Artica

La console Locale de management
d'un serveur d'infrastructure.

Révision Du 9 Mai 2011 version 1.5.050923

Table des matières

Introduction : 7

Historique du projet :..... 7
A qui s'adresse Artica ?..... 7
Licence et support..... 7
Que fait Artica ?..... 7

Installation d'Artica..... 8

Matériel et système supportés..... 8
Distributions Linux supportées :..... 8
Quelle est la distribution conseillée ?..... 8
Architecture 32 ou 64 bits ?..... 8
Matériel :..... 8
Virtualisation 9

Utilisation d'une Image ISO..... 9

Compte par défaut de l'interface 9

Installation sur une distribution Linux..... 10
Installation sur CentOS..... 10

Premiers pas 14

Modifier le mot de passe du Super Utilisateur..... 14

Modifier le mot de passe du compte mysql..... 15

Créer sa première organisation..... 16

Créer son premier utilisateur..... 17

Sécurité de la console de gestion :..... 18
Visualisation des évènements..... 18
Être notifié par email des accès à la console..... 19

Gestion et Administration des paramètres réseaux..... 20
Modifier le nom d'hôte 20
Modifier l'adressage TCP/IP du serveur..... 21
Modifier l'adressage réseau..... 21
Définir un routage avec la carte réseau..... 21

Centraliser les bases de données..... 22
Un trio..... 22
Le moteur Open LDAP..... 22
Le Moteur Mysql..... 23
Comptes utilisateurs distants..... 24

Répliquer la base LDAP..... 25
Définition du maître..... 25
Activation du serveur esclave..... 26

Artica et le Partage de fichiers..... 27

Un contrôleur de domaine ?..... 28
Gestion de la sécurité utilisateur..... 28
Sécurité des données via les profils..... 28
Partage des équipements..... 28
Mise en place avec Artica..... 29
Les pré-requis..... 29

Transformez votre serveur Artica en contrôleur de domaine....29
Vérification de la présence de Winbindd....29
Activez le contrôleur de domaine....30
Édition du compte Administrateur (Administrator)....31
Ajout des postes de travail dans la base de données Artica....31
Raccordement de l'ordinateur au domaine....33
Ajoutez un utilisateur et l'inscrire dans le domaine....34
Vérification de la session....36
Activez les profils itinérants....37

La Déduplication ?....39
Quel est l'intérêt ?....39
Gain d'espace disque....39
Virtualisation !....39
L'inconvénient....39
Mise en place avec Artica....40
Installation des modules principaux....40
Premiers pas....42
Les paramètres du moteur....42
La taille du tri de comptage de la base : 42
Le cache....42
Les répertoires....43
Utilisation de l'explorateur....43
La réplication....44
Le maître 44
L'esclave....44

La sauvegarde temps réel avec greyhole....45
Principe :....45
Mise en place 45
Ajout des ressources de sauvegarde....46
Affectation des sauvegardes aux partages....47

Quotas sur les partitions....48
Activation des quotas dans les partitions....48
Définition des quotas....49

Permissions sur les répertoires et ACLs....51
Mise en place des ACL sur les Disques....52
Application des permissions sur les répertoires....52
Vérification de l'application des ACL....54
Visualisation des ACL mis en place....55

Artica : proxy cache et filtrage d'url....56

Introduction....57

Le filtre ufdbGuard....57
Installation et activation du filtre....57
Installation....57
Activation du filtre ufdbguard....58
Etats et maintenance des bases de données....59
Communauté Artica:....59
Les bases UfDbguard: 59
Etat des bases de la communauté....59
Recherches dans les bases de la communauté....60
Compilation des bases de la communauté....61
Re-compilation des bases....61
Programmation de la re-compilation des bases....62

Les règles de filtrage....63
Création d'une nouvelle règle....63
Affectation d'adresses IP....64
Affectation par groupes d'utilisateurs....64
Affectation des catégories....65

Gestion des utilisateurs et ordinateurs....66

Privilèges des utilisateurs et délégations 66
Niveaux d'affectation des privilèges....66
Niveaux des privilèges 68
Fusion des privilèges....68

Reveil par le réseau « Wake-on-Lan » **69**

Artica et la messagerie 70

Préface, Artica une passerelle SMTP Anti-spam et antivirus **71**
Mécanismes de filtrage **71**
Principales fonctionnalités du mode relais **72**
Facilités d'administration 72
Filtrage du courrier entrant : 72
Filtrage du courrier sortant : 72

Le Multiple-instances **73**
Introduction : Pourquoi le multiple-instances ? : **73**
Le comportement standard **73**
Les limitations **73**
Le multiple-instance **74**
Les avantages 74
Les inconvénients 74
Artica 74
Mise en place du multiple-instances dans Artica **75**
Cas pratique **75**
1) Création de l'organisation 75
2) Création et affectation des adresses IP 76
3) Activation du mode multiple-instances 77
4) Définition des privilèges 78
5) Administration des instances 80

Le Domain throttling avec Postfix **82**
Les principaux fournisseurs limitent la fréquence de réception de leur serveurs 82
Pouvoir envoyer des messages en masse 82
Accélérer la cadence 82
Mise en place avec Artica **82**
Le principe est le suivant : 83
Création des démons 83
Paramètres du démon **83**
nombre maximal par défaut de livraisons parallèles: 83
Rétention d'acheminement: 83
nombre initial de livraisons parallèles: 83
Limite de destinataire de destination par défaut: 83
Limite Extra du nombre de destinataire: 83
Prêt de slot de livraison: 84
Rythme d'ordonnancement: 84
moment d'une préemption de message: 84
Ajouter des domaines aux démons de transmission **84**

La rotation TCP/IP **85**
Qu'est-ce ? **85**
Différentes utilisations **85**
Mise en place avec Artica **85**

Postfix Instant IpTables **87**
Quel est l'intérêt ? **87**
Déchargez votre serveur ! 87
Assurez une bande passante de qualité 87
Comment ca marche ? **88**
Esprit communautaire 88
Mise en place avec Artica **88**
Personnaliser la sensibilité du scanner 89
Visualiser , désactiver les règles 89
Listes blanches 89

PostScreen **90**
Les Zombies et BotNets, 99% du Spam reçu **90**
PostScreen, une solution **91**
Les différents tests effectués par PostScreen **91**
Les lignes « vides » 91
Le half-duplex 91
Les commandes NON-SMTP 91
Requêtes sur les serveurs DNS Blacklist 92
Mise en place de PostScreen **93**
Les protocoles de tests 94
Les serveurs de blacklist DNSBL 95

Le VIPTrack **96**
Une fonctionnalité politique qui assure le service Informatique **96**
Informer l'administrateur que des messages sont restés dans la file d'attente du relais de messagerie 96

Créer des rapports réguliers de messages bloqués entrants/sortants....96
Mise en place de VIPTrack....97
Activation et Réglages de l'ordonnancement....98
Exécuter les rapports chaque et calculer depuis....98
Vérifier dans la file d'attente chaque :....98

Postfwd un pare-feu de la messagerie....99
Postfwd est un serveur de « délégation de règles»....99
Postfwd dans Artica....99
Ou trouver Postfwd en multiple-instances ? :....99

Postfwd un pare-feu de la messagerie....100
Postfwd est un serveur de « délégation de règles»....100
Postfwd dans Artica....100
Ou trouver Postfwd en multiple-instances ? :....100
Ou trouver Postfwd en mono-instance ? :....101
Mise en place....101
Les règles....102
Action de la règle....102
Attributs de détection 103
Les opérateurs....104
Les variables 104
Les additions des attributs et exemples....105
Les sauts de règles 105
Les scores 106

Nombre maximum de destinataires 107
Sans le filtre amavisd-new....107
Avec le filtre amavisd-new....107

Listes Blanches....108
Liste blanche globale....108
Liste de blanche des connexions....109
Fusionner les listes blanches....111

Historique et visibilité....112
PostFinder....112
Le principe : 112
Rotation des fichiers de logs....113
Analyse du filtre de contenu....114

Performances....116
Performance du filtre de contenu....116
Choix des modules de filtrage....117
Couplage du filtre avec Postfix....118
La méthode milter :....118
La méthode d`Après Queue-Postfix....118
Quelle méthode choisir ?....118
Comment modifier le couplage ?....118

Créer ses premiers domaines de messagerie....119
Domaine local :....119
Domaine acheminé :....119

Récupération du courrier distant....120
Utilisation de fetchmail....120
Activation du service de récupération de courrier....121
Ajouter des règles de rapatriement de courrier....122
Options du serveur :....122
Options Utilisateur....123

Des sites Internet avec FreeWebs....124

Ajouter un nouveau site web....124
Base de données....125
Accès FTP....125
Accès au site web....126
Vous disposez d'un serveur DNS local ou Internet :....126
Modification du fichier hôtes....126
Utilisation d'Artica en serveur DNS (PowerDNS)....127
Utilisation d'Artica en serveur DNS (dnsmasq)....127
Tests du site web....128

Partage Web (WebDAV) 128
Activer un site FreeWebs en partage Webdav....128
Accès au partage Web....130

Sécurisation 131
Authentification du site web 131
Limitation du site Web par adresses 131
Les règles de réécritures 132
Permissions sur les dossiers et fichiers 133
Activation de la QOS 135

Gestion du système 136

Centraliser les évènements systèmes 136

Maintient du système 137
Synchroniser les paquetages systèmes 137
Sauvegarde des données du système 138
Ajouter une tâche de sauvegarde 139
Vérifier la santé de vos disques durs 141
Accéder aux données SMART dans Artica 141
Vérification RBL (serveurs de listes noires) 143
Liste des serveurs RBLS 143
Paramètres 144
Affichage des résultats 144

Gestion automatique des points de montage 145
Créer une connexion vers un répertoire distant 146

Artica Client ou fournisseur iCSCI 148
Artica fournisseur iCSCI 148
Client iCSCI sous MS Windows 150
Dans Windows Server 2008 R2 : 150
Dans Windows 7 : 150
Dans Windows 2003 et XP 150
Client iCSCI sous Artica 152

Introduction :

Historique du projet :

Le projet Open Source Artica est né en *Janvier 2004*.

Le projet Artica a pour but de valoriser les fonctionnalités offertes par la plate-forme Linux à travers une console d'administration locale installée sur le serveur Linux.

Cette console permettant alors de configurer un serveur Linux sans connaissances Unix particulières.

Artica propose alors la gestion de la messagerie, du partage de fichiers, des accès VPN, du proxy Internet avec les sécurités qui s'imposent comme l'anti-Spam, l'antivirus et le contrôle des sites web.

A qui s'adresse Artica ?

Artica assure le paramétrage des logiciels Open Source et du système Linux.

De cette mission, toute personne ou entreprise désireuse de disposer d'un serveur de messagerie et/ou d'un serveur Web et/ou d'un serveur de fichiers et/ou d'un proxy Internet peut s'équiper du logiciel Artica.

Licence et support

Artica est un logiciel libre, il peut être installé, déployé librement et sans contraintes de licence.

Artica Technology propose des services d'installation, de maintient et de support du logiciel Artica.

Elle propose aussi des services d'adaptation afin d'offrir des fonctionnalités spécifiques .

Aussi, si vous désirez revendre Artica en adaptant le logiciel à votre infrastructure.

Pour ce faire, veillez contacter par eMail
Mr Tougeron Florent ftougeron@artica-technology.com
Bur :09.61.07.21.53
Mobile : 06.72.95.40.52

Que fait Artica ?

La force des logiciels Microsoft est de pouvoir fournir une interface IHM (Interface Homme/Machine) permettant à des personnes non familières à l'administration du système de pouvoir gérer, surveiller, administrer un serveur.

Artica à pour but de proposer les mêmes fonctionnalités sur des systèmes Linux.

Artica offre alors la possibilité de « **piloter** » un système Linux à travers une interface web SSL.

Des profils administrateurs peuvent être créés afin de pouvoir dédier les tâches d'administration à plusieurs personnes

Les tâches d'administration sont les suivantes :

- Administrer, surveiller les **mises à jour** du système.
- Administrer les paramètres **réseau** du serveur.
- Gérer les **comptes utilisateurs** à travers une base OpenLDAP.
- Administrer un serveur de **messagerie** complet comprenant la **gestion des boîtes aux lettres** (cyrus-imap ou bien Zarafa), le **routage** de la messagerie (Postfix), **l'antispam** (Spamassassin, Kaspersky Anti-Spam Gateway, amavis, milter-greylist), la sécurité **antivirus** (ClamAv, Kaspersky For Linux mail server).
- Administrer un **Proxy Web** (Squid) comprenant la gestion des **caches**, le **filtrage d'URL** (ufdbguard, squidGuard), **l'antivirus** (C-ICAP, squidclamav, Kaspersky For Proxy server).
- Administrer un **serveur de fichiers** (Samba) qu'ils soit de façon autonome ou en **contrôleur de domaine** comprenant **la** gestion **antivirus** avec ClamAv et Kaspersky For Samba server**.**
- Administrer un serveur **VPN** (OpenVPN**).**
- Administrer un système de **virtualisation** (VirtualBox) et de VDI

Installation d'Artica

Artica est un logiciel qui a pour but de prendre la main sur le système d'exploitation.
L'ensemble des paramètres du systèmes vont être alors modifiés et verrouillés par Artica.
Il n'y a pas de sens d'installer Artica sur un système déjà utilisé/paramétré et en production.
Pour ce faire, vous devez utiliser une machine « vierge », installer une des distribution supportée et « poser » Artica dessus.

Matériel et système supportés

Distributions Linux supportées :

Artica supporte les distributions suivantes que ce soit en **32 ou 64 bits.**

- CentOS 5.2,5.3,5.4,5.5 ,
- Fedora 11,12,13,14
- OpenSuse 11.1,11.2,11.3,
- Mandriva 2009,2010
- Ubuntu 8.04,8.10,9.04,9.10,10.04,10.10
- Debian 4.x,5.x,6.x

Quelle est la distribution conseillée ?

Bien que Artica supporte les systèmes Red Hat, ces distributions souffrent d'un manque de paquetages et de logiciels.

Artica s'adapte lorsque des logiciels sont manquants. Les fonctionnalités sont alors masquées.

Il se peut alors que vous ne retrouvez pas certaines fonctionnalités décrites dans ce document si vous décidez d'installer Artica sur des systèmes tels que *CentOS* ou *Fedora*.

Si vous n'avez pas de griefs nous vous conseillons donc **Ubuntu** ou **Debian**.

La distribution **Ubuntu** offre de nombreux paquetages, toutefois cette distribution est régulièrement mise à jour.

SI vous souhaitez disposer d'un système stable dans le long terme, optez alors pour la distribution **Debian**.

Architecture 32 ou 64 bits ?

Artica support les deux architectures toutefois, et d'un façon générale si votre matériel supporte du 64bits, optez pour du 64bits.

Matériel :

D'une façon minimale, Artica et ses logiciels associés nécessitent un processeur Core 2 duo 1.6Gz avec 1Go de mémoire vive et 8Go de disque dur.

Il est possible de descendre le niveau de mémoire de la machine à 512Mb de mémoire vive mais Artica risque automatiquement de désactiver certains services pour pouvoir faire vivre le système de façon optimale.

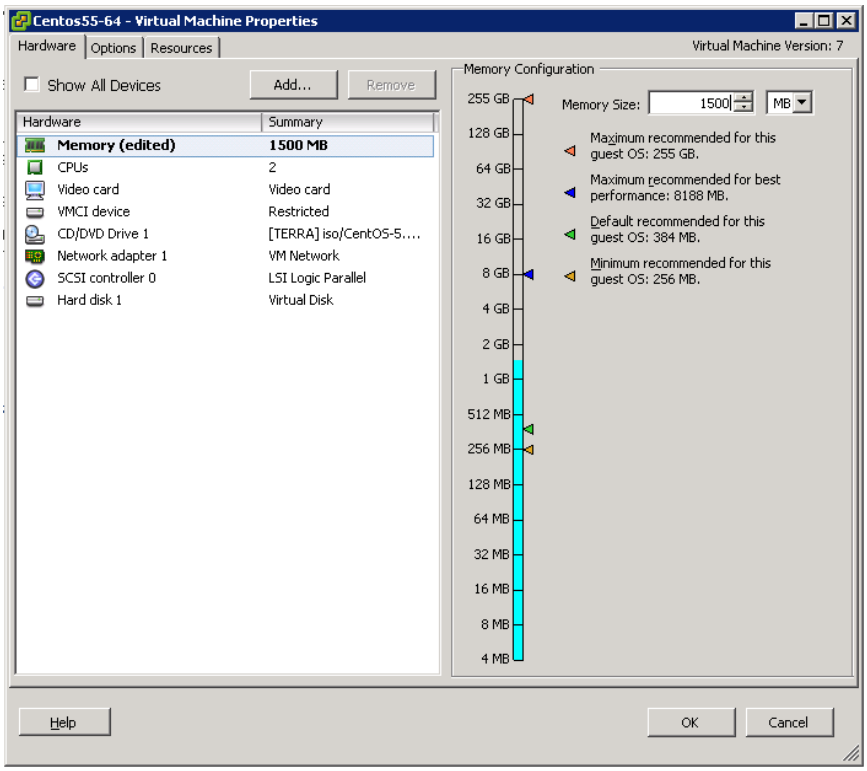
Une configuration optimale commence à 1.5 Go de mémoire vive avec 1 processeur Core 2 duo

La vitesse du disque dur est importante. Plus le disque dur est de bonne qualité et rapide, plus le système fonctionnera de façon optimale.

Virtualisation

Artica est compatible sur des systèmes virtualisés, toutefois pour une utilisation optimale du système, veuillez associer deux processeurs virtuels à la machine

Assurez-vous aussi que le virtualisateur dispose de bonne performances en matière de lecture/Ecriture disque (I/O)



Utilisation d'une Image ISO

Artica est proposé en image ISO d'installation. Ces images ISO (sur une base Debian 5 32 bits) sont disponibles à l'adresse suivante :

<http://sourceforge.net/projects/artica-postfix/files/Artica%20ISO/>

Compte par défaut de l'interface

Que ce soit via une image ISO ou via l'installation sur une distribution, deux comptes « aléatoires » par défaut sont utilisés (sans les guillemets) :

Compte : « **Manager** » et mot de passe « **secret** »

Compte : « **admin** » et mot de passe « **secret** »

Attention au respect de la casse

Installation sur une distribution Linux.

Installation sur CentOS

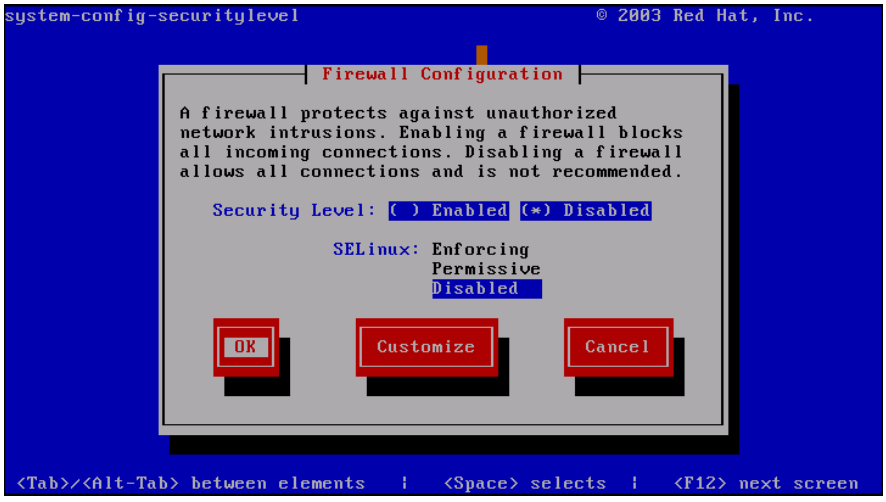
Nous ne détaillerons pas les étapes d'installation de CentOS, toutefois, il est inutile de précisez un système de serveur à installer.

Artica sera en charge d'installer les paquetages nécessaires au serveur que vous désirez utiliser.

Lors de l'étape de sélection des paquetages de CentOS, **veillez à ne rien côcher** afin de passer en installation minimale.

Au redémarrage de la machine et à l'éxécution du Setup Agent, sélectionnez le menu « Firewall configuration »

Désactivez le Pare-feux et le module SELinux.



Une fois l'installation de CentOS effectuée tapez

wget http://www.artica.fr/download/setup-centos.tgz

```
--2011-01-30 13:44:11--  http://www.artica.fr/download/setup-centos.tgz
Resolving www.artica.fr... 93.88.245.88
Connecting to www.artica.fr|93.88.245.88|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 343990 (336K) [application/x-tar]
Saving to: `setup-centos.tgz'
100%[======================================>] 343,990      550K/s   in 0.6s
2011-01-30 13:44:11 (550 KB/s) - `setup-centos.tgz' saved [343990/343990]
```

tar -xf setup-centos.tgz

./setup-centos

```
Exporting path in /root/.profile...
ERROR while exporting PATH
initialize...
Detected:CENTOS ""... Major version:5 Minor:5 Arch:64bits
Loaded plugins: fastestmirror
Determining fastest mirrors
 * addons: mirror.ovh.net
 * base: mirror.ovh.net
 * extras: mirror.ovh.net
 * updates: mirror.ovh.net
addons                                                   |  951 B     00:00
../...
Checking.............: system...
Checking.............: SeLinux...
Artica is not compliance with SeLinux installed on your system...
Do you want to uninstall it ? [Y]
```

Cette première question vous demande de retirer le système SeLinux qui si il est activé risque d'empêcher l'exploitation des différents services que gère Artica.

Tapez Y puis Entrée

```
You need to reboot your computer.....
after rebooting , launch the command
"/root/setup-centos"
```

Exécutez à nouveau le programme

./setup-centos

```
Detected:CENTOS ""... Major version:5 Minor:5 Arch:64bits
Checking.............: system...
Checking.............: SeLinux...
Checking.............: Building package list...
Checking.............: waiting for rpm exporting list
Checking.............: Exporting list done...
Some mandatories packages need to turn you distribution into:
          ***************
              rpmForge
          ***************
Do want to make this operation ?[Y]
```

le setup va détecter si les serveurs de ressources logiciels sont présents dans la configuration du serveur afin de pouvoir installer l'ensemble des composants.

Tapez Y puis Appuyiez sur la touche Entrée

```
Some required packages need to turn you distribution into:
          ***************
        atrpms, epel,elrepo
          ***************
Do want to make this operation ?[N]
```

Le programme d'installation va détecter si les serveurs de ressources logiciels sont présents dans la configuration du serveur afin de pouvoir installer l'ensemble des composants.
Tapez Y puis Entrée

```
Some dependencies will missing for next installation if you
continue, some packages installed will failed...
Press Enter key to continue or press "c" and Enter if you want to skip mandatories checking
```

Une fois les serveurs de sources ajoutés, le programme d'installation va installer les paquetages standards afin de faire fonctionner Artica dans un environnement optimal.

Appuyiez sur la touche Entrée

```
########################################
##                                    ##
##  Artica-postfix modules installation  ##
##                                    ##
########################################

"Be sure to not install Artica on a production server already set
Artica will transform this system to fit it`s needs that should not encounter
your same parameters strategy. use a free system before installing it!"
Select the modules you want to install:

#################################################################
##                                                             ##
## Install mandatories dependencies..:.................[ENTER] ##
##                                                             ##
#################################################################

This will install 135 package(s):
Quit the installation program.........................:[Q]
Type the option.....................................:
```

> *Ne vous inquiétez pas sur le nombre important (135) de paquetages qui vont être installés. Beaucoup sont des outils de compilation, librairies et sources nécessaires afin de compiler et de déployer des logiciels que Artica est amené à piloter.*

Appuyiez sur la touche Entrée deux fois.

Patientez pendant l'installation des paquetages primaires.

```
Artica is ready to be installed...
Do you want to install artica now ? [Y]
```

Une fois les paquetages primaires installés, Appuyiez sur la touche Entrée afin d'installer Artica

```
#############################################################################
##                                                                         ##
## You can access to artica by typing https://yourserver:9000              ##
## Use on logon section the username "Manager"                             ##
## Use on logon section the password "secret"                              ##
## You have to logon to artica web site, set yours domains and apply policies  ##
##                                                                         ##
## You can install others package by executing artica-make                 ##
## /usr/share/artica-postfix/bin/artica-make --help                        ##
##                                                                         ##
#############################################################################

Select the modules you want to install:
Install all modules.......:................................[A]

SMTP MTA (include postfix and securities modules):.....[1]
23 package(s) are not installed
*********************************************************
Files Sharing (include Samba and Pure-ftpd):...........[3]
11 package(s) is not installed
*********************************************************

Squid Proxy:...........................................[4]
3 package(s) are not installed
*********************************************************

NFS System :...........................................[6]
3 package(s) are not installed
*********************************************************

PowerDNS System :.....................................Installed
*********************************************************

OpenVPN System :......................................Installed

----------------------------
Install/upgrade Artica-postfix:.......................[5] (1.5.010118)
reboot  Artica-postfix:...............................[R]
Get SuperAdmin Infos:.................................[I]

Quit the installation program.........................:[Q]
Type the option.....................................:
```

Une fois Artica installé, le programme d'installation vous propose d'ajouter des paquetages additionnels afin de transformer votre serveur en serveur de messagerie (touche 1) , Serveur de fichiers (touche 3), Proxy internet (touche 4)

Tapez la touche correspondante et Appuyiez sur la touche Entrée

Ouvrez votre navigateur et tapez l'adresse https://ip.de.votre.serveur:9000

Premiers pas

Modifier le mot de passe du Super Utilisateur.

Le mot de passe par défaut : « secret » n'est pas un mot de passe que l'on peut appelé de « sécurisé », il est nécessaire que vous changiez tout de suite le mot de passe d'accès « Super Utilisateur ».

Pour ce faire, cliquez dans le menu du haut «**PARAMETRES GLOBAUX** » puis sur l'icône « **Compte** »

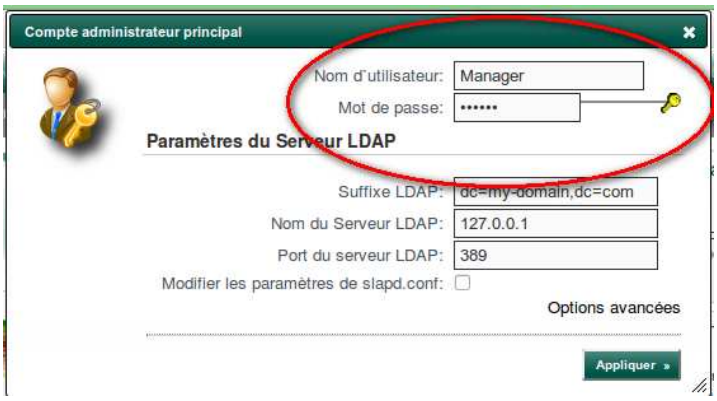
Indiquez le nom d'utilisateur et le mot de passe du Super Utilisateur. Et cliquez sur « appliquer »

L'interface va déconnecter votre session et vous devrez rentrer les nouvelles coordonnées.

Le compte Super Utilisateur est aussi le compte « Master » du serveur LDAP

Si vous avez oublié le mot de passe, vous pourrez toujours le retrouver en ligne de commande sur le système en tapant la commande suivante :

« cat /etc/ldap/slapd.conf »



Modifier le mot de passe du compte mysql

Artica utilise Mysql en tant que moteur de base de données.

Ce moteur sert à la fois à Artica pour stocker certains paramètres mais aussi pour stocker les évènements du systèmes et les messages email sauvegardés et/ou mis en quarantaine.

Il est nécessaire de s'assurer que Atica à bien pris connaissance des coordonnées MYSQL.

Pour ce faire, cliquez dans le menu du haut «**PARAMETRES GLOBAUX** » puis sur l'icône «**Paramètres MySQL**»

Sélectionnez l'icône « Nouveau compte utilisateur... »

Indiquez un nouveau nom d'utilisateur et mot de passe qui sera administrateur du serveur Mysql.

Créer sa première organisation

Que ce soit un serveur de fichiers, un serveur de messagerie, un serveur VPN ou bien même un proxy Internet, Artica utilise le principe des « organisations ».

Une **organisation** est un conteneur permettant de rendre hermétique certaines fonctionnalités. Ce peut être un service spécifique dans votre entreprise ou bien le nom d'une entreprise.

Ce principe d'organisation permet de pouvoir découper un serveur en plusieurs parties. La partie « messagerie » de Artica est très avancée à ce sujet. En effet il est même possible d'offrir un serveur de messagerie par organisation.

On peut dire qu'avec cette méthode, il est possible « d'héberger » un serveur Artica afin d'offrir la messagerie en mode **SAS**.

La première opération à effectuer est de créer une organisation....

Si votre serveur ne dispose pas d'organisation, la page d'accueil vous le fera savoir

A ne pas confondre avec la notion de « groupes » qui quand à elle est aussi prise en charge par Artica.

Dès que vous vous êtes connecté sur la console, utilisez le menu de gauche et cliquez sur « **organisations** »/ « **Ajouter** »

Une boîte message va apparaître, indiquez un nom dans le champs.

Évitez les caractères spéciaux lorsque vous remplissez le champ.

L'organisation que vous aller ajouter fera partie d'une « branche » LDAP.

Créer son premier utilisateur.

Une fois avoir créé votre première organisation, vous pouvez maintenant créer votre premier utilisateur.

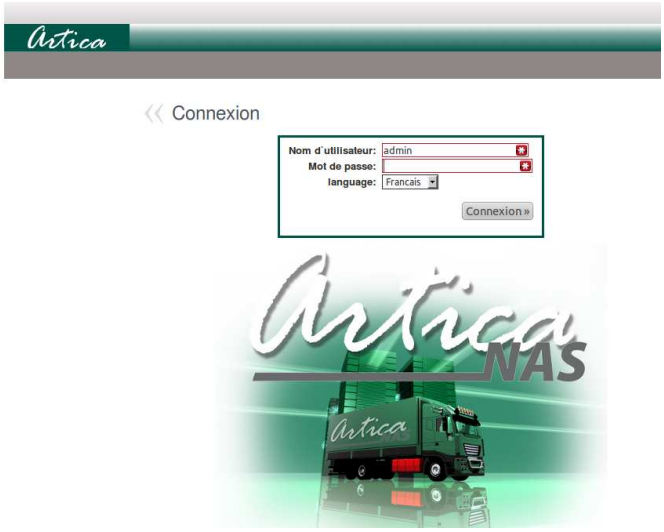
Cet utilisateur peut être un compte d'accès au serveur de fichier ou bien une boîte aux lettres ou une adresse eMail. Toujours est-il que avant tout c'est un humain qui est censé utiliser les services du serveur que vous venez d'installer.

Vous pouvez créer un utilisateur à plusieurs endroits, en effet, cette opération peut être exécutée plusieurs fois. C'est la raison pour laquelle, plusieurs chemin à travers l'interface vous sont proposés afin d'opérer rapidement à cette tâche.

Dans le menu de gauche, sélectionnez votre nouvelle organisation puis cliquez sur « **Ajouter un Utilisateur** », en cliquant aussi sur l'organisation vous avec un icône « **Créer un compte utilisateur** »

Sécurité de la console de gestion :

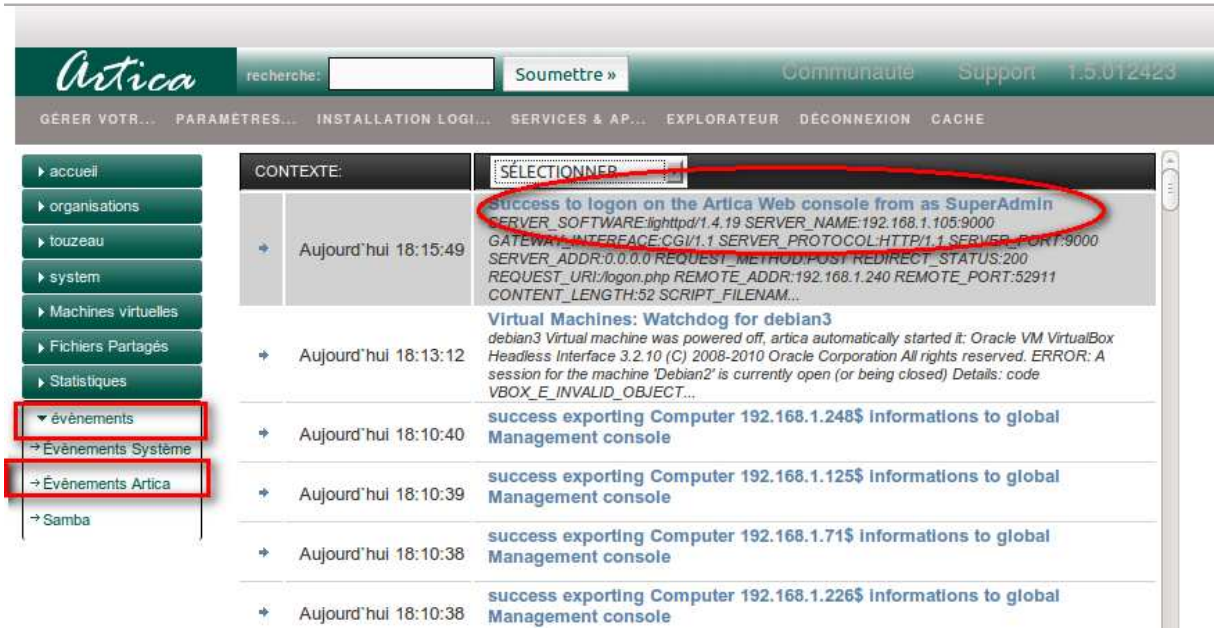
A partir de la version **`1.5.012518`**, lorsqu'une personne tente de se connecter sur la page d'administration, un événement est enregistré dans la table des évènements d'Artica.



La page de connexion dispose d'une surveillance des tentatives d'accès

Visualisation des évènements.

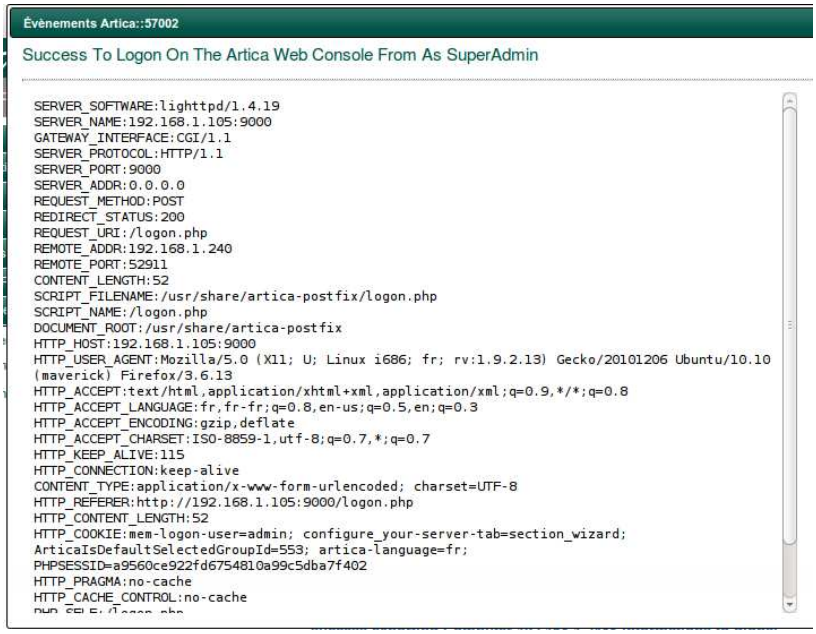
Dans le menu de gauche « **Évènements/ Évènements Artica** » vous pouvez visualiser les tentatives de connexions sur la console web afin de savoir si elles sont en succès ou en échec.



En cliquant sur l'évènement, une boite message s'affiche.

Elle vous permet de visualiser toutes les informations captées par le moteur Web.

Si le serveur Artica est connecté à la console globale de management « Artica Meta » les évènements sont alors aussi envoyés à la console globale de management afin de vérifier les connexions sur un ensemble de serveurs.



Être notifié par email des accès à la console.

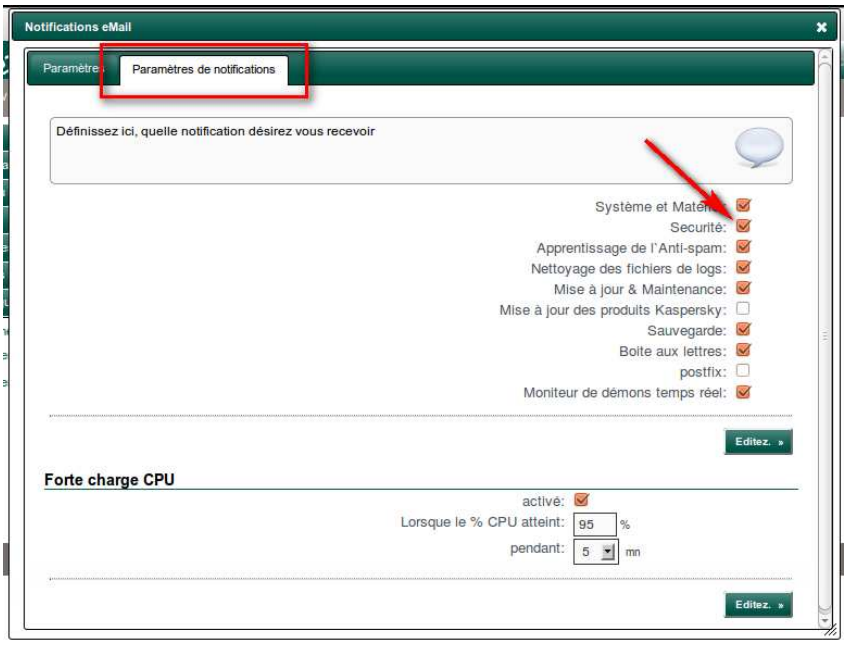
Pour être notifié par email des tentatives d'accès :

Cliquez sur le menu du haut « **Paramètres globaux** »

Sélectionnez l'icône « **Notifications eMail** »

Cliquez sur l'onglet « **Paramètres de notifications** »

Cochez la case « **Sécurité** »



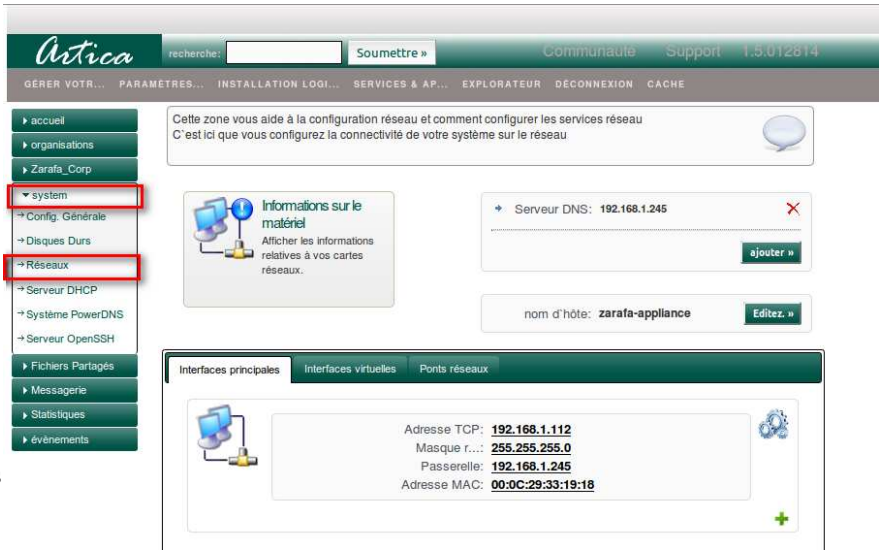
Gestion et Administration des paramètres réseaux

Artica permet aux administrateurs de pouvoir modifier les paramètres réseaux du serveur.
L'administrateur qui souhaite modifier les réseaux doit avoir comme privilège « Administrateur Système »

On admet 3 paramètres fondamentaux pouvant être administrés :

- Le nom d'hôte
- L'adressage TCP/IP
- Les routes réseaux

Ces 2 paramètres se trouvent dans le menu de gauche dans « **System** »/ « **Réseaux** »



L'écran est composé de deux parties distincts

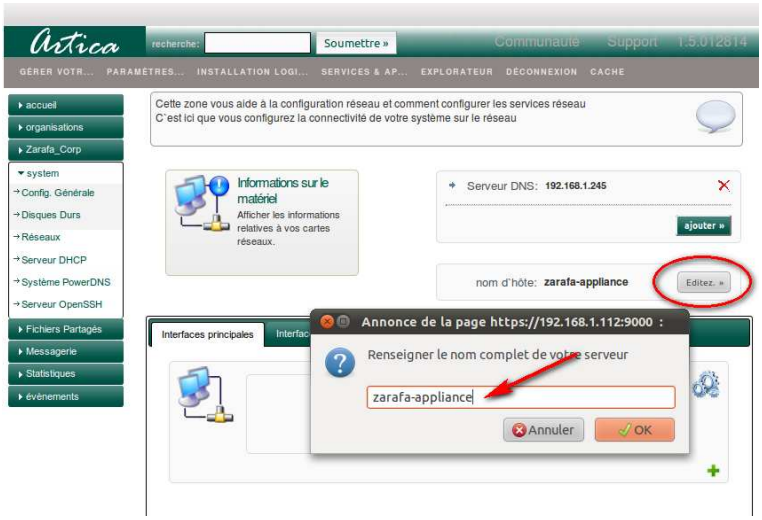
La première partie concerne les paramètres réseaux généraux tels que le nom de l'ordinateur et les serveurs DNS utilisés par l'ensemble des cartes réseaux.

La deuxième section vous liste les cartes réseaux physiques disponibles sur votre serveur.

Modifier le nom d'hôte

Le nom d'hôte est le nom de la machine sur laquelle elle va s'identifier. Son nom permet d'identifier la machine plus facilement mais aussi de pouvoir résoudre son adressage à travers les DNS.

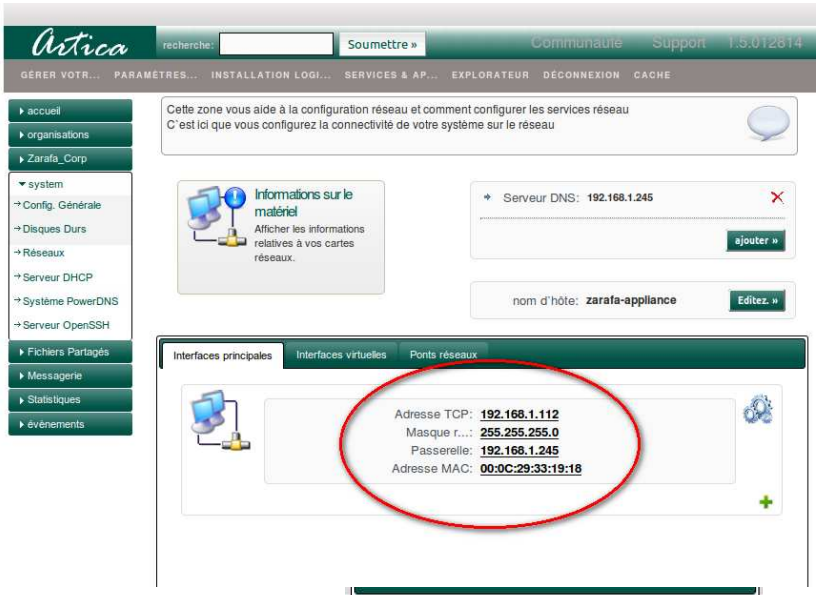
Cliquez sur le bouton « **Editez** » dans la section « nom d'hôte »
Dans la boîte messages, indiquez le nom fqdn du serveur
Le nom fqdn indique le nom de la machine ainsi que le domaine principale comme server.domain.org



Modifier l'adressage TCP/IP du serveur

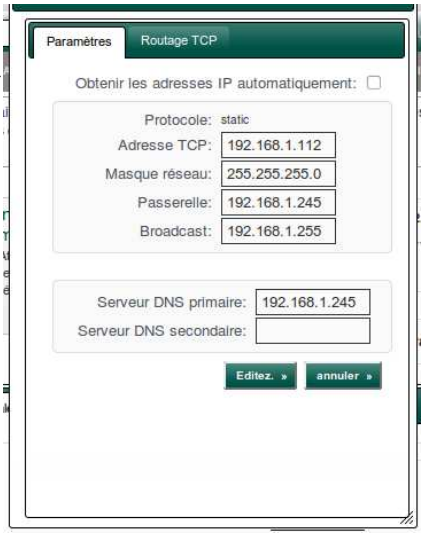
En cliquant sur les liens de la carte réseau, vous entrez dans la section vous permettant de modifier les paramètres de la carte réseau

Certaines cartes ne sont pas modifiables car elle correspondent à des cartes virtuelles (disponibles dans une autre section) ou bien des adressages réseaux applicatifs tels que l'adresse 127.0.0.1 ou les cartes VPN.



Modifier l'adressage réseau

Cliquez sur le bouton « propriétés » afin d'ouvrir le formulaire en mode Édition.



Indiquez l'adressage réseau de la carte (si par exemple le serveur doit utiliser un DHCP ou un adressage fixe).

Indiquez les DNS que doit utiliser le serveur.

Cliquez sur « Editez » pour sauvegarder les informations

Définir un routage avec la carte réseau.

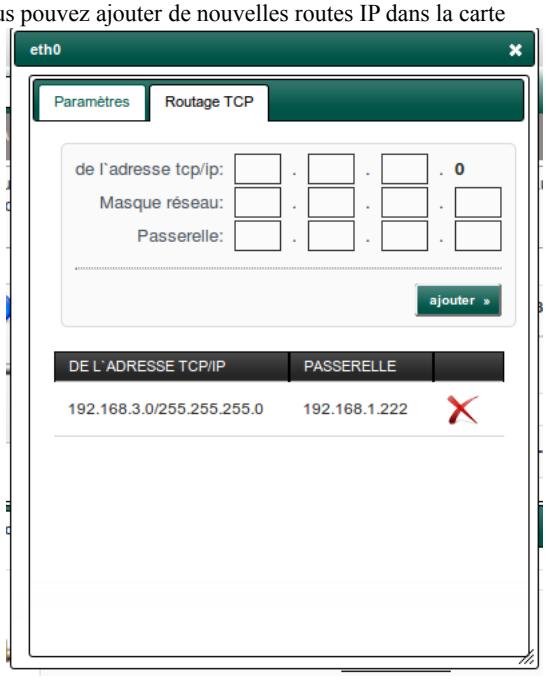
En dehors du routage définit par défaut (celui de l'adresse principale) vous pouvez ajouter de nouvelles routes IP dans la carte

Ces routes seront ajoutées que si et seulement si la carte réseau est bien montée.
Elle sont automatiquement supprimées si les la carte réseau est désactivée.

Cliquez sur l'onglet « **Routage TCP**»

Définissez le routage avec l'adresse IP de départ, le masque de réseau et la passerelle qui sera en charger de transférer les paquets réseaux.

Cliquez sur le bouton « **ajouter** »



Il est possible que la route ne soit pas ajoutée toute de suite sur le serveur.
Dans ce cas, forcer un redémarrage de la machine.

