH** et d'utiliser le service **terminal** proposé. PORTAIL→Ma boîte à outils→Terminal. C'est beaucoup plus simple et moins contraignant à utiliser.

16-Formulaires et sondages

Cette section (PORTAIL→Ma boîte à outils→Mes formulaires et sondages) n'ont rien à voir avec les services **formulaire** (formallin) et **sondage** (framadate) proposés. Ici ce sont des options internes propres à farmserv. **Formulaire** permet d'accéder à une liste de formulaire proposé en interne à la gestion de farmserv, et ainsi que **sondage**. C'est en rapport direct avec les **utilisateurs/adhérents** et l'**administration** de l'instance. Les sondages sont adressés soit à l'ensemble des utilisateurs, soit aux responsables des entités. Ils peuvent être consultés en fin de date de validité par l'ensemble des utilisateurs.

17-Recherche

KerHost propose un **moteur de recherche minimaliste**. On peut y accéder depuis PORTAIL→mon en bas ou depuis PORTAIL→Ma boîte à outils→Recherche. Vous pouvez saisir un terme de recherche propre à vous (3 caractères minimum), comme un alias mail, ou un site web perso… Vous aurez alors accès directement aux réglage de cette recherche. La recherche se fait dans l'intégrité de la base de données et vous renvoit les résultats si vous y êtes lié. mon_recherche2.png

---

18-Mon espace membre du bureau

PORTAIL→Ma boîte à outils→Mon espace président/secrétaire/trésorier permet **aux membres du bureau** seulement d'accéder à des réglages supplémentaires propre à leur statuts. Pour le moment, on ne peut qu'y gérer sa **signature électronique**. signature.png

19-Sécurité

Parlons un peu sécurité. Un serveur dédié, autonome, tout ça c'est bien beau mais quid de la sécurité ? Et bien c'est la chose la plus importante à laquelle nous tenons sur **Famrserv**. Disons qu'elle est… solide ! (mais pas infaillible hein… rien n'est infaillible!). Tous les services web sont proposés sécurisés **HTTPS** (certificats et cryptage), et la messagerie également. Ce qui apporte une bonne

base à l'édifice. Mais le serveur est également équipé d'un système redoutable : **fail2ban**. C'est une application qui analyse en temps réel les **logs** (activité sur le serveur) et qui agit en cas d'anomalies détectées. Faisons simple : **Fail2ban** comptabilise le nombre de tentatives infructueuses (connexion web, mail, ssh...) et bannit les adresses IP à la volée en cas d'erreur de connexion. Une adresse IP (par défaut) est bannie après **3 tentatives** consécutives de connexions échouées, pour **une durée de 24h** ! C'est une procédure drastique et discutable, mais terriblement efficace ! Donc soyez vigilant à ceci : si vous vous trompez plus de 3 fois dans une connexion (mauvais login, ou mauvais mot de passe), vous vous verrez dans l'impossibilité de contacter le serveur ! Alors avant de crier « au loup, ça marche pas, remboursez ! », contactez l'administrateur pour voir si vous n'avez pas été automatiquement banni. Si c'est le cas et que l'administrateur est disponible, il vous débloquera immédiatement l'accès. Sinon attendez 24h... Ce système peut paraître contraignant et lourd, mais garantit une sécurité accrue du système, **alors retenez bien vos mots de passe** !!! Il est donc impératif de disposer d'un tel système. En revanche vous pouvez vous protéger d'éventuels bannissements si vous disposez d'une **adresse ip fixe**. Une adresse ip fixe dépend de votre **FAI** (Fournisseur d'accès Internet) et n'est pas obligatoirement attribuée. Elle assure que votre box qui se connecte à chaque fois sur internet dispose toujours de la même adresse IP. Ce qui est rarement le cas ! Orange n'en propose pas. Free oui à condition de la demander. Donc, si vous disposez d'une adresse ip fixe, vous pouvez l'indiquer au serveur pour vous mettre en **liste blanche**. Pour cela, il faut passer par : PORTAIL ⇒ Mon compte ⇒ Mes adresses ip fixes .

Vous devez impérativement être sûr que votre adresse ip est fixe avant de l'**ajouter** en **liste blanche**. Cela peut mettre en danger le serveur si ce n'est pas le cas !

Nous ne le répéterons jamais assez, **la meilleure sécurité est votre mot de passe !** Un bon mot de passe réduit considérablement tout type d'attaque.