Centraliser les bases de données.

Artica utilise deux moteurs de base de données.
Open LDAP est utilisé pour gérer les utilisateurs et les informations de routage et l'inscription des domaines de messagerie.
MySQL est utilisé pour effectuer les statistiques et stocker des paramètres spécifiques. (Paramétrages IP et multiples-instances par exemple.)
Chaque installation d'Artica utilise ses propres moteurs de base de données en local.

Un trio

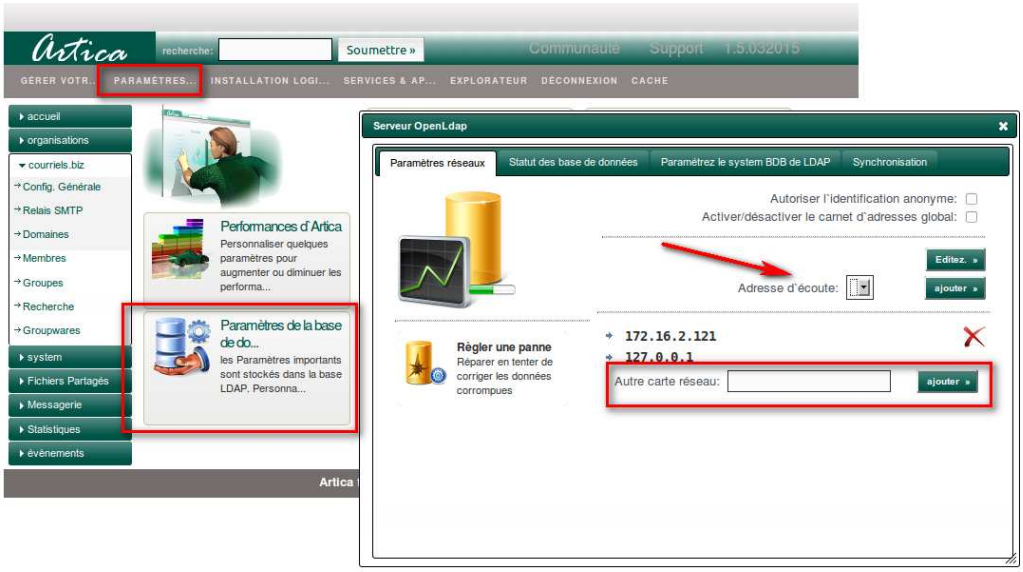
Le cas le plus singulier, et bien souvent rencontré dans la messagerie, est de pouvoir bénéficier d'une centralisation des paramètres lorsque l'on souhaite utiliser une infrastructure redondante.

De plus, le traitement des évènements peut coûter sur les serveurs de production.
Lorsque les serveurs effectuent des requêtes sur Mysql ou LDAP, les serveurs de base de données risquent de surcharger la machine.
Déporter la puissance de calcul des bases de données limite la charge car elle sera déportée sur un serveur dédié à cet effet.

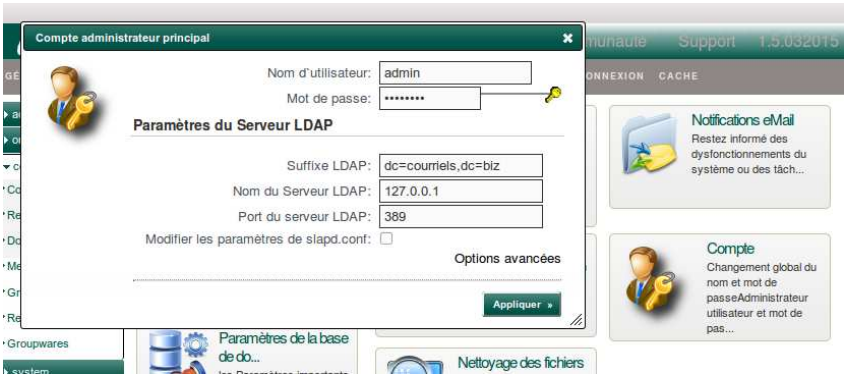
Le moteur Open LDAP

Sur le serveur qui sera considéré comme « serveur de base de données », il faut débrailler le fait qu'il n'écoute que son interface locale (127.0.0.1).

Dans le menu « Paramètres » puis « Paramètres de la base de donnée Open LDAP » onglet « Paramètres réseaux », sélectionnez dans le champs « Addresse d'écoute » l'adresse IP sur laquelle vous désirez que le serveur Open LDAP écoute en plus de la 127.0.0.1.
Si l'adresse n'existe pas dans la liste déroulante, utilisez le champs « Autre carte réseau » et tapez l'adresse IP.



Cliquez sur l'image « **Compte** »



Récupérez les informations

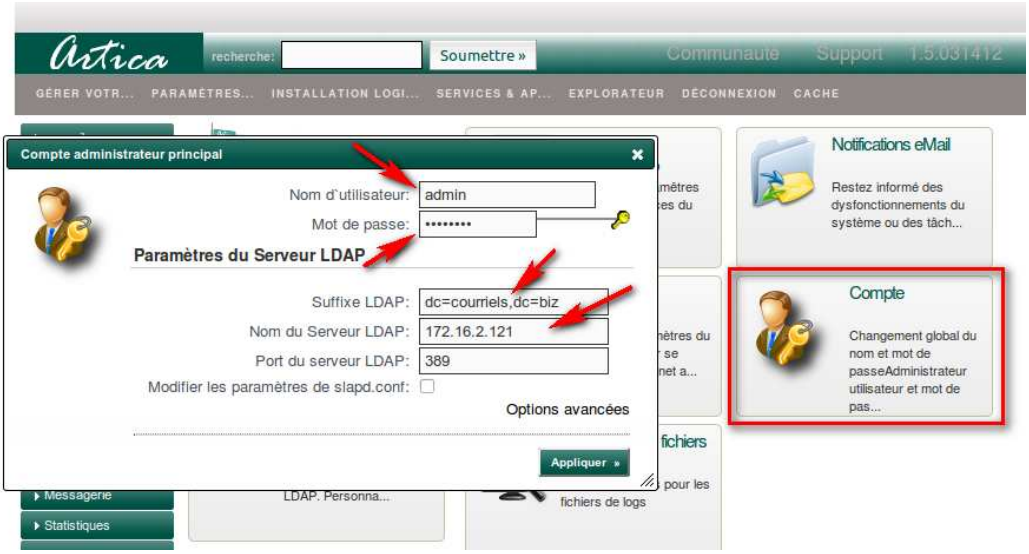
- Nom d'utilisateur
- Mot de passe
- Suffixe LDAP

Vous allez devoir les reproduire sur les serveurs Artica qui vont devoir utiliser ce serveur comme base centrale.

Sur le ou les serveurs « utilisateurs » dans la section compte, reproduisez respectivement les paramètres du serveur centralisateur des bases de données.

Indiquez au lieu de la 127.0.0.1, l'adresse du serveur de base de données que vous avez précédemment ajouté dans son interface.

Reproduisez cette méthode sur l'ensemble des serveurs que vous désirez centraliser.

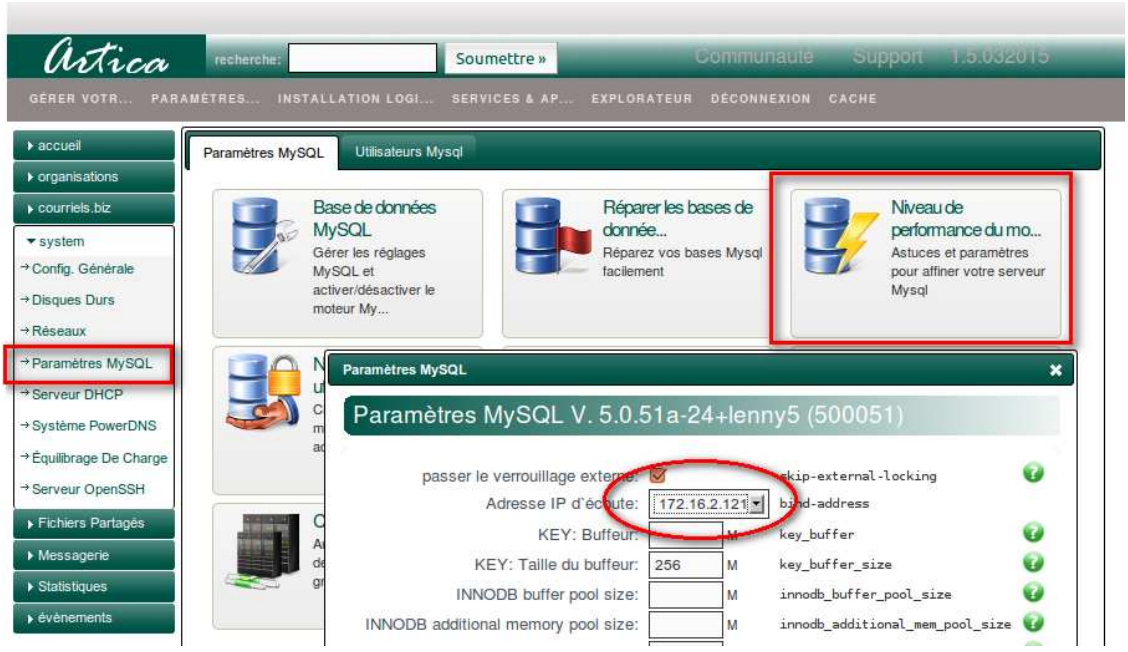


Le Moteur Mysql

Sur le serveur qui sera considéré comme « serveur de base de données », il faut débrailler le fait qu'il n'écoute que son interface locale (127.0.0.1).

Dans le menu de gauche, cliquez sur « System » Puis « Paramètres MysSQL ». Sélectionnez l'image « Niveau de performances du Moteur ».

Dans la liste déroulante du champs « Adresse IP d'écoute », indiquez l'adresse IP locale du serveur.



Comptes utilisateurs distants.

Cliquez sur l'onglet « Utilisateurs Mysql » puis cliquez sur l'image « Ajouter un utilisateur »

Mysql authentifie les utilisateurs distants par un triplet de 3 paramètres :

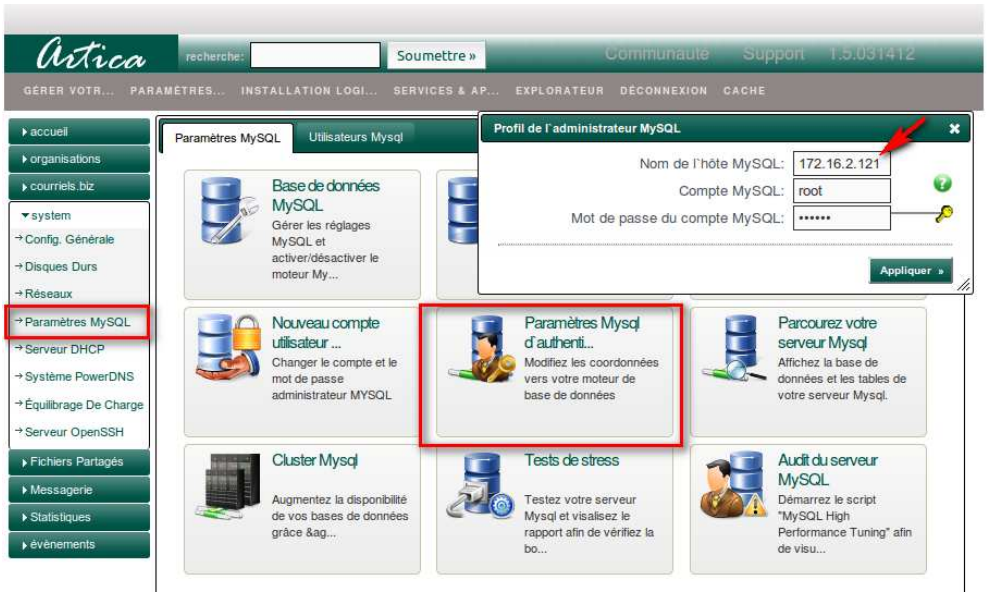
- Le nom d'hôte et/ou l'adresse IP du client.
- Le compte utilisateur
- Le mot de passe de l'utilisateur.

Il faudra alors soit ajouter les noms d'hôtes et/ou les adresses IP des serveurs qui seront autorisés à s'adresser au serveur de base de données, soit utiliser le caractère jocker « * » afin de préciser plusieurs serveurs.
Ainsi on peut ajouter simplement le joker qui indiquera « tous serveurs » soit une partie du nom du serveur comme **mail*.net**

1. **Préférez le nom d'hôte comme paramètre réseau authentification par exemple « server1.domain.tld » comme nom de serveur.**
2. **Indiquez des « comptes différents » si vous souhaitez créer un triplet par serveur client.**

Une fois ces opérations effectuée, placez-vous sur le serveur Artica client du centralisateur de bases de données.

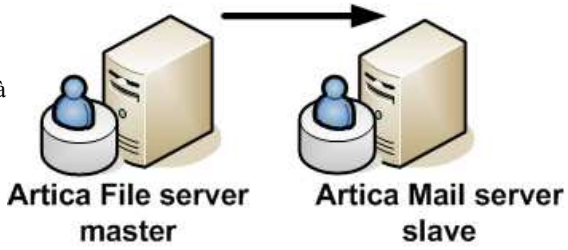
Au même endroit, sélectionnez l'image Paramètres Mysql d'authentification.
Indiquez l'adresse IP du serveur centralisateur des bases de données et les paramètres d'authentification précédemment ajoutées.



Répliquer la base LDAP.

Principalement les comptes utilisateurs sont stockés dans la base de données LDAP.
Cette initiative permet de bénéficier du principe de réplication natif à Open LDAP.

Ansi, la création d'un utilisateur sur un Artica positionné en tant que serveur de fichiers peut automatiquement se retrouver sur le serveur de messagerie.



Ce principe ne s'applique que si le système que vous avez choisi assure l'installation d'un serveur OpenLDAP avec le mode de réplication. Les systèmes Debian et Ubuntu assure ce mode.

Vous aurez très peu de chances de bénéficier de ce mode sur les système RedHat tels que Fedora ou CentOS.

Définition du maître.

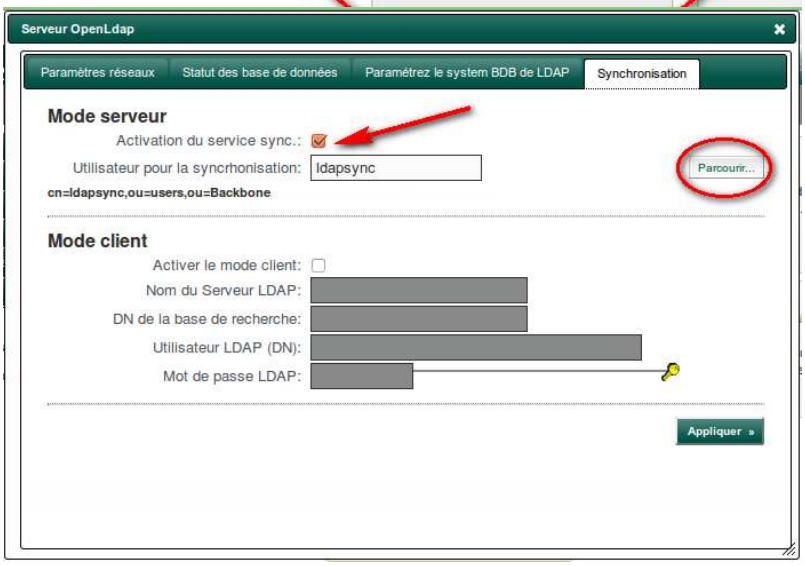
1) **Créez un nouvel utilisateur** dans l'organisation de votre choix .
Il servira d'utilisateur permettant au serveur esclave de se connecter sur le serveur LDAP.

Ouvrez l'interface Artica du serveur maître.

Cliquez sur « **Paramètres** » puis choisissez l'image « **Paramètres de la base de données LDAP** »

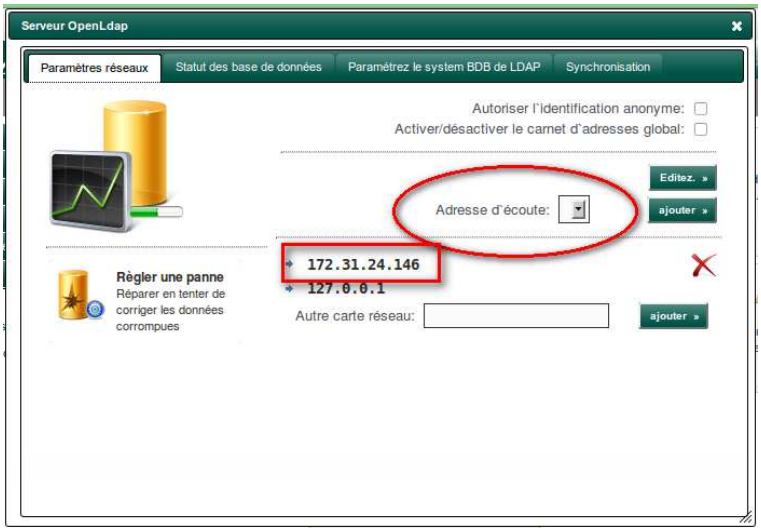
Dans la section « **Mode Serveur** », côchez la case « Activation du service sync »

à l'aide du bouton « **Parcourir** », choisissez l'utilisateur que vous venez de créer, plus cliquez sur « **appliquer** »



Cliquez sur l'onglet « **Paramètres réseaux** »

Par défaut, le serveur LDAP écoute sur l'adresse IP locale 127.0.0.1, vous devez alors ajouter l'adresse IP de la carte réseau afin que le serveur distant puisse ouvrir le port 389 sur ce serveur.



Activation du serveur esclave

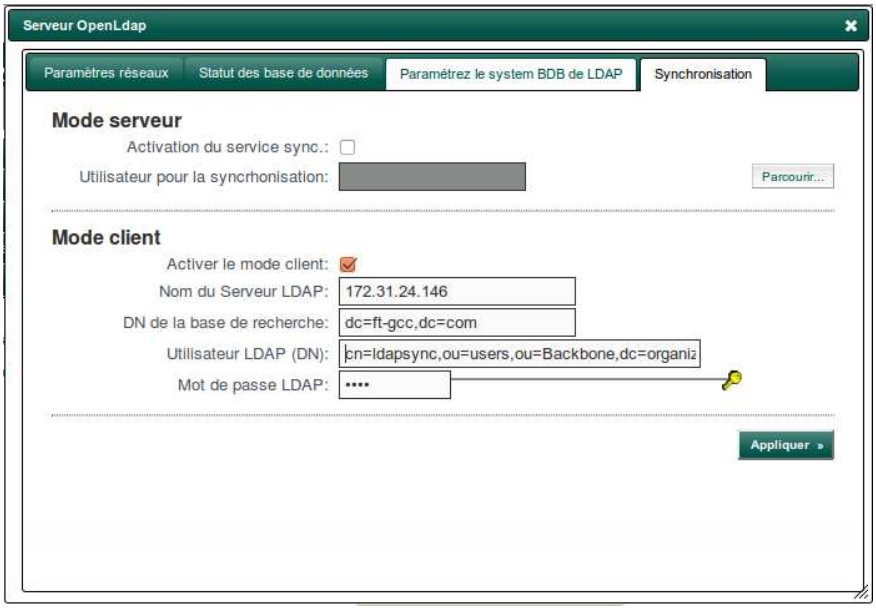
Ouvrez la console Artica sur le serveur qui sera le répliquant

Cette fois-ci, cochez la case « Activer le mode client »

Dans DN de la base de recherche, indiquez le « suffix » du serveur maitre. C'est à dire la branche LDAP principale.

Dans « Utilisateur LDAP (DN) » recopiez exactement le DN (chemin) que l'interface Artica vous affiche dans la section « **Mode Serveur** »

Indiquez le mot de passe de l'utilisateur que vous avez ajouté sur le serveur Maitre.



Artica et le Partage de fichiers

Un contrôleur de domaine ?

Outre le partage de fichiers, Samba permet aux postes de travail de connecter leur système à leur compte géré par le serveur.

Techniquement un contrôleur de domaine est bien souvent nommé PDC (Primary Domain Controller)

Ce principe offre 3 avantages primordiaux :

Gestion de la sécurité utilisateur.

La notion d' « *utilisateur avec pouvoir »*, utilisateur « *Administrateur* », utilisateur « *simple »* n'est plus géré localement par le système mais par la base de données du serveur auxquels sont raccrochés les postes de travail.

Ainsi au lieu d'effectuer les modifications des pouvoirs sur les postes de travail, on effectue ces modifications sur le serveur et par conséquences, au redémarrage de la session, le système applique les nouveaux jetons des privilèges.

Sécurité des données via les profils.

Les « données » de l'utilisateur, c'est à dire les contenus de « Mes documents » et du « Bureau » sont stockés sur le serveur et peuvent être synchronisés si l'utilisateur est mode itinérant.

Si l'utilisateur s'habitue à sauvegarder ses documents dans ces espaces, il s'assure qu'en cas de crash ou de vol de son ordinateur, les données sont déjà conservées sur le serveur.

En se connectant sur un autre ordinateur relié au domaine avec son compte utilisateur, il retrouve automatiquement ses données.

Partage des équipements.

Grâce aux principes précédents, l'ordinateur peut être alors partagé entre plusieurs utilisateurs.

Chaque utilisateur disposant alors de son propre compte et mot de passe, lorsqu'il charge sa session, les données sur le serveur sont alors récupérées.

Ceci permet alors de proposer un ordinateur avec très peu de disque dur puisque l'ensemble des données utilisateur sont stockées dans l'espace de stockage du contrôleur de domaine.

Mise en place avec Artica

Les pré-requis

Outre l'ordre à Samba via Artica de devenir contrôleur de domaine, il faut s'assurer de **4 pré-requis primordiaux** :

1. Le serveur Samba devra **être reconnu par les postes de travail**, c'est à dire qu'à travers l'explorateur de documents de Windows , vous devez visualiser le serveur.
2. **Les comptes utilisateurs doivent être ajoutés** et **activés** en tant que compte « Samba »
   Artica supporte l'installation à la fois d'un serveur de messagerie et de fichiers sur la même machine.
   Les utilisateurs devront disposer du privilège « Samba » afin des les activer en tant **qu'utilisateur d'un système partagé**.
3. **Les ordinateurs, futurs clients du domaine, doivent être précédemment inscrits** dans Artica.
   Seul des ordinateurs explicitement dictées peuvent se connecter au domaine. Il est alors inutile de tenter de raccrocher un ordinateur dans le domaine si le poste n'est pas inscrit.
4. **Le compte « Administrateur du domaine » doit être présent et actif**
   Seul le compte Administrateur du domaine (un équivalent virtuel du compte root) est autorisé à raccrocher un ordinateur au domaine.

Nous allons donc parcourir les pré-requis et enfin vous donner la procédure de raccordement d'un poste Windows XP sur le domaine.

Transformez votre serveur Artica en contrôleur de domaine

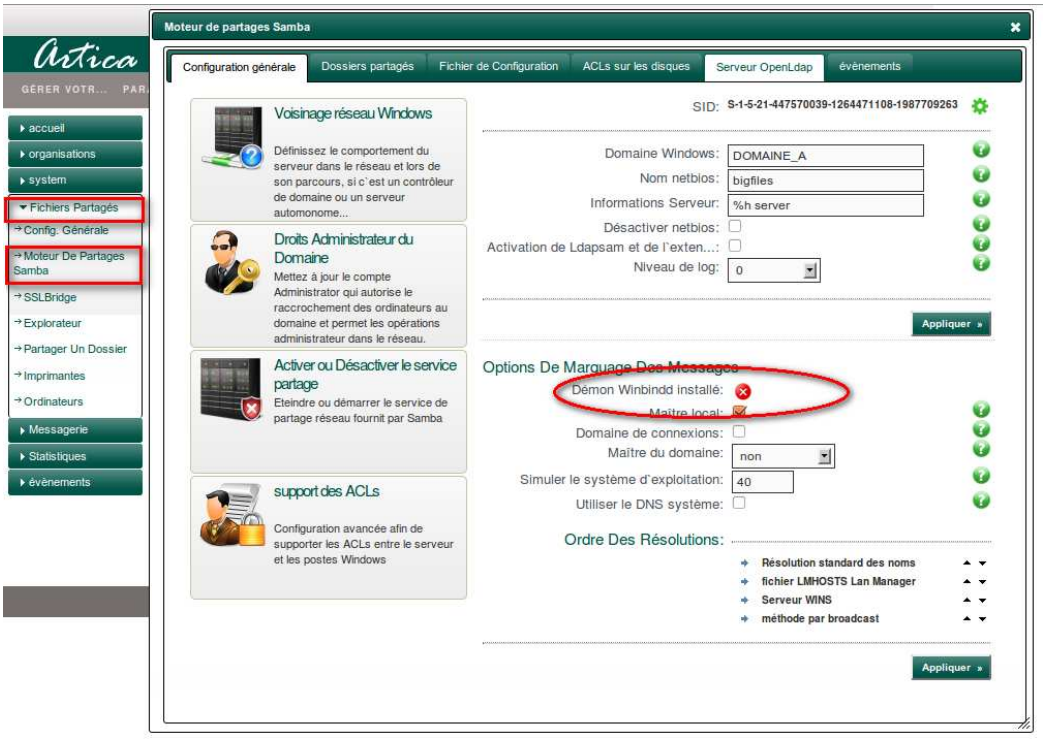
Vérification de la présence de Winbindd

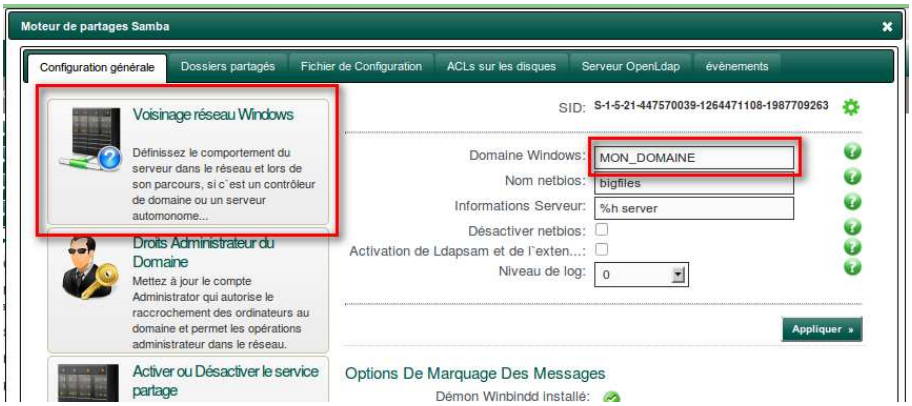
Dans le menu de gauche, choisissez « **Fichiers Partagés** » puis « **Moteur de Partages Samba** »

Si une croix rouge est indiquée dans le champ « **Démon Winbindd installé** » c'est que vous utilisez en ce moment le moteur Samba installé avec votre distribution Linux.

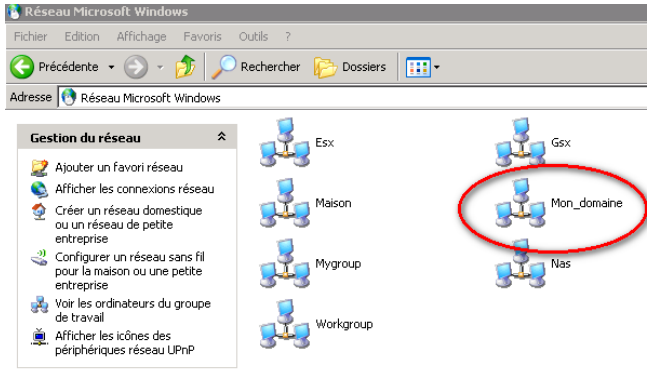
Certaines distributions n'intègrent pas Winbindd il faut alors mettre à jour Samba à travers Artica afin de bénéficier de ce démon.

Utilisez donc l'option « **Installation de Logiciels** » à travers l'interface d'Artica pour mettre à jour votre moteur Samba.





- Retournez dans la section du moteur Samba
- Dans « **Domaine Windows** », indiquez le nom du domaine « Workgroup » que visualiseront les utilisateurs dans le parcours du réseau Microsoft. *(ne mettez pas d'espace ni de caractères accentués ou spéciaux dans le champ)*



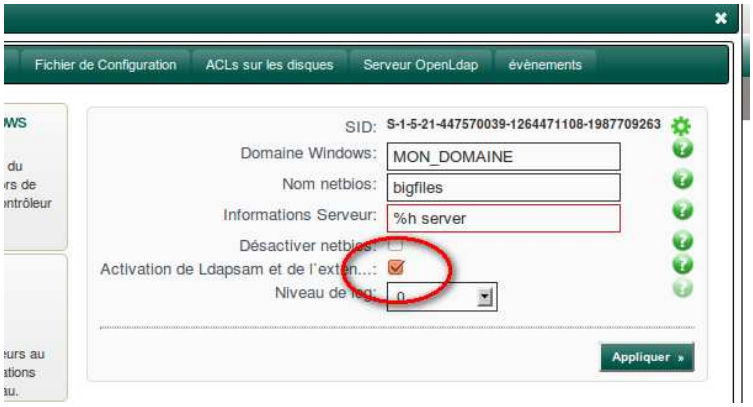
*Ce domaine sera alors le domaine « netbios » principal de votre réseau. Pour cette documentation, nous ferons référence au domaine « **MON_DOMAINE** »*

Activez le contrôleur de domaine

Cliquez sur l'icône « **Voisinage réseau Windows** »

Tournez le rond en vert au niveau de l'option « **Contrôleur de Domaine Primaire** » puis cliquez sur le bouton « **appliquer** »

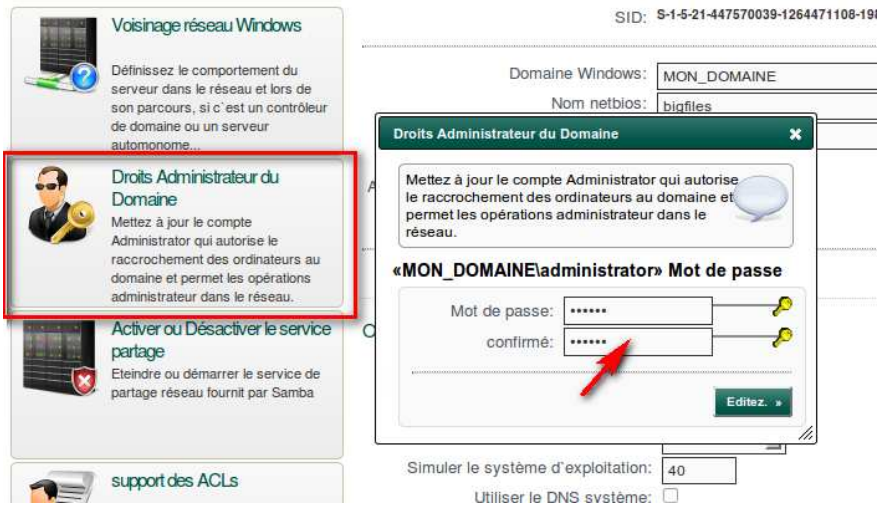
Dans la section principale, activez l'option « **Activation de Ldapsam et de l'extention EditPosix** »



Édition du compte Administrateur (Administrator).

Le compte administrateur va vous servir à raccrocher les systèmes clients au domaine du serveur. Il est nécessaire de le changer

- Cliquez sur l'icône « **Droits Administrateur du Domaine** »
- Modifiez le mot de passe de l'utilisateur « **administrator** »



Lors du raccordement des postes clients au domaine,
vous utiliserez « administrator », pas « administrateur »

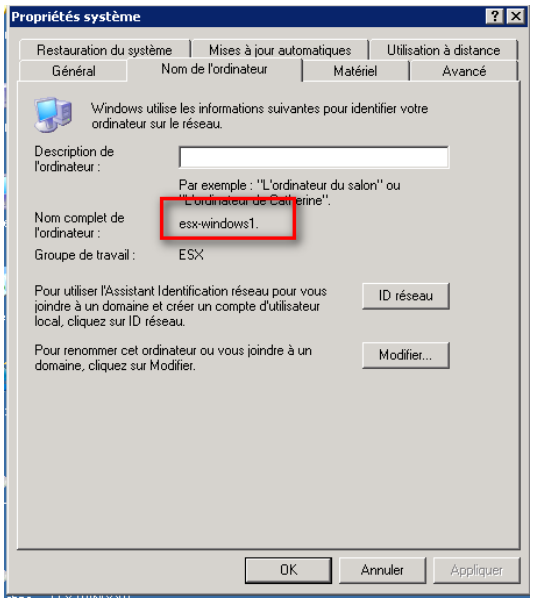
Ajout des postes de travail dans la base de données Artica

Pour pouvoir raccorder un poste de travail, il faut que celui-ci soit connu du serveur. Vous devez par conséquence rajouter les ordinateurs clients dans la base Artica.

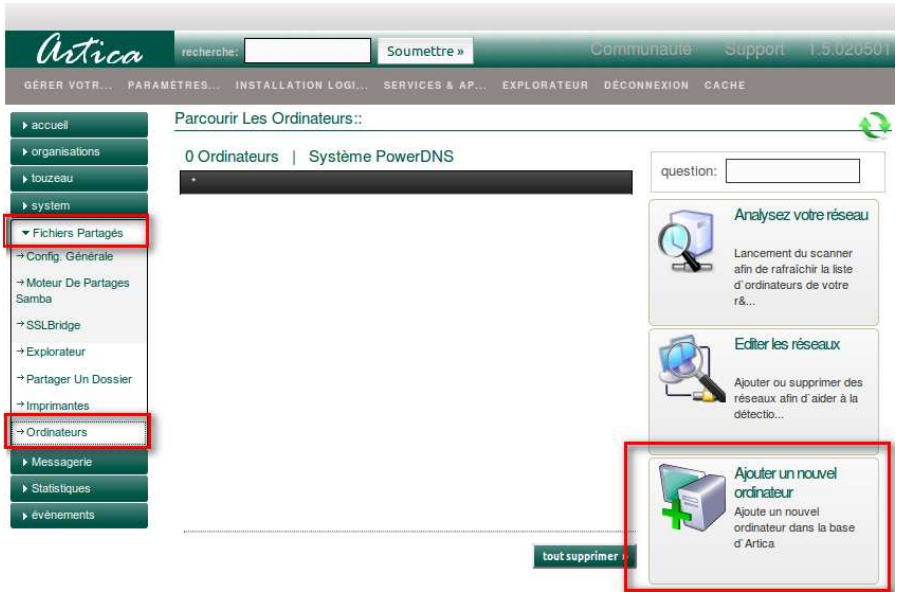
Récupérez le nom netbios du poste de travail dans l'environnement Windows.

On retrouve cette information par les propriétés du « Poste de travail » sous Microsoft Windows XP.

Dans l'exemple de cette documentation nous souhaitons raccrocher « esx-windows-1 » au domaine « MON_DOMAINE »



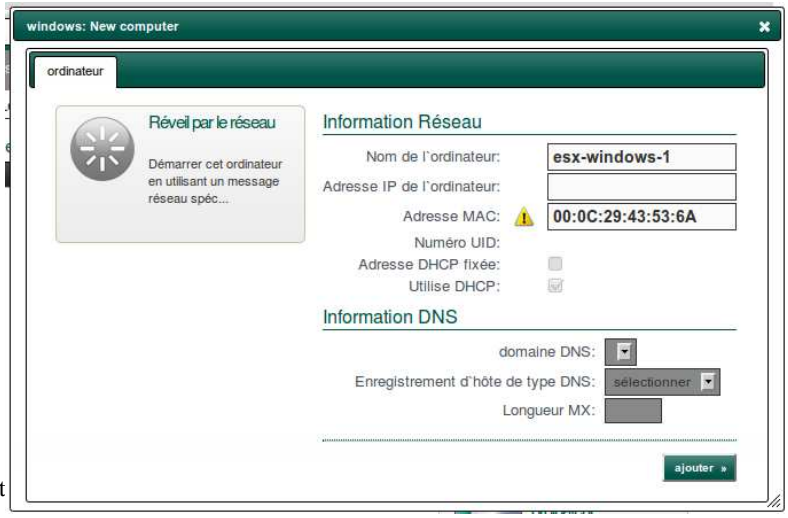
- Dans le menu de gauche, sélectionnez « **Fichiers Partagés** » puis « **Ordinateurs** »
- Cliquez sur l'icône « **Ajouter un nouvel ordinateur** »



Deux informations importantes doivent être ajoutées :

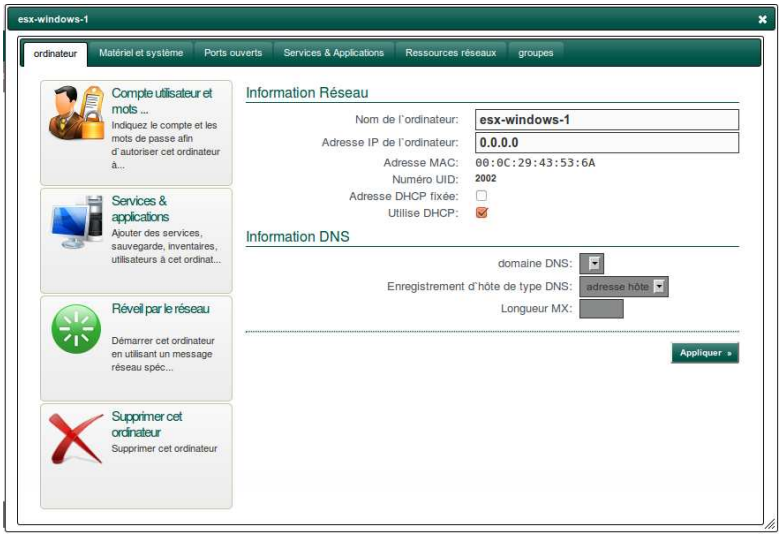
Le « **Nom de l'ordinateur** », identique à celui que vous allez trouver dans les propriétés Windows.

« **L'adresse MAC** » de l'ordinateur que vous allez retrouver avec la commande **`ipconfig /all`** sur le Windows client.



L'adresse MAC n'est pas principalement utilisée par le moteur Samba, mais elle permet à Artica de définir cet ordinateur comme un élément unique dans la base de données afin de pouvoir « centraliser » les différents services autour de l'ordinateur tels que la sauvegarde, l'inventaire, le déploiement de logiciels....

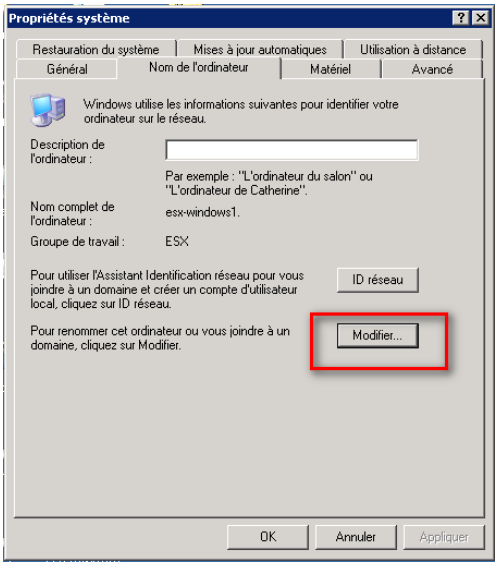
Une fois que l'ordinateur est ajouté dans la base de données, le formulaire vous permet d'accéder à plus d'informations tels que ses ressources réseaux, ses groupes logiques etc.



Raccordement de l'ordinateur au domaine.

1. Le moteur Samba est identifié en tant que contrôleur de domaine.
2. Le compte Administrator à été modifié
3. L'ordinateur est ajouté dans la base.

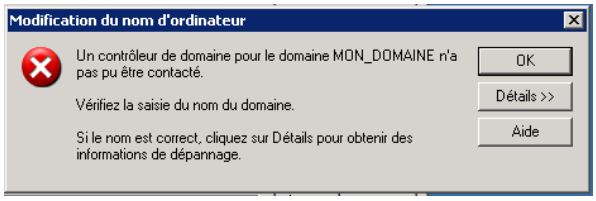
Vous pouvez désormais raccorder l'ordinateur au domaine.

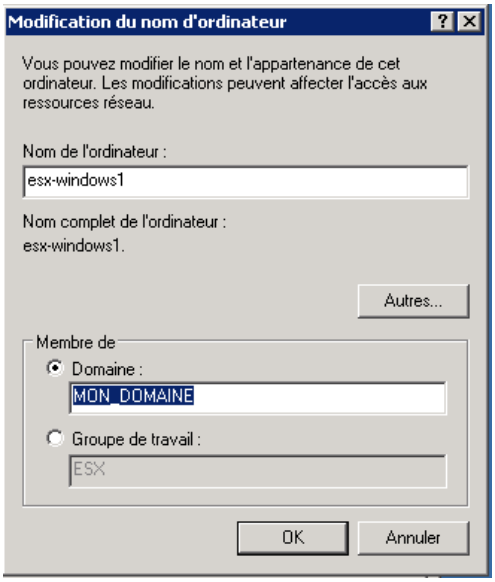


Dans les « **Propriétés système** » de l'ordinateur sur le poste Windows XP,

Sélectionnez l'onglet « **Nom de l'ordinateur** » puis cliquez sur le bouton « **Modifier** »

Dans la section « **Membre de** » , Cochez la case « **Domaine** » puis indiquez le domaine que vous avez spécifié dans les paramètres du moteur Samba.





Si vous avez l'erreur suivante, c'est que vous n'avez pas attendu assez de temps pour que votre serveur s'inscrive sur le réseau.

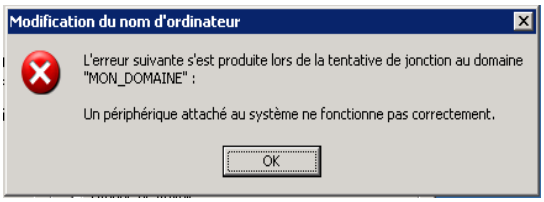
Patientez quelques minutes.

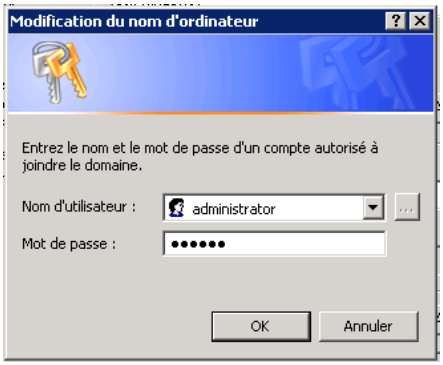
Si elle se reproduit redémarrez les services Samba.

Si le serveur est visible dans le réseau alors un boite message doit s'afficher afin de vous demander le compte Administrateur du domaine

Indiquez le compte « **administrator** » et le mot de passe que vous avez indiqué dans la section « **Droits Administrateur du Domaine** »

Si vous rencontrez des erreurs comme celle-ci





Assurez-vous que vous disposez de la version d'Artica au minimum 1.5.0202200 et de la dernière version du moteur Samba supportée par Artica.

Ouvrez un terminal et lancez la commande suivante :

```
/usr/share/artica-postfix/bin/artica-install --nsswitch --verbose
```

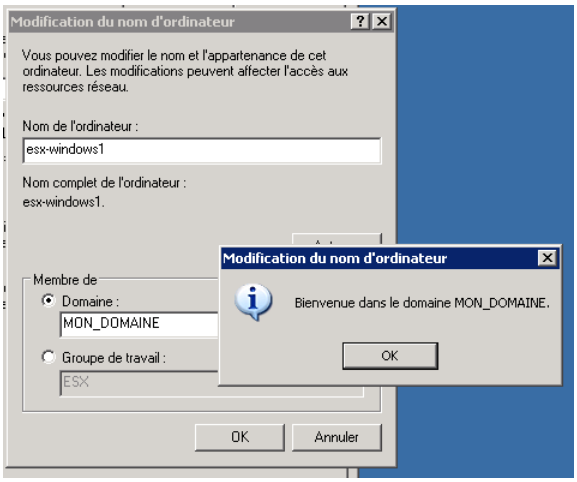
et redémarrez votre serveur.

Si les erreurs continuent, veuillez contacter le support Artica Technology.

Si les procédures on correctement étés établies alors le système client Windows vous indiquera une message de bienvenue.

Toutefois, l'opération n'est pas terminée car seul le compte « Administrateur » est capable d'ouvrir une session.

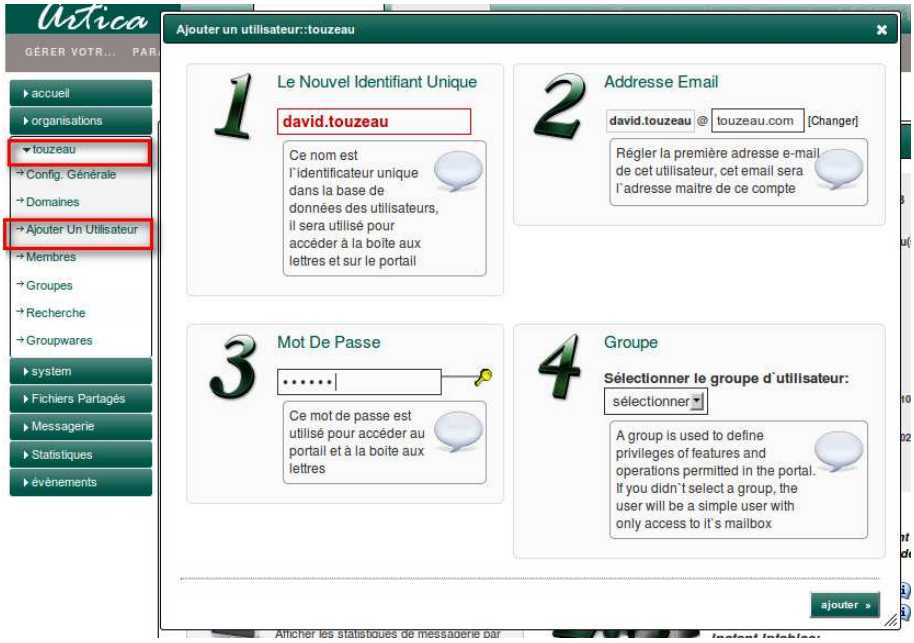
Nous allons voir dans le paragraphe suivant comment ajouter un nouveau compte utilisateur.



Ajoutez un utilisateur et l'inscrire dans le domaine.