20-Mot de passe

Votre mot de passe est ce qu'il y a de plus précieux. Vous ne devez pas le communiquer. Il est possible de le changer à partir de : PORTAIL ⇒ Mon compte ⇒ Mon mot de passe. Cette procédure change automatiquement votre mot de passe pour tous les services (mais pas celui de votre compte MySQL/PhpMyAdmin ni celui de vos sites web perso !).

Choisissez toujours un mot de passe **robuste**. Votre mot de passe doit obligatoirement :

- faire **12** caractères minimum
- contenir un **chiffre**
- contenir une **majuscule**
- contenir une **minuscule**

- contenir un des **caractères spéciaux** suivant : **~ { } [ ] - _ / @ = + % * , ? . : !**
- ne doit pas contenir de lettres accentuées, ni d'espace et aucun de ces caractères spéciaux : **$ & # ” ' (|) ` \ ;**

Si vous oubliez votre mot de passe (ce qui ne devrait pas arriver en principe !), il est possible de le réinitialiser à partir de PAGE D'AUTHENTIFICATION ⇒ Mot de passe perdu ?. Deux possibilités :

- **Vous vous souvenez de votre adresse mail de secours**, vous remplissez le champ **Nom de connexion** et **Adresse mail de secours**, et vous recevez dans l'instant suivant la procédure pour réinitialiser votre mot de passe.
- **Vous ne vous souvenez plus de l'adresse mail de secours que vous avez déclarée**, vous indiquez juste votre Nom de connexion, et l'administrateur reçoit un mail de demande de réinitialisation de mot de passe. L'administrateur se débrouille alors pour vous communiquer la procédure de réinitialisation de votre mot de passe.

Quand vous demandez à **réinitialiser** votre mot de passe, vous recevez la procédure suivante par mail :

- cliquer sur le **lien** unique qui vous est attribué pour une période de **deux heures**. Au delà, il ne sera plus valable.
- saisissez votre **login** ainsi que le **code 4 chiffres** que vous avez reçu dans le mail
- saisissez votre **nouveau** mot de passe qui doit répondre aux exigences minimum de sécurité et confirmez-le

init_password.png

Comprenez bien que votre mot de passe vous donne accès à **tout** sur votre compte (mails, services...) et que le **communiquer** à quelqu'un d'autre (même de confiance) est une **grossière erreur**, même si celui-ci est en mesure de vous débloquer une situation urgente que vous ne maîtrisez pas. Accompagnez cette personne physiquement pour saisir vous même votre mot de passe au moment opportun, mais ne faites pas ça par téléphone !

21-Confidentialité

VOS DONNÉES sont VOS DONNÉES ! Et vous appartiennent pleinement. Elles ne sont accessibles que par vous et personne d'autre, hormis les données que vous aurez décidé de partager (site perso et nextcloud). Toutefois, comme pour tout système informatique, le serveur dispose d'un compte **administrateur *root*** [26] qui a plein pouvoir sur le serveur, et donc forcément sur les données des

utilisateurs !!! Et heureusement, sinon il serait impossible d'intervenir en cas de problème. L'administrateur interviendra sur vos données personnelles uniquement si vous en faites la demande, et seulement à cette condition. Vous êtes donc responsable de vos données. KerHost est basé sur la confiance. Il n'y a aucun ***robot*** [27)] interne qui analyse le contenu de vos données personnelles à des fins commerciales ou autres. Cependant, concernant les espaces web perso hébergés sur **votre_sous_domaine**, nous n'empêchons pas l'indexation de robots externes (exemple, référencement de votre site chez Google). C'est à vous d'en assurer la diffusion (ou non).

22-Supprimer mon compte utilisateur

Vous pouvez **supprimer** votre compte utilisateur quand bon vous semble. La seul condition et de léguer votre responsabilité d'entité si vous êtes le responsable de votrez entité ! Pour cela, il suffit de vous rendre dans mon→mon entité et de cliquer sur **supprimer mon compte utilisateur** dans la liste des utilisateurs de votre entité. Vous êtes alors redirigé vers une page qui va vous établir une **liste** de tous ce qui est lié à votre compte et qui va disparaitre si vous confirmer la suppression de votre compte. Quelque soit votre raison de supprimer votre compte, pensez à faire une sauvegarde de vos données et de les réccupérer avant de confirmer. mon_infos.png

---

1)

Unix : système d'exploitation de AT&T, basé sur le langage C et sur le principe que les relations entre les programmes sont plus importantes que les programmes eux-mêmes.