Dans le menu de gauche sélectionnez votre organisation et cliquez sur « **Ajouter un Utilisateur** »

Remplissez les champs correspondants et cliquez sur le bouton « **ajouter** »



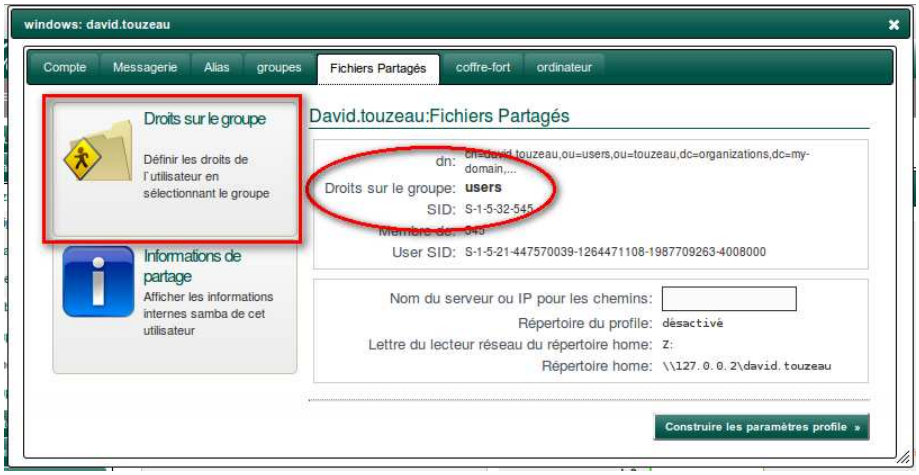
Une fois ajouté, la fenêtre va se transformer en une section spécifique à l'utilisateur.

Remarquez que cette section vous informe que l'utilisateur n'est pas encore activé en tant que membre du domaine

Cliquez sur le bouton « **activer** » afin de l'inscrire dans le moteur de partage de fichiers.

Cliquez sur l'onglet « **Fichiers Partagés** »

Cette section vous permet de visualiser les données des droits de l'utilisateur dans le domaine.

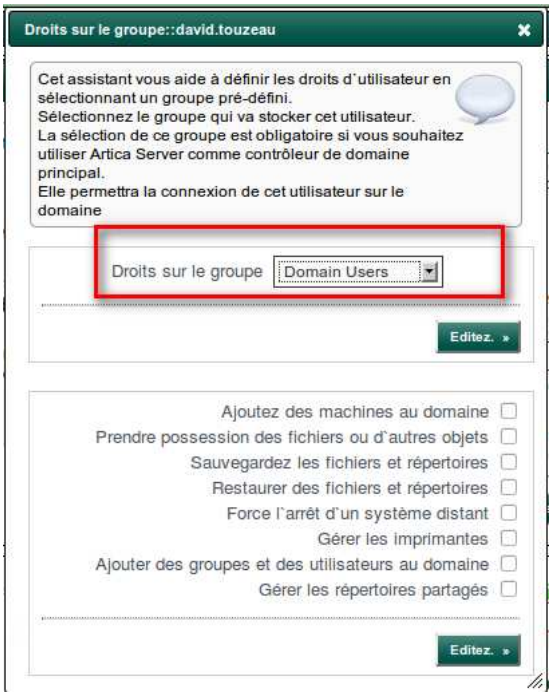


Remarquez que l'utilisateur à les droits provenant du groupe « **users** » plus communément c'est un utilisateur builtin c'est à dire local au serveur et n'appartenant pas au domaine.

Pour le changer de groupe, cliquez sur l'onglet « **Droits sur le groupe** »

Une nouvelle fenêtre s'affiche et une liste déroulante vous permet de modifier le groupe principal de cet utilisateur.

Vous pouvez en faire un Administrateur en choisissant le groupe « **Domain Admins** » voir lui donner encore plus de pouvoirs en cochant les cases correspondantes en dessous de la liste déroulante.

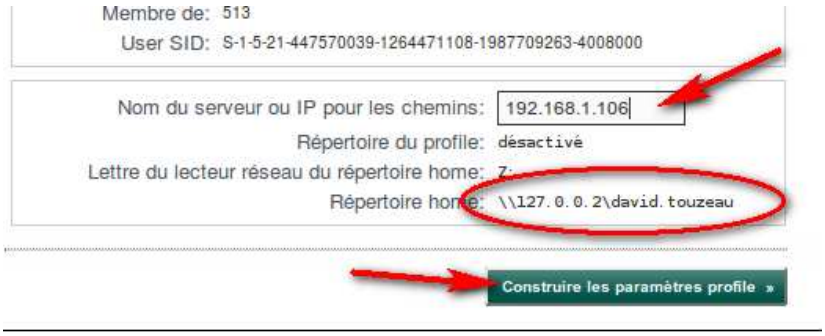


Pour notre exemple, nous lui donnons que les droits utilisateur du domaine avec le groupe « Domain Users ».

Dans la section principale vérifiez le chemin du « **répertoire home** ». Souvent, le serveur n'arrive pas à résoudre l'adresse qu'il devra utiliser en tant que contrôleur de domaine.

Si cela ne correspond pas, utilisez le champ « **Nom du serveur ou IP pour les chemins »** et indiquez l'adresse IP du serveur (ou son nom si le serveur peut être résolu.) et cliquez sur « **construire les paramètres profil** »

dans notre exemple, nous rencontrons ce cas de figure :



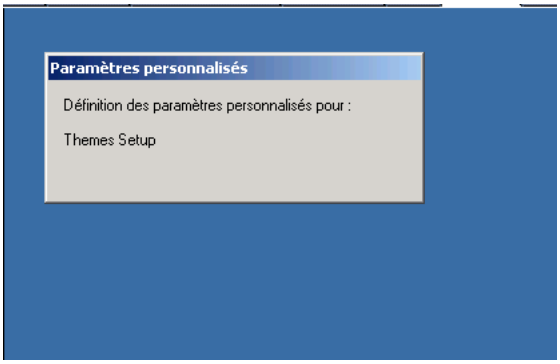
Vérification de la session

Une fois l'utilisateur ajouté et paramétré, il ne vous reste plus qu'à redémarrer le client Windows

Lorsque la boite de connexion s'affiche, cliquez sur le bouton « **Options** », sélectionnez le domaine dans la liste déroulante « **Se connecter à** »

Indiquez le nom de l'utilisateur que vous avez ajouté et son mot passe puis cliquez sur «**OK**»

Le système Windows devrait autoriser la session et construire les premiers paramètres pour cet utilisateur.



Activez les profils itinérants

Pour l'instant l'utilisateur peut se connecter sur le domaine et parcourir le serveur puisqu'il en fait partie.

Mais ses données personnelles sont encore stockées sur le poste de travail.

Vous pouvez en rester la, toutefois nous allons continuer et activer la notion de profil.

Avec le menu de gauche, sélectionnez, « **Fichiers Partagés** » puis « **config générale** »

Cliquez sur l'onglet « **Partage réseau Windows** » puis sur l'icône « **Profils itinérants** »

Transformez le rond rouge en vert puis cliquez sur « **appliquer** »

Le serveur va activer la notion de profil et va instruire les postes de travail à sauvegarder leur environnement et données utilisateur sur le serveur.

Revenez dans la section « **Fichiers Partagés** » de l'utilisateur et assurez-vous que le « **répertoire du profil** »

correspond bien au nom ou à l'adresse IP du serveur.

Si cela ne correspond pas, utilisez le champ « **Nom du serveur ou IP pour les chemins** » et indiquez l'adresse IP du serveur (ou son nom si le serveur peut être résolu.) et cliquez sur « **construire les paramètres profil** »

(cette opération ne s'effectue qu'une seule fois, en effet, les prochains utilisateurs disposeront de la bonne adresse)

Déconnectez votre utilisateur et reconnectez votre utilisateur sur son poste.

Vous ne verrez pas grand chose sauf que les données stockées dans les répertoires suivants :

- Application Data
- Bureau
- Cookies
- Favoris
- IETldCache
- Menu Démarrer
- Mes documents
- Modèles
- Recent
- SendTo
- Voisinage d'impression
- Voisinage réseau

Sont synchronisés entre le serveur et le poste de travail à travers la session Windows.

Pour s'assurer que la fonctionnalité fonctionne si vous avez les capacités de connecter un terminal sur le serveur vous pourrez lister ces répertoires dans le dossier

```
/home/export/profile/[user]
```

Si vous vous connectez avec le compte utilisateur sur un autre poste de travail connecté au domaine, vous verrez que sa session Windows à récupéré l'ensemble de ces répertoires et aussi son environnement.

La Déduplication ?

La déduplication est une technique qui consiste à identifier, dans les fichiers, des redondances permettant la « factorisation » et la conservation « unique » d'un élément.

Cette technique se situe au niveau système de fichiers et des blocs.

Cela ressemble à de la compression « à la volée » mais de façon plus intelligente.

Pour simplifier : Si sur un disque dur, vous copiez deux fois le même DVD de 4Go, cette opération va vous coûter 8Go sur le disque.

Avec la déduplication, seul 4Go sera alors stocké même si vous visualisez deux fichiers de 4Go !

Cette technologie est toute récente.

Les grands constructeurs comme EMC, HP ou NetApp viennent tout juste de s'y mettre.

> *(partant du principe que cette documentation est écrite en Janvier 2011)*

Voici un extrait du wikipedia qui résume bien la chose :

*En informatique, la **déduplication** (également appelée factorisation ou stockage d'instance unique) est une technique de sauvegarde de données, consistant à factoriser des séquences de données identiques afin d'économiser l'espace utilisé.*

Chaque fichier est découpé en une multitude de tronçons. À chacun de ces tronçons est associé un identifiant unique, ces identifiants étant stockés dans un index. L'objectif de la déduplication est de ne stocker qu'une seule fois un même tronçon. Aussi, une nouvelle occurrence d'un tronçon déjà présent n'est pas à nouveau sauvegardée, mais remplacée par un pointeur vers l'identifiant correspondant.

La déduplication est utilisée en particulier sur des solutions du type VTL (Virtual Tape Library).

Quel est l'intérêt ?

Gain d'espace disque

C'est l'avantage principal de cette technique, aujourd'hui l'espace disque est le coeur du problème.

Cette technique permet alors d'assurer plus d'espace disque que l'on souhaite assurer.

Virtualisation !

Les images virtuelles sont souvent presque identiques et aisément déduplicables.

Une partition système d'une machine virtuelle «dupliquée » vers une autre bénéficie totalement de ce principe.

L'inconvénient

Comme vous l'avez compris, des calculs sont nécessaires afin d'assurer une factorisation d'un flux de données.

La déduplication consomme plus de ressources mémoire et CPU qu'avec l'utilisation « pure » d'un disque dur.

> *Toutefois, comme je le dis souvent les problèmes de mémoire et de CPU ne sont qu'une histoire de dimensionnement et de « budget »*

> *Retrouvez un article très intéressant et sérieux à ce sujet sur le blog « Sur le Fil Technologique » disponible à cette adresse.*
> *http://www.synergeek.fr/2010/07/zfs-deduplication-mythe-ou-realite/*
> *« Blog que je remercie tout particulièrement pour la clarté de son article à ce sujet... »*

Mise en place avec Artica

Artica vous permet de mettre en place facilement la déduplication à travers de l'utilisation des modules Fuse, ZFS-Fuse, tokyocabinet et lessFS.
À part Fuse (mais pas en tout dernière version), les autres logiciels ne sont pas encore disponibles sur les principales distributions Linux.

Il faudra alors faire confiance à Artica pour la mise en place du quatuor.

Installation des modules principaux

Avec le menu de gauche, cliquez sur « **System** » puis « **Config Générale** »

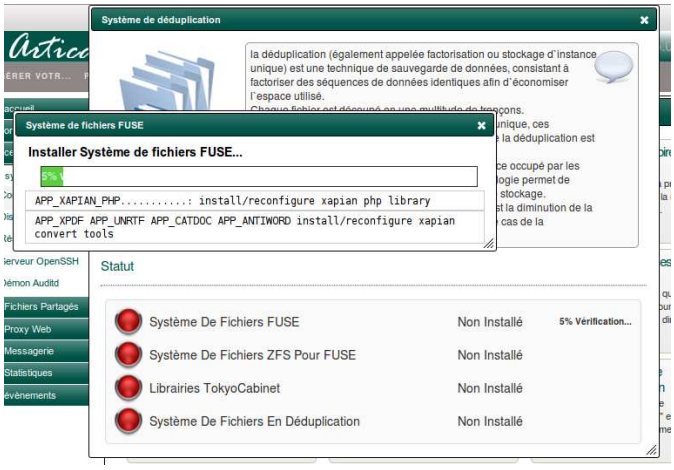
Vous y trouverez un menu nommé « **Système de déduplication** », cliquez dessus.

Dans la logique de la documentation, aucun module n'est encore installé.

Pour ce faire, l'interface va vous proposer d'installer les modules les uns après les autres et dans l'ordre annoncé.

Cliquez sur le bouton « **installer** » à chaque procédure.

A chaque procédure d'installation, Artica vous affichera l'état de l'installation du module et sa progression d'installation.



Une fois qu'un module est installé, l'interface vous propose d'installer le suivant.

Dès que l'ensemble des modules sont installés, l'interface va changer et vous permettra de commencer à paramétrer le système de déduplication.

Premiers pas

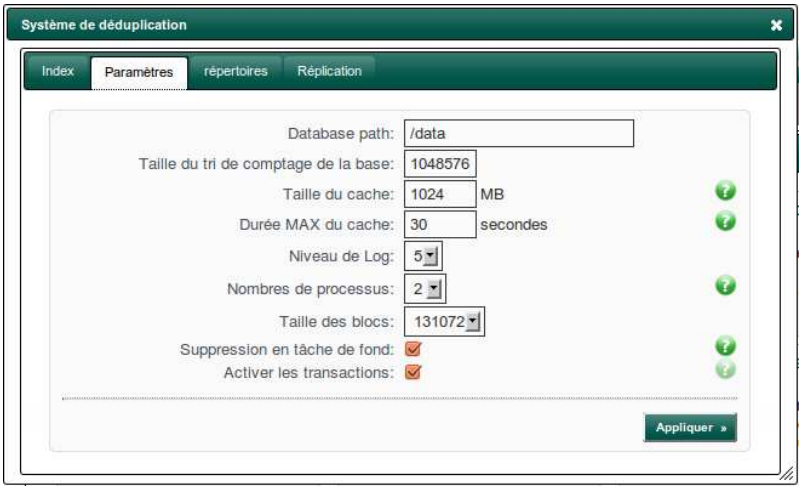
L'interface se compose principalement en 3 parties.

Les « **paramètres** » vous permet de préciser le comportement de la déduplication.

Les « **répertoires** » vous permettent de d'indiquer quel répertoire sera lié à la base de données de déduplication.

« **Réplication** » vous permet de créer un combinaison Maître/Esclave. Une sorte de cluster actif/actif (que dans un sens). Vous assurant une sauvegarde en temps réel du système maitre dédupliqué.

Les paramètres du moteur.



Principalement le paramètre le plus important est celui du **chemin de la base de données**.

En effet, lorsque vous allez placer un document dans un répertoire «lié» en déduplication, vous ne visualiserez qu'une « image » de ce fichier.

Le vrai contenu de ce fichier sera stocké dans le répertoire de la base de données.

Cela veut dire que vous devez identifier la taille de vos disques et indiquer un répertoire stocké sur un disque qui dispose de suffisamment d'espace.

La taille du tri de comptage de la base :

Même si cela semble technique, comprenez que c'est le nombre d'éléments (fichiers, répertoires) que la base de données peut stocker.

On parlera ici d'une unité en Million !

Le cache

Afin d'assurer une bonne performance de lecture et écriture, des données sont stockées en mémoire (**taille du cache**) puis au bout d'un délai, sont écrites sur le disque dur (**Durée MAX**)

Les répertoires

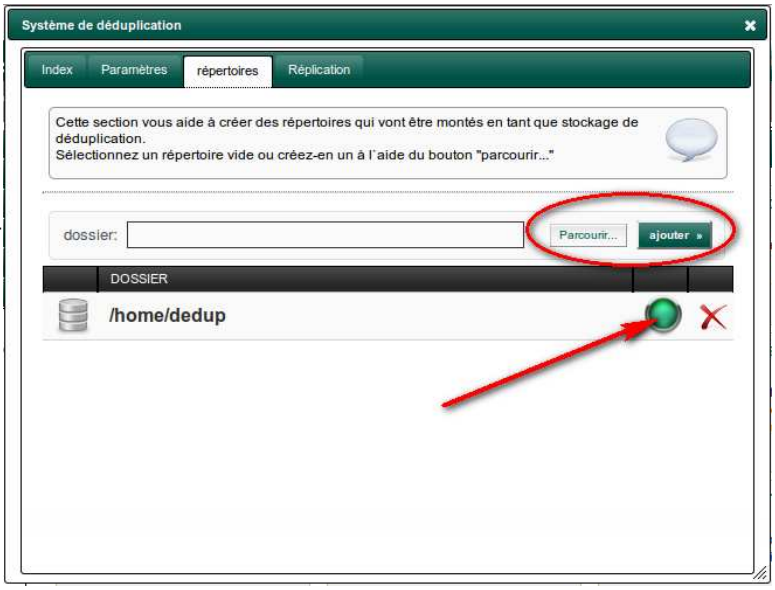
Cette section vous permet d'ajouter les répertoires qui seront liés à la déduplication.

Attention ! Vous ne pouvez pas choisir des répertoires qui stockent déjà des données !

Créez un répertoire, indiquez son chemin et rajouter-le.

Un bouton vert ou rouge vous permettra de voir si le répertoire est actif et est lié à la déduplication.

*« **supprimer le répertoire** » avec la croix rouge supprime uniquement le lien entre le système et la base de données.*
Les données sont toujours présentes et conservées.



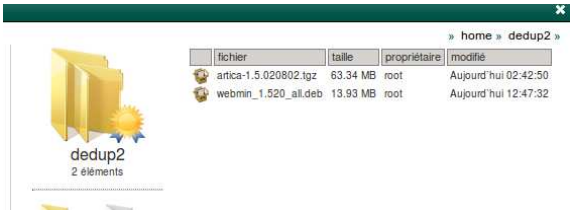
Utilisation de l'explorateur.

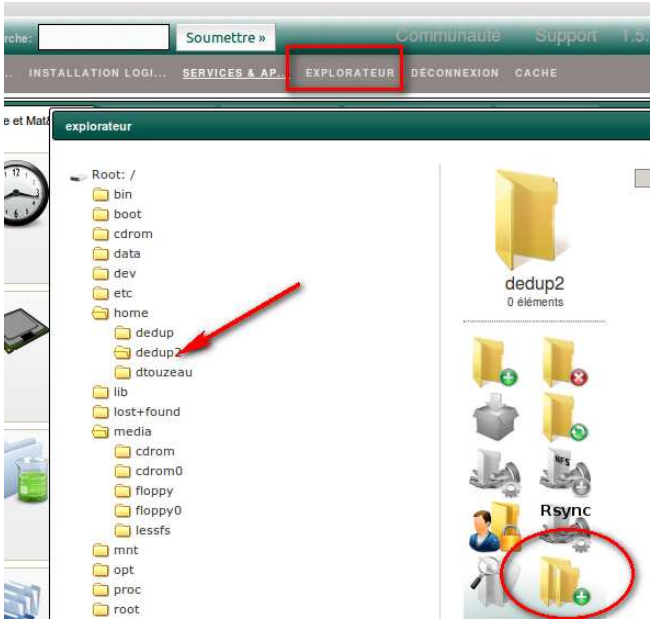
L'onglet répertoire vous permet de rajouter le répertoire à lier à la dédupliquation

Vous pouvez le faire aussi à travers l'explorateur.

Cliquez sur le lien « **EXPLORATEUR** » en haut, parcourez l'arborescence.

Si le répertoire peut être lié à la base de données de déduplication, un icône représentant deux répertoires s'affichera et vous permettra en cliquant dessus de le lier.





L'icône principale du répertoire sera modifié afin que vous puissiez identifier ce répertoire en tant que « liaison » à la déduplication.

La réplication

La réplication consiste à recopier en temps réel les échanges de données d'un serveur maître (le frontal aux utilisateurs) vers un esclave qui servira de sauvegarde.

Le répertoire du serveur esclave quand à lui sera en « lecture seule »

Il vous faudra par conséquent deux serveurs Artica l'un en maître, l'autre en esclave.

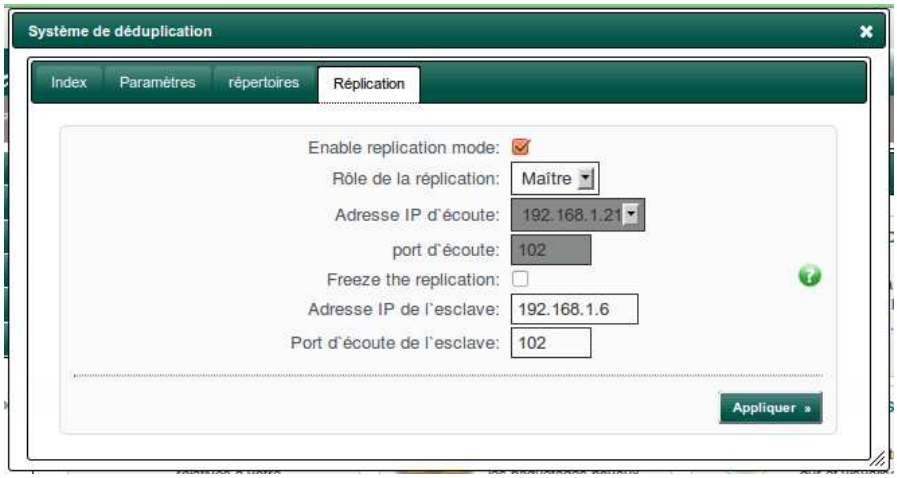
> *Bien que si vous avez les compétences techniques nécessaires, le serveur esclave peut être paramétré en ligne de commande, Artica n'utilisant que les principes « standards » de lessfs.*

Le maître

Cliquez sur l'onglet « **réplication** »

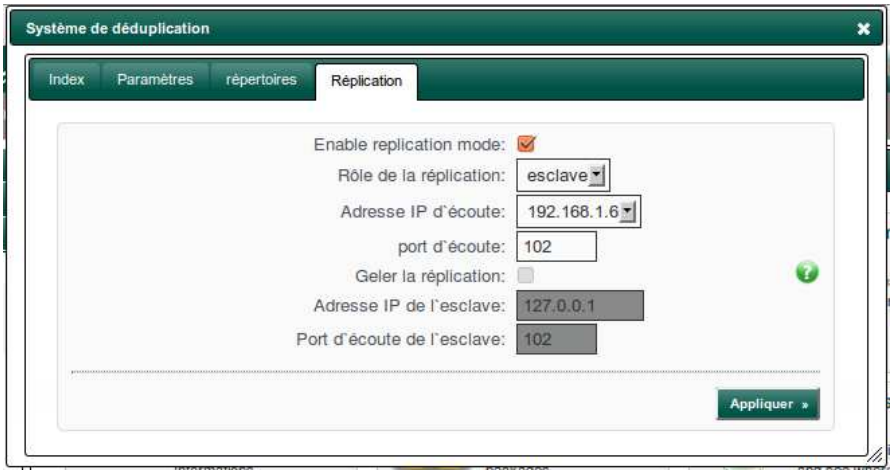
Activez la réplication et sélectionnez « **Maître** » dans le champ « **Rôle de la réplication** »

Indiquez l'adresse IP et le port d'écoute du serveur qui fera office d'esclave.



L'esclave

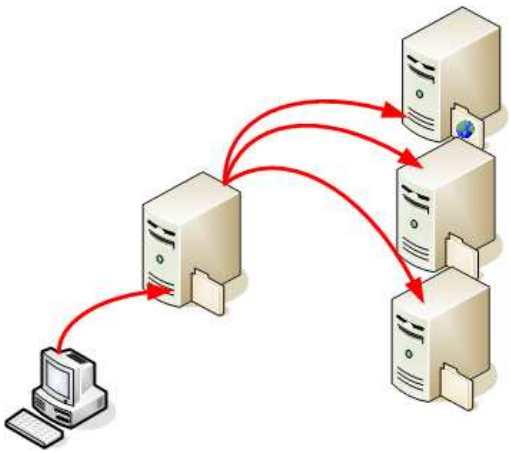
Sur l'esclave, il faut faire simplement l'inverse et indiquer l'adresse IP et le port d'écoute que vous avez spécifié au maître.



Une fois que les services sont redémarrés (bouton redémarrage) dans l'onglet « index », le maître va envoyer ses données à l'esclave et ceci de façon dynamique.

L'ensemble des évènements de la déduplication sont enregistrés dans le gestionnaire de logs central (syslog)

La sauvegarde temps réel avec greyhole



Greyhole est un outil permettant de surveiller les échanges effectués sur les ressources que vous avez partagé.

Il assure la « duplication » des fichiers vers différentes ressources afin d'assurer leur sauvegarde.

Les ressources définies sont alors définies comme un pool de stockage mis en commun.

Principe :

Son principe est simple,

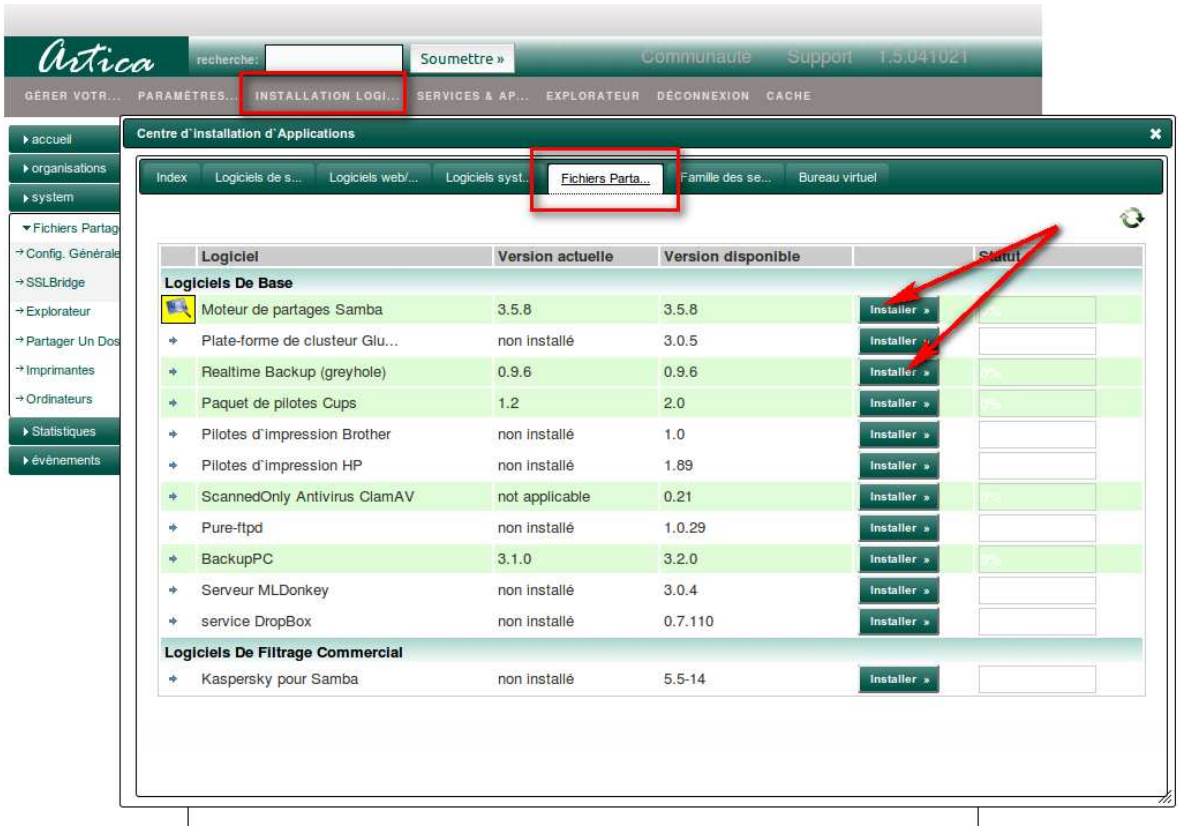
Vous définissez une liste de ressources de stockage disponibles qui vont constituer le « pool » de sauvegarde.

Lorsqu'un utilisateur modifie un fichier sur une ressource partagée, un événement est alors enregistré.

Un processus en tâche de fond est alors en charge de dupliquer ce fichier dans le spool.

Mise en place

Cliquez sur le menu du haut « **INSTALLATION LOGICIELS** » puis choisissez l'onglet « **Fichiers Partagés** ».



Assurez-vous de disposer de la dernière version de Samba (Minimum 3.5.x) en cliquant sur « **Installer** » dans « **Moteur de partages Samba** »

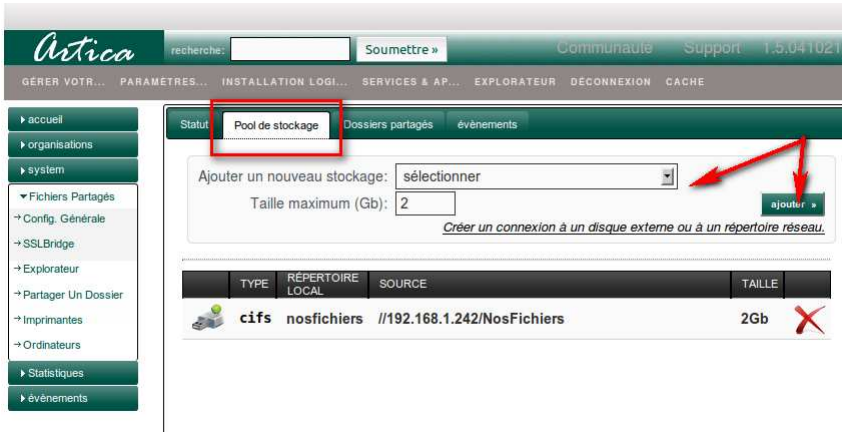
Cliquez sur « **Installer** » dans « **Realtime Backup (greyhole)** »

Ajout des ressources de sauvegarde

Une fois Greyhole installé, cliquez dans le menu de gauche sur « Fichiers Partagés » puis « Config. Générale »

Cliquez sur l'image « **Realtime Backup (greyhole)** »

Sélectionnez l'onglet « **Pool de stockage** »



Une liste déroulante vous permet de choisir les ressources auto-connectées que vous avez ajouté précédemment.

Si vous n'avez pas ajouté des ressources auto-connectée, lisez le paragraphe « **Gestion automatique des points de montage** » (page 145) dans ce document.

La « **Taille maximum** » correspond à la limite de la sauvegarde que vous consentez à cette ressource.

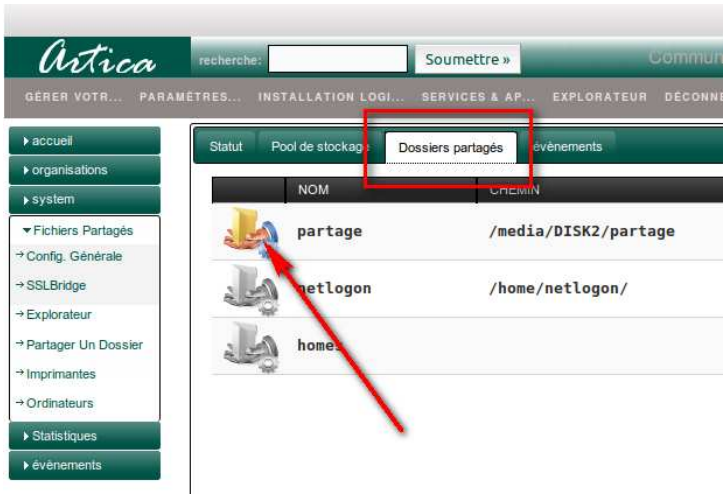
Au delà de cette taille, le système de sauvegarde recherchera une nouvelle ressource libre à utiliser.

Le nombre de ressources est illimité...

Affectation des sauvegardes aux partages

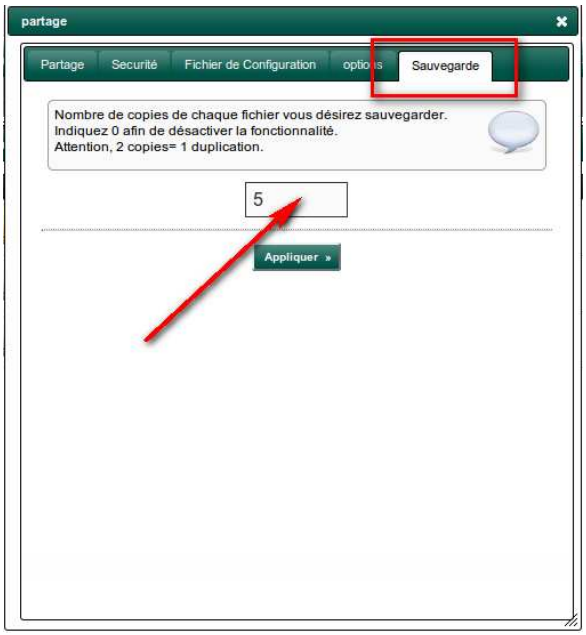
Cliquez sur l'onglet, « Dossiers partagés »

Vous y trouverez un tableau avec tous les dossiers que vous avez précédemment partagé.



Cliquez sur l'un des partages.

Indiquez dans le champs, le nombre de copies de chaque fichier vous désirez sauvegarder. Indiquez 0 afin de désactiver la fonctionnalité.
Attention, 2 copies= 1 duplication.



Quotas sur les partitions

Bien que la gestion de quotas est une fonctionnalité intégrée au système, nous plaçons ce thème dans le dossier « partage de fichiers ». En effet, il n'y a que peut d'intérêt à utiliser la gestion de quotas toute seule et sans système de stockage.

La gestion de quotas permet à l'administrateur du serveur de définir des limites de stockage par groupes utilisateurs ou par utilisateurs.

La limite de stockage comprend à la fois le poids total des fichiers stockés pour tel ou tel utilisateur mais aussi du nombre de fichiers. Ainsi on peut permettre à un utilisateur de déposer des milliers de fichiers mais que la somme de ces fichiers ne dépasse pas une taille maximale.

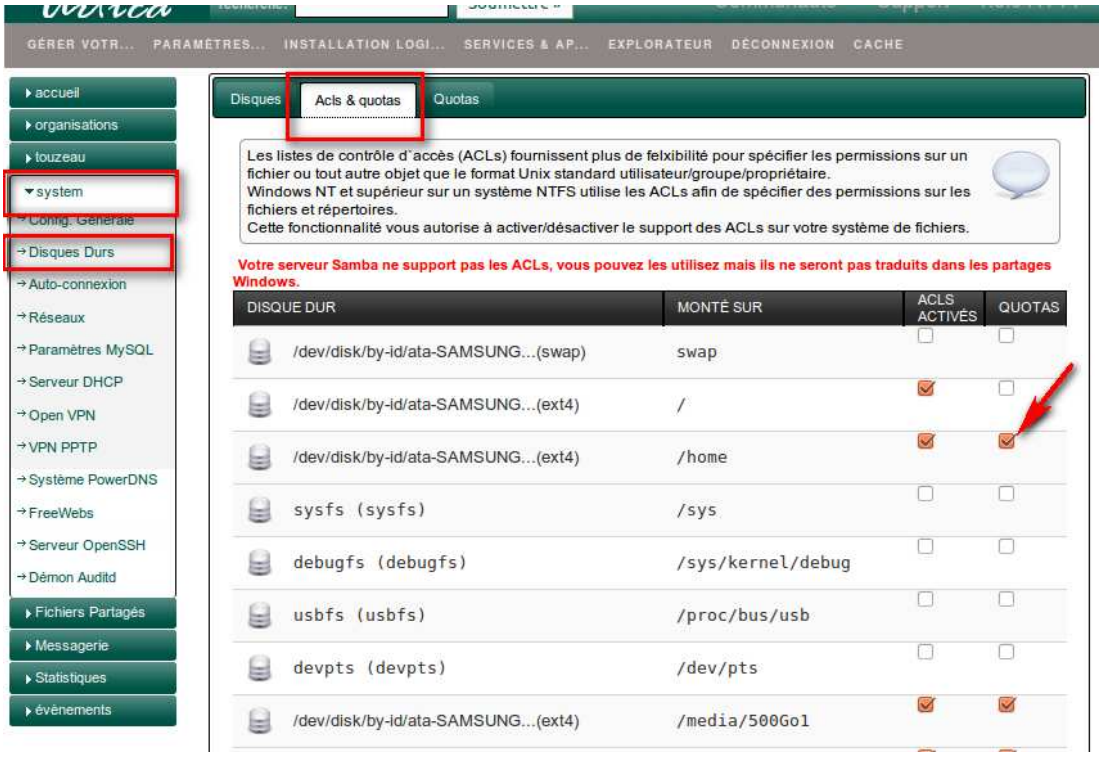
Les quotas s'appliquent par « partition » ne cherchez donc pas à attribuer des quotas par « répertoire », ceci n'étant pas le sujet de cette section.

On va donc trouver l'administration des quotas dans la section **Disques Durs**

> ***Si vous ne visualisez pas la section quota c'est que votre système ne dispose pas du paquetage « quota ».***
> ***effectuez donc ceci :***
> ***apt-get install quota***
> ***yum install quota***
> ***zypper install quota***
> ***urpmi quota***

Activation des quotas dans les partitions.

Dans le menu de gauche, sélectionnez le menu « **System** », puis « **Disques Durs** ».



Cliquez sur l'onglet « **Acls & Quotas** »

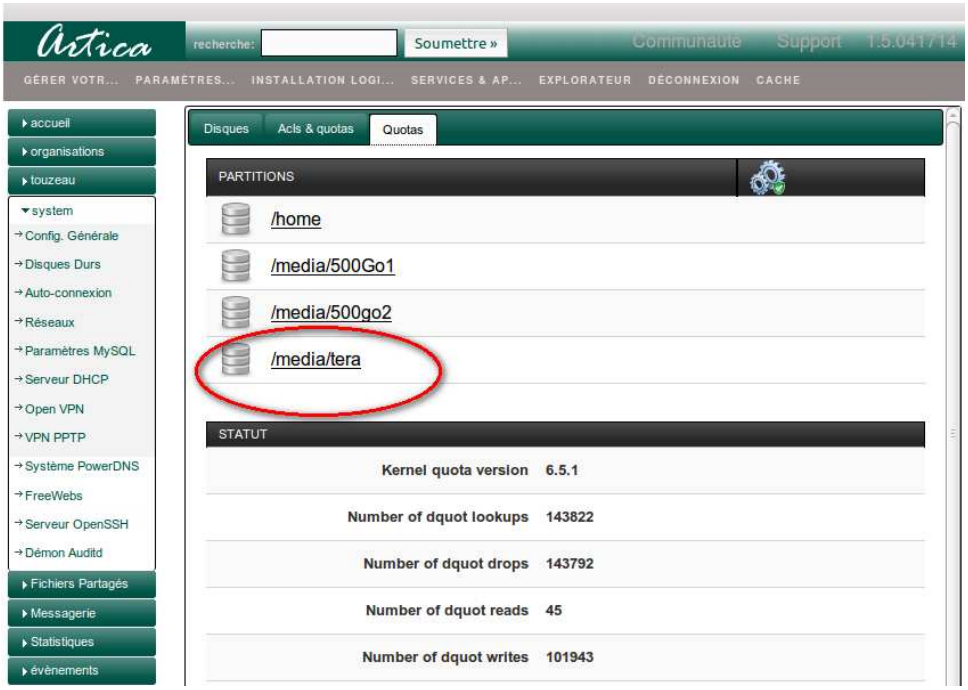
L'interface va vous afficher les partitions ou disques montés sur votre système.

Côchez la case dans la colonne « **Quotas** » sur la partition que vous désirez limiter.

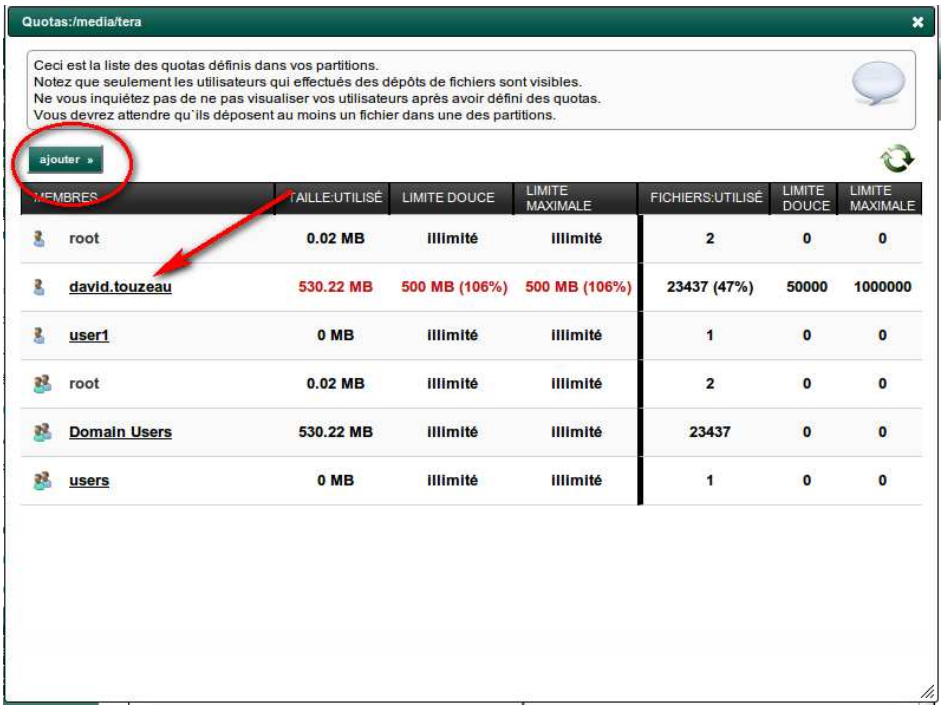
> *Cette opération nécessitera de redémarrer l'ordinateur. Nous vous invitons donc à côcher l'ensemble des partitions désirées et enfin de redémarrer.*

Définition des quotas

- Cliquez sur l'onglet « **Quotas** »
- L'interface va vous lister l'ensemble des partitions activée en surveillance des quotas.
- Cliquez sur l'un d'entre elle.



Un boite message vous affiche un tableau vous permettant de visualiser l'état d'utilisation de votre partition et les quotas appliqués.



Par défaut, et si c'est la première fois que vous avez mis en œuvre les quotas, tous les utilisateurs et groupes disposent d'un quota illimité.

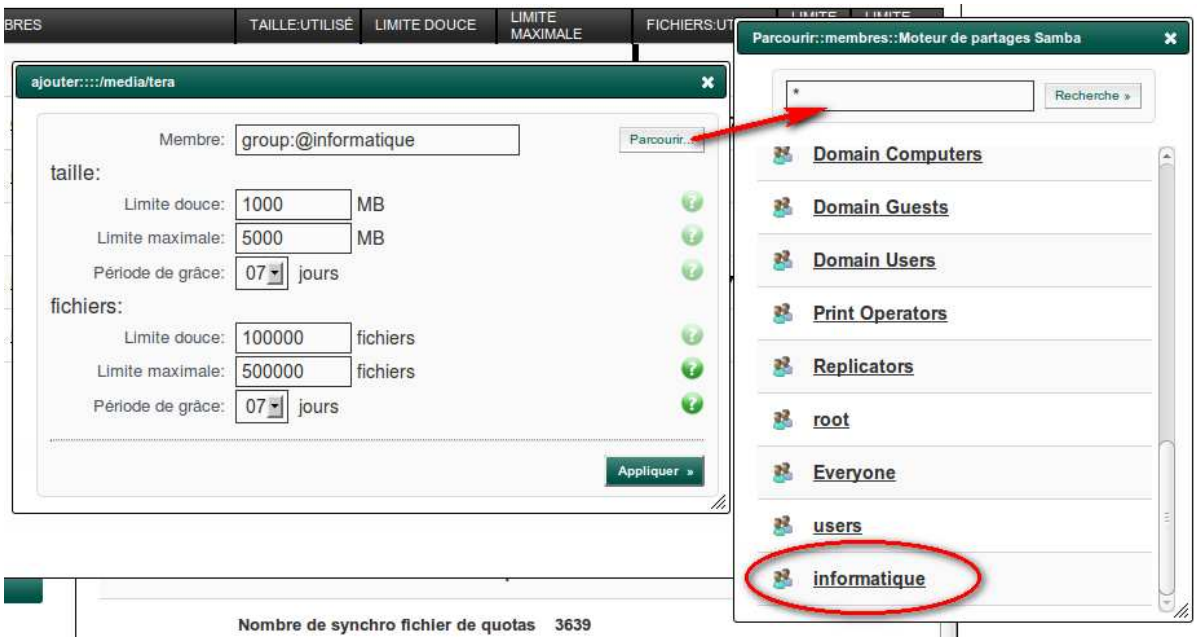
Pour définir un nouveau quota, cliquez sur le bouton « **ajouter** » ou pour modifier un quota, cliquez sur le lien de l'utilisateur ou groupe.

Dans le champ membre, ajoutez le groupe ou l'utilisateur que sera affecté au quota.

Ce champ dispose d'une syntaxe particulière, pour ce faire, utilisez le bouton « **parcourir** » pour rechercher l'élément désiré.

Vous avez deux sections distinctes la « Taille » qui indique le poids des fichiers stockés et les « Fichiers » qui indique le nombre de fichiers stockés.

Indiquez la limite « douce » en MB



Une limite douce est le maximum de la taille/Nb fichiers qu``un utilisateur peut avoir sur une partition.
Le rôle de la limite douce est de donner une période de grâce.
Lorsque cette limite est atteinte, les utilisateurs seront simplement avertis que leur limite à été dépassée.
Lorsque la période de grâce à expirée, les utilisateurs seront bannis du stockage de fichiers.
le chiffre 0 rend la limite illimitée.

Indiquez la limite maximale, celle que l'utilisateur ne pourra pas dépasser.

Faites de même sur le nombre de fichiers que vous voulez accorder à l'utilisateur/Groupe.

Dans notre exemple, nous accordons une limite de 1G au groupe « informatique » qui peut être dépassée pendant 7 jours jusqu'à un maximum de 5G.

Le nombre de fichiers est limité à 100.000 fichiers jusqu'à un maximum de 500.000.

> *Notez que seulement les utilisateurs qui effectués des dépôts de fichiers sont visibles dans le tableau.*
> *Ne vous inquiétez pas de ne pas visualiser vos utilisateurs ou groupes après avoir défini des quotas.*
> *Vous devrez attendre qu'ils déposent au moins un fichier dans la partition.*

Permissions sur les répertoires et ACLs

Bien gérer ses fichiers et ses dossiers ne passe pas forcément par un bon archivage ou une bonne hiérarchie.

Il s'agit aussi de définir judicieusement leurs droits. Qui peut le lire ? Qui peux écrire dedans ? Qui peut exécuter ce programme ? Qui peut accéder à tel répertoire ?

La gestion des droits de fichiers Unix s'effectue suivant 3 orientations :

le droit de lecture (Read), le droit d'écriture (Write) et le droit d'exécution (eXecute).

1. Le droit de lecture permet de lire le contenu d'un fichier.
2. Le droit d'écriture permet la modification et la suppression d'un fichier.
3. Le droit d'exécution sur des fichiers binaires ou shells permet de lancer le programme.

En version numérique :

- Read : 4
- Write : 2
- eXecute : 1

Appliqué pour un répertoire, les droits sont quelque peut différent :

- **r ou Read** : Le fichier peut être lu et Le répertoire peut être parcouru (exemple : obtenir les fichiers contenus dans ce répertoire par la commande ls)
- **w ou Write** : Le contenu du fichier peut être modifié ou ses attributs modifiés. Dans le répertoire, on peut supprimer, créer ou modifier un fichier
- **x ou eXecute** : Le fichier peut être exécuté .On peut entrer dans ce répertoire, qui devient notre répertoire courant

Comme vous l'avez compris, dans certains cas, l'attribution des permissions uniquement sur ces attributs ne suffit pas.