2)

Ssh : Sécure SHell. shell permettant de se connecter de façon sécurisée sur une machine distante et d'y exécuter des programmes, toujours de façon sécurisée.

3)

Home directory : Le « home directory » est le répertoire personnel d'un utilisateur.

4), 22)

Terminal : Application permettant d'exécuter des actions en ligne de commande sur un ordinateur local ou distant (avec SSH).

5)

Https : HyperText Transfer Protocol Secure. protocole de transmission issu de Netscape lié à une connexion par socket sécurisée, autrement dit HTTP avec une pincée de SSL.

6)

Certificat : Document électronique identifiant une entité (personne physique ou morale, équipement...). Il est formé par des informations pertinentes à son utilisation (nom, adresse, société, numéro de téléphone), la clef publique de l'entité, le tout est signé par un tiers de confiance (autorité de certification). Cette signature prouve l'authenticité du certificat et garantit son in-falsifiabilité.

7)

Mail : Courrier électronique. Message mémorisé par l'ordinateur destinataire, et transmis par réseau. Sa distribution est en général bien plus rapide que celle du courrier classique, tout en étant loin d'être instantanée.

8)

IMAP : Internet Message Access Protocol. protocole, dans sa version 4, de gestion de messagerie, destiné à remplacer POP 3, qui est nettement moins performant. IMAP sait ainsi stocker le courrier sur le serveur et pas sur le client, et gérer toute la chose de façon correctement sécurisé.

9)

SMTP : Simple Mail Transfer Protocol. Protocole de la famille IP utilisé pour le transfert de courrier électronique. Utilisé évidemment sur l'Internet et reconnu par l'ISOC. Défini dans la RFC 821.

10)

WebMail : interface web permettant d'accéder à du courrier électronique. Cela permet de lire son courrier de façon simple et d'à peu près n'importe où (au détriment, souvent, de la sécurité).
11)

Adresse canonique : adresse électronique véritable, désignant effectivement un utilisateur sur une machine (même si cette adresse est un compte générique), par opposition aux alias, qui ne font que pointer vers une autre adresse.
12)

FTP : File Transfer Protocol. protocole de transfert de fichier. Par extension, nom de l'utilitaire d'Unix utilisant le protocole TCP/IP pour télécharger des fichiers dans un sens ou dans l'autre.
13)

JABBER (XMPP) : eXtensible Messaging and Presence Protocol. Protocole de messagerie instantanée basé sur XML, dont l'utilisation la plus connue s'appelle Jabber.
14)

Messagerie instantanée : messagerie synchrone, dans laquelle vos correspondants reçoivent quasi immédiatement vos messages, généralement courts (quelques lignes).
15)

SSL : Secure Socket Layer. sockets sécurisées utilisées principalement par Netscape à l'origine, puis reconnues par l'ISOC.
16)

MySQL : SGBDR dont la principale qualité est, selon des théoriciens, d'être libre et, pour le gros du marché, d'être gratuite. Du coup, il est très utilisé pour mettre en ligne sur le Web des applications bâties autour de bases de données.
17)

CardDav est un protocole sur le modèle client/serveur pour gérer un carnet d'adresse. Il a été conçu pour stocker et partager les données des contacts sur un serveur. Ce protocole a été développé par l'IETF et a été publié en août 2011. CardDav est basé sur WebDAV et utilise les vCard comme format de données, et utilisé par de grands acteurs d'Internet
18)

CalDAV (Calendaring Extensions to WebDAV) est une extension à WebDAV définie par le groupe de travail IETF du même nom. Décrit dans la RFC 4791, CalDAV définit un protocole d'édition de calendrier en ligne. Il existe une autre extension à WebDAV traitant des calendriers (Web Calendar Access Protocol) qui définit un protocole de partage de fichiers au format iCalendar utilisant WebDAV. CalDAV contrairement à ce dernier n'est pas un partage de fichiers calendriers mais d'évènements. Un calendrier est, dans CalDAV, un dossier contenant des évènements, des tâches... Chaque évènement est transmis sous la forme d'un fichier VEVENT, VTASK... (voir iCalendar). Il est donc possible contrairement à Web Calendar Access Protocol de manipuler un seul élément sans avoir à échanger l'ensemble du calendrier. CalDAV regroupe au sein d'un même usage plusieurs extensions à WebDAV : WebDAV ACL pour les droits d'accès. On peut noter que l'élément atomique étant l'évènement, on peut définir des droits différents pour chaque évènement; Delta-V (Internet Protocol) définissant un protocole de gestion de version sur WebDAV. Un calendrier étant un dossier (une collection au sens WebDAV) ne contenant que des éléments de calendrier, CalDAV définit un verbe supplémentaire pour la création d'un calendrier : MKCALENDAR.
19)