Les ACLs sont alors l'outil permettant de pouvoir affiner les permissions.

La mise en place des ACL permet une gestion fine des accès des utilisateurs, des groupes, aux répertoires et aux fichiers d'une partition qui dispose d'un système de fichier qui accepte les acl.

Les accès consentis par une liste de contrôle d'accès vont venir enrichir, et non remplacer, les protections offertes par le schéma classique. Les trois classes d'appartenance (User, Group, Other) vont pouvoir être vues comme trois entrées (de base) dans une liste de contrôle des droits d'accès, potentiellement plus riche de caractérisations spécifiques.

Nous vous conseillons vivement de mettre en place les ACL surtout si vous utilisez Artica en mode partage de fichiers.

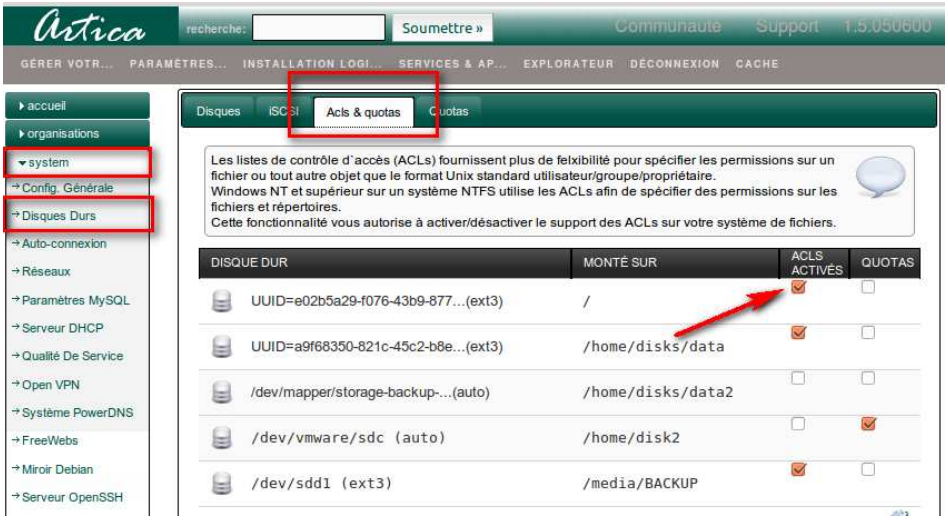
Mise en place des ACL sur les Disques.

Par défaut votre système Artica dispose de disques durs qui n'ont pas été activés afin d'héberger les ACL.

Pour ce faire, vous devez simplement activer l'option ACL sur vos disques et partitions.

Cliquez dans le menu de gauche sur « **System** » puis « **Disques Durs** »

Dans la section disques durs, cliquez sur l'onglet « **Acls & Quotas** »



Cochez les cases dans la colonne « ACLS ACTIVES » correspondantes aux partitions que vous souhaitez enrichir avec des ACL.

Une fois les cases cochées sur les partitions désirées, vous pouvez désormais appliquer les permissions sur les répertoires.

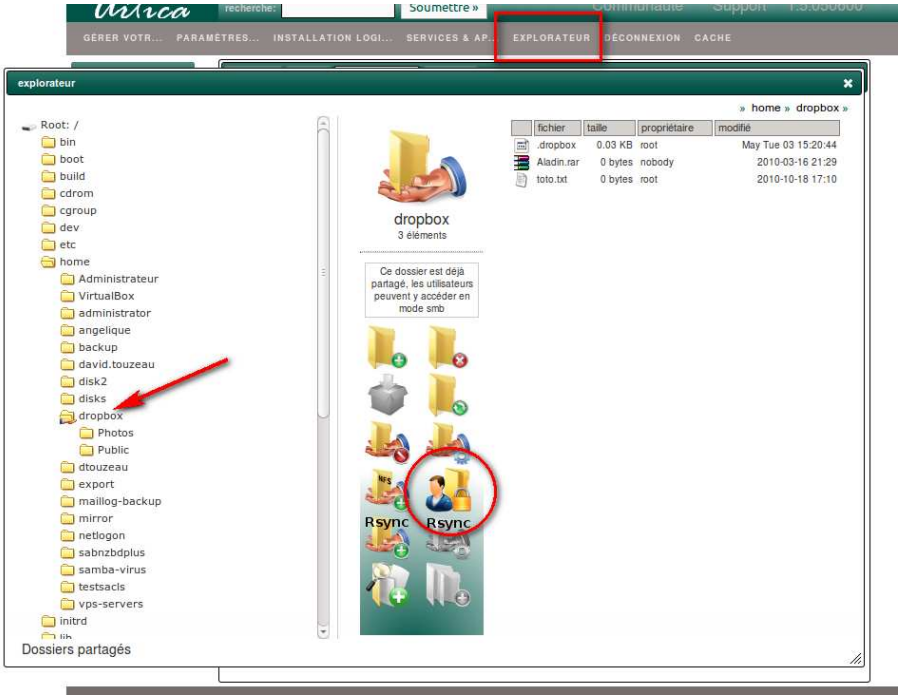
Application des permissions sur les répertoires

Artica dispose d'une sorte « d'explorateur » avancé. Cet explorateur vous permet de parcourir vos disques et répertoires locaux.

Lorsque vous naviguez à travers la section de gauche, la section de droite vous propose la liste des fichiers disponibles dans un répertoire donné mais aussi de fonctions permettant de partager le répertoire, de le supprimer...

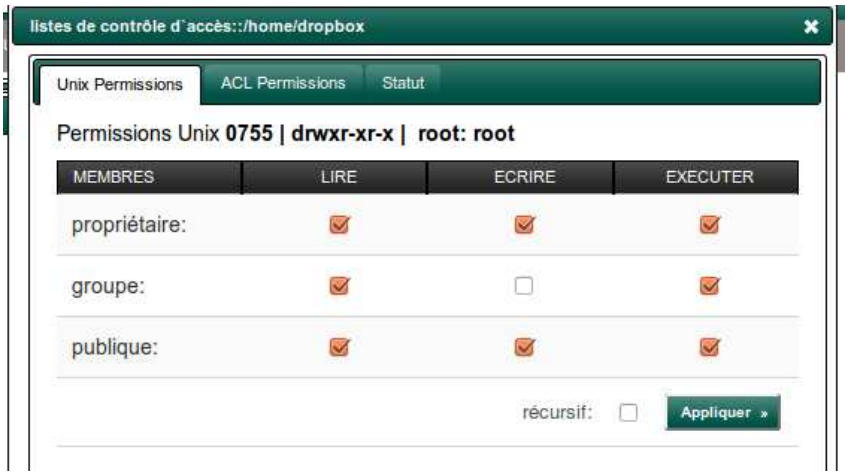
Ce qui nous intéresse est l'icône représentant un cadenas.

Cet icône nous permet d'ouvrir les paramètres des permissions du répertoire sélectionné.



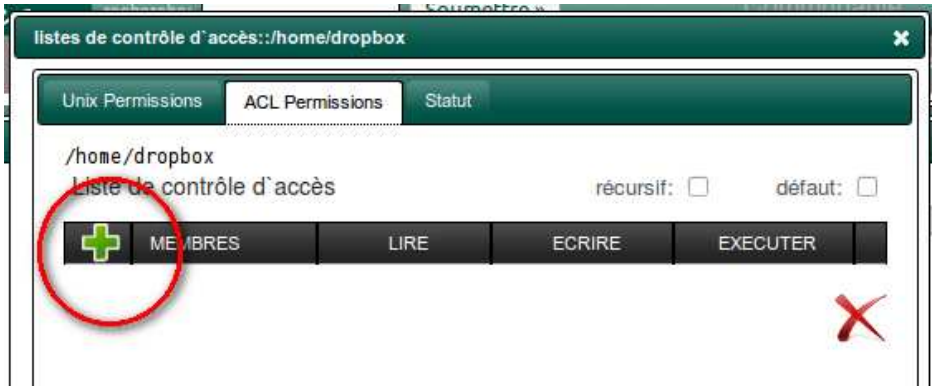
Une nouvelle boite message s'affiche vous proposant les deux formats de permissions disponibles pour le répertoire sélectionné.

L'onglet **Unix Permissions** vous permet de définir les propriétés Unix du répertoire avec les 3 groupes standards.



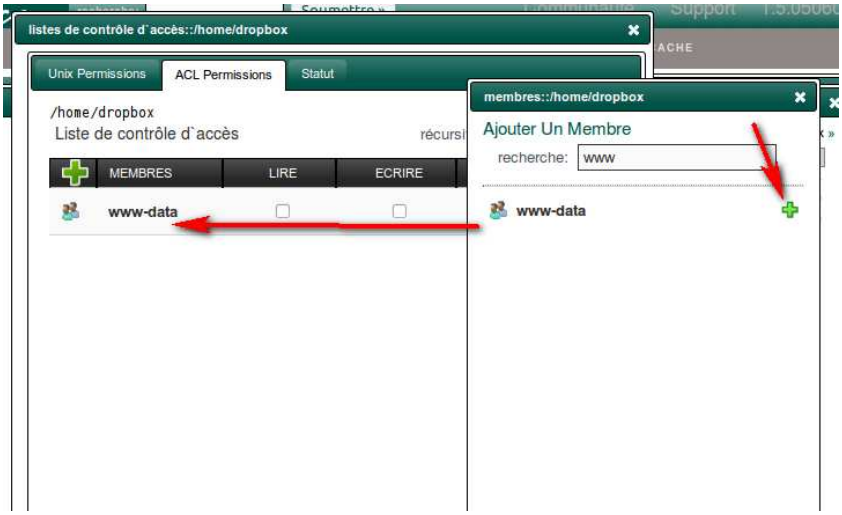
L'onglet ACL Permissions vous permet de définir d'autres propriétaires et droits sur le répertoire.

C'est ici que se définit ces fameux ACL.

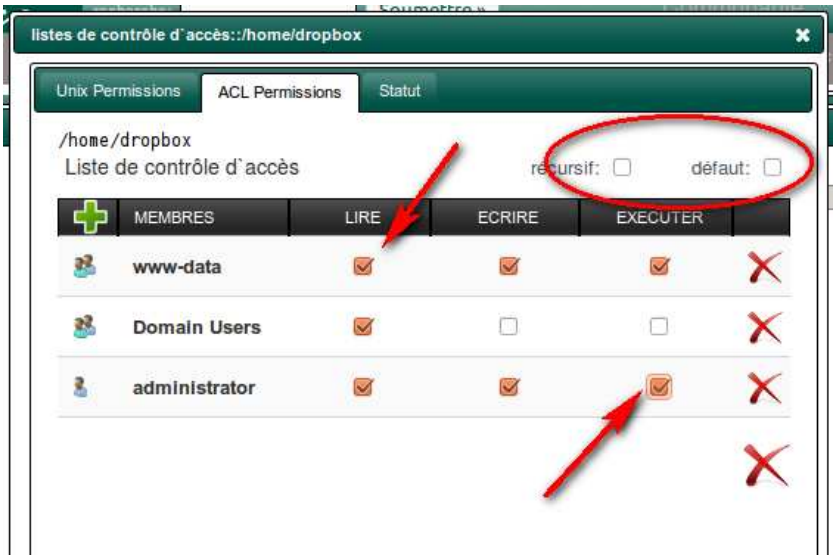


Cliquez sur la croix afin de rajouter un groupe ou un membre du serveur qui va disposer de privilèges spécifiques.

Une nouvelle fenêtre s'affiche vous permettant de rechercher et de sélectionner les groupes et/ou les membres à rajouter dans les permissions.



Une fois les membres ajoutés, il ne vous reste plus qu'a côcher les case correspondantes aux accès que vous voulez offrir.



Remarquez les deux cases à côcher « récursif » et « défaut » elles ont une fonction bien particulière.

« **Récursif** » indique que tous les fichiers et sous-dossiers vont subir les ACL que vous venez de mettre en œuvre. Il sera alors inutile de refaire l'opération sur les sous-dossiers.

« **Défaut** » indique que tout nouveau sous-dossier et fichier qui sera créé dans se répertoire va hériter automatiquement des ACL définis.

Vérification de l'application des ACL

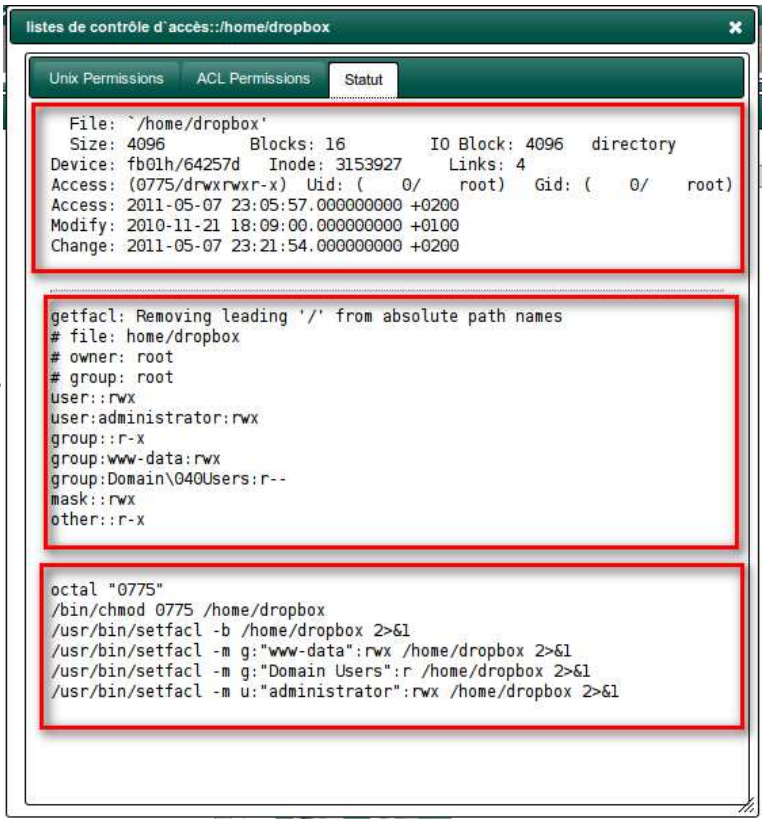
Lorsque vous créez des ACL, Artica applique vos paramètres en tâche de fond.

L'application de ces paramètres peuvent durer un certain temps. Tout dépend du nombre sous-dossiers et de la charge de la machine.

Cliquez sur l'onglet « **Statut** »

La section statut vous propose 3 sections :

- La première section vous indique les privilèges Unix appliqués.
- La deuxième section vous affiche les ACL qui ont étés appliqués par Artica.
- La 3ème section vous affiche les commandes que Artica à mis en place afin d'appliquer les paramètres que vous avez indiqué.

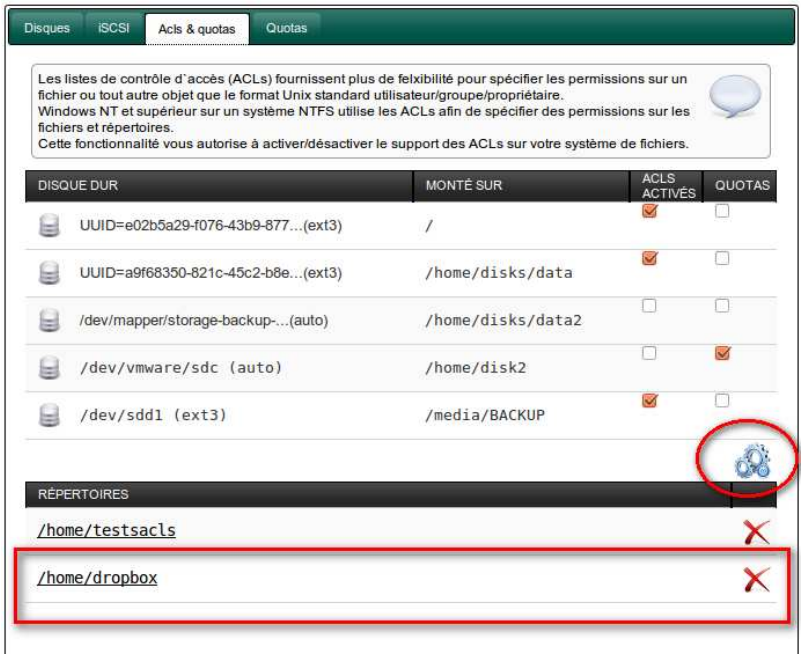


Visualisation des ACL mis en place.

L'explorateur d' Artica, dans un certain cas peut être contraignant pour modifier ou retrouver les ACL mis en place.

Pour ce faire , Artica vous propose un résumer des ACL que vous avez créé.

Pour retrouver les ACL appliqués , retournez dans la section vous permettant d'activer les ACL sur vos partitions.



Vous y verrez un deuxième tableau vous permettant de retrouver les répertoires qui subissent des permissions spécifiques et de retourner dans le formulaire d'édition des acl.

Remarquez la croix rouge, elle ne supprime par le répertoire mais remet à 0 les permissions sur le répertoire.

Remarquez aussi l'icône en haut à droite du tableau. Il permet de de reconstruire toutes les permissions de tous les répertoires que vous avez personnalisé.

Artica : proxy cache et filtrage d'url

Introduction

Artica est capable de piloter le fameux logiciel SQUID et ses additions afin d'offrir toutes les fonctionnalités nécessaires à la bonne navigation des sites web sur Internet.

Le filtre ufdbGuard

Ufdgguard est l'élément principale utilisé pour effectuer le filtrage par catégories des sites Web via Artica.

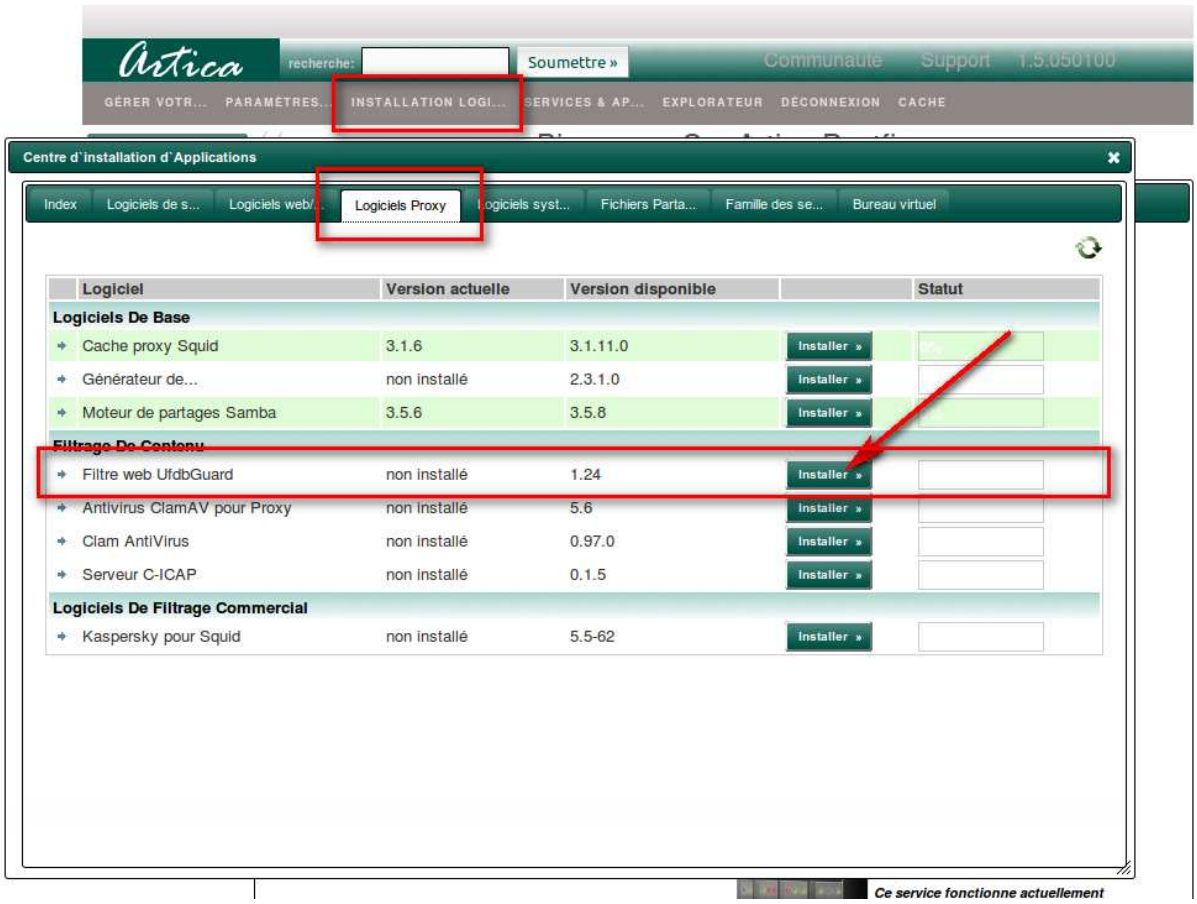
C'est un « redirecteur » puissant permettant de charger des bases de données de sites web par catégories afin de rediriger les sites web interdits vers une adresse Web de votre choix.

Installation et activation du filtre

Installation

L'installation s'effectue par le centre d'installation de Artica.

Dans le menu du haut, cliquez sur « I**NSTALLATION LOGICELS** », choisissez l'onglet « **Logiciels Proxy** » et cliquez sur le bouton « Installer » dans la ligne correspondante à « **Filtre Web UfdbGuard** »



Une fois l'opération d'installation terminée, cliquez sur le lien « cache » afin de forcer Artica à reconstruire le menu de gauche.

Vous y trouverez alors un nouveau menu « **Règles de filtrage** »

Activation du filtre ufdbguard.

Même si il est installé, Artica n'a pas rajouté ufdbGuard au système de proxy SQUID.

Pour ce faire, vous devez indiquer que vous souhaiter utiliser UfdbGuard en compagnon de SQUID.

- Dans le menu de gauche, cliquez sur « **Proxy Web** », puis « **Config. Générale** ».
- Cliquez sur l'onglet « **Filtres** »
- Cliquez sur l'image « **Activation des plugins Proxy** »
- Mettez en vert l'option « **Activer le Filtre Web UfdbGuard** »

Etats et maintenance des bases de données.

Le filtre utilise des bases locales afin de vérifier les sites web.

Vous avez deux bases de données :

Communauté Artica:

Ces bases de données (environ 1.500.000 entrées) sont automatiquement téléchargées depuis les serveurs de mise à jour Artica et stockés dans la base Mysql.

Elles sont le fruit de la communauté des utilisateurs Artica.

Artica dispose d'une technologie permettant d'enrichir automatiquement les bases de sites web grâce aux administrateurs des Proxy Artica.

En effet, lorsqu'un site web n'est pas catégorisé, Artica vous motive à le « ranger » dans une catégorie.

Lorsque vous catégorisez un site web, votre catégorisation est envoyée automatiquement au serveur de mise à jour Artica.

Celui-ci effectue des statistiques de votre site web : Si au moins 3 autres personnes on catégorisé le site de la même façon, le serveur de mise à jour sur Internet va placer le site web et sa catégorie comme « disponible » et cette catégorisation sera alors rapatrié par l'ensemble des serveurs Artica.

Bien entendu nous ne facturons pas le travail des propres utilisateurs Artica, le rapatriement de ces bases est gratuit.

> *Pour résumer : plus vous catégorisez les sites web que vos utilisateurs visitent, plus vous bénéficiez d'une base mise à jour.*

Les bases UfDbguard:

Ce sont des bases propriétaires et payantes (environ 9.000.000 d'entrées).

Ces bases sont déjà compilées et sont prêtes à l'emploi.

Contactez le support Artica si vous désirez obtenir une licence pour obtenir ces bases de données.

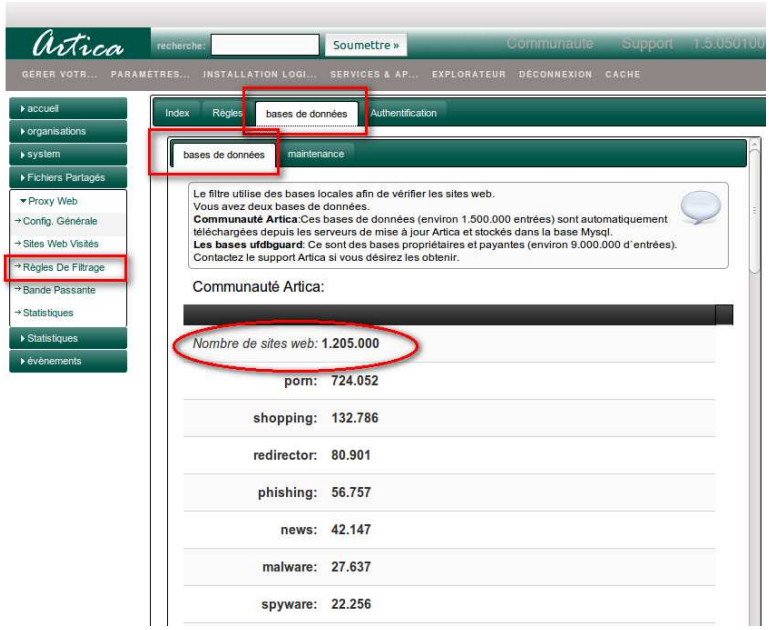
Etat des bases de la communauté.

Cliquez sur le menu de gauche « Proxy Web » puis « Règles de Filtrage »

Sélectionnez l'onglet « Bases de données »

Artica vous affiche une première page qui vous indique le nombre total de sites web référencés dans la base de données MySQL.

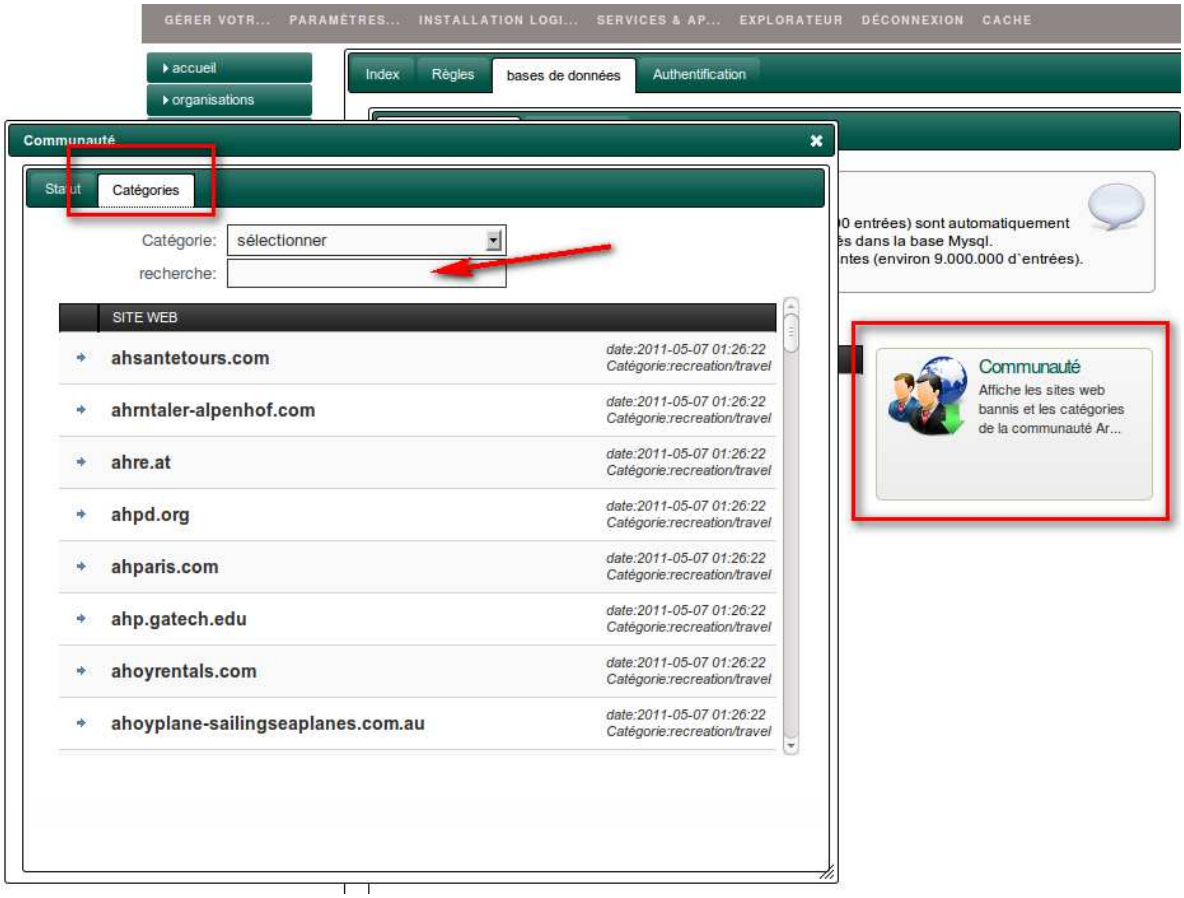
Puis, une liste des catégories disponibles ainsi que le nombre de sites web disponibles dans la catégorie.



Recherches dans les bases de la communauté.

Vous avez la possibilité de rechercher des sites web dans les différentes catégories des bases de la communauté.

Pour ce faire, cliquez sur l'image « Communauté »



Puis sélectionnez l'onglet « **Catégories** ».

un formulaire vous permet de rechercher un site web afin de vous assurer qu'il est bien présent dans les bases.

Compilation des bases de la communauté

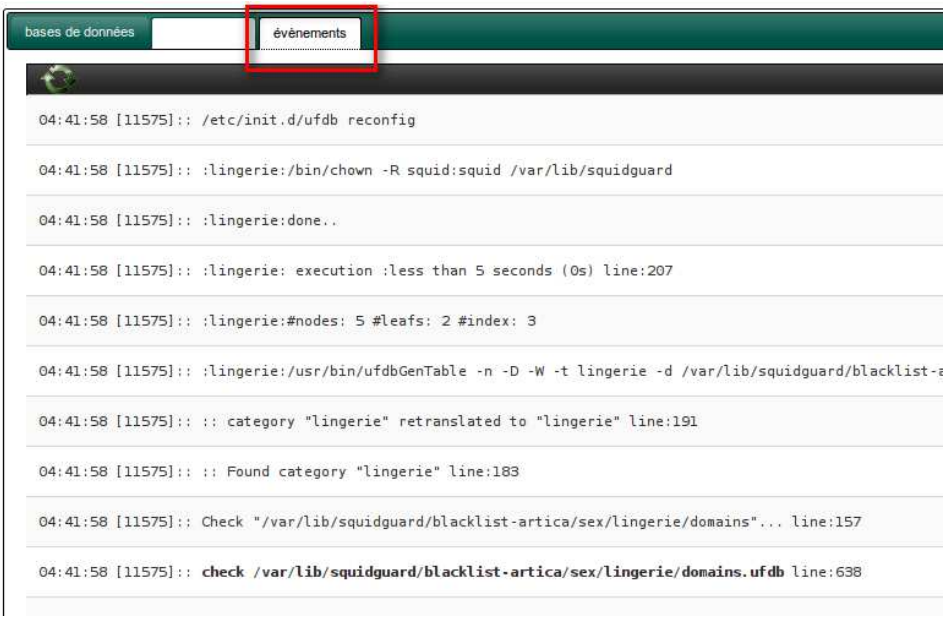
L'onglet « **Maintenance** » vous permet d'effectuer des opérations concernant les bases de données locales qui sont utilisées par le filtre.

Si vous avez créé des règles et que c'est la première fois que vos catégories ont été rajoutées, un message d'avertissement vous indique qu'il est nécessaire de compiler les bases de données afin que le filtre fonctionne.

Cliquez alors sur l'image « **Compiler les DB manquantes** »

Ceci aura pour effet de lancer la compilation locale des bases en attente de transfert d'une simple fichier texte en un format de base de données compris par le filtre et permettant de disposer de temps de réponse convenables.

Après avoir cliquer sur la compilation, vous pouvez visualiser les évènements de la compilation en cliquant sur l'onglet « **évènements** »



Re-compilation des bases.

Si vous rajoutez des sites web à filtrer ou que vous mettez à jour la base communautaire d'Artica, assurez vous que les bases soient re-compilées afin qu'elle puissent prendre en compte les modifications..

Pour ce faire, vous pouvez cliquer sur le bouton « **Re-compiler toutes les bases** ».

Cette fonctionnalité aura pour effet de supprimer les bases compilées sur le disque, de reconstruire les sources à partir de la base MySQL et de lancer une compilation locale.

Programmation de la re-compilation des bases.

Tout au long de la journée, vous aller certainement rajouter des catégories et des sites web.

Artica va aussi régulièrement récupérer des nouveaux sites web et catégories à travers les serveurs de mise à jour.

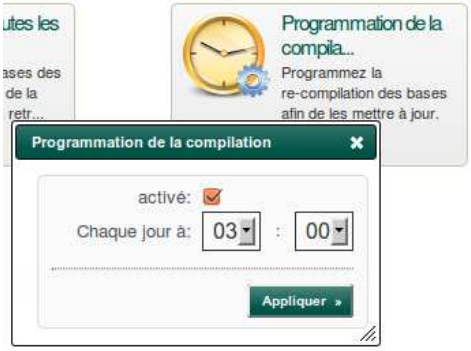
Pour ce faire, vous devez re-compiler les bases de données régulièrement.

Soit vous décidez de le faire manuellement, soit vous « *programmez* » une fréquence de re-compilation.

Cliquez sur l'image « **Programmation de la compilation** »

Une fenêtre va s'afficher vous permettant d'activer la programmation en cliquant sur la case à côcher « **Activé** ».

L'ordonnancement s'effectuera tous les jours à heure que vous allez déterminer.



Les règles de filtrage

Que ce soit avec C-ICAP, SquidGuard ou UfdbGuard, le principe d'affectation des règles est toujours identique.

Les règles de filtrage interdit à un utilisateur ou une adresse IP et/ou à un groupe d'utilisateurs ou groupe d'adresses IP d'accéder à des sites web stockés dans des catégories.

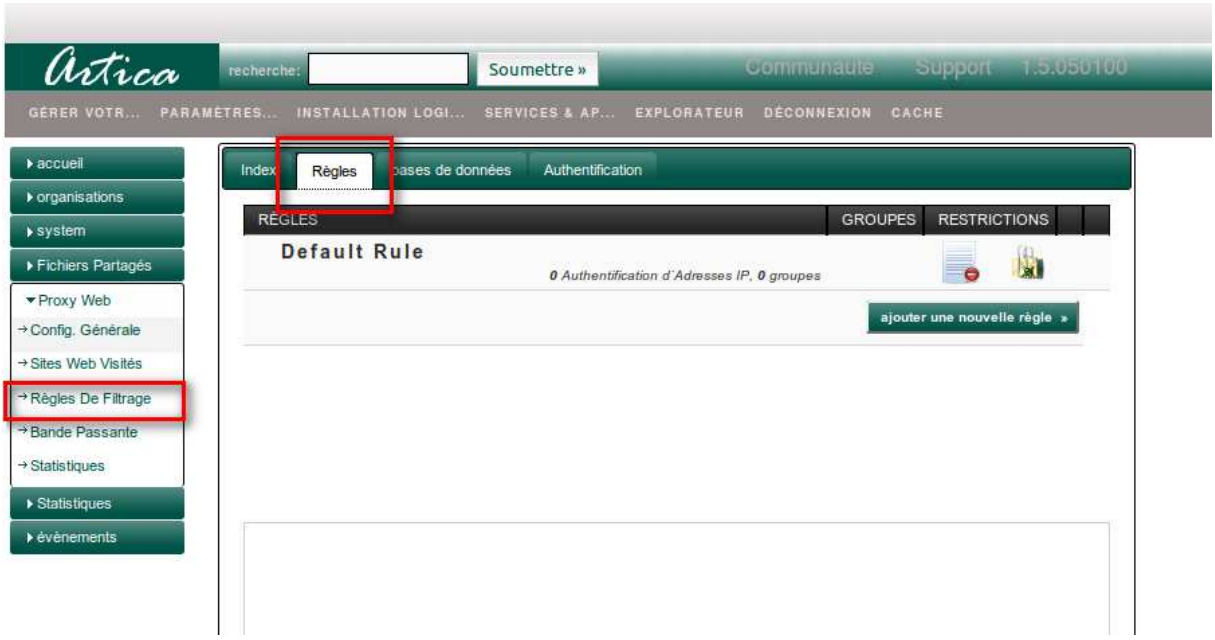
Les règles se trouvent à travers le menu de gauche dans « **Proxy Web »**, puis « **Règles de filtrage** ».

Cliquez sur l'onglet « **Règles** »

Vous disposez d'une seule règle qui est celle par défaut. Cette règle est prévu pour répondre à tzous les utilisateurs qui ne sont hébergés par les règles que vous avez définit.

De cette manière, vous pouvez interdire l'accès aux sites pornos et de hacking à tout le monde et pour une population particulière laisser ces sites web en accès libre.

Il suffit alors d'affecter les catégories à la règle « **Default rule** »



Création d'une nouvelle règle

Cliquez sur le bouton « **Ajouter une nouvelle règle** »

Une boite message apparaît vous proposant d'indiquer un nom à cette règle.

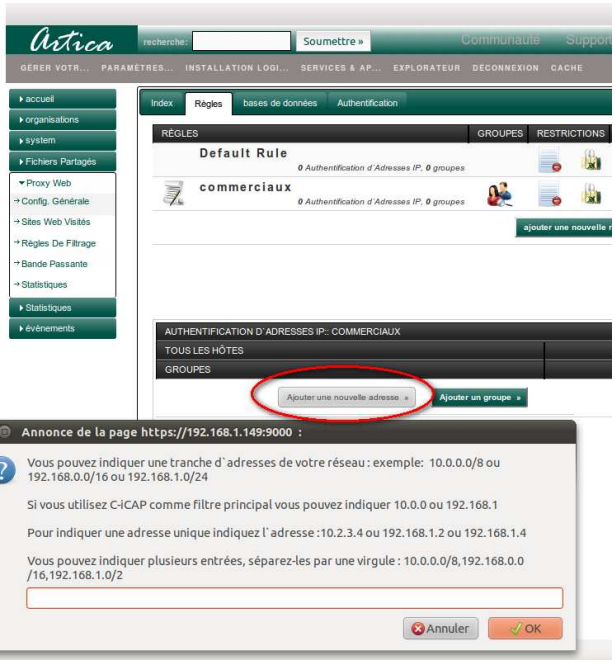
La règle va se rajouter dans le tableau.

Cliquez sur l'image deux personnages avec une loupe.

SI vous créez une nouvelle règle, vous devez obligatoirement indiquer des utilisateurs ou adresses dans cette règle.

Seule la règle « **Default Rule** » autorise la possibilité de ne pas mettre d'utilisateurs.

Une nouveau tableau s'affiche vous permettant d'ajouter une groupe d'utilisateur ou bien des adresses IP.



Affectation d'adresses IP

Le bouton « **Ajouter une nouvelle adresse** » vous permet d'indiquer une adresse IP ou un groupe d'adresses IP.

Vous pouvez indiquer une tranche d'adresses de votre réseau : exemple: 10.0.0.0/8 ou 192.168.0.0/16 ou 192.168.1.0/24

Pour indiquer une adresse unique indiquez l'adresse : 10.2.3.4 ou 192.168.1.2 ou 192.168.1.4

> *Vous pouvez indiquer plusieurs entrées, séparez-les par une virgule : 10.0.0.0/8,192.168.0.0/16,192.168.1.0/2*

Affectation par groupes d'utilisateurs.

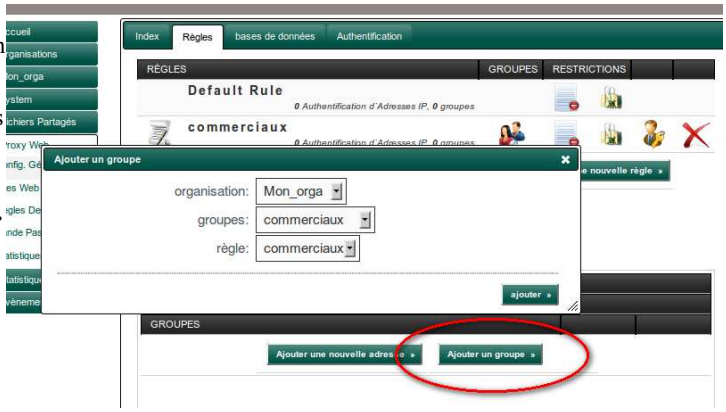
Cette fonctionnalité s'applique que :

Si vous avez mis en place un système d'authentification sur le proxy.

Si vous avez préalablement renseigné les groupes et les utilisateurs dans la base d'Artica (ou bien vous avez effectué une connexion à un serveur Active Directory).

Cliquez sur le bouton « **Ajouter un nouveau groupe** »

Indiquez dans le formulaire l'organisation, puis le groupe et cliquez sur « **Ajouter** »



Affectation des catégories

Une fois après avoir indiqué la population de votre règle, vous allez pouvoir affecter des catégories qui vont interdire l'accès aux sites web référencés.

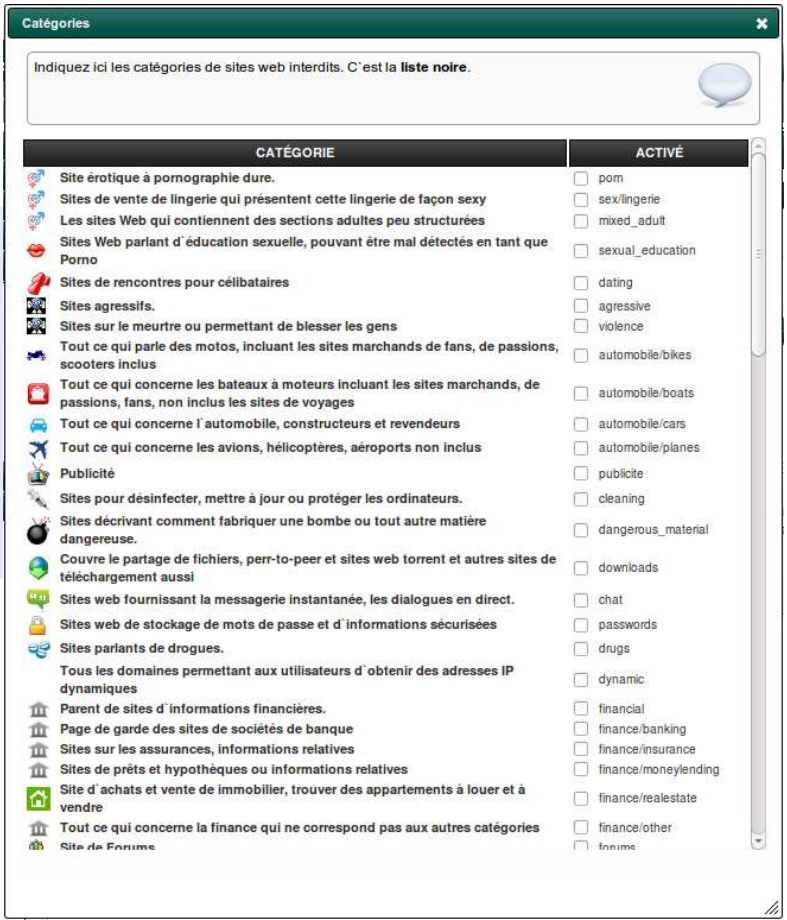
Sur votre règle, cliquez sur l'icône représentant une feuille avec un sens interdit.

Le tableau du bas se transforme et vous propose plusieurs fonctionnalités.

- **Catégories** : utilisation des bases de données rapatriées automatiquement.
- **Catégories personnelles** : Utilisation de vos propres catégories.
- **Exeptions** : Liste blanche de sites web qui va contredire les catégories.

Cliquez sur l'image « **Catégories** »

Une nouvelle fenêtre s'affiche vous permettant de côcher les cases correspondantes au thèmes de sites web que vous désirez interdire.



Attention !

Côcher une case ne veut pas dire que les bases sont compilées.

*Reportez-vous au paragraphe **maintenance des bases de données** afin de compiler les bases et de les mettre en mode production afin que la navigation de vos utilisateurs soit réellement interdite.*

Gestion des utilisateurs et ordinateurs

Artica permet de gérer des « clients ».

Ces clients peuvent être à la fois des ordinateurs (machines) et des utilisateurs.

On peut y associer des services particuliers et des droits particuliers

Privilèges des utilisateurs et délégations

La console de management change son comportement en fonction des droits accordés aux utilisateurs.

Par défaut, seul le compte Manager/Admin est capable d'administrer l'ensemble du serveur.

Lorsque vous ajoutez un utilisateur, celui-ci n'a le droit que de se connecter sur une interface dédiée.

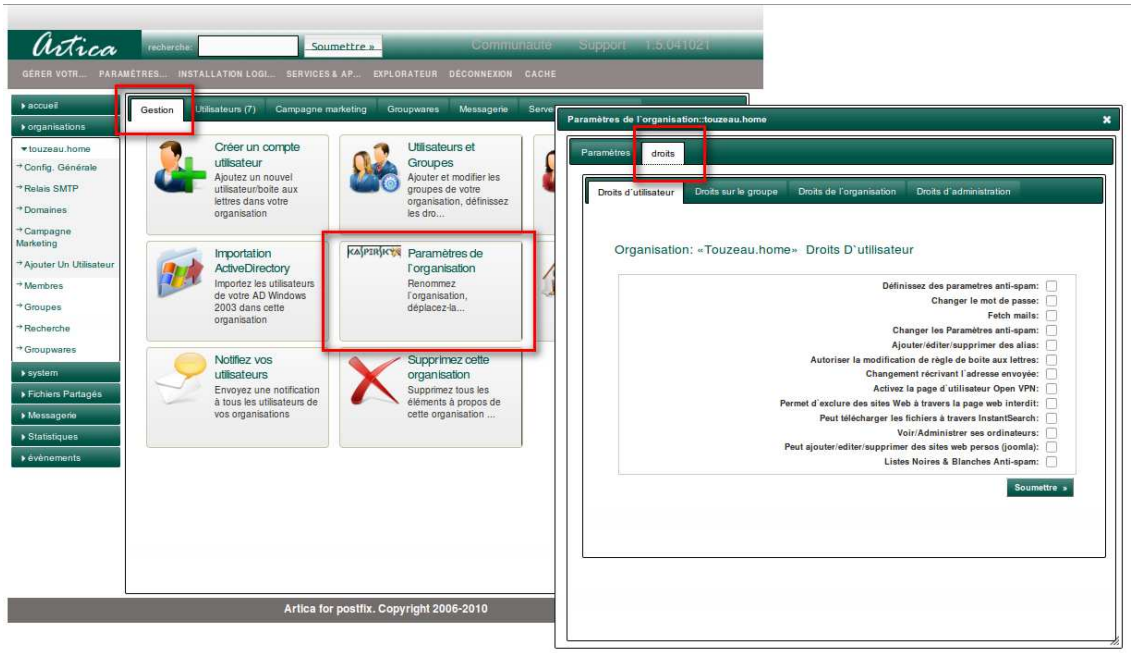
Le principe des privilèges offre la capacité à « déléguer » une partie de l'administration du système à des utilisateurs ou groupes d'utilisateurs précis.

Niveaux d'affectation des privilèges

Artica propose 3 niveaux d'affectation des privilèges.

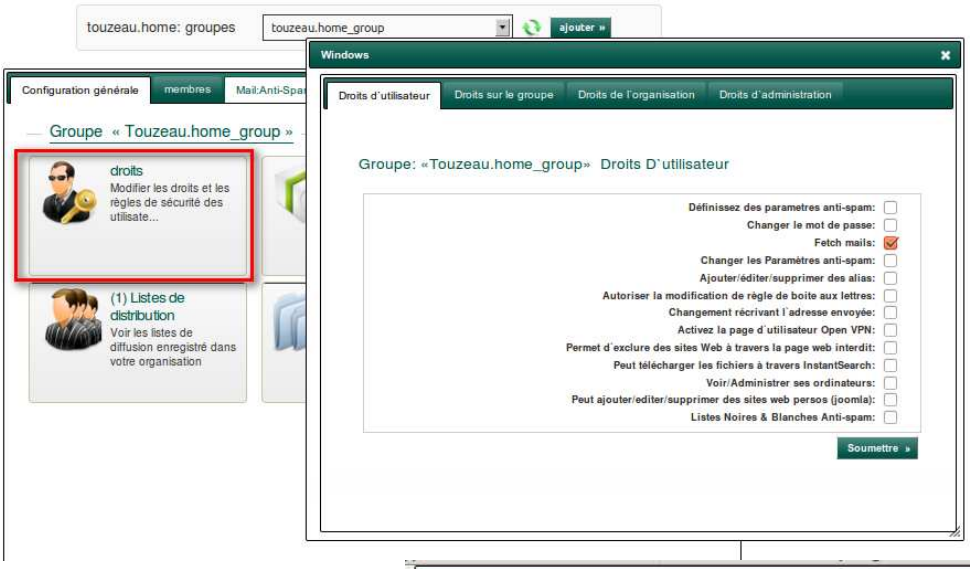
Dans l'organisation :

Sélectionnez une organisation, cliquez dans l'onglet « Gestion » puis sur l'image « Paramètres de l'organisation » et enfin sur l'onglet « Droits » de la boîte message « Paramètres de l'organisation »



Dans les groupes :

Sélectionnez un groupe puis dans l'onglet « **Configuration Générale** », cliquez sur l'image « **Droits** »



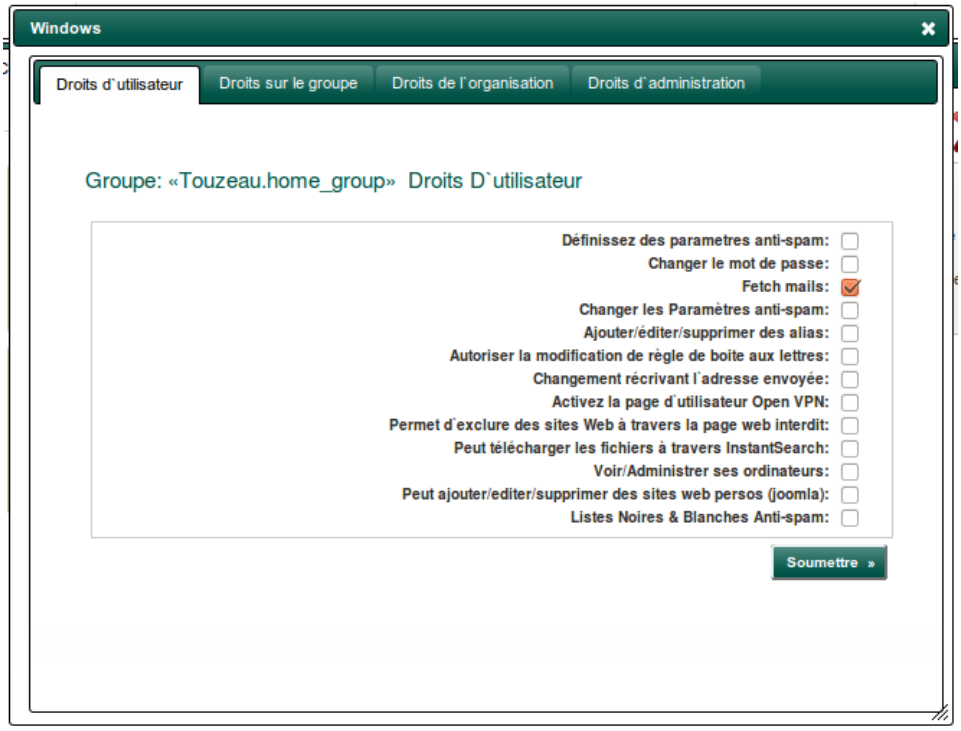
Au niveau de l'utilisateur :

Recherchez votre utilisateur, cliquez sur l'onglet « Compte » et sur l'image « droits »

Niveaux des privilèges

Artica possède 4 niveaux de privilèges :

1. **Droits de l'utilisateur** : Que peut faire l'utilisateur avec ses données personnelles ?
2. **Droits sur le groupe** : Que peut faire l'utilisateur avec les services et les membres du ou des groupes à qui il appartient.
3. **Droits sur l'organisation** : Que peut faire l'utilisateur avec les services et les membres de son organisation.
4. **Droits d'administration** : Que peut faire l'utilisateur sur les services « systèmes » du serveur.



Fusion des privilèges

Les privilèges fusionnent entre groupes : C'est à dire que si vous avez affecté un utilisateur dans deux groupes, il va hériter des droits des deux groupes correspondants.

Les privilèges fusionnent entre groupes et l'organisation : Si vous avez affecté des privilèges dans l'organisation, ceux-ci seront aussi fusionnés avec ceux des groupes.

Les privilèges au niveau de l'utilisateur cassent les fusions :

Si vous définissez des privilèges dans le compte utilisateur, il seront pris comme prioritaires.

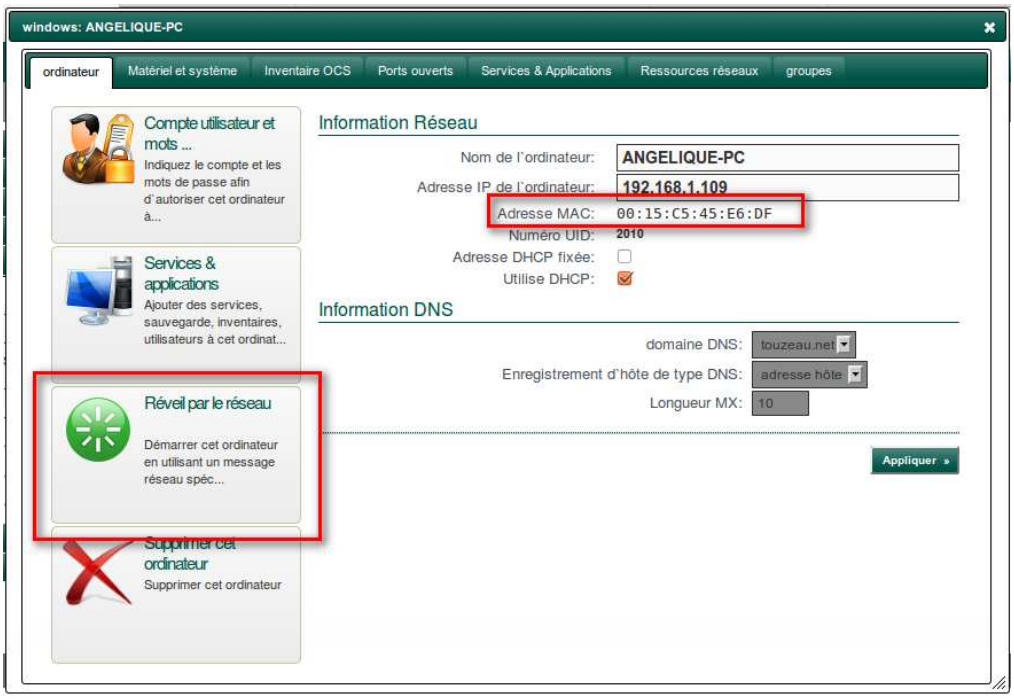
Il s'agit ici d'une exception qui permet par exemple de créer un administrateur système dans un groupe qui n' en n'a pas les droits.

Reveil par le réseau « Wake-on-Lan »

A travers l'interface d'Artica, il est possible de démarrer « électriquement » un ordinateur à distance.

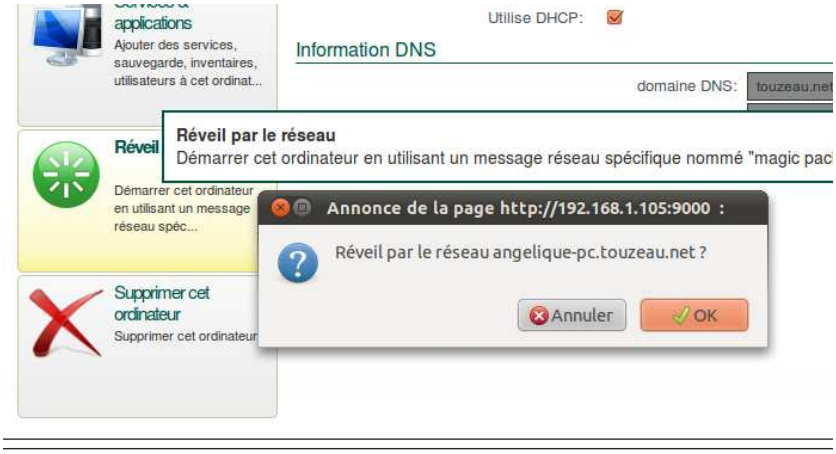
Cette fonctionnalité utilise le principe du Wake-on-Lan en envoyant un « magic packet » à l'ordinateur concerné.

Si l'adresse de la Carte MAC de l'ordinateur est correctement renseignée dans l'interface d'Artica, vous aurez la possibilité de cliquer sur l'icône « Réveil par le réseau »



Une fois avoir cliqué sur l'icône, un message de confirmation est affiché.

Et Artica vous donnera le résultat de l'émission du magic packet.



Artica et la messagerie

Préface, Artica une passerelle SMTP Anti-spam et antivirus.

Artica permet de proposer un routeur SMTP matériel intégrant des mécanismes de contrôles avancés du protocole SMTP. Pour ce faire, il suffit simplement de ne pas installer de processus de gestion de boîte aux lettres afin de transformer Artica en passerelle SMTP.
Vous transformerez alors Artica en une solution de sécurisation de la passerelle de messagerie.

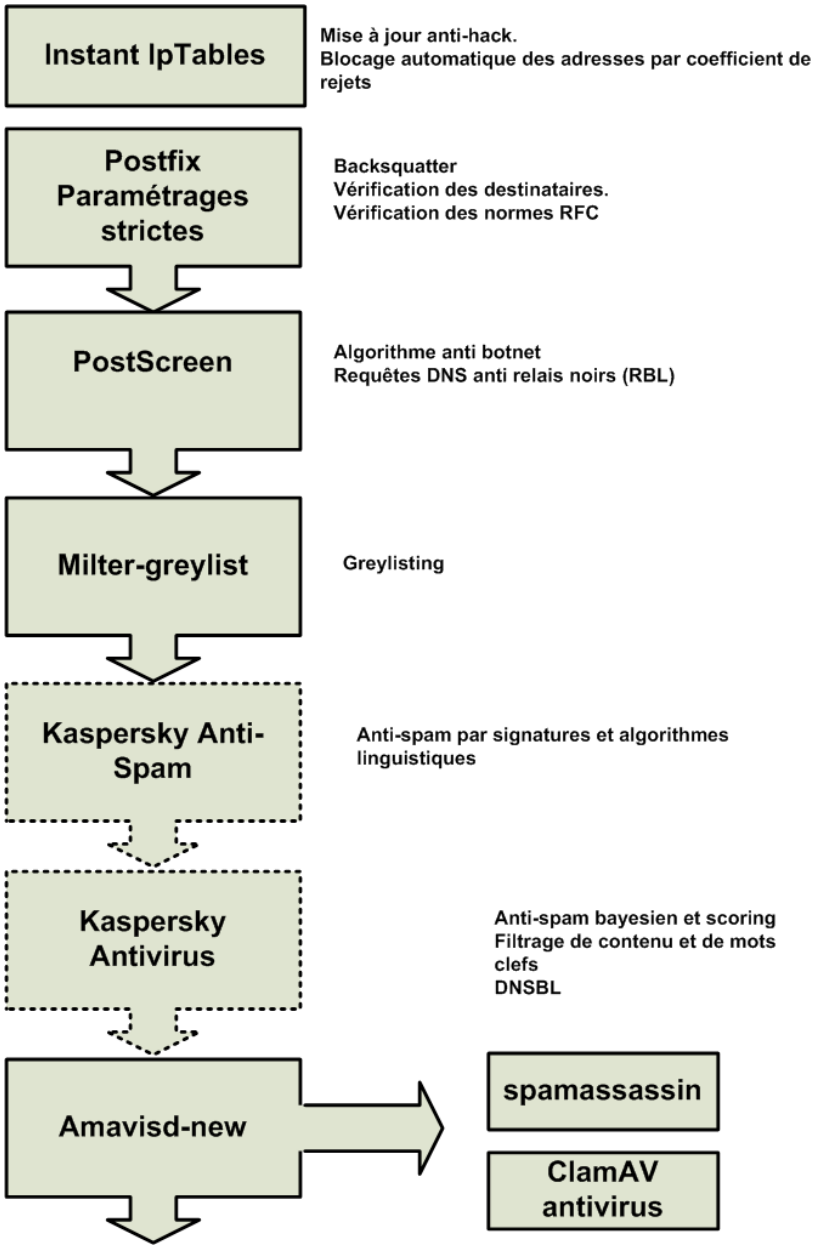
Cette passerelle s'intègrera facilement dans n'importe quel réseau et, grâce à son système d'interface.

Il n'est pas nécessaire d'être familier avec UNIX, Linux, Solaris ou même une autre plate-forme.

En mode relais, la passerelle Artica s'installe donc au niveau de la DMZ, la zone neutre protégée par le pare-feu et en amont des flux des serveurs de messagerie.

Mécanismes de filtrage

Artica associe différents mécanismes de filtrage afin d'offrir le meilleur taux d'anti-spam.



Principales fonctionnalités du mode relais

Facilités d'administration

Artica Postfix en mode relais offre une série de fonctionnalités qui facilitent la gestion de la sécurité de la messagerie.

- Console d'administration de type web qui permet "en quelques clics" une administration facile et rapide du système.
- Définition de politiques pour la gestion des virus, du spam, des pièces jointes et des contenus indésirables.
- Un chiffrage SSL et une prise en charge des certificats personnalisés pour un accès sécurisé à la console web d'administration et à l'interface web utilisateur
- Suivi des messages en continu avec recherches dans les journaux, les files d'attentes et dans la quarantaine
- Intégration avec Microsoft Active Directory® et autres systèmes LDAP qui facilite la configuration, l'application de politiques et l'authentification des utilisateurs
- Rapport de quarantaine ou interface web pour la gestion de la quarantaine utilisateur
- Listes d'expéditeurs approuvés et bloqués applicables globalement ou à un utilisateur
- Système d'alerte intégré en cas de panne matérielle ou logicielle

Filtrage du courrier entrant :

- Le MTA intégré intercepte les messages entrants au niveau de la passerelle de messagerie
- Les messages sont analysés à la recherche de spam, de virus et d'autres menaces définies au préalable dans les politiques de filtrage
- Des tests et des actions spécifiques sont appliqués aux messages
- Les messages sont redirigés afin d'être remis au bon destinataire, placés en quarantaine ou supprimés.

Filtrage du courrier sortant :

- Les messages sont redirigés des serveurs de messagerie internes en sortie vers Artica
- Les messages sont analysés à la recherche de virus et d'autres menaces définies au préalable dans les politiques de filtrage
- Des tests et des actions spécifiques sont appliqués aux messages
- Les messages sont relayés vers le MTA intégré pour être renvoyés vers l'extérieur ou vers la quarantaine pour une nouvelle analyse

Lors de la configuration initiale, l'administrateur a la possibilité d'appliquer aux messages les politiques et les actions configurées par défaut.

La console d'administration de type web permet de modifier ces politiques à tout moment et de personnaliser les tests et les actions à mener.

Le Multiple-instances

Introduction : Pourquoi le multiple-instances ? :

Le multiple-instances est né avec la version 2.6 de postfix.

Le comportement standard.

Postfix est capable par défaut de modifier son comportement en fonction de différentes sources ou base de données.
Il est donc possible de rendre hermétique les tables de routages, compte utilisateurs et de scinder l'administration de la messagerie par entités virtuelles.

Chaque organisation partage le même service SMTP
Celui-ci dispose d'une seule file d'attente et les plugins (filtres) qui l'entoure.

Lorsqu'il s'agit d'un serveur standard type mono-organisation, cette architecture se prête très bien. Les filtres associés peuvent être mono-configuration et appliquent les règles globales définis par l'administrateur globale de la messagerie.

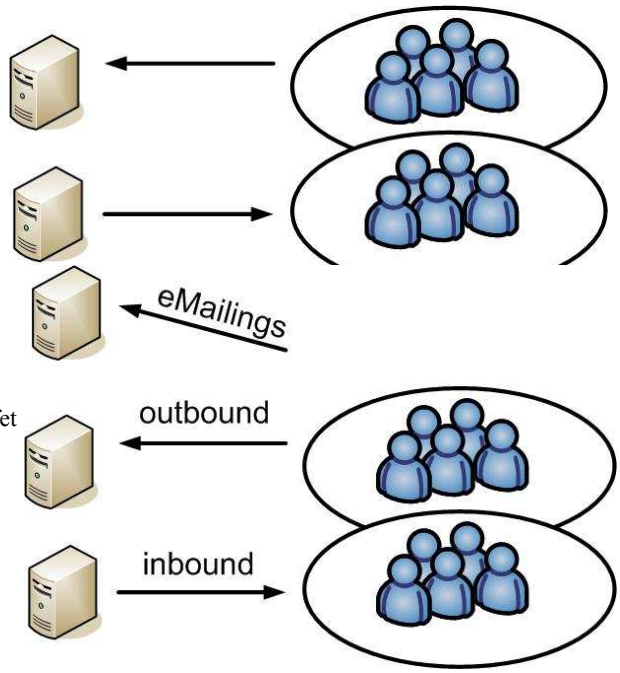
Les limitations

Dans un environnement avec des organisations qui se doivent être réellement hermétiques et des services SMTP qui doivent disposer d'un comportement différent, cette architecture mono-service devient moins adaptée.

Pour pallier à ce manque, les administrateurs messagerie sount obligés d'installer d'autre machines avec des services SMTP.

Si nous prenons le cas d'une architecture standard où les **flux sortants doivent être séparés des flux entrants**, deux serveurs physiquement séparés répondent au besoin.

De la même façon, si l'entreprise dispose d'un service marketing qui a pour mission d'émettre des **eMailings de masse** nous sommes obligés de rajouter un troisième serveur destiné à cet effet afin que les envois de masse ne perturbent pas la communication électronique de l'ensemble de l'entreprise.

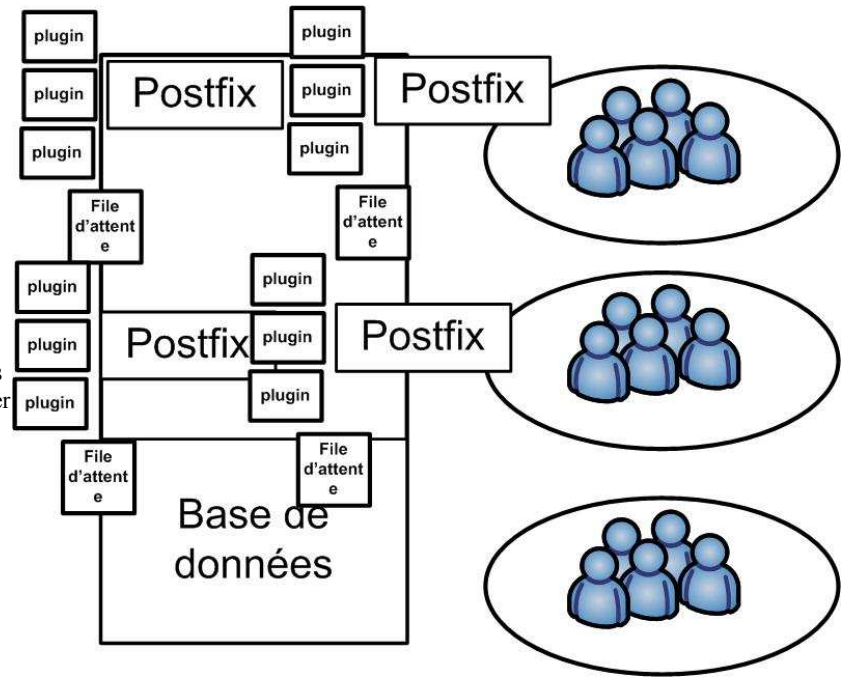


Le multiple-instance

Le multiple-instance à pour but de pallier à ces limitations, il se comporte comme des serveurs « virtuels » hébergés par le même serveur.
Cette approche à pour but de rendre complètement hermétique les différents services SMTP tout en pratiquant l'administration et le gestion d'un seul serveur.
Les deux approches alors se combinent et renforce leurs avantages.

Le mode multiple-instances de postfix ne se comporte pas toute à fait comme les serveurs virtuels « apache » chaque instance va utiliser sa propre adresse IP.

Nous verrons par la suite que la gestion des adresses IP virtuelles dans Artica prend alors tout son intérêt.



Les avantages.

Ce procédé permet d'offrir les avantages suivants :

- Une instance « malade » ne contamine pas les autres instances.
- Chaque instance gère sa propre file d'attente. C'est à dire qu'une instance ralentie par une file d'attente trop volumineuse ne dégrade pas les autres flux de messagerie.
- Chaque instance possède ses propres filtres associés avec ses propres configurations où une instance (par exemple les flux sortants ne se verra pas enrichie d'une filtre de greylisting

Les inconvénients.

Si le serveur doit gérer plusieurs instance, il doit être performant, comme les filtres peuvent être répliqués. La multiplication des instances et des filtres peuvent dégrader la performance du serveur.

Artica

fort de cette fonctionnalité, Artica met en valeur l'implémentation d'une telle architecture en simplifiant les procédures d'implémentation et d'administration des paramètres.
Ainsi, chaque organisation peut avoir un nombre d'instance illimité pour ses besoins.
Chaque administrateur des organisations et capable alors de paramétrer ses instances, de les activer ou de les supprimer à volonté et d'administrer les filtres associés.

Mise en place du multiple-instances dans Artica

Cas pratique.

Ce document va se baser sur un cas pratique :

Une organisation nommée KLIX doit disposer de 3 services SMTP :

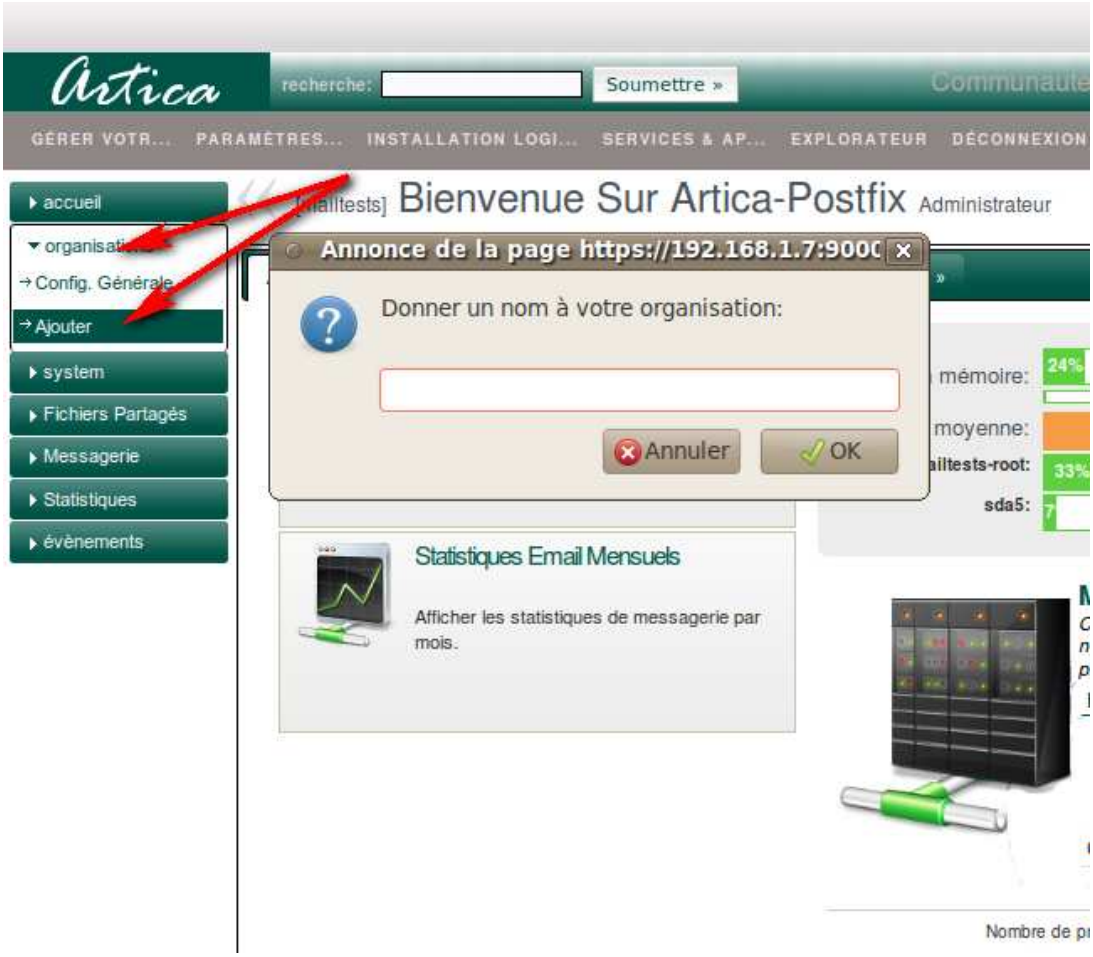
1. Le premier est un service de flux entrants qui doit disposer de toutes les vérifications anti-spam et antivirus.
2. Le deuxième est un service de flux sortants qui doit être performant et léger.
3. Le troisième est un service dédié pour le service marketing. Celui-ci doit bénéficier d'un service particulier pour les envois de messages en masse pour ses besoins marketing.

1) Création de l'organisation

Si votre serveur Artica est tout neuf, aucune organisation est crée, vous devez en créer une au minium.

Dans le menu de gauche, sous « organisations », cliquez sur « **Ajouter** »
Dans la boite message nous allons indiquer « klix »

L'organisation se rajoute dans le menu de gauche.
Elle va nous servir à affecter les adresses IP à cette organisation.



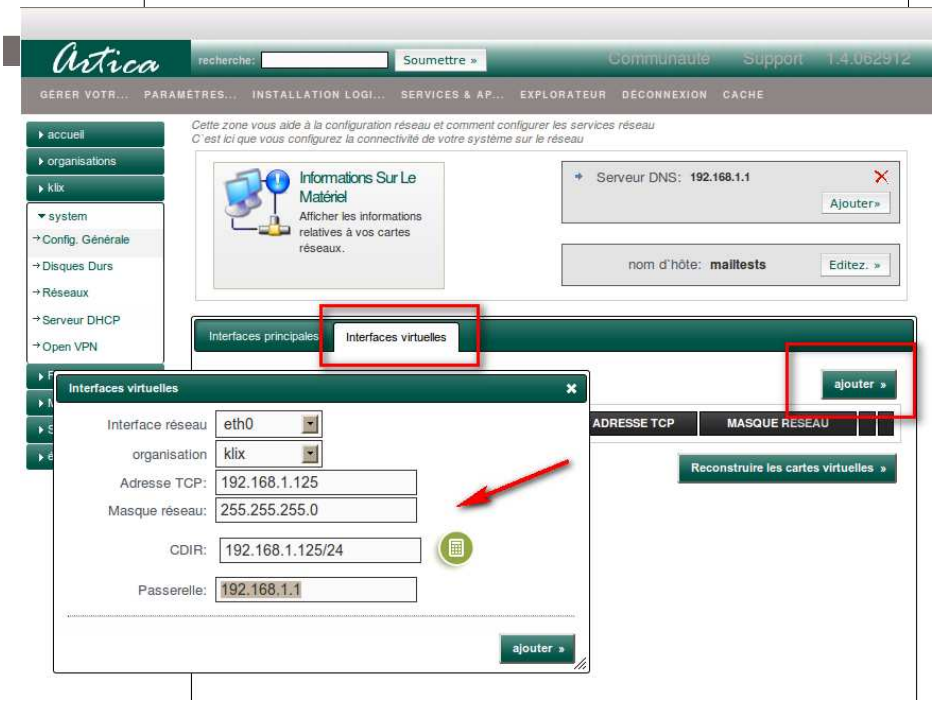
2) Création et affectation des adresses IP.

Artica possède une gestion des adresses IP virtuelles.
Comme chaque instance doit disposer de sa propre adresse IP, nous allons en créer respectivement 3 dont 192.168.1.125, 192.168.1.126, 192.168.1.127

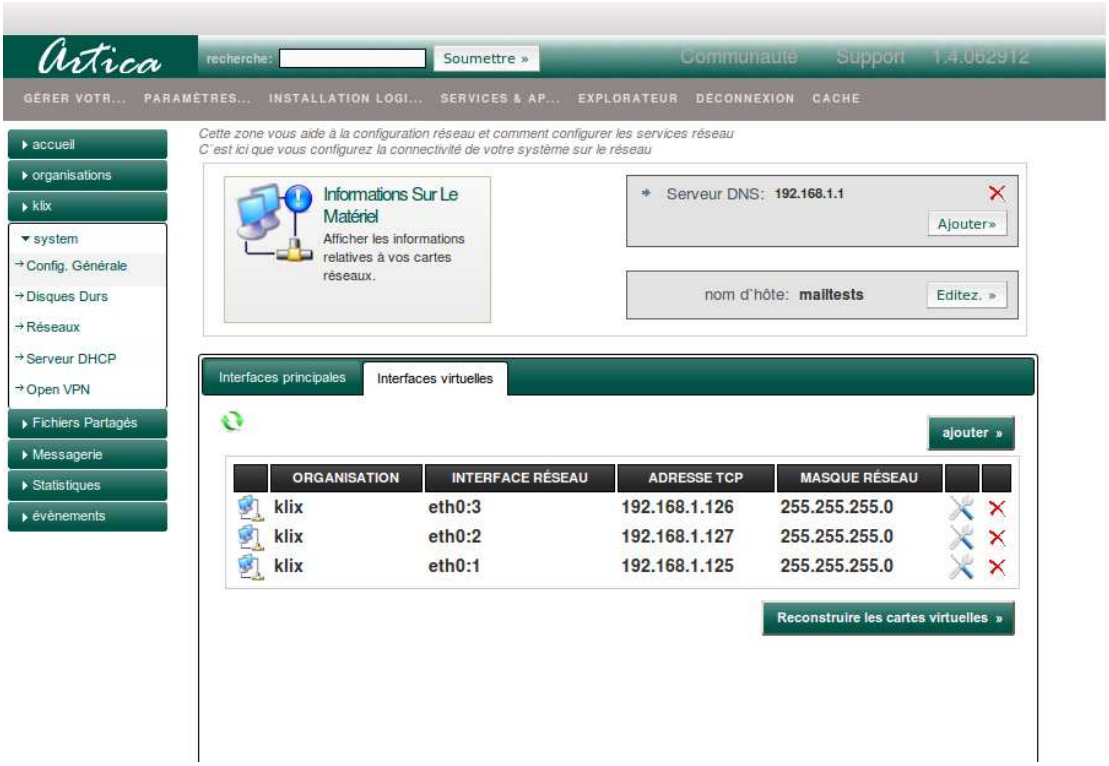
Dans le menu de gauche, sous la section « **system** » sélectionnez le menu « **Réseaux** »

Dans la section réseaux, cliquez sur « interfaces virtuelles » puis sur le bouton « **ajouter** »

Pour les 3 adresses IP, nous allons indiquer dans le champs « organisation » le nom de l'organisation klix



Une fois toutes les adresses ajoutées nous pouvons passer à l'étape suivante, c'est à dire l'activation du mode multiple-instances.

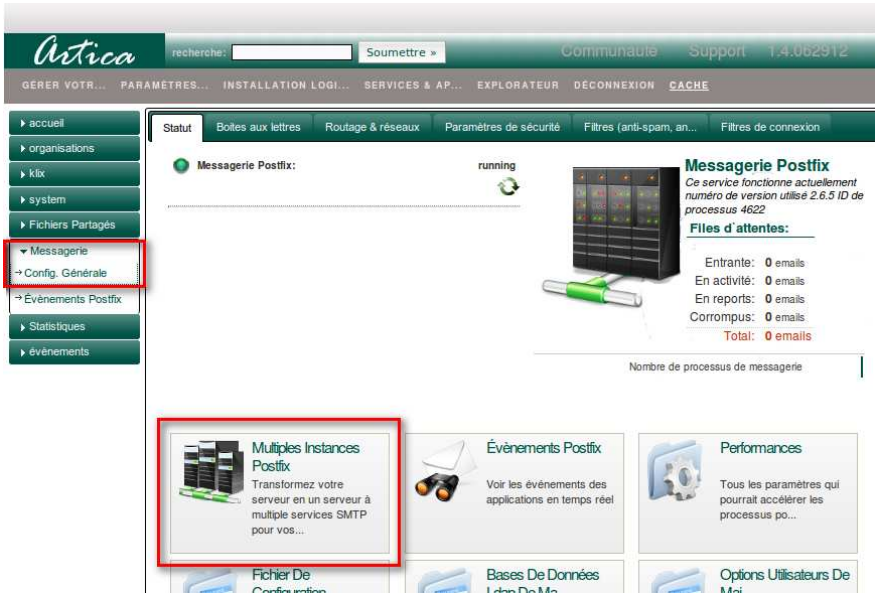


Il est à noter que vous pouvez par la suite affecter de nouvelles adresses IP pour la même organisation ou d'autres organisation.

3) Activation du mode multiple-instances.

Dans le menu de gauche, choisissez « **Messagerie** » / « **Config. Générale** ».

Cliquez sur l'image « **Multiples Instance Postfix** ».



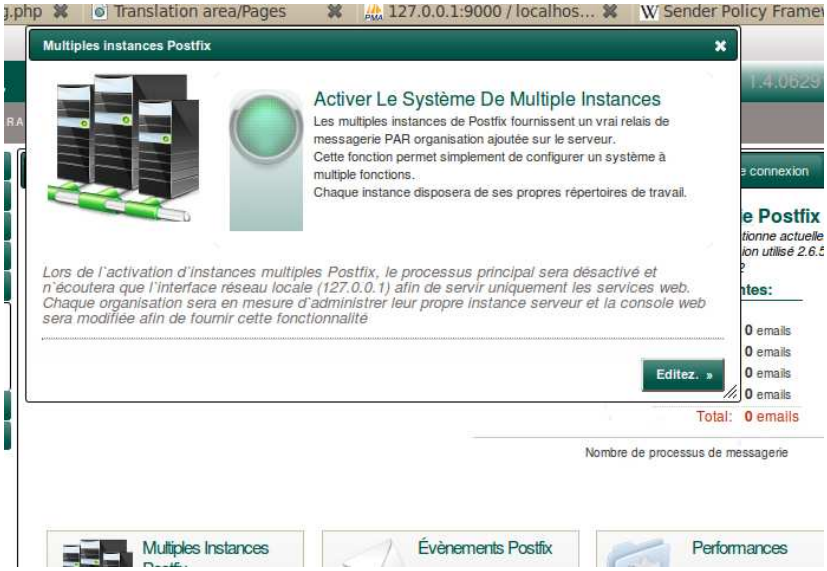
Passer le bouton en vert et cliquez sur le bouton afin de passer en mode multiple instances.

Une fois le mode multiple instances activée, l'interface d'Artica va s'adapter au nouveau mode.

En effet, l'instance principale n'étant plus maître de le messagerie les options dédiée au mode mono-instance seront retirée.

Dans le mode multiple-instances, l'administrateur principale du système n'est plus maître de la messagerie.

Ce privilège est alors transféré vers les organisations qui disposent d'adresses IP affectée à leur organisation.



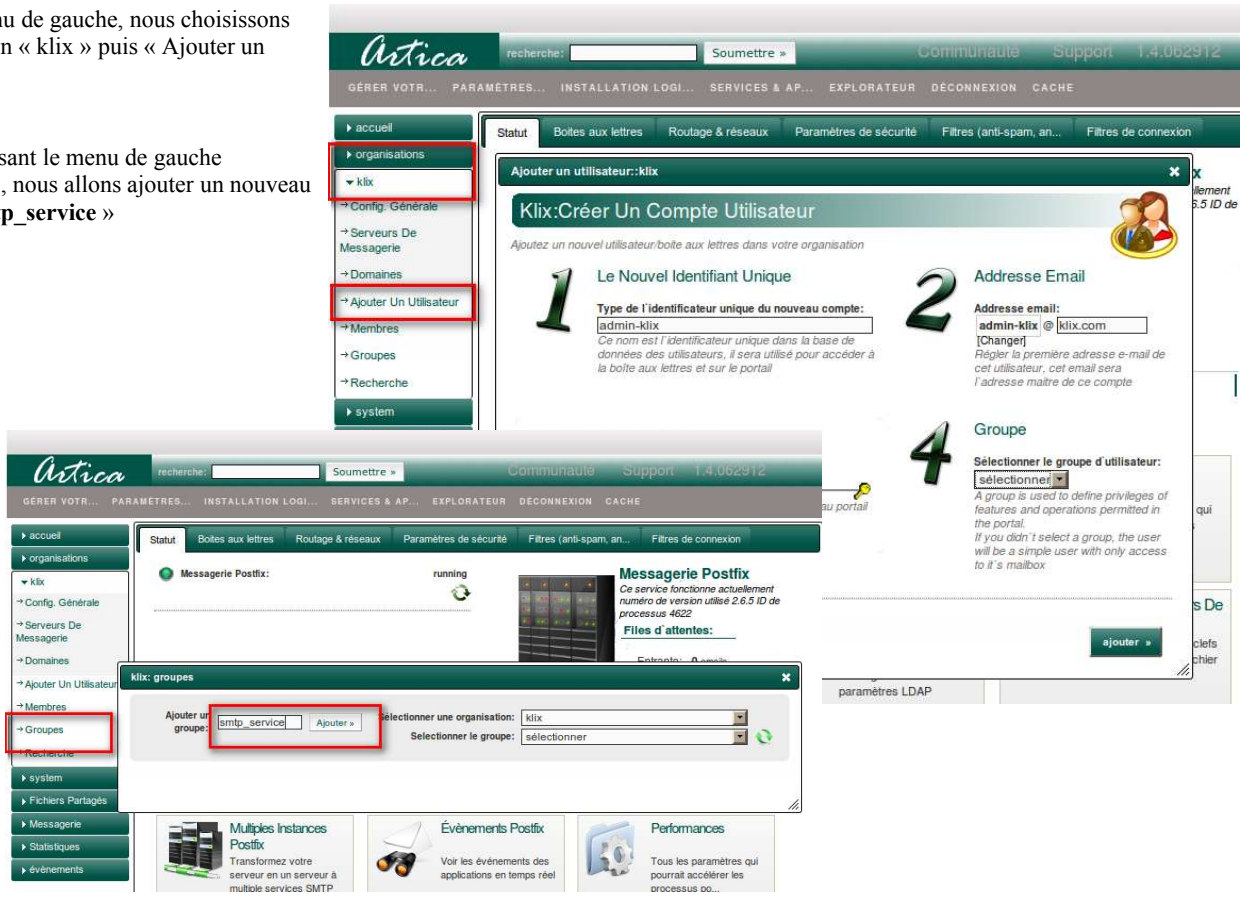
4) Définition des privilèges

L'idée principale est que l'administrateur système délègue l'administration des services SMTP à des administrateurs situés dans les organisations respectives.

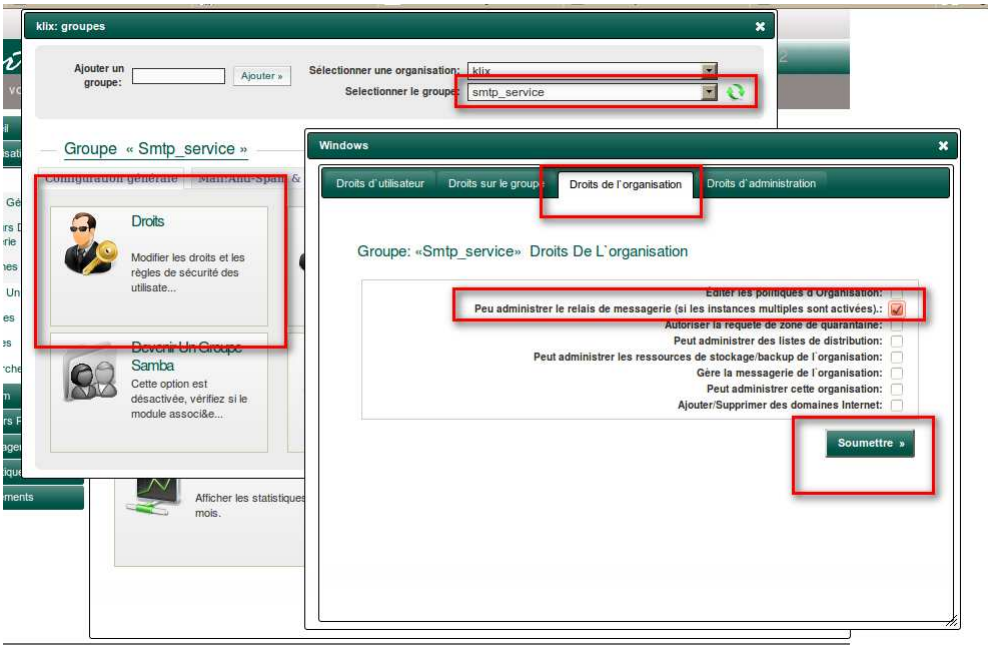
Pour notre organisation « klix » nous allons ajouter un utilisateur « **admin-klix** »

Dans le menu de gauche, nous choisissons l'organisation « klix » puis « Ajouter un utilisateur »

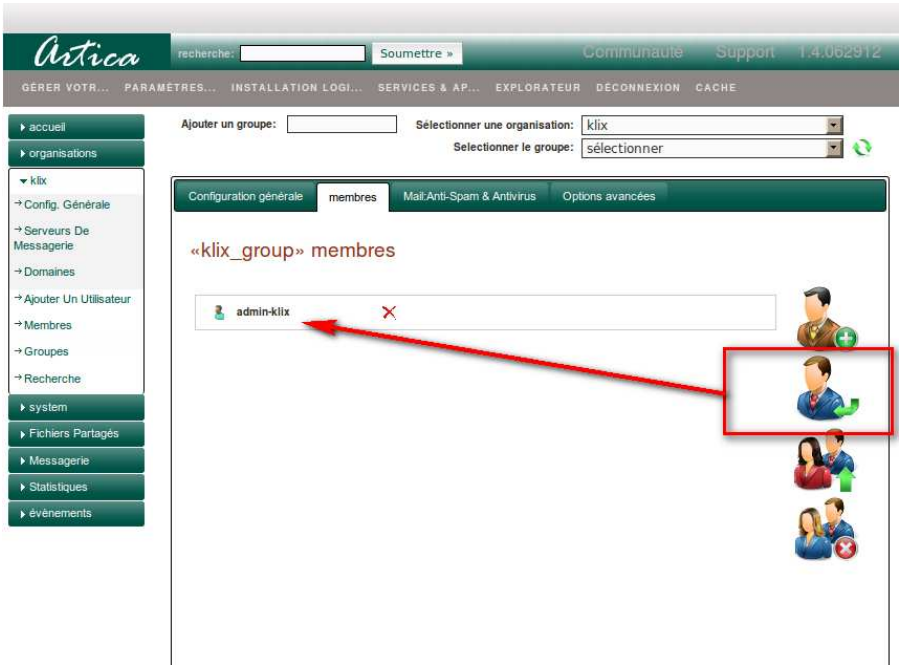
Puis en utilisant le menu de gauche « Groupes », nous allons ajouter un nouveau group « **smtp_service** »



Une fois le groupe créé, cliquez sur l'image « Droits » afin de rajouter un privilège d'organisation «**Peut administrer le relais de messagerie (si les instances multiples sont activées)** .. »

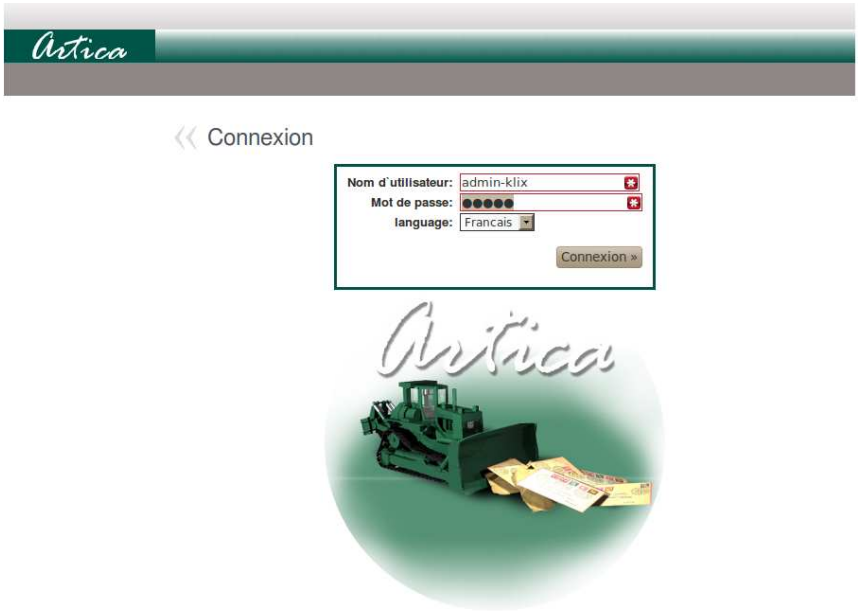


Puis importez l'utilisateur admin-klix dans le groupe.