WebDAV (Web-based Distributed Authoring and Versioning) est un protocole (plus précisément, une extension du protocole HTTP) définie par le groupe de travail IETF du même nom. Décrit dans la RFC 4918, WebDAV permet de simplifier la gestion de fichiers avec des serveurs distants. Il permet de récupérer, déposer, synchroniser et publier des fichiers (et dossiers) rapidement et facilement. L'objectif principal de WebDAV est de rendre possible l'écriture à travers le web et pas seulement la lecture de données. WebDAV permet à plusieurs utilisateurs d'éditer le contenu d'un dossier web simultanément. Il saura gérer les droits d'accès aux fichiers (ou dossiers), en verrouillant momentanément les fichiers et dossiers édités.
20)

Rss : RDF Site Summary ou Rich Site Summary. Contenu d'un site web décrit en XML conformément au RDF. Défini à l'origine par Netscape pour ses canaux Netcenter, ce type de sommaire permet de publier des titres de nouvelles ou d'articles, et de permettre à d'autres sites de les exploiter dynamiquement.
21)

Liste de diffusion : est une utilisation spécifique du courrier électronique qui permet le publipostage d'informations aux utilisateurs qui y sont inscrits. Celle-ci est gérée par un logiciel adéquat installé sur un serveur. On différencie les listes d'annonces destinées à envoyer des informations aux abonnés sans retour de leur part, des listes de discussion où toute personne inscrite peut envoyer un message ou y répondre.
23)

Proxy : Appliance ou logiciel servant d'intermédiaire entre un réseau rapide ou uniquement peuplé d'amis (qui bénéficie de ses services et où se trouvent ses clients) et un autre plus lent ou hostile. Le premier réseau est souvent un LAN et le second l'Internet.
24)

VPN : Tunnel chiffré établi entre au moins deux machines en utilisant un réseau non sûr mais peu onéreux, et en y faisant circuler les données après les avoir chiffrées afin que les autres usagers ne puissent espionner.Dans le passé pour interconnecter deux machines (ou deux réseaux) physiquement distantes en rendant l'espionnage difficile, on établissait entre elles une couche réseau physique propre, par exemple une LS. Cela coûtait cher. Un réseau privé virtuel ménage la confidentialité et est économique. Le réseau existant, dit de transport, est souvent l'Internet.En pratique cela implique un peu plus que du chiffrement puisque les interconnectés s'inter-identifient bien (sinon une interposition reste possible) et le routage réseau doit être bien assuré (afin que des informations confidentielles ne circulent que chiffrées).
25)

Routeur : dispositif matériel ou logiciel chargé du routage. Il est connecté à au moins deux réseaux et copie des paquets de l'un à l'autre en fonction d'informations qu'ils véhiculent et de règles définies par l'administrateur. Les informations employées sont par exemple l'adresse du destinataire (se trouve-t-il sur un réseau différent de celui de l'émetteur?), l'urgence, le protocole… Les règles reflètent la politique de routage et, par exemple, interdisent/autorisent/privilégient un type de trafic (ce qui vient de telle patte et est destiné à telle machine ne passe pas, ce qui est destiné à telle machine passe avant le reste…).
26)

Root : Nom du compte administrateur sous certains systèmes Unix. Voir aussi rootkit. On dit traditionnellement qu'il existe deux types d'administrateurs : ceux qui ont fait une grosse bêtise sous root, et ceux qui vont en faire une… Root signifie racine en anglais.
27)

Robot : c'est aussi l'abréviation de bot. Ce genre de bidule logiciel vous permet d'exécuter des actions relativement complexes, en partie, d'effectuer des recherches dans des base de données sur un réseau, ou bien de surveiller un canal IRC.