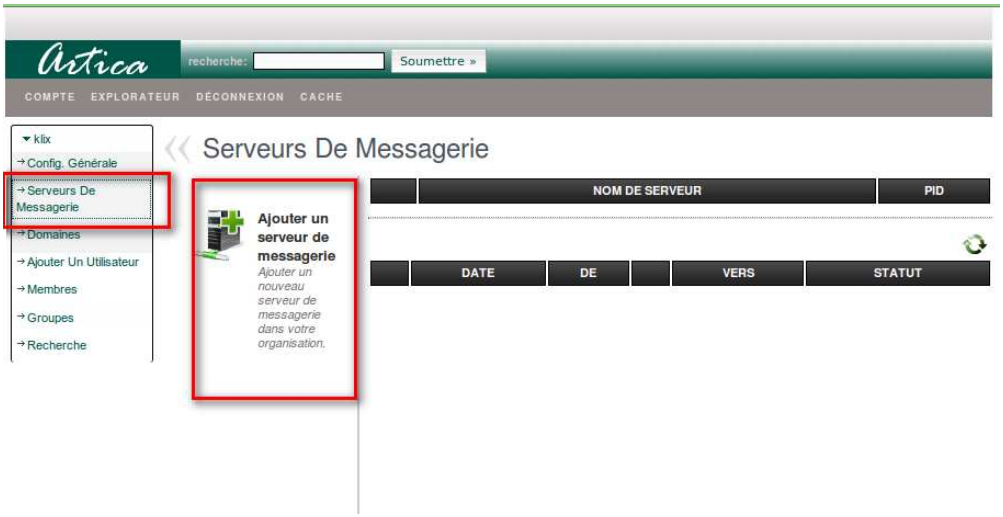


5) Administration des instances

L'administrateur « admin-klix » dispose maintenant des privilèges du groupe smtp_service et peut se connecter sur l'interface Artica afin de gérer son organisation et ses instances SMTP.

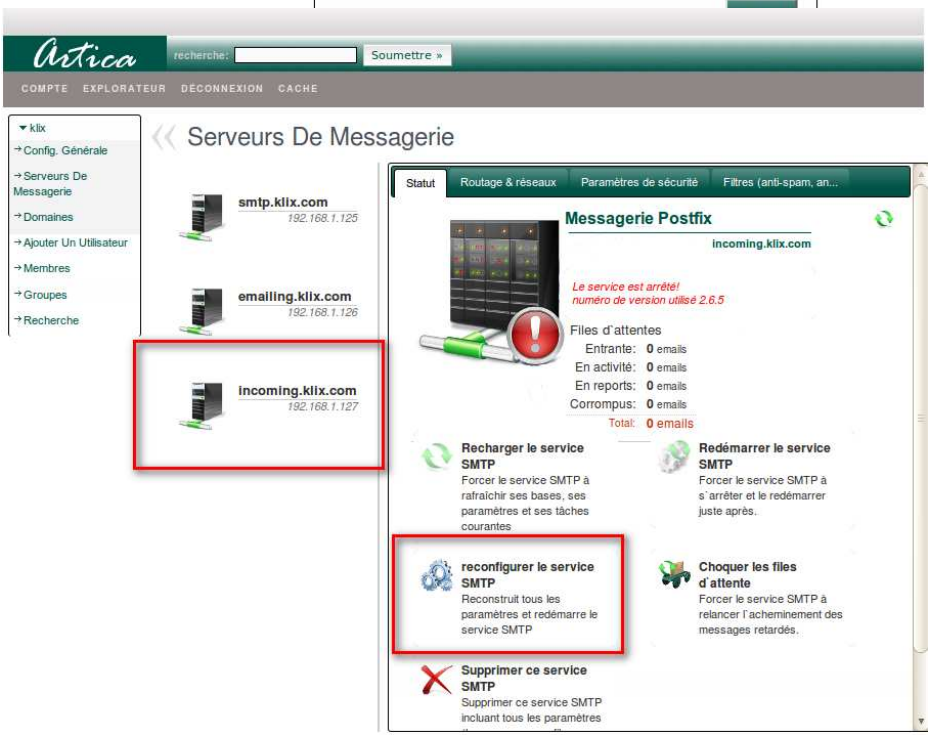


Au départ,
l'administrateur de
l'organisation ne dispose pas d'instances préétablies.
Dans la section « Serveurs De messagerie », il devra cliquer sur « Ajouter un serveur de messagerie »

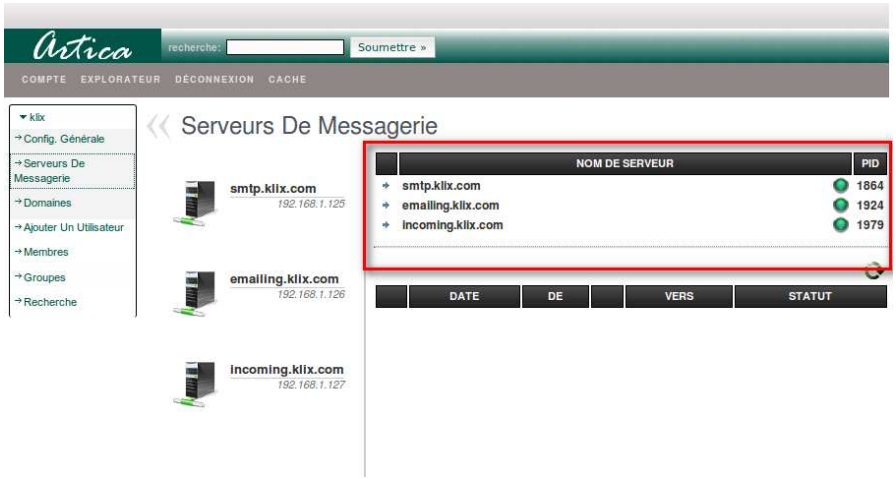


Lorsqu'il ajoute un serveur de messagerie, il doit choisir une adresse IP disponible, le domaine de messagerie et le nom du serveur.
Les adresses IP sont celles qui ont étés affectées par l'administrateur système. Dans notre cas, il dispose de 3 IP donc 3 serveurs disponibles.

Pour activer le démarrage du service SMTP, l'administrateur de l'organisation devra sélectionner « reconfigurer le service SMTP » afin de voir l'état du serveur en succès.



Une fois les services reconfigurés, les états des instances doivent être toutes au vert.



Le Domain throttling avec Postfix

Le « Domain throttling » ou en français « Limite de Domaine » permet de de personnaliser la transmission des messages à destination des domaines spécifiques.

Cette technique permet de répondre aux éventualités suivantes :

Les principaux fournisseurs limitent la fréquence de réception de leur serveurs.

Yahoo, Hotmail, OVH et bien d'autres utilisent des défenses permettant d'éviter de relayer des flux importants de messages soit à destination de leurs clients, soit en transmission vers des serveurs de messagerie sur Internet.

Cette technique aussi « chevalière » soit-elle perturbe de temps en temps le routage de la messagerie.

En effet un refus de ces serveurs (parce que votre serveur émets trop de messages en même temps) amplifie le retard de transmission vers vos destinataires.

Un serveur qui reçoit un refus va placer les messages en file d'attente sur votre serveur et les messages devront patienter 15 minutes (valeur par défaut) avant d'être réémis une nouvelle fois.

Or si au cours de la ré-émission, votre serveur dépasse à nouveau la limite du serveur de destination, alors le cycle va se remettre en place.

Pouvoir envoyer des messages en masse

Pour une tout autre initiative, s**i vous désirez envoyer un « mailing »** en passant par des serveurs ou à destination de serveurs qui demandent un flux spécifique, vous risquez de ne jamais pouvoir finir l' émission de votre emailing.

Accélérer la cadence...

Tout au contraire, vous pouvez souhaiter que des messages à destination d'un domaine spécifique soit émis plus rapidement. Par exemple votre serveur de messagerie interne...

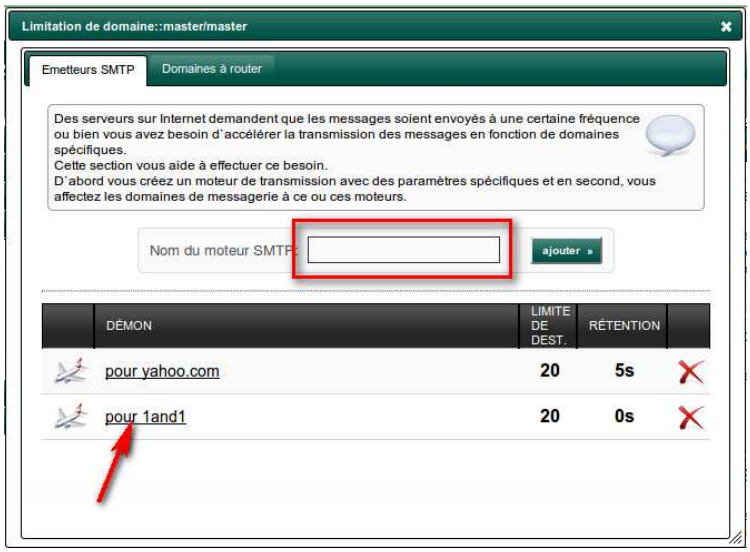
Mise en place avec Artica

Artica permet de mettre en place facilement la technique du « domain throttling ». Cette technique peut s'implémenter à la fois en utilisant une instance simple ou bien en mode multiple instances.

En mode multiple instances les combinaisons sont multipliées où chaque instance peut disposer de ses propres règles de throttling et ainsi bénéficier d'une meilleur souplesse d'émission.

- Dans le menu de gauche, sélectionnez le menu « **messagerie** » puis « **Config. Générale** »
- Choisissez l'onglet « **routage & réseaux** »
- Cliquez sur l'icône « **Limitation de domaine** »

Le principe est le suivant :



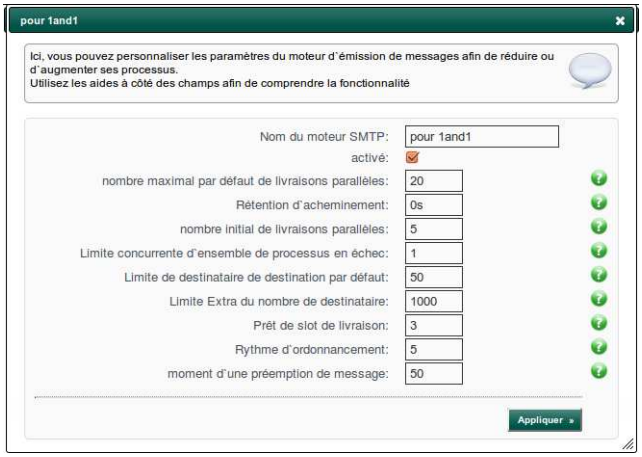
Vous créez en premier des démons de transmissions . Ces démons de transmission disposeront de paramètres de rétention personnalisés afin de réduire le processus d'acheminement ou bien, au contraire de l'augmenter.

Une fois que vous avez créer vos différents démons, vous aller affecter des domaines de destination à ces démons.

Création des démons

- Indiquez dans le formulaire, dans le champs « **Nom du moteur SMTP** » un nom afin que vous puissiez identifier votre moteur de transmission.
- Un démon sera alors ajouté dans la liste des démons avec des paramètres par défaut.
- Cliquez sur son nom dans le tableau afin de personnaliser ses paramètres.

Paramètres du démon



En cliquant sur le lien du démon, une page s'affiche vous permettant de modifier les processus d'acheminement qu'il va utiliser lorsqu'il devra procéder au transfert des messages vers un domaine.

nombre maximal par défaut de livraisons parallèles:

Par défaut le nombre maximal de livraisons parallèles vers la même destination.
Il s'agit de la limite par défaut à la livraison par lmtp, pipe, smtp et les agents de prestation virtuels.

Rétention d'acheminement:

Le temps de retardement qui est inséré entre les livraisons individuelles vers la même destination;
à la limite des destinataires par destination > 1, une destination est un domaine, sinon elle est un destinataire
Afin de permettre le délai, spécifier une valeur non nulle de temps (une valeur entière, plus éventuellement un suffixe à une lettre qui indique l'unité de temps)
Les unités de temps:. s (secondes), m (minutes), h (heures), d (jours), w (semaines). L`unité de temps par défaut est s (secondes).

nombre initial de livraisons parallèles:

Le nombre initial de livraisons parallèles vers la même destination. Cette limite s'applique aux livraisons via les agents de livraison smtp, pipe et virtual.
Attention : avec une valeur fixée à 1, un seul message incorrect peut suffire à bloquer le courrier de tout un site.

Limite de destinataire de destination par défaut:

Nombre maximum de destinataires par livraison.
Ceci est la limite par défaut pour la livraison via les agents lmtp, pipe, smtp et virtual delivery.
L'établissement de ce paramètre à une valeur de 1 change la signification de la correspondance de la limite de simultanéité par destination depuis la simultanéité par domaine dans la simultanéité par destinataires

Limite Extra du nombre de destinataire:

Valeur par défaut de la limite extra de chaque transport imposée au nombre de destinataires en mémoire. Cet espace destinataire extra est réservé pour le cas ou l'ordonnanceur du gestionnaire des files d'attente de Postfix donne la priorité à un message sur un autre et soudainement requiert d'autres slot destinataires pour ce message pour éviter une dégradation des performances.

Prêt de slot de livraison:

paramètre:default_delivery_slot_loan
Ce paramètre détermine le moment où une préemption de message peut avoir lieu. Au lieu d'attendre que le compteur ait atteint la valeur désirée, la préemption peut arriver lorsque transport_delivery_slot_discount% de la valeur requise plus transport_delivery_slot_loan restent à accumuler. Notez que la valeur totale doit être atteinte avant qu'une autre préemption puisse avoir lieu ultérieurement.

Rythme d'ordonnancement:

Rythme où l'ordonnanceur du gestionnaire des files d'attente de Postfix est autorisé à donner la priorité à un message sur un autre.

Chaque transport maintient un "compteur de slot de livraison valide" pour chaque message.

Un message peut prendre la priorité à un autre lorsqu`il peut être livré sans utiliser plus de slot (c`est à dire des invocations d`agents de livraison) que le compteur de message courant a accumulé (ou va accumuler - voir plus loin).

Ce paramètre contrôle à quel rythme ce compteur est incrémenté - ceci arrive chaque fois que default_delivery_slot_cost destinataires ont été livrés. Le coût 0 est utilisé pour désactiver le droit de préemption.

La valeur minimale que l`algorythme de l`ordonnanceur peut utiliser est 2 - utilisez-la si vous voulez maximiser la rapidité de transfert des messages. B

ien qu`il n`y ai pas de maximum, les valeurs élevées telles 50 n`ont aucun sens.

La seule raison pour laquelle 2 n`est pas la valeur par défaut est qu`il affecte le livraison des listes de diffusion.

Dans le pire des cas, leur temps de livraison peut prendre entre (coût 1/coût) et (coût/coût-1) plus de temps que si le droit de préemption est désactivé.

La valeur par défaut 5 est un compromis raisonnable évitant que les livraisons des listes de diffusions ne soient ralenties de 20 à 25% dans le pire des cas.

moment d'une préemption de message:

paramètre:default_delivery_slot_discount

Ce paramètre détermine le moment où une préemption de message peut avoir lieu.

Au lieu d'attendre que le compteur ait atteint la valeur désirée, la préemption peut arriver lorsque transport_delivery_slot_discount% de la valeur requise plus transport_delivery_slot_loan restent à accumuler.

Notez que la valeur totale doit être atteinte avant qu'une autre préemption puisse avoir lieu ultérieurement.

Ajouter des domaines aux démons de transmission

Cette opération consiste à faire correspondre des domaines de destination aux démons de transmission que vous avez personnalisé.

Ainsi, lorsqu'un message doit être émis à destination de l'un de ces domaines, les moteur utilisera les paramètres spécifiés.

Cliquez sur l'onglet « Domaines à router »

Sélectionnez dans la liste déroulante le démon précédemment ajouté et indiquez dans le champs le domaine qui sera affecté.

La rotation TCP/IP

Qu'est-ce ?

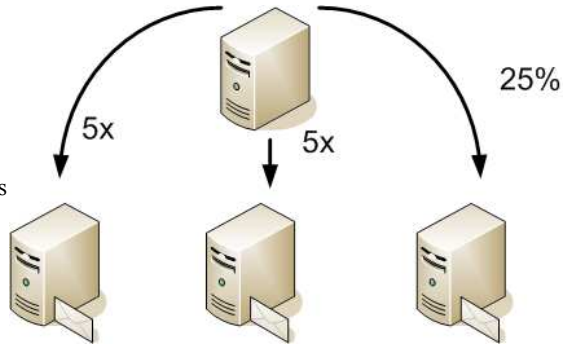
La rotation TCP/IP utilise le pare-feu local afin de fournir un système de rotation des connexions SMTP vers plusieurs relais de messagerie.

Les relais de messagerie peuvent être internes (avec l'utilisation des instances multiples) ou bien externe, vers d'autres serveurs.

Différentes utilisations.

On peut effectuer une rotation « externe » permettant de transférer les connexions SMTP vers plus autres « serveurs » relais.

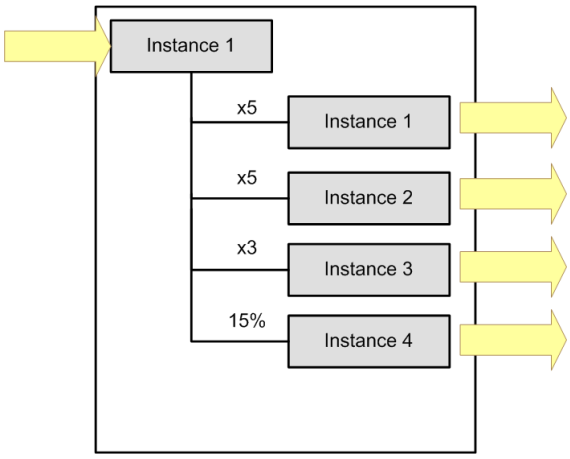
Dans cet exemple, le serveur qui reçoit les connexions transfert les connexions au bout de 5 sessions SMTP vers le serveur 1, 5 sessions SMTP vers le serveur 2 et 25% de chances vers le serveur 3



On peut effectuer une rotation « interne » en utilisant les différentes instances Postfix crées.

Dans cette approche notre instance 1 reçoit les connexions SMTP et les renvoi vers l'instance 1 ou 2 ou 3 ou 4 en fonction des statistiques du nombre session reçues.

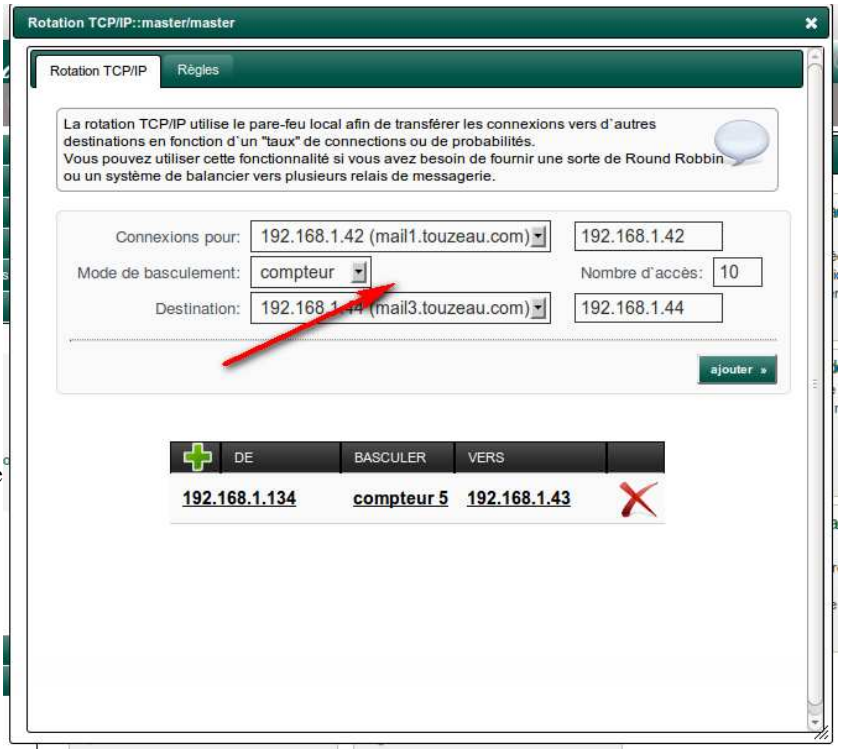
L'instance 4 : 25% veut dire 25% de chances de recevoir les connexions.



Mise en place avec Artica

- Dans le menu de gauche, sélectionnez **Messagerie** puis « **Config. Générale** »
- Choisissez l'onglet « **Routage & réseaux** »
- Cliquez sur l'image « **Rotation TCP/IP** »

Un nouveau formulaire s'affiche.



Le formulaire principale vous permet de créer ou d'éditer une nouvelle règle.

Le principe est simple :

Dans le champs « **Connexions pour** », vous indiquez l'adresse IP qui va recevoir les connexions SMTP.

Cette adresse fera alors office de « routeur »

Vous définissez le mode de basculement :

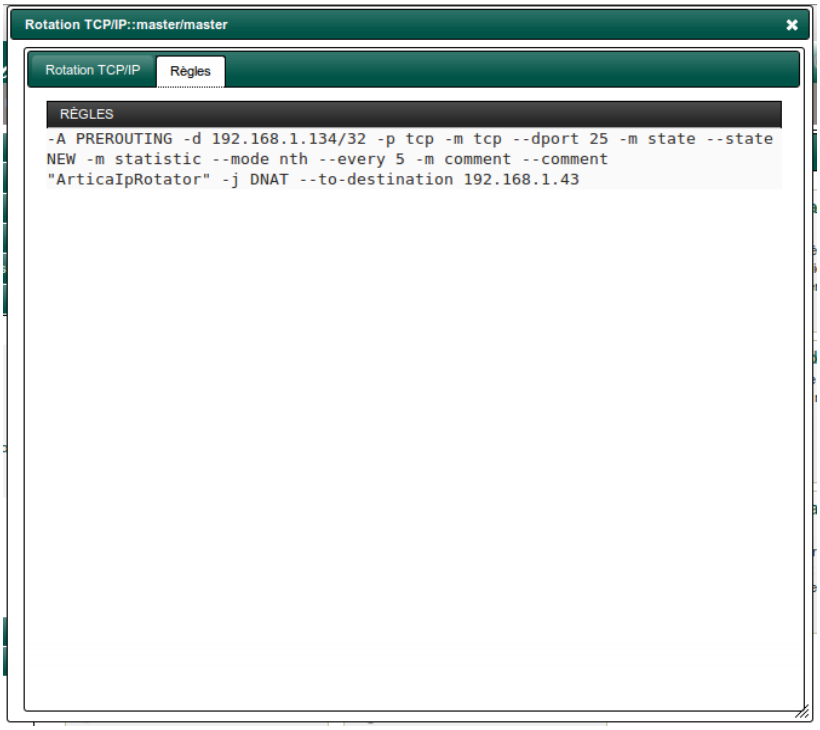
Compteur : au bout de combien de connexions, la connexion va être redirigée vers la destination.

Aléatoire : Combien de % de chances de nombre de connexions, la connexion va être redirigée vers la destination.

Destination : Indiquez ici l'adresse IP du serveur qui va recevoir la connexion SMTP redirigée.

Une fois que vous avez ajouté les règles de basculement, vous pouvez cliquer sur l'onglet « règles ».

Ceci vous permet de visualiser les différentes règles ajoutées au pare-feu.



Postfix Instant IpTables

« Postfix Instant IpTables » ou en français « Règles IpTables instantanées » permet de créer des règles de pare-feu sur un émetteur de façon instantanée en fonction d'évènements particuliers.

> *IpTables est un par-feu installé de base sur un système Linux.*
> *Sans le savoir un propriétaire d'un système Linux dispose déjà d'un pare-feux de très bonne qualité.*

Quel est l'intérêt ?

Beaucoup d'adresses d'émetteurs sont des spammeurs.

Même si les paramètres de Postfix, Kaspersky Anti-Spam, Spamassassin ou Amavis permettent de bloquer les messages provenant de ces adresses, **votre serveur se fatigue énormément**.

En effet, lorsqu'un spammeur connu tente d'envoyer un Spam, votre serveur effectue ces mécanismes :

1. Ouverture du port sur le démon Postfix.
2. Écriture des premières commandes SMTP.
3. Vérification DNS, résolution du nom d'hôte, voir envoi les premières commandes aux filtres additionnels.
4. Rejet de la connexion

Ces 4 opérations vont se répéter autant de fois que l'émetteur souhaite émettre un message.

Déchargez votre serveur !

Multipliez ces 4 opérations par 500 voir 600 adresses de Spammeurs en même temps et vous retrouvez votre serveur ne faire que :

- Rejeter des connexions
- Ne faire que des requêtes sur les serveurs DNBSL
- Augmenter sa charge par la création de PIPE(S) vers Amavis, spamassassin ou Kaspersky.

Même si à la finalité vous ne recevez pas de SPAM !

L'idée de cette technologie est d'endiguer le phénomène par la création d'une règle de pare-feu sur les adresses IP de Spammeurs « habitués » à vous émettre du spam.

De ce fait, le noyau interdit l'ouverture du port et aucun processus n'est alors alerté d'une connexion.

Ce principe se retrouve dans un produit bien connu nommé « Fail2Ban ». Toutefois Fail2ban ne propose pas l'esprit communautaire bien qu'il se peut qu'il soit intégré dans le futur.

Assurez une bande passante de qualité

L'intérêt supplémentaire est de pouvoir décharger la bande passante. En effet les ouvertures de connexion sur le serveur,aussi infimes soit-elles, consomment de la bande passante de façon globale.

De surcroît la bande passante utilisée est la bande passante « montante » (upload), celle qui dans le cas d'une connexion ADSL est très limitée (quelques kb/s)

Une règle de pare-feu enraye le phénomène définitivement.

Comment ca marche ?

Artica dispose d'un processus qui surveille en temps réel les évènements de Postfix « postfix-logger ».

Une succession d'expressions régulières permet à ce processus de détecter un comportement anormal d'un serveur émetteur.

> *Ce comportement anormal est notifié par Postfix mais cela ne veut pas dire que Postfix va rejeter la connexion. Il va simplement informer dans le système des évènements.*

1. Il va ranger ces comportements anormaux dans des catégories que vous pouvez visualiser à travers l'interface.
2. Chaque catégorie dispose d'un seuil maximal de comportement détecté.
3. Lorsque le serveur dépasse le seuil, alors une règle de pare-feu est automatiquement ajoutée et le serveur est rejeté d'un point de vue réseau définitivement.

Les règles créées se focalisent que sur le port 25...

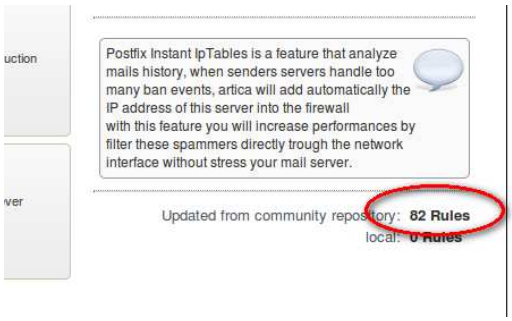
Esprit communautaire

L'idée du principe est de « prévenir » d'une éventuelle connexion d'une adresse de spammeur.

Aussi Artica met en place un système « communautaire automatique ».

À fréquences régulières (environ toutes les 300 minutes) , le script « exec.smtp-hack.export.php » est en charge d'exporter les règles que votre serveur à détecté vers le serveur central Artica et d'importer les règles des autres serveurs.

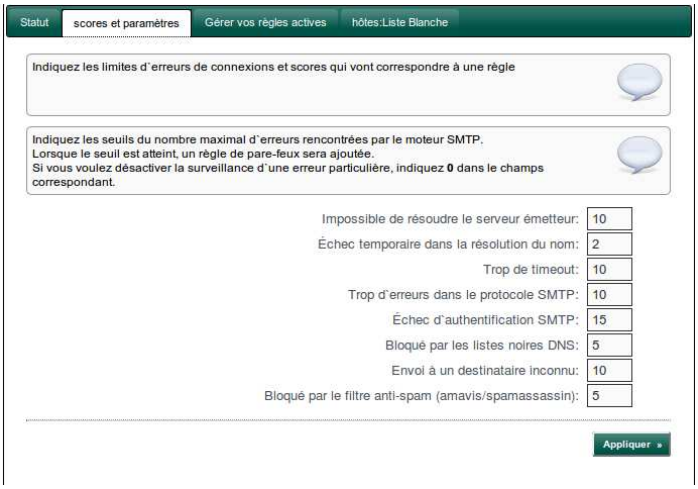
Au bout d'une heure environ, vous devriez retrouver des nouvelles règles dans le champ « communauté »



Mise en place avec Artica

- Dans le menu de gauche, sélectionnez « **messagerie** » puis « **Instant Iptables** »
- Passer le rond rouge à vert afin d'activer la fonctionnalité.

Personnaliser la sensibilité du scanner



L'onglet « **Scores et paramètres** » vous permet d'augmenter les seuils de détection et de création d'une règle automatique.

Le principe est simple :

Au bout de combien d'erreurs dans chaque catégorie l'adresse de l'émetteur sera bloquée ?

Si par exemple, vous indiquez la valeur « Trop de Timeout » à 2 , au bout de deux messages tentés d'être émis mais avec un temps d'émission des données trop long, le serveur sera définitivement bloqué.

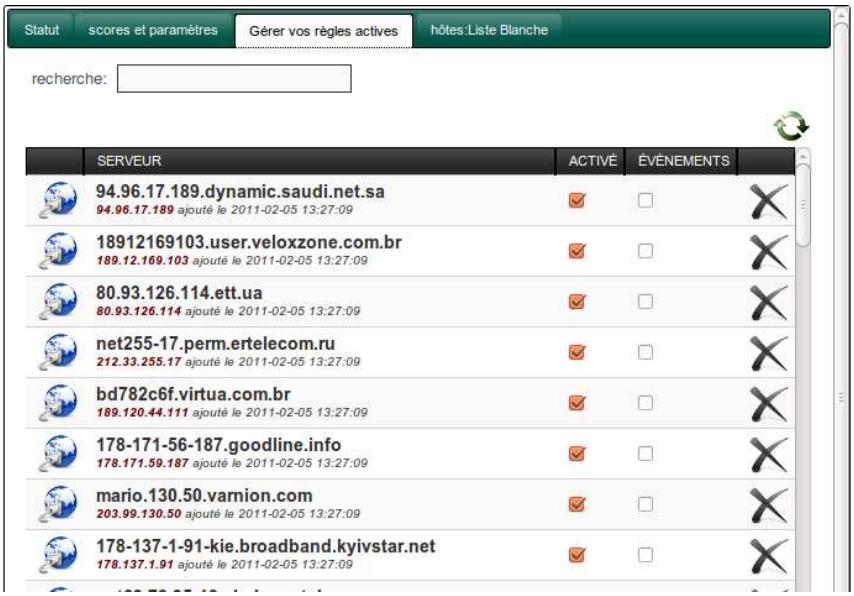
Visualiser , désactiver les règles.

L'onglet « Gérer vos règles actives » vous permet d'influer sur le comportement du pare-feu.

Remarquez que certaines règles dispose de l'icône de suppression « grisé ».

Cela veut dire que la règle provient de la « **communauté** ».

La supprimer n'a pas de sens puisqu'elle sera à nouveau ajoutée à la prochaine mise à jour.



Si vous désirez supprimer une règle de la « communauté »,

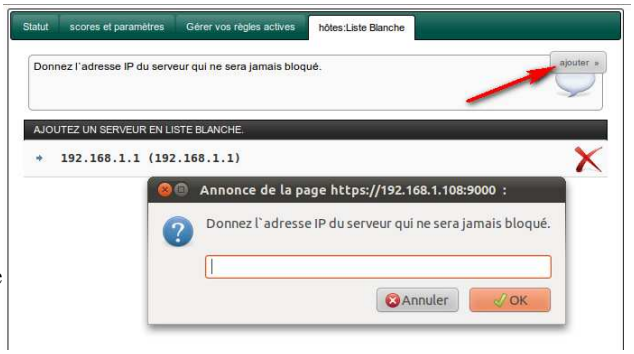
décochez alors la case « Activé » sur la règle. Elle sera alors retirée du pare-feu.

Listes blanches

Il se peut qu'un serveur de vos correspondants soit ajouté par le moteur. Mais comme vous le connaissez vous pouvez le désactiver complètement.

*En faites, la section « **Hôtes:Liste Blanche** » influe à la fois sur le moteur Instant IpTables mais aussi sur les autres filtres associés.*

Cliquez sur le bouton « **ajouter** » et indiquez l'adresse IP de l'émetteur qui doit être mis en liste blanche.



PostScreen

Les Zombies et BotNets, 99% du Spam reçu.

La version 2.8 de Postfix dispose désormais d'une nouvelle fonctionnalité contre 99% du SPAM.

Cette fonctionnalité se présente sous la forme de 3 démons « postscreen » qui effectue des tests sur le protocole SMTP, « dnsblog » qui est charge des vérifications des émetteurs avec les serveurs de blacklist DNS et « tlsproxy » permettant de prendre en charge le STARTTLS du protocole SMTP.

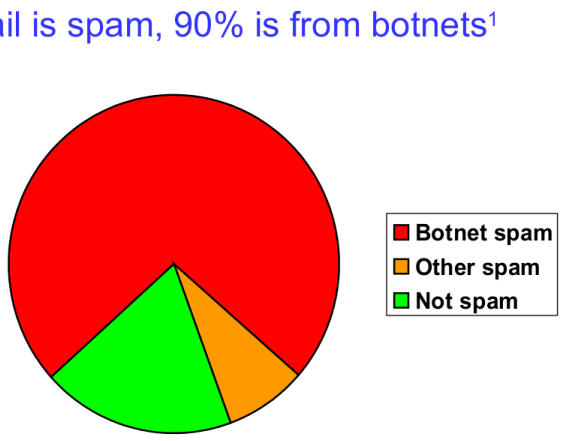
Wietse, le fondateur de Postfix dit : “Zombies suck the life out of the mail server.” pendant la conférence des serveurs de messagerie en 2009 en collaboration avec IBM research.

Il exprime en ces thermes que les Zombies ou Botnets sont la cause de 99% du spam reçu.

> *Les Zombies ou Botnets sont des programmes malicieux installés sur des ordinateurs dont le but est d'utiliser la puissance et la bande passante de son hôte afin d'envoyer des pourriels à toutes destinations.*

MessageLabs en 2008 confirmait déjà cette tendance.

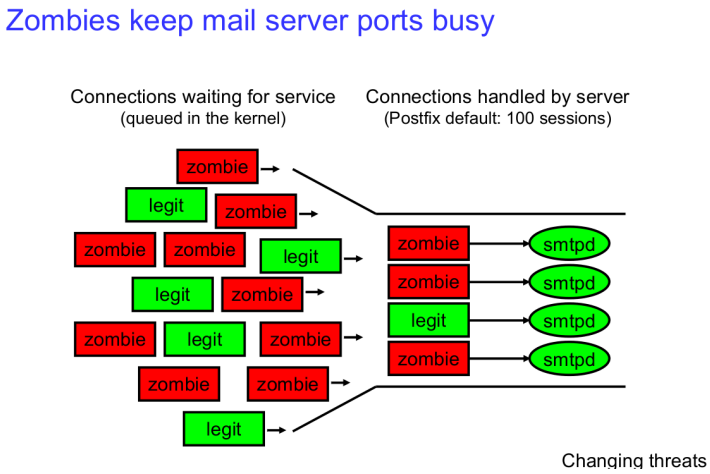
Celle-ci s'est amplifiée depuis...



[1]MessageLabs 2008 annual report

Même si des ressources et filtres sont ajoutés afin d'endiguer l'émission du SPAM, les zombies engorgent les connecteurs SMTP et ralentissent considérablement le traitement des messages de production.

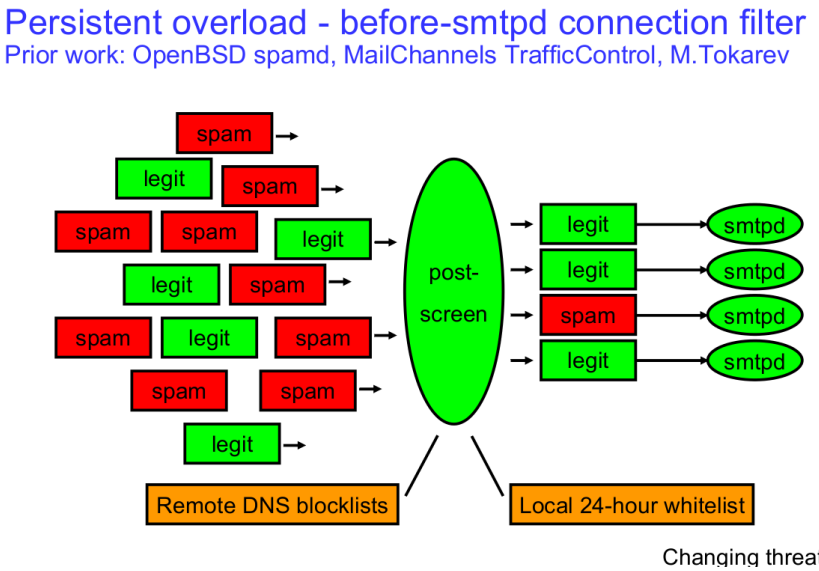
En effet, les connecteurs de sessions SMTP sont occupés à traités des connexions illégitimes.



Changing threats

PostScreen, une solution

Les recherches de Weitse, l'ont amené à élaborer un nouveau processus qui sera en charge d'effectuer un filtre en amont des connecteurs SMTP.



Ce démon est développé afin d'effectuer des vérifications rapides pour déterminer si l'émetteur est un Zombie ou pas.

Ces tests rapides sont accompagnés d'une gestion de cache qui assure un bon niveau de performances de traitement.

Les différents tests effectués par PostScreen

PostScreen s'attarde sur 4 niveaux de vérifications :

Les lignes « vides »

Le protocole SMTP est une protocole qui utilise des retours chariots de type CRL+LF avec un taille de ligne déterminée.

Beaucoup de Botnets corromps cette « tradition » par l'utilisation unique d'un LF. Cette forme de fin de ligne est souvent acceptée par les serveurs de messagerie.

Cette première détection permet de rejeter un grand nombre d'émetteurs « non-conformes »

Le half-duplex

Le protocole SMTP est un protocole de communication bi-latérale, l'émetteur se doit d'envoyer une commande SMTP et d'en attendre la réponse du récepteur.

Pour les botnets, il est plus facile d'envoyer les commandes SMTP et les données du message en une seule fois dans la session SMTP en lieu et place d'un vrai processus de communication avec le serveur récepteur (ce qui complique la codification d'un moteur de messagerie et alourdit le code viral).

Cette seconde détection détermine si l'émetteur du message utilise les normes de communication et est développé en tant que vrai processus d'émission de message.

Les commandes NON-SMTP

Beaucoup de BotNets utilisent un proxy pour sortir sur Internet afin d'émettre des messages de Spam.

L'utilisation d'un proxy rajoute des commandes non standard comme « CONNECT », « GET »... Ces commandes relatives au protocole HTTP sont généralement ignorées par les serveurs de messagerie et les messages peuvent être transmis.

Dans le cadre de l'utilisation de PostScreen, la détection de ces commandes assurent le rejet de la session SMTP et endigue le SPAM.

Requêtes sur les serveurs DNS Blacklist

Les adresses réseau des mauvais émetteurs sont référencés dans des bases disponibles sur Internet et pouvant être consultées par le protocole DNS.

PostScreen via le démon dnsblog permet de consulter ces bases et de s'assurer que l' émetteur n'est pas référencé en tant que mauvais émetteur.

L'association de cette techologie avec un outil Anti-Spam de « contenu » tel que SpamAssassin ou Kaspersky Anti-Spam permet de rapprocher le taux de rejet de pourriels à 100%

Artica assure le maintient et la mise en place de ces technologies.

La mise en place de PostScreen dans Artica à la fois supportée en utilisant une seule instance du moteur Postfix mais aussi en utilisant le principe des multi-instances.

Vous pouvez retrouver les déclarations de Weitse sur PostScreen à cette adresse : http://www.artica.fr/download/postscreen.pdf et

La documentation en ligne technique et mise en place en ligne de commande à cette adresse :

http://www.postfix.org/POSTSCREEN_README.html

Mise en place de PostScreen

Vous devez vous assurer que votre serveur Postfix est en version 2.8.

Utilisez alors le gestionnaire d'installation afin de mettre à jour Postfix.

Une fois cette opération et après avoir « vidé le cache de la console », placez-vous dans la section « **Paramètres de sécurité** »

Un nouvel icône « **PostScreen** » apparaît. Cliquez sur cet icône.

Activez le service PostScreen en passant en vert le rond rouge et cliquez sur « **appliquer** »

Les protocoles de tests

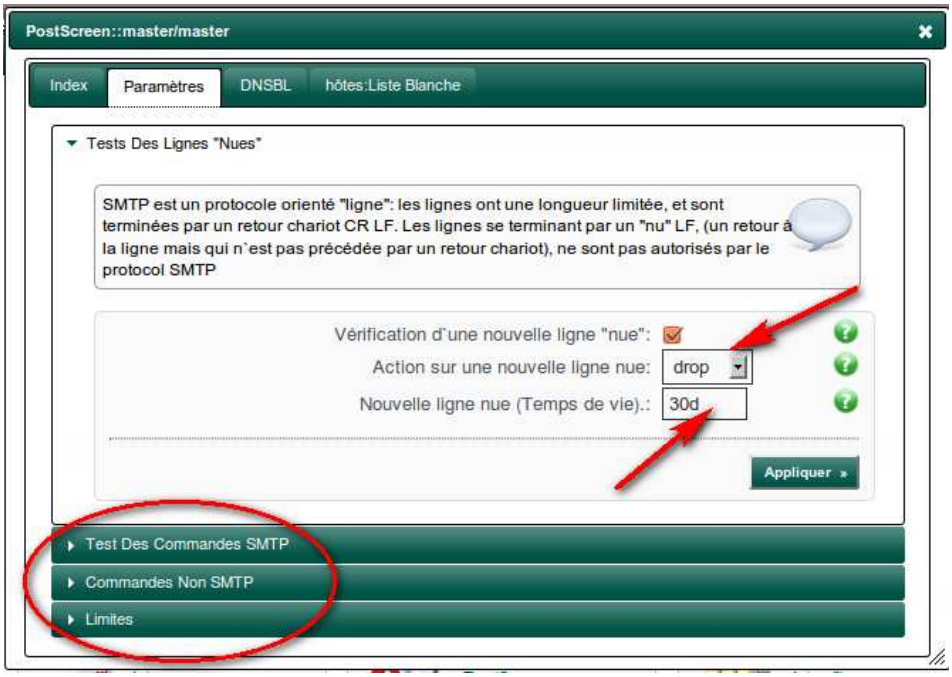
Cliquez sur l'onglet « **Paramètres** »

Dans cette section vous pourrez activer ou désactiver les **3 principaux protocoles** de tests de PostScreen :

> *Les lignes « nues » (non CR+LF), les commandes SMTP (half-duplex) et les commandes Non SMTP.*

Chaque protocole de test vous permet de définir une action à entreprendre si le serveur émetteur fait correspondre une détection.

- « **drop** » : rejette la session et met en cache, le rejet. A la prochaine connexion, l'émetteur sera directement rejeté sans le tester.
- « **ignore** » : une trace est générée dans les logs mais le serveur passe au protocole de test suivant, très utile pour tester avant de bloquer.
- « **enforce** » : Autorise PostScreen à lancer les autres vérifications mais rejettera les tentatives de livraison des courriers en émettant une réponse SMTP 550, inscrit les informations dans le journal. Il n'y a pas de mise en cache, a la prochaine tentatives ce test sera à nouveau effectué.



Chaque protocole de test dispose d'un « **temps de vie** » (ou TTL). Le résulat est alors enregistré pendant un période déterminée ce qui permet à PostScreen de ne pas refaire le test à la prochaine connexion.
Le serveur sera rejeté ou accepté directement si il revient émettre un message.

Les serveurs de blacklist DNSBL

Cliquez sur l'onglet « **DNSBL** »

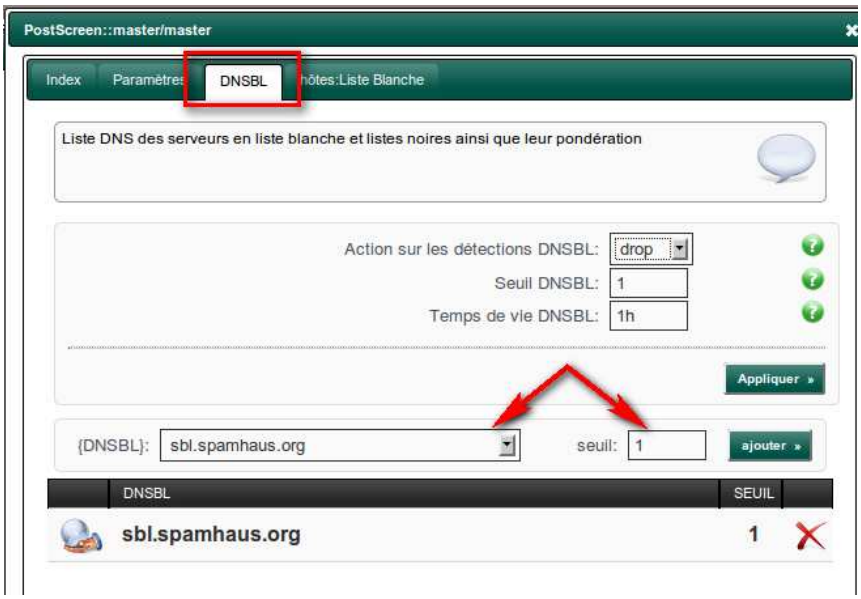
Cette section vous permet d'ajouter des services sur Internet nommés serveurs DNS de Blacklist (DNSBL) qui seront questionnés par PostScreen à chaque connexion d'un nouvel émetteur de messages.

Indiquez un note globale des réponses DNSBL dans le champ « Seuil DNSBL ».

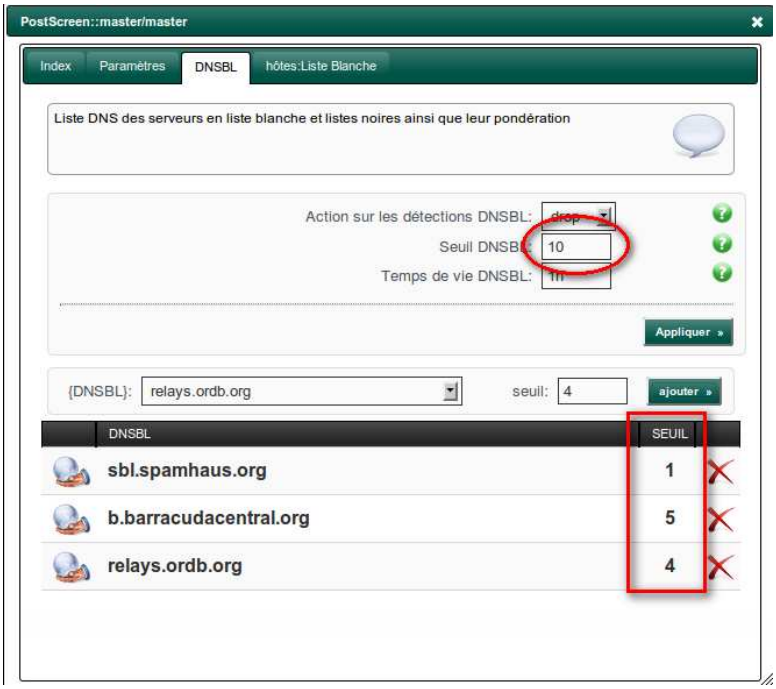
Par exemple, si vous indiquez 5, le serveur émetteur devra disposer de 5 points pour être rejetés.

Utilisez la liste déroulante DNSBL qui vous permet d'ajouter les serveurs DNS de base de données.

Ajoutez un point de détection dans le champs « seuil »



Dans notre exemple précédent si nous indiquons une note globale de 5, l'émetteur doit, par exemple, correspondre à 5 serveurs de listes avec une note de 1 ou bien deux serveurs de liste dont la première note est 3 et la deuxième note est 2



Cette méthode permet de faire confiance à la totalité des serveur de blacklist avec des préférences afin d'éviter le principes des « fausses alertes » à travers un serveur de liste qui n'est pas mis à jour régulièrement

Le VIPTrack

Une fonctionnalité politique qui assure le service Informatique.

Certaines personnes dans l'entreprise disposent d'un poste associé à la messagerie plus ou moins important.

Lorsque des personnes importantes sont en attente de réception ou envoient des dossiers importants par messagerie, il est crucial que le ou les responsables des maillons de la messagerie soient informés d'une quelconque défaillance.

Ceci afin de prévenir la personne avant qu'elle s'en inquiète.

Nous indiquons le mot « politique » dans le titre car bien entendu, un Directeur Général ou un Directeur commercial n'a pas le même poids lorsque celui-ci s'inquiète qu'un message tant attendu n'a pas été reçu .

Le fait que les responsables de la messagerie anticipe cette inquiétude voir étudie le problème assure un service informatique professionnel et de qualité auprès de ces personnes influentes.

Bien sur la fonctionnalité peut s'étendre à d'autres adresses que celle des VIP mais nous resteront dans ce sujet.

La fonctionnalité VIPTrack permet d'effectuer deux choses :

Informer l'administrateur que des messages sont restés dans la file d'attente du relais de messagerie

Un message qui doit être transmit doit rester que quelques secondes dans la file d'attente.

Toutefois une faute d'orthographe dans l'adresse eMail destinatrice ou bien un serveur destinataire « malade » force le relais à mettre en attente le message et réitère les tentatives de transmission toutes les X minutes.

Or le VIP en question n'est pas au courant que le message qu'il à émis n'est pas encore arrivé à destination.

VIPTrack informe alors par notification email qu'un message provenant d'un VIP reste anormalement dans la file d'attente.

Charge alors à l'administrateur d'effectuer les opérations d'information auprès du VIP ou bien de corriger le problème d'acheminement.

Créer des rapports réguliers de messages bloqués entrants/sortants.

Si des filtres anti-spam, antivirus, de connexion sont mis en place, il se peut que des messages légitimes soient bloqués par la passerelle.

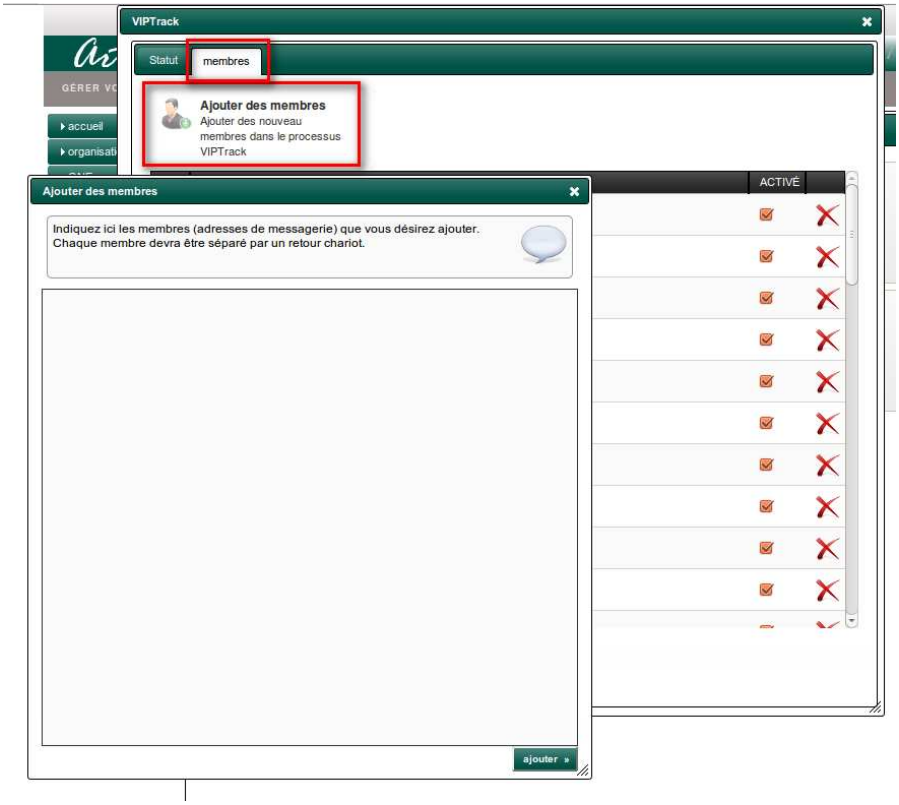
Soit parce que l'expéditeur ne répond pas au normes SMTP (blacklist, mauvaise communication SMTP, virus...), soit parce que des règles spécifiques sont en inadéquation avec l'habitude de communication du VIP.

VIPTrack émet alors des rapports et informe par eMails de la liste des messages bloqués entrants et/ou sortants et des quarantaines stockées par VIP.

Mise en place de VIPTrack

La mise ne place est assez simple.

- Munissez-vous de la liste des adresses Email des personnes importantes ou à surveiller.
- Dans le menu de gauche, choisissez « Messagerie » puis « Config. Générale »
- Au centre, choisissez l'onglet « Paramètres de sécurité »
- Cliquez sur l'image « VIPTrack »



- Cliquez sur l'onglet « Membres » puis sur l 'image « Ajouter des membres »
- Dans la nouvelle interface, mettez avec des retours chariots les adresses eMails précédemment choisies.
- Une fois les adresses ajoutés, vos membres seront affichés dans un tableau.
- Vous serez alors en mesure de les désactiver ou de les supprimer.

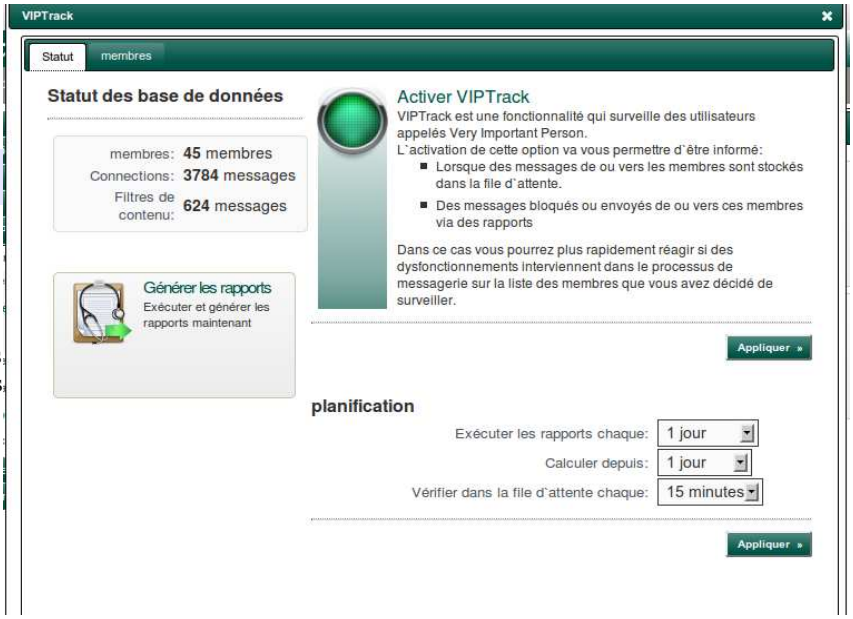
Activation et Réglages de l'ordonnancement

Passer le bouton « **Activer VIPTrack** » en vert puis cliquez sur Appliquer.

La fonctionnalité est alors en exécution.

Sous le titre « planification » vous disposez de 3 listes déroulantes.

Exécuter les rapports chaque et calculer depuis



Indique la fréquence d'exécution des rapports e synthèse sur les messages bloqués en entrée et en sortie pour chaque membre depuis X heure.

> *Si aucun message n'est bloqué il n'y aura pas de rapport envoyé.*

Par exemple, vous pouvez Exécuter les rapports chaque 1 jour calculer depuis 1 jour.

Ceci aura pour conséquence que les rapports seront envoyés toutes les 24 heures avec les derniers messages détectés et transmis pour/par le VIP depuis les dernières 24H

Vérifier dans la file d'attente chaque :

Ce paramètre indique la fréquence de parcours de la file d'attente afin de vérifier si un message à destination d'un VIP ou depuis un VIP n'est pas stocké dans la file d'attente.

Si tel est le cas, une notification est alors envoyée.

Dans notre exemple, cette fonctionnalité est exécutée toutes les 15Minutes.

Vous pouvez ne pas attendre l'ordonnancement afin de vérifier comment les rapports sont générés, il vous suffit simplement de cliquer sur « Générer les rapports » pour exécuter VIPTrack tout de suite.

Postfwd un pare-feu de la messagerie

Postfwd est un serveur de « délégation de règles».

Postfix, le MTA principal permet de crocheter son processus de communication lors de l'établissement d'un session SMTP.

On appelle se type de crochetage la « **Policy delegation** ».

Postfix envoi au serveur de politiques quelques informations et il en attend un réponse.

Cette réponse peut être un rejet, une acception ou l'émission d'une erreur.

Postfix émet les informations comme ceci :

```
content_filter: smtp-amavis:[127.0.0.1]:10024
named_attribute: rewrite_context=remote
sender: aaaa@live.com
named_attribute: log_client_name=col0-omc2-s15.col0.hotmail.com
named_attribute: log_client_address=65.55.34.89
named_attribute: log_client_port=24710
named_attribute: log_message_origin=col0-omc2-s15.col0.hotmail.com[65.55.34.89]
named_attribute: log_helo_name=col0-omc2-s15.col0.hotmail.com
named_attribute: log_protocol_name=ESMTP
named_attribute: client_name=col0-omc2-s15.col0.hotmail.com
named_attribute: reverse_client_name=rcol0-omc2-s15.col0.hotmail.com
named_attribute: client_address=65.55.34.89
named_attribute: client_port=24710
named_attribute: helo_name=col0-omc2-s15.col0.hotmail.com
named_attribute: protocol_name=ESMTP
named_attribute: client_address_type=2
warning_message_time: Wed Apr 27 17:40:23 2011
named_attribute: dsn_orig_rcpt=rfc822;aaa@mydomain.com
original_recipient: aaa@mydomain.com
recipient: aaaa@mydomain.com
```

A partir de ces informations, un processus de délégation de règles peut intervenir et décider si oui ou non le message doit continuer son acheminement.

Postfwd est donc un serveur de politiques qui est installé de base dans les versions d'Artica supérieures à 1.5.042814

Il dispose d'un avantage majeur est que sont comportement permet d'établir des règles complexes et qui permettent de s'adapter à l'ensemble des besoins pour restreindre l'utilisation de la messagerie et les SPAMs.

Postfwd dans Artica.

Postfwd est présent à la fois lorsque vous utilisez un Artica en mode simple serveur ou bien en mode multiple-instances. (voir page 73 « Le multiple-instances »)

Ou trouver Postfwd en multiple-instances ? :

Choisissez votre relais SMTP et cliquez sur l'onglet « **Filtres (Anti-spam an...)** », activez le module « Règles de délégation », cliquez sur l'image « **Règles de délégation** »

Postfwd un pare-feu de la messagerie

Postfwd est un serveur de « délégation de règles».

Postfix, le MTA principal permet de crocheter son processus de communication lors de l'établissement d'un session SMTP.

On appelle se type de crochetage la « **Policy delegation** ».

Postfix envoi au serveur de politiques quelques informations et il en attend un réponse.

Cette réponse peut être un rejet, une acception ou l'émission d'une erreur.

Postfix émet les informations comme ceci :

```
content_filter: smtp-amavis:[127.0.0.1]:10024
named_attribute: rewrite_context=remote
sender: aaaa@live.com
named_attribute: log_client_name=col0-omc2-s15.col0.hotmail.com
named_attribute: log_client_address=65.55.34.89
named_attribute: log_client_port=24710
named_attribute: log_message_origin=col0-omc2-s15.col0.hotmail.com[65.55.34.89]
named_attribute: log_helo_name=col0-omc2-s15.col0.hotmail.com
named_attribute: log_protocol_name=ESMTP
named_attribute: client_name=col0-omc2-s15.col0.hotmail.com
named_attribute: reverse_client_name=rcol0-omc2-s15.col0.hotmail.com
named_attribute: client_address=65.55.34.89
named_attribute: client_port=24710
named_attribute: helo_name=col0-omc2-s15.col0.hotmail.com
named_attribute: protocol_name=ESMTP
named_attribute: client_address_type=2
warning_message_time: Wed Apr 27 17:40:23 2011
named_attribute: dsn_orig_rcpt=rfc822;aaa@mydomain.com
original_recipient: aaa@mydomain.com
recipient: aaaa@mydomain.com
```

A partir de ces informations, un processus de délégation de règles peut intervenir et décider si oui ou non le message doit continuer son acheminement.

Postfwd est donc un serveur de politiques qui est installé de base dans les versions d'Artica supérieures à 1.5.042814

Il dispose d'un avantage majeur est que sont comportement permet d'établir des règles complexes et qui permettent de s'adapter à l'ensemble des besoins pour restreindre l'utilisation de la messagerie et les SPAMs.

Postfwd dans Artica.

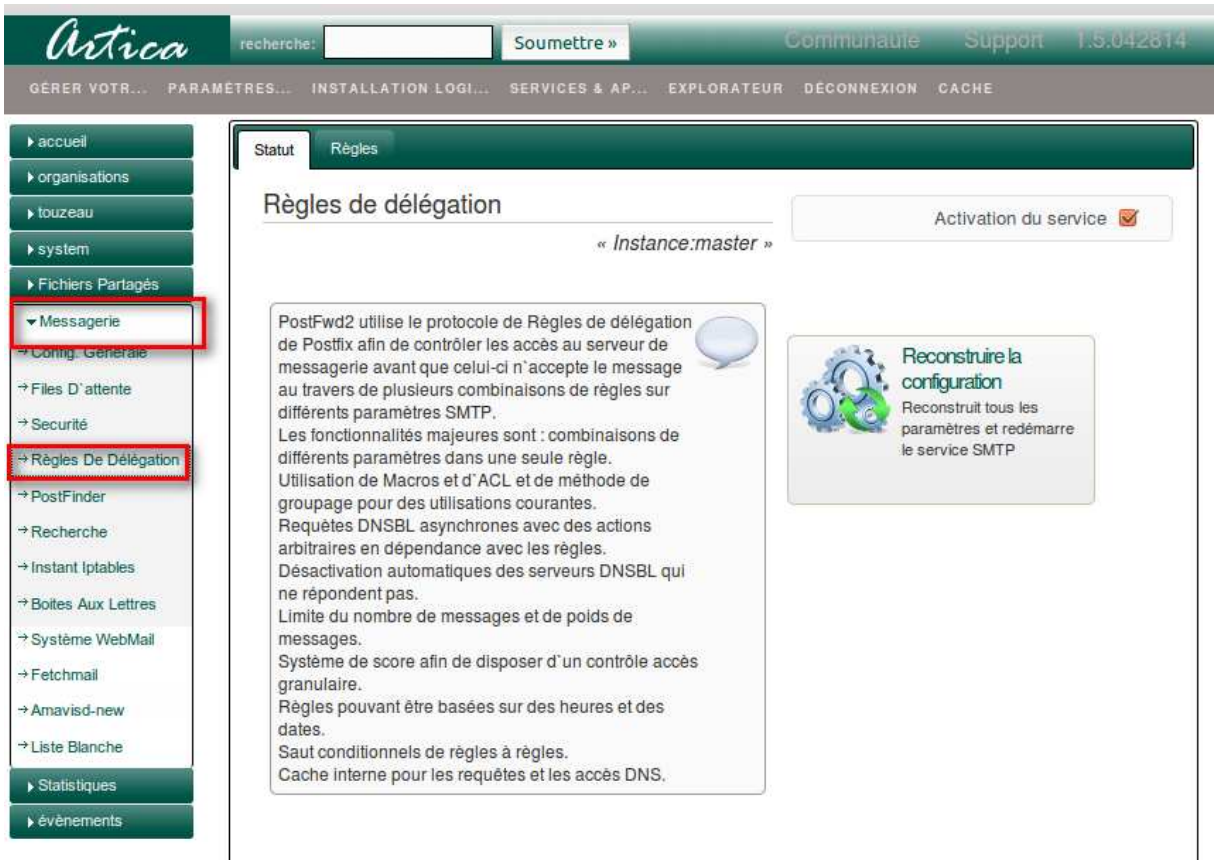
Postfwd est présent à la fois lorsque vous utilisez un Artica en mode simple serveur ou bien en mode multiple-instances. (voir page 73 « Le multiple-instances »)

Ou trouver Postfwd en multiple-instances ? :

Choisissez votre relais SMTP et cliquez sur l'onglet « **Filtres (Anti-spam an...)** », activez le module « Règles de délégation », cliquez sur l'image « **Règles de délégation** »

Ou trouver Postfwd en mono-instance ? :

Dans le menu de gauche, cliquez sur « **Messagerie** » puis « **Règles de délégation** »

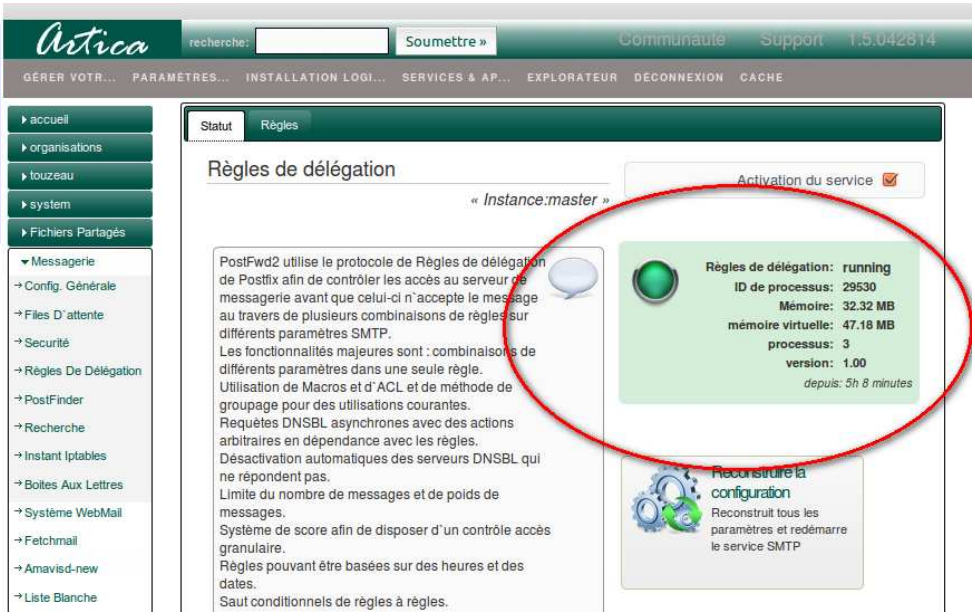


Mise en place.

Pour activer le service, cochez la case « **Activation du service** ».

Le service ne s'activera pas si il n'y pas de règles sauvegardées. Si vous activez le service avant d'avoir créé des règles, cliquez sur « Reconstruire la configuration » après avoir créé vos règles.

Si le service est activé et que des règles sont enregistrés, la page vous affichera un état du service.



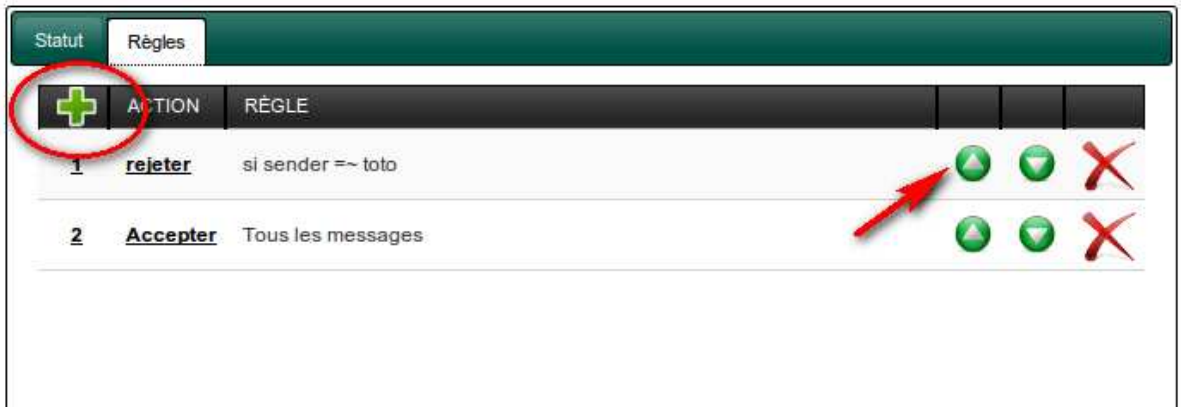
Les règles

Le principe des règles sont identiques à celle d'un pare-feu, la première règle qui correspond exécute l'action déterminée.

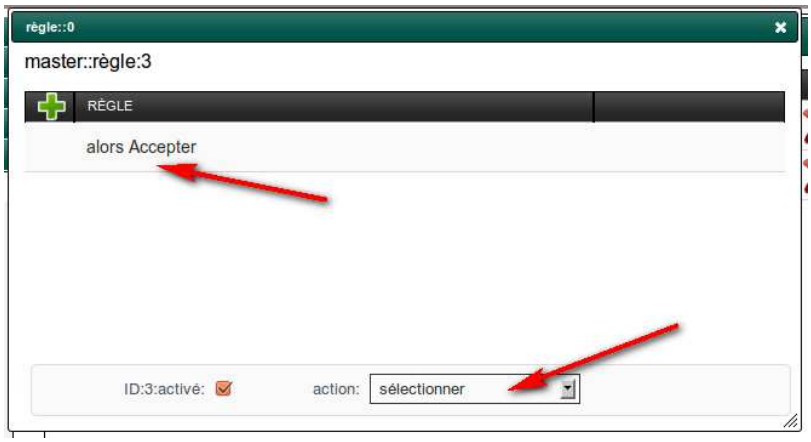
Une règle est une somme de vérification d'attributs qui aboutie à une action déterminée.

Des flèches vous permet de monter ou de descendre les règles afin d'accorder leur priorité dans leur lecture.

Pour ajouter une règle, cliquez sur le plus situé à gauche



Lorsque vous ajoutez une règle, l'interface écrit une nouvelle entrée qui,par défaut , accepte tous les messages.



Action de la règle.

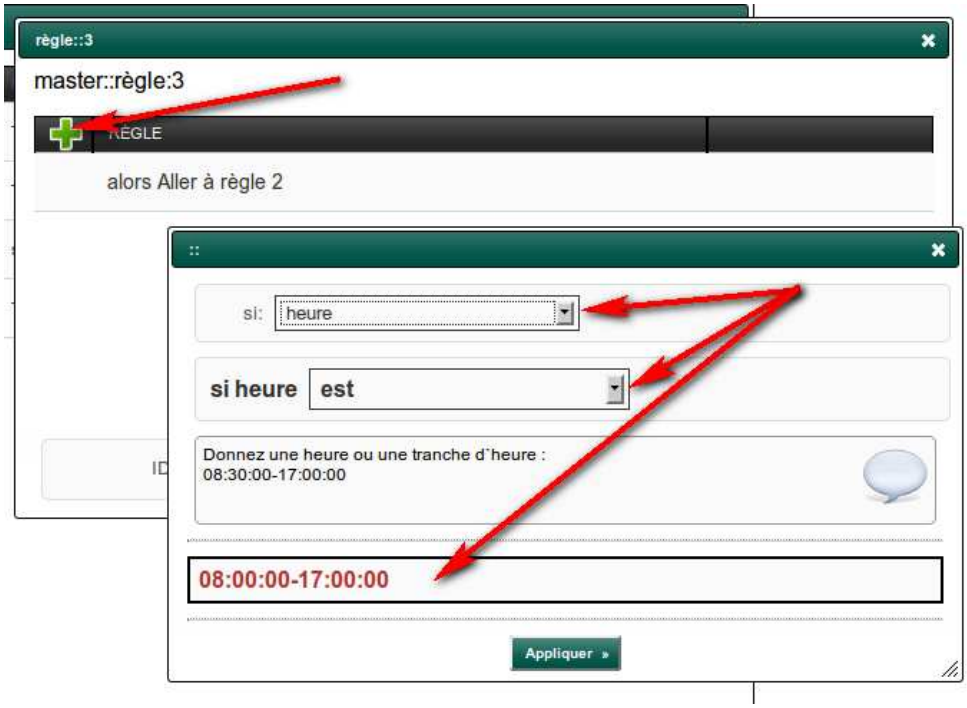
Utilisez la liste déroulante afin de spécifier qu'elle est la finalité de la règle.

Les possibilités sont les suivantes :

- **Aller à la règle X** : C'est au saut vers une autre règle.
- **Limite par taux d'émission** :Limite le nombre de messages par adresse de connexion sur un tranche en secondes.
- **Limite par taille** :Limite la somme des messages émis par adresse de connexion sur un tranche en secondes.
- **Limite par destinataires** : Limite le nombre de destinataires par adresse de connexion sur un tranche en secondes.
- **Rejeter** : Rejette le message
- **Accepter** : Laisse le message à d'autres processus.
- **Placer en file d'attente inactive** : La file d'attente inactive est une file d'attente sans réémissions automatiques.
- **Rediriger vers une autre adresse** : les destinataires sont remplacés par celui indiqué.
- **Limitation de domaine** : Utilise les limitations de domaines pré-enregistrées (voir page 82)

Attributs de détection

Afin de faire correspondre la règle, vous pouvez mettre en œuvre plusieurs attributs, cliquez sur le plus dans le tableau de la règle.



Une nouvelle boîte message d'affiche vous proposant de créer un attribut à détecter.

Un attribut peut être :

- **heure** : Une heure ou une tranche d'heure
- **jours** : Un jour ou des jours de la semaine
- **Mois** : Des mois ou un tranche de mois
- **RBL** : Une opération de vérification de listes noires
- **Comptage RBL** : Le résultat du comptage de vérification de listes noires
- **Adresse dans le HELO** : Adresse IP de l'hôte spécifiée lors du HELO (**`helo_name`**)
- **Nom de l'émetteur dans le HELO** :Nom de l'hôte spécifié lors du HELO (**`helo_address`**)
- **Nom du serveur** : Nom du serveur émetteur (**`sender_ns_names`**)
- **Adresse IP** : Adresse du serveur émetteur. (**`sender_ns_addrs`**)
- **MX Nom de serveur** : Nom du serveur émetteur lors de la résolution MX du domaine du destinataire. (**`sender_mx_names`**)
- **MX Adresse IP** : Adresse IP du serveur émetteur lors de la résolution MX du domaine du destinataire. (**`sender_mx_addrs`**)
- **Adresse du Client** : Adresse IP de connexion du serveur émetteur.(**`client_address`**)
- **Nom du client regex** : Nom d'hôte du serveur émetteur. (**`client_name`**)
- **Résolution inverse du nom** : Ce qu'a trouvé comme nom d'hôte le MTA avec l'adresse IP de connexion. (**`reverse_client_name`**)
- **Emetteur :** adresse eMail de l'émetteur. (**`sender`**)
- **Destinataire** : adresse eMail du destinataire.(**`recipient`**)
- **Nombre de destinataires** : Nombre des destinataires associés au destinataire principale (CC)
- **Taille du message** : Poids en bytes du message (entête et contenu).

Les opérateurs

Chaque attribut dispose d'opérateur afin de « comparer » et d'indiquer que la valeur de l'attribut active la règle.

Les opérateurs sont :

- est correspond à **=**
- est égale correspond à **==**
- N'est pas égale correspond à **!=**
- est supérieur correspond à **>=**
- N`est pas supérieur correspond à **!>=**
- est inférieur correspond à **=<**
- n`est pas inférieur correspond à **!=<**
- Correspond (regex) est un expression régulière
- Ne correspond pas (regex) ne correspond à une expression régulière.

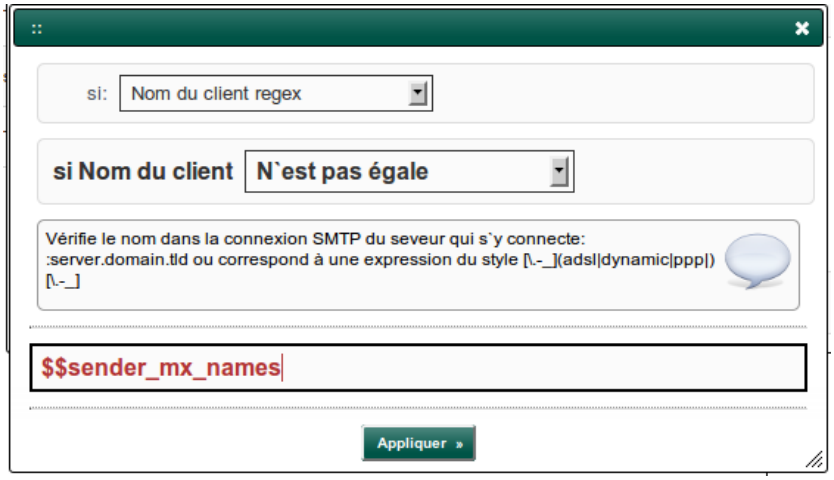
Les variables

Les variables est la possibilité de placer les valeurs des attributs et de les comparer elles sont précédées par **$$**

Si l'on souhaite par exemple valider que le nom de la résolution MX est égale/Pas égale au nom du serveur qui se connecte,

on indique ceci : « **Nom du client regex** » « **N'est pas égale** » **$$sender_mx_names**

dans l'interface



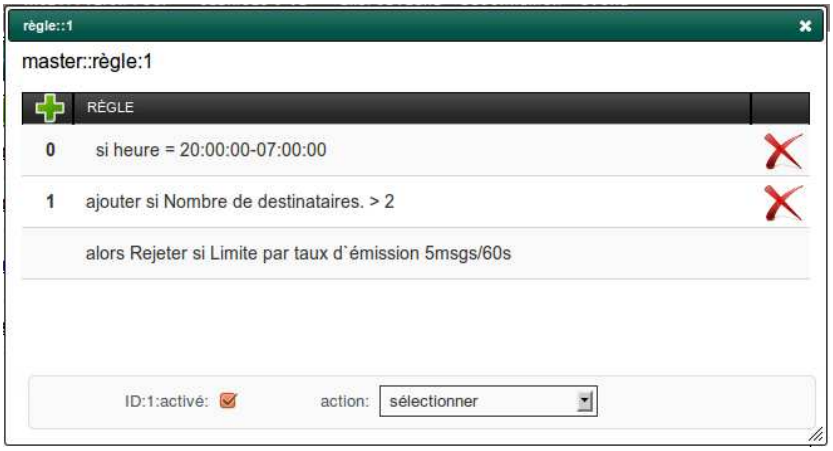
Les additions des attributs et exemples.

Les attributs s'additionnent, cette addition permet de « préciser » la règle afin de s'assurer de sa pertinence.

Admettons que nous souhaitions :

Uniquement activer de quota par session pour les émetteurs qui émettent des messages à plus de deux personnes et ceci en dehors des heures de bureau.

Nous allons donc utiliser deux attributs, l'heure et le nombre de destinataires



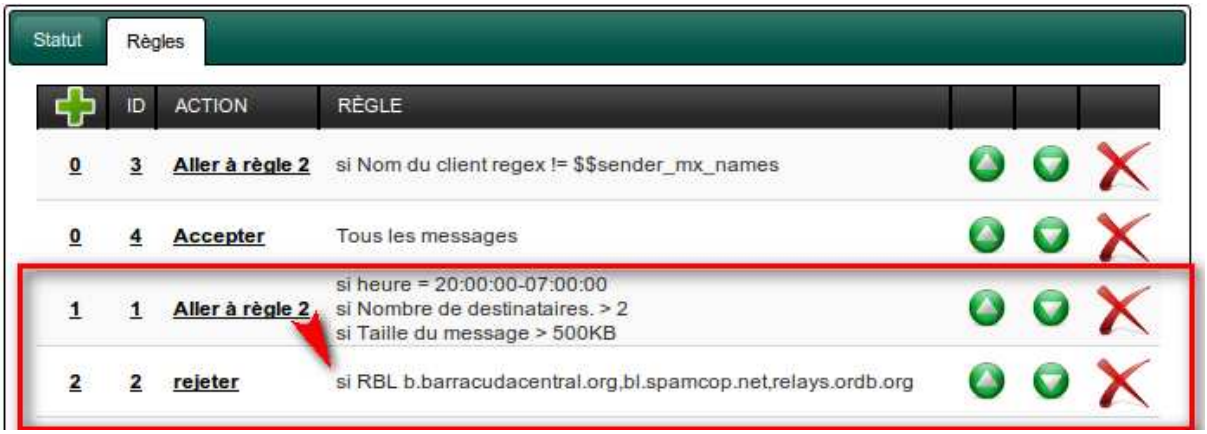
Les sauts de règles

Les sauts de règles sont très pratiques car il permettent d'offrir des conditions supplémentaires.

Admettons que nous souhaitions :

Uniquement Activer les RBL en dehors des heures de bureau et pour les messages d'un poids inférieur à 500Ko avec plus de deux destinataires

On peut effectuer une seule règle pour ceci mais on peut faire ceci :



Les scores

Les scores permettent de faire en sorte qu'une règle ne soit pas vorace, si le message correspond aux attributs on peut alors affecter une « note » à la règle.

Cette note peut être alors incrémentée, soustraite, divisée ou multipliée.

Lorsque le message arrive, il dispose d'un score de départ de 0 et ne devra pas dépasser un score de 5. (en cas de dépassement le message est alors rejeté).

La valeur doit être en format décimale ex:(0.01 or 1.5).

Vous pouvez incrémenter la valeur grâce à des opérateurs :

`+ n.nn` ajoute n.nn au score actuel

`-n.nn` soustrait n.nn au score actuel

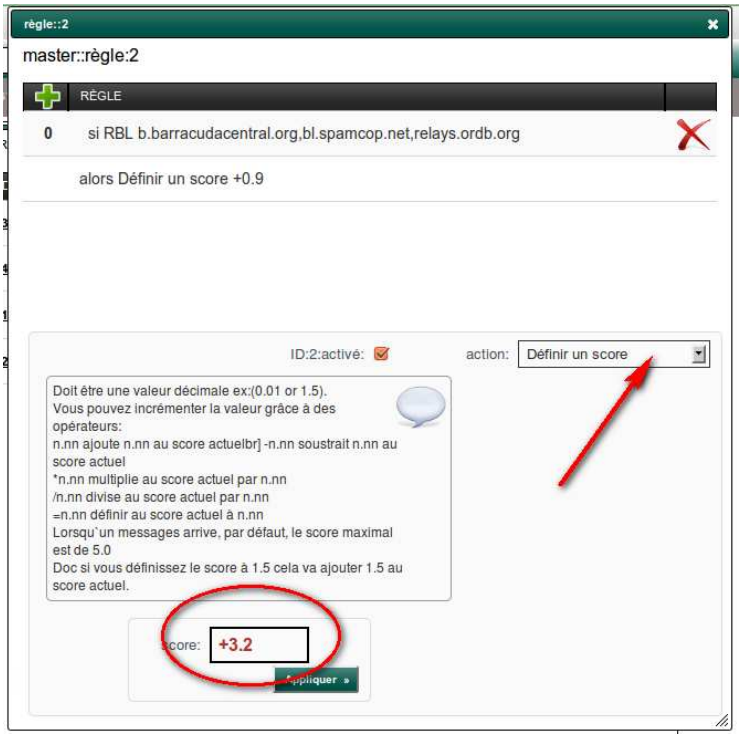
`*n.nn` multiplie au score actuel par n.nn

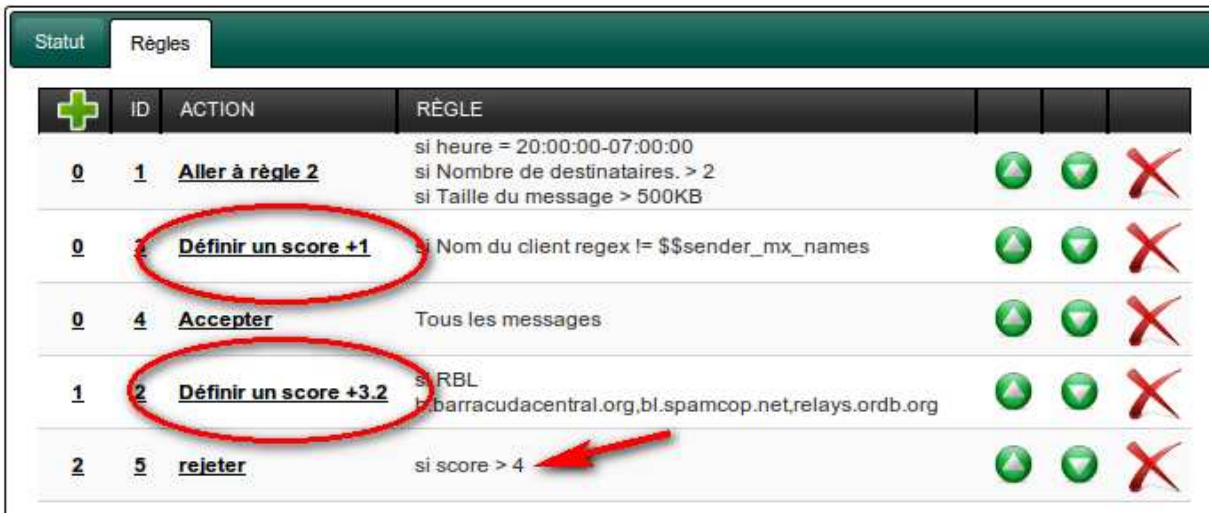
`/n.nn` divise au score actuel par n.nn

`n.nn` définir au score actuel à n.nn

Lorsqu'un messages arrive, par défaut, le score maximal est de 5.0

Donc si vous définissez le score à 1.5 cela va ajouter 1.5 au score actuel.

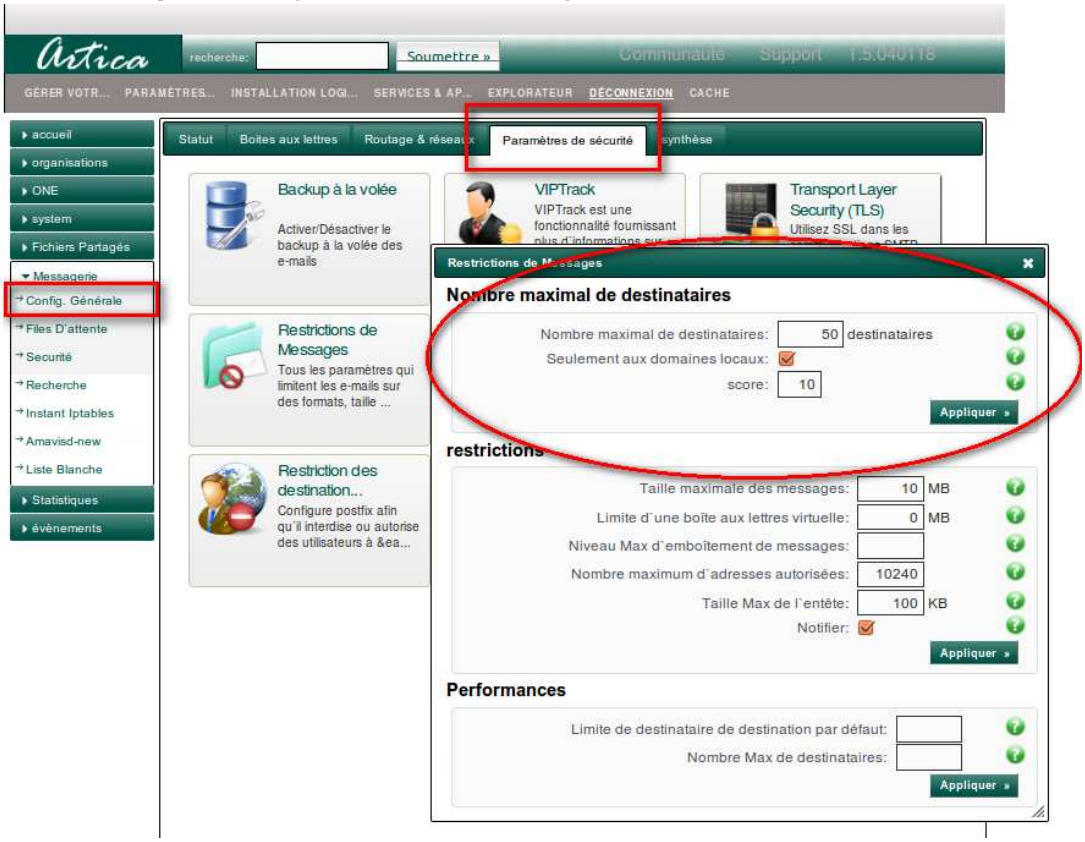




Nombre maximum de destinataires

Cette fonctionnalité permet de rejeter les messages si celui-ci est destination d'un trop grand nombre de destinataires et aussi dans les destinataires en copie (cc:). Le comportement de cette fonctionnalité **diffère** si vous avez installé et activé l'outil de filtrage de contenu Amavisd-new et Spamassassin.

L'option se trouve en cliquant sur « **Config. Générale** » dans le menu de gauche, puis en choisissant l'onglet « **Paramètres de sécurité** » et en cliquant sur l'image « **Restrictions de Messages** »



Une boîte message « **Restrictions de Messages** » s'affiche et vous propose une section « **Nombre Maximal de destinataires** »

Sans le filtre amavisd-new

Si vous n'avez pas activé ou installé le filtre amavisd-new, uniquement le champs « Nombre Maximal de destinataires » sera disponible.

Dans cette perspective les messages qui disposeront de plus de X destinataires dans le champs To ou CC seront alors **rejetés** par le serveur SMTP et un événement sera enregistré.

Avec le filtre amavisd-new

Dans le cas contraire, deux champs vous seront proposés.

Le premier « **Seulement aux domaines locaux** » indique que le filtre ne comptabilisera que les destinataires qui seront à destinations des domaines que le serveur est en charge d'acheminer.

Ainsi, un destinataire « Internet » ne sera pas comptabilisé.

La deux option « **score** » vous permet non pas de rejeter le message comme dans le premier comportement mais d'ajouter des points qui en s'ajoutant augmente le taux de jugement du message en tant que SPAM.

Par défaut, le filtre comprend que le message est un SPAM si il atteint un score de 6.35.

Dans l'exemple de la photo, on ajoute un score de 10, veut dire que le simple fait d'avoir plus de 50 destinataires va de toutes façon placer le message en catégorie SPAM.

En fonction du score, le message peut être alors placé en zone de quarantaine au lieu d'être simplement rejeté comme le premier comportement.

Listes Blanches

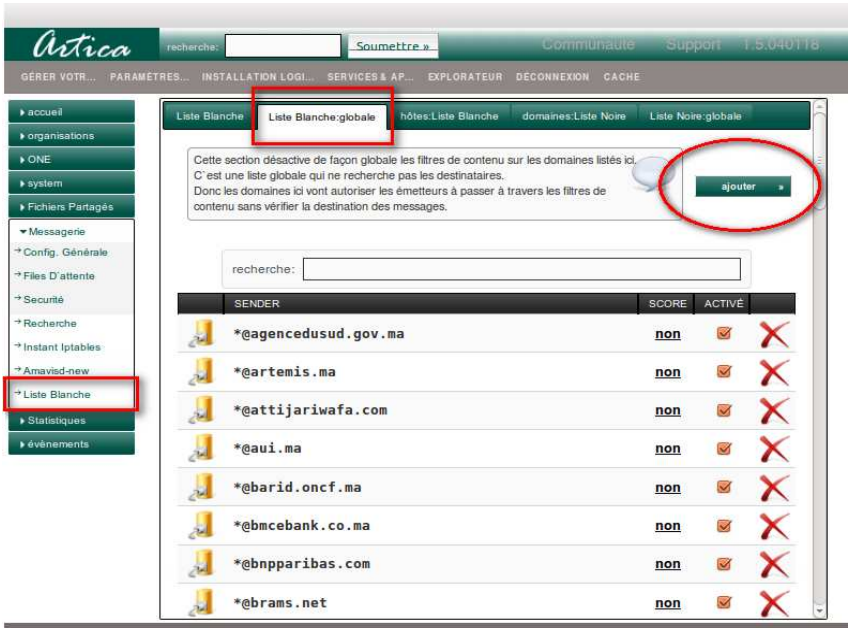
Liste blanche globale

La liste blanche globale permet à un message en fonction des expéditeurs de forcer les filtres de contenu à laisser passer le message.

> *Attention, cette liste ne tient pas en compte certains filtres qui effectuent des vérifications avant même de prendre la connaissance des expéditeurs.*

On y trouvera les filtres qui s'attardent sur les adresses de connexion comme PostScreen et les règles IP du MTA postfix.

Cette liste blanche se trouve lorsque vous cliquez sur le Menu de gauche « **Liste Blanche** » puis sur l'onglet « **Liste Blanche : Globale** »



Cette liste ne s'attarde pas non plus sur les destinataires. Ainsi un message « **provenant de** » sera considéré comme blanchit sans vérifier sa destination.

Pour ajouter des destinataires, cliquez sur le bouton **ajouter** :

Une nouvelle fenêtre s'affiche vous permettant d'ajouter une ou plusieurs entrées.

Mettez ici des domaines de messagerie ou des adresses (séparées par des retours chariots) que vous voulez autoriser et traverser les barrières de filtrage de **contenu**.
Vous pouvez indiquer les valeurs suivantes :
***@domain.tld** afin de bloquer tout le domaine domain.tld.
domain.tld afin de bloquer tout le domaine domain.tld.
@domain.tld afin de bloquer tout le domaine domain.tld.
user@domain.tld afin de bloquer l`émetteur user@domain.tld.

Remarquez dans la liste la colonne « **score** ». Cette colonne permet d'être moins permissif pour le filtre de contenu.

Par défaut, le filtre comprend que le message est un SPAM si il atteint un score de 6.35.

En ajoutant un score vous indiquez qu'un message provenant d'un expéditeur dispose de points supplémentaires par rapport à un destinataire inconnu.

Par exemple si un message provient de *@gmail.com il peut avoir 5 points supplémentaires avant d'être considéré comme SPAM;

Cela veut dire que le score devra atteindre 11.35 pour être considéré comme un SPAM en lieu et place des 6.35 habituels.

Liste de blanche des connexions

Cette liste assure le passage des messages à travers les **barrières de connexions**.

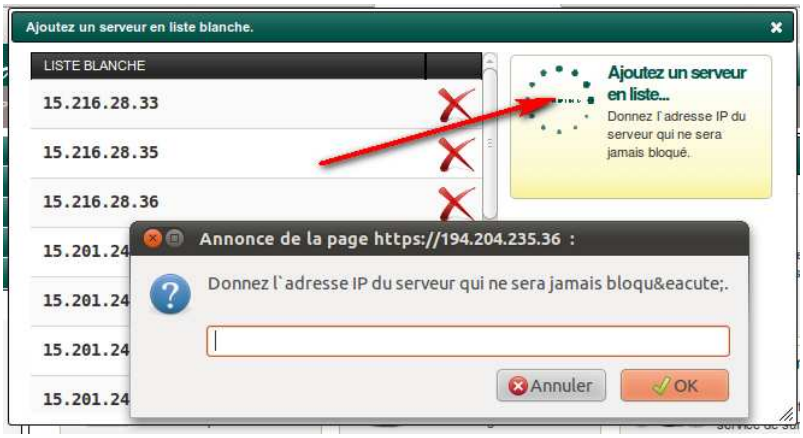
En effet, plusieurs filtres tels que PostScreen ou bien milter-greylist voir Instant IpTables s'attardent sur les adresses Ips des serveurs d'émission que le contenu du message.

Le nom de domaine des destinataires ou des expéditeurs n'est pas analysé par ces filtres.

Pour placer une adresse IP en liste blanche sur les filtres de connexion :

Dans le menu de gauche, cliquez sur « **Sécurité** », puis sur l'onglet « **Filtres de connexion** » et enfin sur l'image « **Ajoutez un serveur en liste blanche** »

Cliquez sur l'image « **Ajoutez un serveur...** » et indiquez l'adresse IP publique du serveur que vous désirez faire passer à travers les filtres.



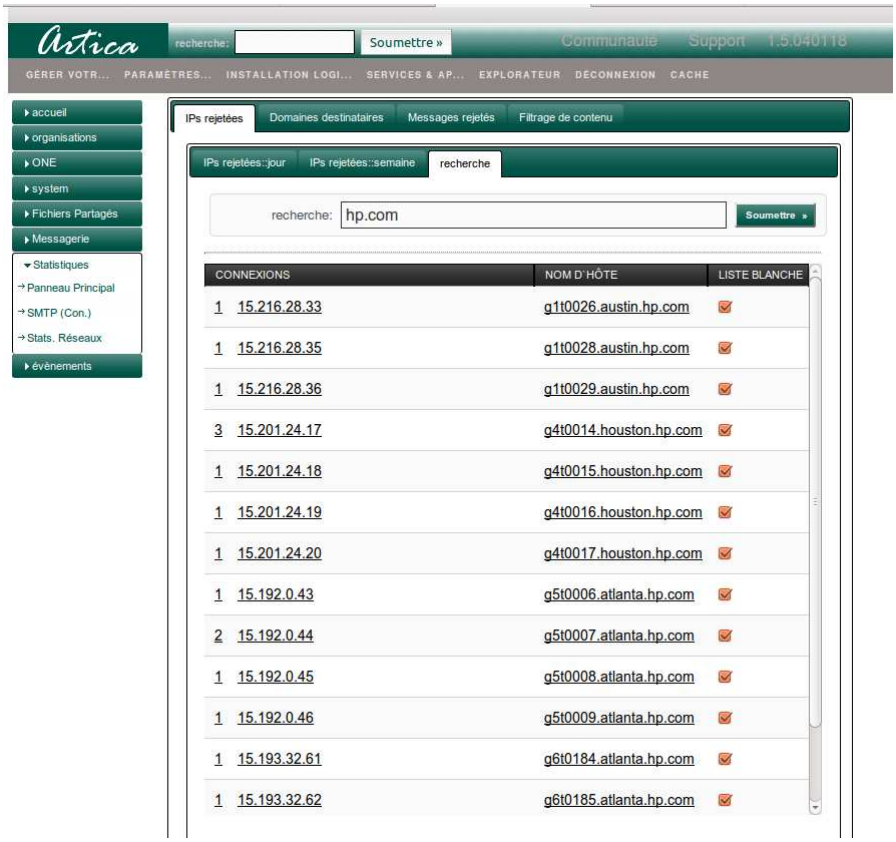
Une autre méthode consiste à s'appuyer sur les statistiques que gère Artica et notamment si vous n'avez pas la connaissance du ou des adresses du domaine.

Cliquez dans le menu de gauche sur «**Statistiques** » puis sur « **SMTP (Con.)** » dans l'onglet « **Ips rejetée**s », sélectionnez l'onglet « **Recherche** »

Recherchez un nom de serveur (le caractère jocker *) étant autorisé.

Si des adresses s'affichent, c'est qu'elles ont déjà été rejetées.

Une case à côcher vous permet de les rajouter ou de les retirer de la liste blanche de connexions.



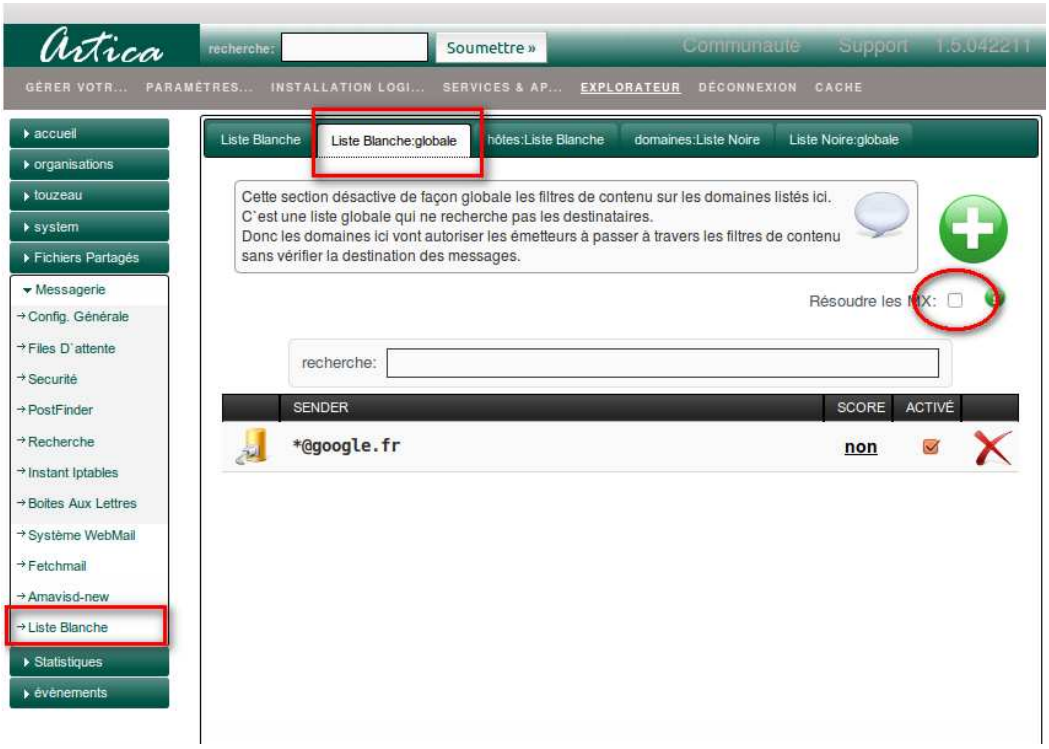
Fusionner les listes blanches

Comme vous avez put le constater, il existe deux listes blanches:

- Celle pour le filtre de contenu qui a la connaissance des destinataires et émetteurs
- Celle pour les filtres de connexion qui ne s'attardent que sur les adresses TCP/IP.

Si vous souhaitez que lorsque vous indiquez un domaine dans la liste blanche du filtre de contenu, celui-ci soit automatiquement ajouté aussi dans la liste de la liste blanche des adresses IP

Dans la section « **Liste Blanche globale** », cochez la case « **Résoudre les MX** ».

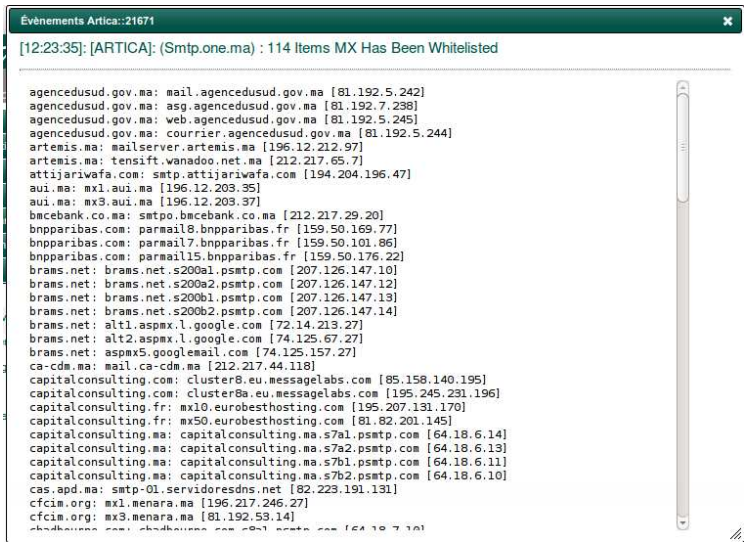


Cette opération aura pour but d'indiquer à Artica de résoudre les MX de chaque domaine que vous ajoutez (adresse eMail comprise).

Tous les MX des domaines vont être résolus et mis en liste blanche.

Lorsque vous cochez cette case, Artica va reprendre l'historique et remplir la liste et à chaque fois que vous ajouterez un domaine, cette opération va se renouveler.

Une notification sera envoyée si des adresses on été trouvées et mises en liste blanche.



Historique et visibilité

PostFinder

PostFinder est un outil permettant de rechercher dans l'historique des fichiers d'évènements « bruts » afin d'en sortir les séquences de routage des messages.

Les historiques des évènements sont stockés par défaut dans le répertoire **/home/maillog-backup**

L'interface d'accès se trouve dans le menu de gauche « **Messagerie** » puis « **PostFinder** »

Ce menu ouvre une nouvelle page vous permettant de « **construire des requêtes** »

Le principe :

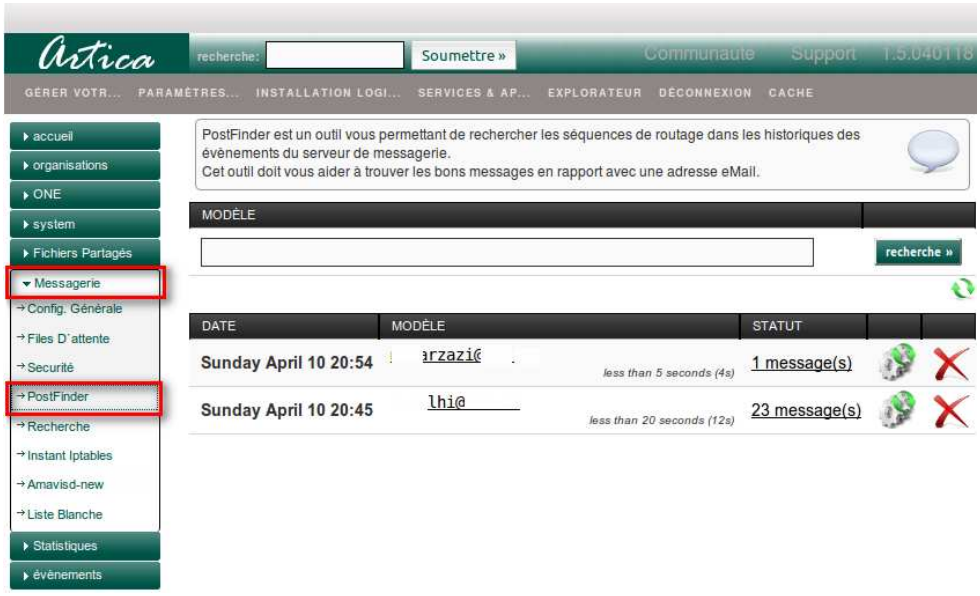
Dans l'option Modèle, vous indiquez l'adresse eMail que vous voulez rechercher (le caractère joker « * » étant autorisé).

Ainsi, il est possible de recherche les séquence de user@domain.tld mais aussi @domain.tld ou usr*@domain.tld

> *Lorsque vous remplissez une requête, celle-ci va être « **programmée** ».*

En effet, la construction de la recherche peut durer plusieurs minutes. Le serveur est en charge de construire les réponses en tâche de fond.

Ces requêtes sont stockées « à long terme ». Une fois les séquences trouvées, elle seront ajoutés dans la base MySQL. Ainsi vous pourrez les consulter à nouveau sans avoir à relancer l'opération de recherche.



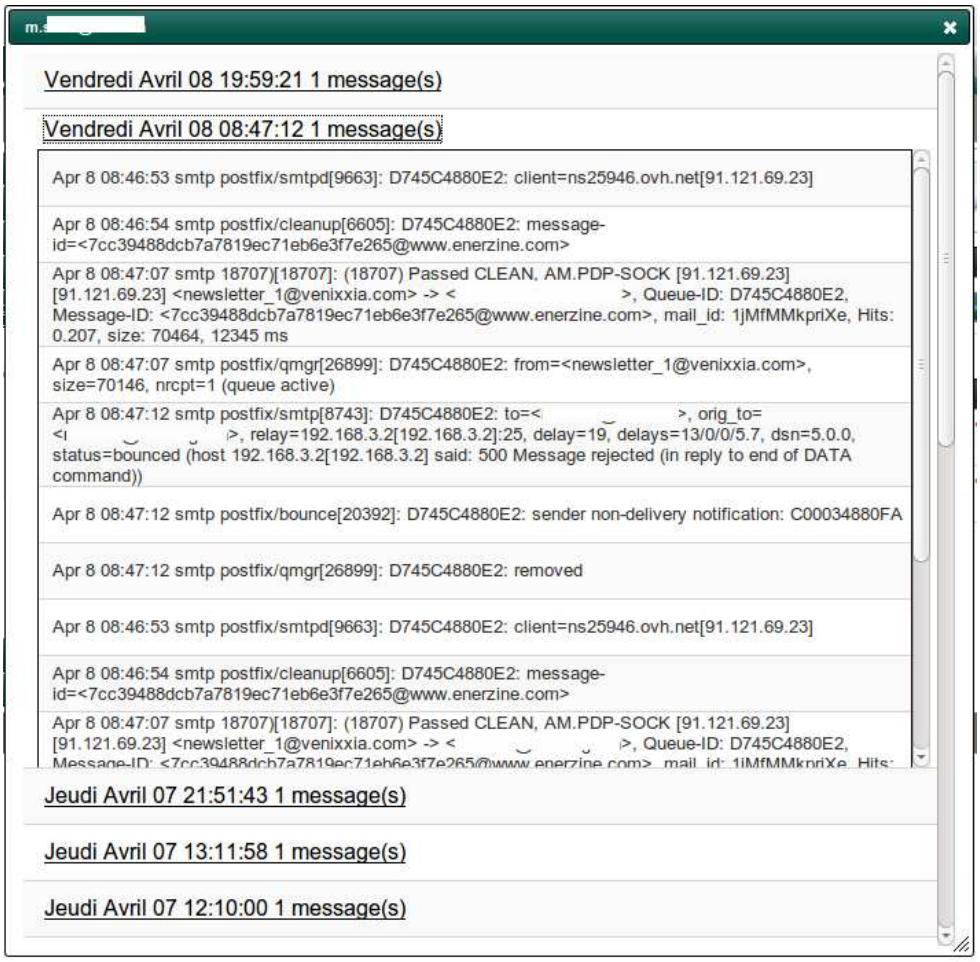
Les séquences trouvées étant « figées » au moment de la recherche, le moteur ne va pas rechercher les nouvelles séquences dans les nouveaux évènements.

Pour ce faire, lorsque vous cliquez sur l'icône représentant des rouages, vous indiquez que le moteur doit faire à nouveau la recherche dans tous les historiques sauvegardés.

Si les opérations de recherche sont terminées, vous avez la possibilité de cliquer sur la requête programmée.

Une nouvelle fenêtre s'affiche.

Elle vous proposera toutes les séquences des messages trouvés dans l'ordre des messages les plus récents.



En cliquant sur la date, la fenêtre vous affiche toute la séquence des messages trouvés.

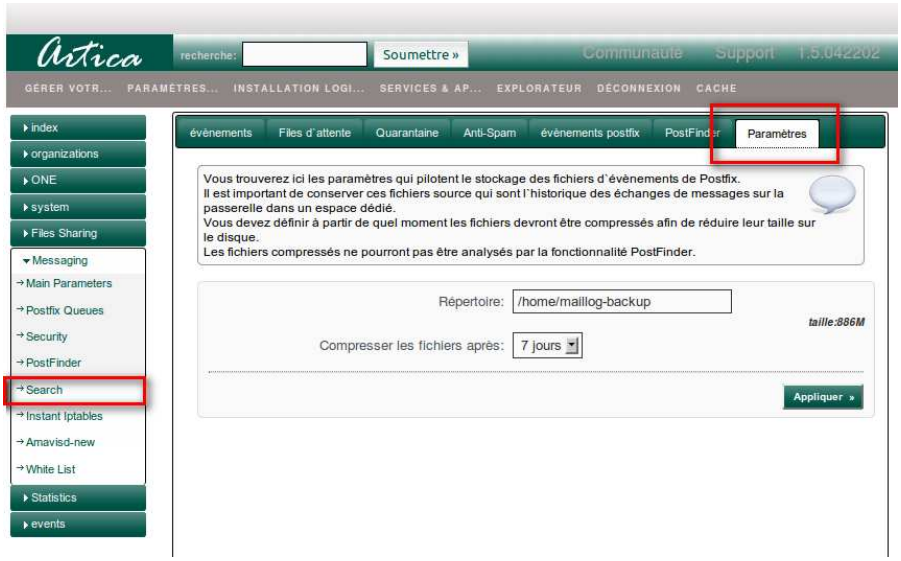
Rotation des fichiers de logs

Pour pouvoir faire fonctionner PostFinder, Artica conserve les fichiers d'évènements dans un répertoire (par défaut dans /home/maillog-backup)

Ces fichiers risquent de prendre de la place sur le disque dur.

Dans le menu de gauche, « Messagerie »/ « recherche » puis onglet « Paramètres », vous trouverez les paramètres de rotation de ces fichiers.

Indiquez la durée de rétention pour pouvoir effectuer des recherches avec PostFinder (après les fichiers sont compressé).



Analyse du filtre de contenu.

Si vous avez activé le filtre de contenu « Spamassassin » il est intéressant de vérifier son comportement sur un échantillon de messages.

Vous disposez d'une fonctionnalité permettant de vérifier le filtre de contenu sans avoir à envoyer un message.

Pour ce faire, munissez-vous des sources des messages qui vont être votre échantillon.

(tout client de messagerie propose d'afficher la source des message ou bien d'enregistrer le message au format txt).

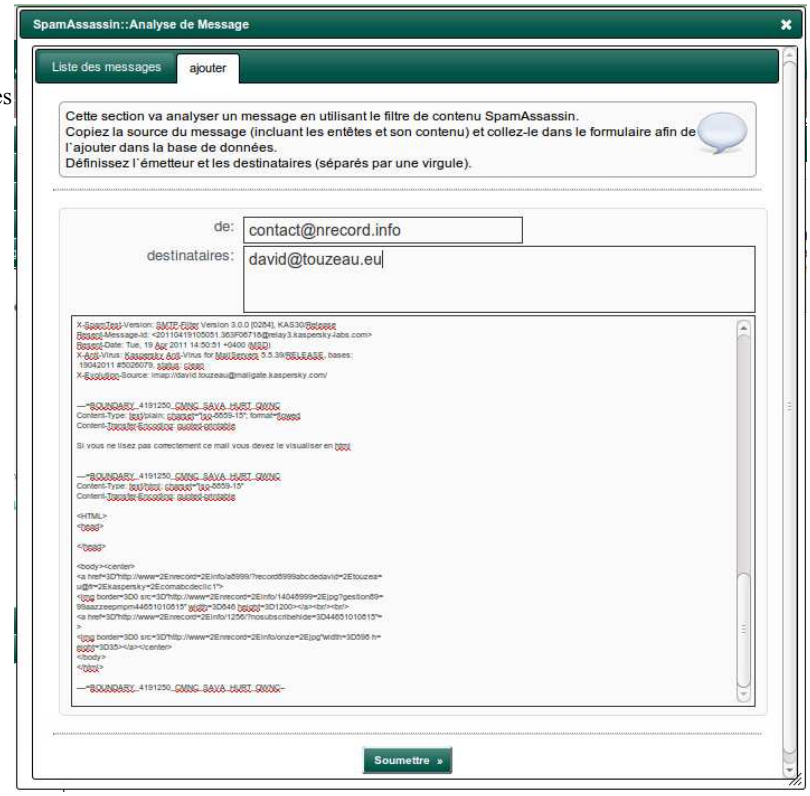
Dans le menu de gauche, choisissez « **sécurité** », cliquez sur l'onglet « **Filtrage de contenu** ».

cliquez sur l'image « **Analyse de message** »

Une nouvelle fenêtre s'affiche, cliquez sur l'onglet « **Ajouter** »

Indiquez l'expéditeur et les destinataires (séparés part une virgule)

Copiez le source du message dans la partie centrale du formulaire, cliquez sur « **soumettre** »



Une fois le message sauvegardé, cliquez sur l'onglet « **liste des messages** ».

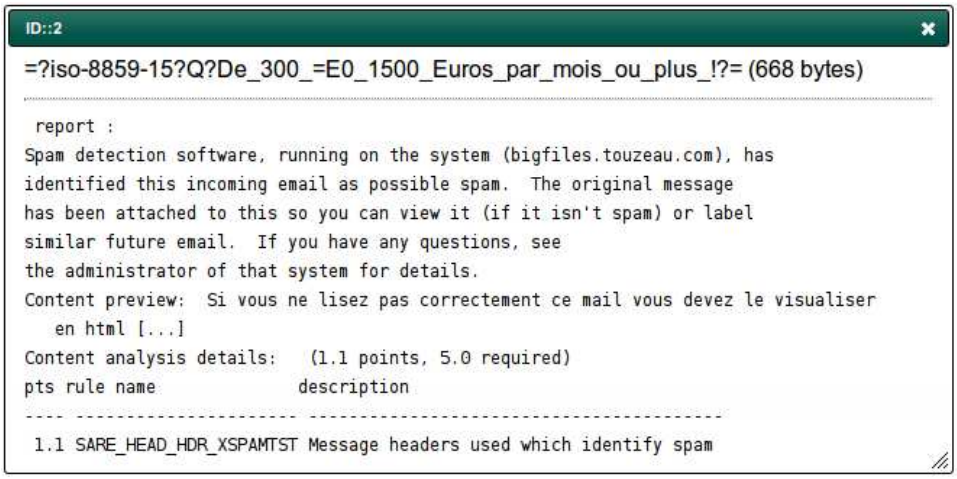
Le statut « **analysé** » vous permet de visualiser le résultat en cliquant sur les liens.

Vous pouvez soit relancer l'analyse en cliquant sur l'image de la 5ème colonne , soit supprimer le message.

Lorsque vous cliquez sur le lien du message, un rapport s'affiche vous permettant de visualiser un rapport

Ce rapport vous donne le nombre de points (score) que le filtre à jugé.

Dans un tableau, vous y voyez aussi les règles qui ont activé la notation.



Ici vous testez que le filtre de contenu. En effet d'autres règles et filtres sont ajoutés par le concentrateur Amavis qui peut quand à lui influer sur la notation du message.
Toutefois, cette première analyse vous permet de comprendre en grande partie les raisons d'une classification d'un message.

Performances

Performance du filtre de contenu.

Le filtre amavisd-new utilise un processus de démons enfants créés au besoin afin de répartir les messages à analyser.

Chaque démon « fils » nouvellement créé dispose d'une durée de vie (par défaut 50 minutes ou 5*600) ou bien d'un nombre maximal de messages traités (par défaut à 30 messages)

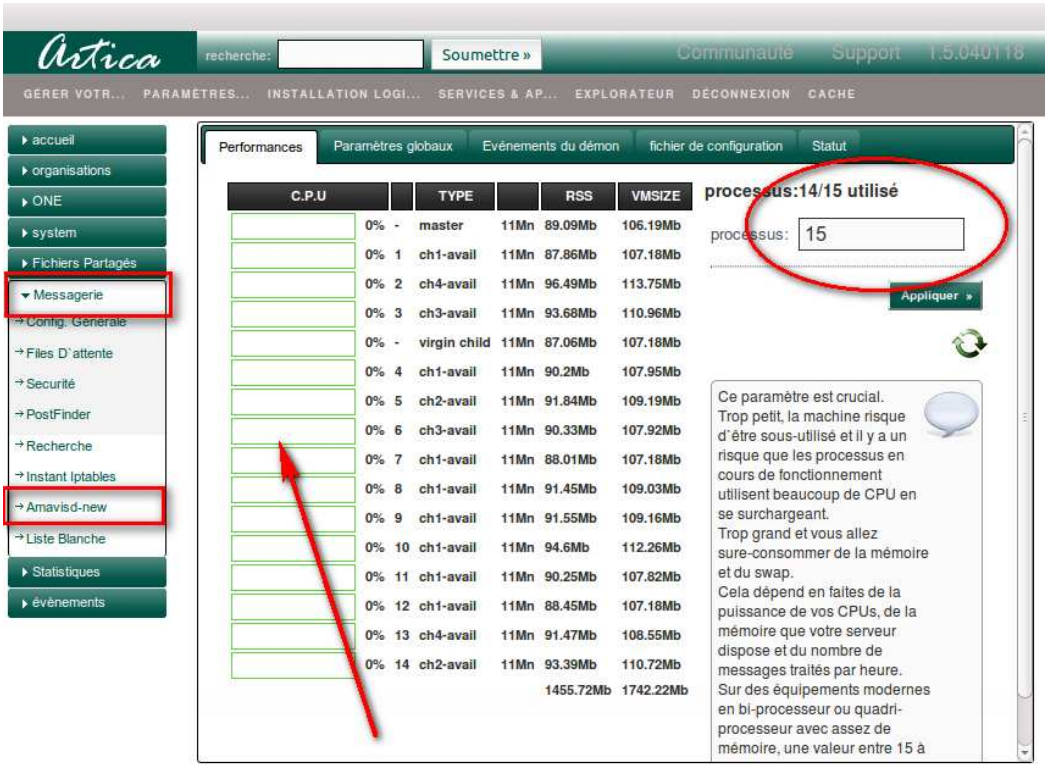
Une fois cette durée de vie échue, le démon est tué de la mémoire et un nouveau démon fils « tout frais » est alors lancé en mémoire.

Le paramètre le plus important afin d'assurer une bonne fluidité du serveur est le « le nombre de processus » que le filtre de contenu amavisd-new est autorisé à lancer en mémoire.

Ce paramètre dispose alors d'une section dédié.

Lorsque vous cliquez sur le menu de gauche dans « **Messagerie** », « **Amavisd-new** » , une section « **Performances** » est affichée.

Celle-ci vous affiche le nombre de processus en cours de fonctionnement, le taux d'utilisation CPU, leur durée de vie, leur mémoire système (RSS) et leur mémoire mise en cache (VMSIZE).



Si le paramètre est trop petit, la machine risque d'être sous-utilisée et il y a un risque que les processus en cours de fonctionnement utilisent beaucoup de CPU par une surcharge de leur travail.

Si le paramètre est trop grand et vous allez sur-consommer de la mémoire et du swap pour rien...

Cela dépend en faites de la puissance de vos CPUs, de la mémoire que votre serveur dispose et du nombre de messages traités par heure.

> *Sur des équipements modernes en bi-processeur ou quadri-processeur avec assez de mémoire, une valeur entre 15 à 30 est raisonnable.*

Choix des modules de filtrage

Le filtre de contenu est un filtre modulaire.

Des fonctionnalités peuvent ajoutées ou retirées.

La performance du filtre dépend énormément du type des modules et du nombre de modules ajoutés.

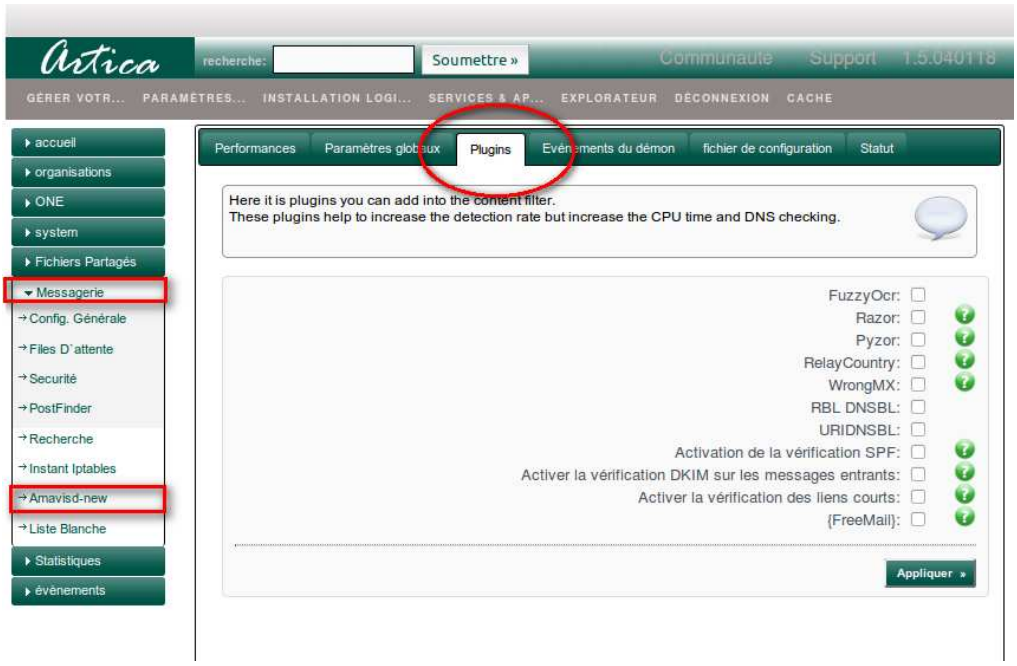
Certes, le nombre de modules augmente le taux de détection mais aussi celui de la charge machine et des requêtes DNS que celui-ci devra effectuer.

L'ajout des modules dépend alors de la puissance de votre machine et de la qualité des serveurs DNS que vous disposez.

Pour choisir les modules cliquez dans le menu de gauche « **Messagerie** » puis « **Amavisd-new** »

Une nouvelle page s'affiche, cliquez alors sur l'onglet « **Plugins** »

Il vous suffira de côcher et de décocher les cases correspondantes.



Couplage du filtre avec Postfix.

Le Filtre de contenu amavis permet d'utiliser 2 méthodes de couplage.

La méthode milter ou bien la méthode postqueue.

La méthode milter :

Cette méthode oblige le MTA à envoyer les données du message en même temps qu'il reçoit le message.

En effet cette méthode appelée « pré-queue » n'appelle pas le MTA à écrire le message en file d'attente sur le disque pour que le filtrage s'effectue.

Le message est véhiculé en mode flux du MTA au filtre.

Le filtre répond directement en mémoire, pendant la connexion.

La méthode d`Après Queue-Postfix

Cette méthode créé deux files d'attente.

Le MTA place le message en file d'attente « spéciale filtrage » et le fournir au filtre de contenu.

Le filtre de contenu, une fois avoir analysé le message le renvoi au MTA pour être placé en file d'attente pour transfert vers le prochain serveur de destination (ou la boîte aux lettres).

Quelle méthode choisir ?

Bien que la méthode milter soit sur le papier plus performante, les deux techniques se valent en matière de performances.

L'utilisation du mode Après-queue dispose d'un avantage : Si le filtre est indisponible, le message est sauvegardé en file d'attente et le MTA est en charge de retenter l'envoi plus tard.

Contrairement au mode « milter » où le message est rejeté avec comme erreur « `Content Scanner malfunction` ».

Artica active par défaut le mode « milter ». Si Artica vous notifie trop souvent des messages de type :

`« Warning Amavis socket is not available ».`

C'est que le filtre milter est trop souvent indisponible.

Dans ce cas, préférez la méthode « Après-Queue »

Comment modifier le couplage ?

Dans le menu de gauche, sélectionnez « **Messagerie** » puis « **Amavisd-new** ».

Cliquez sur l'onglet « **Paramètres globaux** » et cliquez sur l'image « **Couplage Postfix** »

Dans la nouvelle fenêtre, choisissez la méthode « **Pré-queue** » ou « **Après-queue** » puis cliquez sur Appliquer.

Créer ses premiers domaines de messagerie.

Même si vous avez choisi un serveur de fichier ou un boitier VPN, la création d'un domaine « internet » est nécessaire.

Cette opération permet de disposer d'un cohérence si vous avez à faire interagir plusieurs serveurs d'infrastructure entre eux.

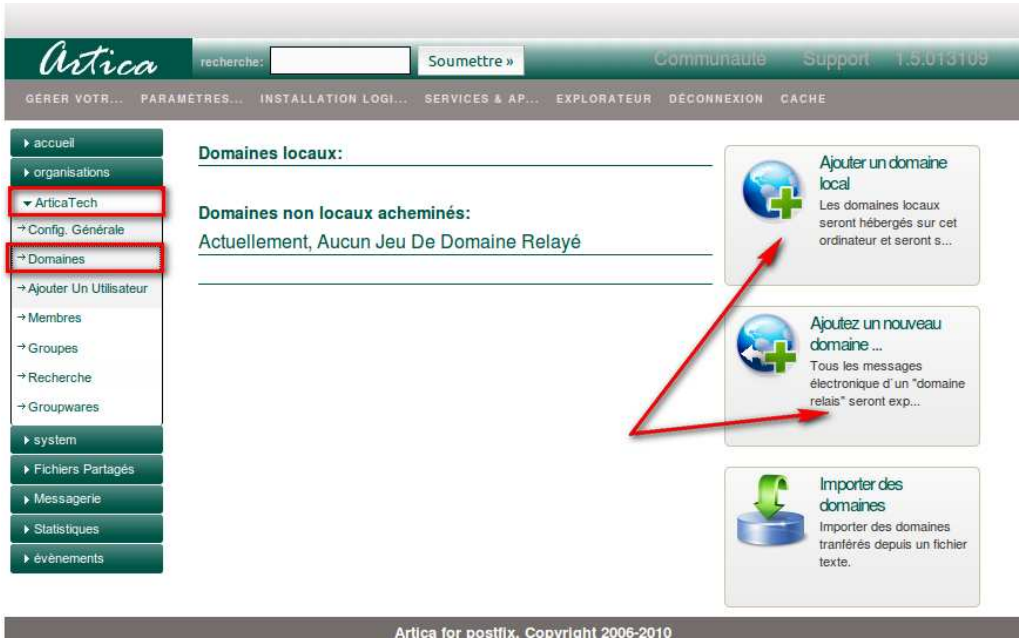
Il en est d'autant plus important si vous avez décidé d'utiliser Artica en tant que serveur de messagerie ou bien relais de messagerie.

> *Les domaines de messagerie s'administrent dans les organisations.*

Chaque organisation peut alors disposer de ses propres domaines.

Cette structure, notamment sur un serveur de messagerie, permet de bien séparer et de visualiser l'intérêt des organisations.

Les utilisateurs qui seront créés dans les organisations se verront alors attribués des adresses eMail avec les domaines que vous stipulerez dans cette section.



Sélectionnez votre organisation dans le menu de gauche et cliquez sur le menu « Domaines »

Si vous avez décidé d'utiliser Artica en tant que « server de messagerie », c'est à dire hébergeant aussi des boîtes aux lettres, vous aurez la possibilité de créer deux types de domaines de messagerie.

Domaine local :

Un domaine local indique au serveur qu'il est propriétaire du domaine.

Si il reçoit des messages dont l'adresse eMail dispose du domaine en question, il tentera de l'acheminer vers son système de boîte aux lettres.

Domaine acheminé :

Un Domaine acheminé indique au serveur qu'un message à destination de ce domaine doit être transférer à un autre serveur de messagerie spécifique.

Récupération du courrier distant

Utilisation de fetchmail

Bien souvent, et par historique, les entreprises passent d'abord par l'utilisation de boîtes aux lettres chez les fournisseurs d'accès.

Cette initiative permet de pourvoir communiquer avec d'autres entreprises.

Au cours de l'évolution d'autres besoins se font ressentir comme communiquer avec d'autres salariés sans passer par le fournisseur d'accès ou offrir un calendrier partagé etc.

Toutefois, abandonner la boîte aux lettres externe est compliquée car elle est connue de tous et les clients et fournisseurs ont l'habitude de communiquer par son intermédiaire.

Artica permet d'associer les deux principes : Conserver la ou les boîtes aux lettres distantes tout en commençant à utiliser une messagerie dédiée.

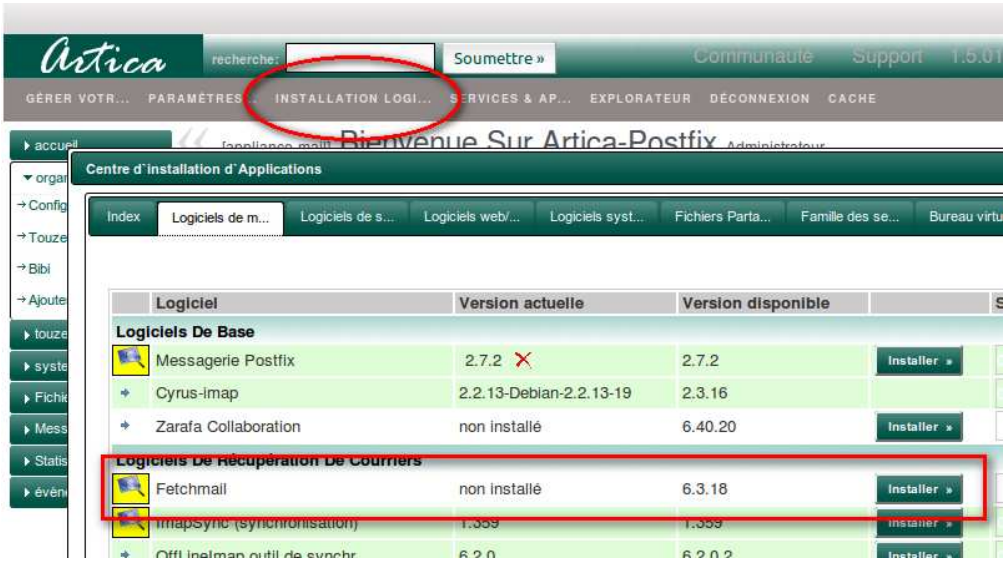
La récupération du courrier distant s'effectue à travers le logiciel « **fetchmail** »

Fetchmail est un démon qui à pour but de télécharger via POP3/IMAP les nouveaux messages sur des boîtes aux lettres distantes et de les renvoyer sur le port local SMTP Postfix du serveur Artica.

Le serveur SMTP Postfix sera en charge de transmettre le message rapatrié à l'utilisateur local et que vous avez créé sur le serveur que vous devrez spécifier dans les règles.

Artica n'affiche les options de récupération distantes que si et seulement si ce logiciel est installé.

Pour ce faire cliquez sur l'option INSTALLATION LOGICELS, Sélectionnez l'onglet Logiciels de messagerie et cliquez sur le bouton « installer » au niveau de Fetchmail.

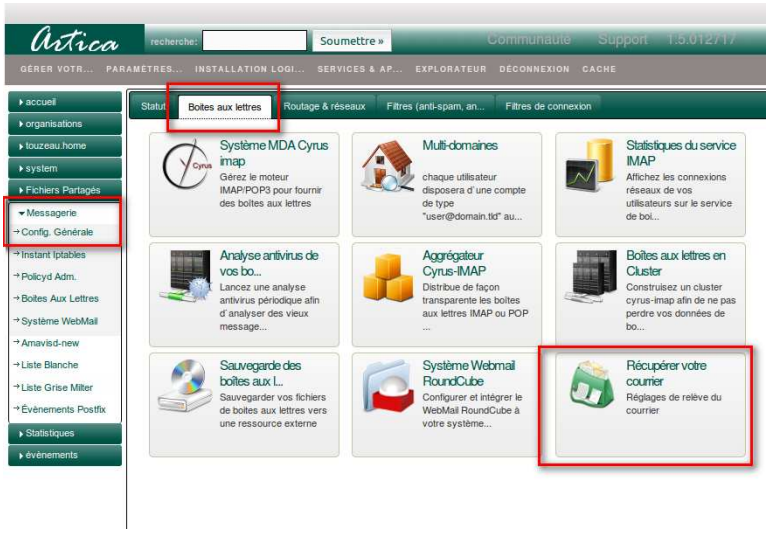


Activation du service de récupération de courrier

Une fois que l'installation s'est effectuée, dans le menu de gauche, sélectionnez le menu « Messagerie » puis Config. Générale.

Note : Tant que des règles de récupération de courrier n'ont pas été enregistrées, le démon ne s'activera pas (il n'y a pas de sens de charger un démon en mémoire qui n'a pas d'opération à effectuer)

Cliquez sur l'onglet « Boîtes aux lettres » et sélectionnez l'icône « Récupérer votre courrier »



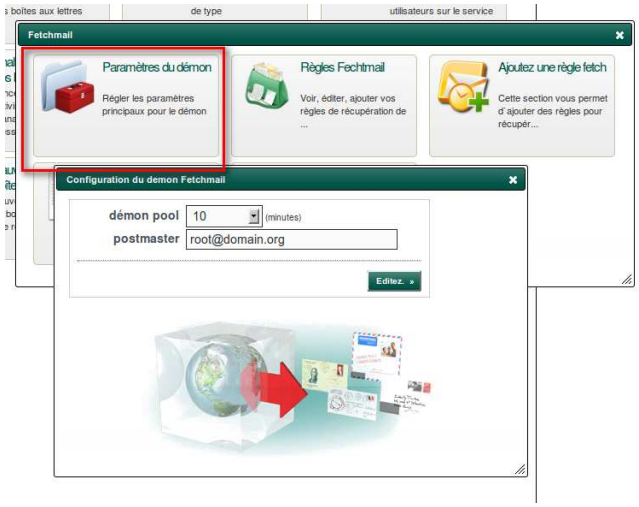
Une nouvelle fenêtre s'affiche vous proposant de piloter le service de récupération de courrier.

Cliquez sur l'icône « Paramètres du démon »

Vous allez pouvoir indiquer la fréquence de connexion sur les boîtes aux lettres distantes en minutes dans l'option « Démon pool »

Par défaut, le démon va vérifier les nouveaux messages sur les boîtes aux lettres internet toutes les 10 minutes.

Indiquez l'adresse eMail du postmaster, adresse qui sert à émettre des notifications d'échec.



Ajouter des règles de rapatriement de courrier

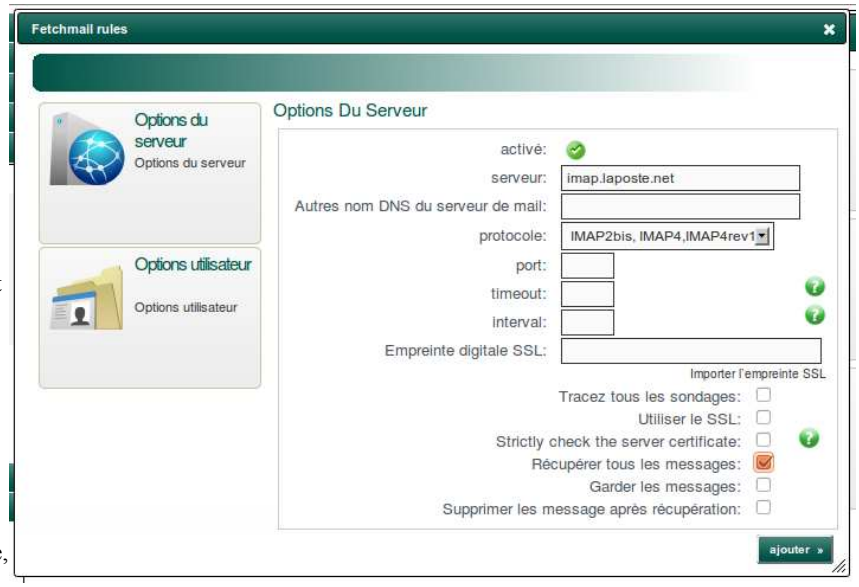
Cliquez sur l'icône « Ajoutez une règle fetchmail »

Un nouveau formulaire va apparaître

Il se compose de deux sections :

- Les options du serveur qui indiquent les propriétés d'accès réseau au serveur de la boîte aux lettres distante
- Les options Utilisateur qui indiquent les propriétés d'accès de le boîte aux lettres distante ainsi que l'utilisateur local concerné par les messages rapatriés.

Options du serveur :



Cliquez sur l'icône « activé » afin d'activer la règle.

Dans le champs « **serveur** » indiquez le nom ou l'adresse IP du serveur sur Internet qui héberge la boîte aux lettres.

Dans le champs « **protocole** « indiquez si il s'agit du boîte aux lettres POP3 ou IMAP

Indiquez dans le champ port le port d'écoute du serveur de boîte aux lettres si son numéro de port n'est pas standard.

Si il s'agit d'une boîte aux lettres POP3 SSL ou IMAP SSL, cochez la case « **Utiliser SSL** »

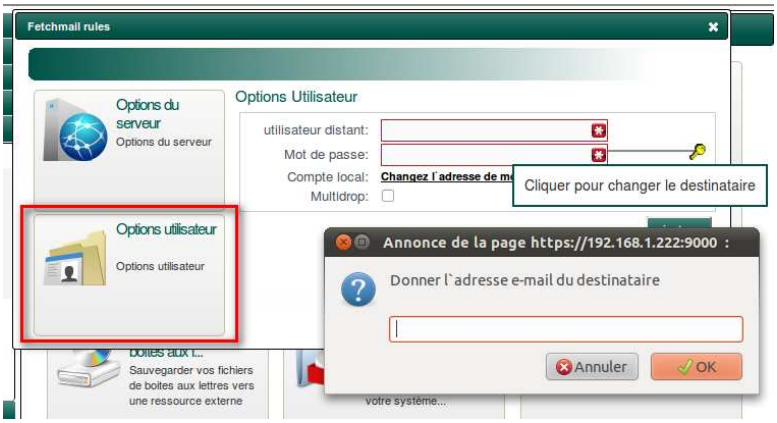
Si vous désirez récupérer tous les messages qui sont déjà stockés dans la boîte aux lettres distante, cochez la case « **Récupérer tous les messages** »

Si vous ne voulez pas que les messages une fois rapatriés ne soient pas supprimés automatiquement, côchez la case « Garder tous les messages » sinon cochez la case « **Supprimer les messages après récupération** »

Options Utilisateur

Cliquez sur l'icône « **Options Utilisateur** »

Dans le champ utilisateur distant et Mot de passe, indiquez le compte et le mot de passe utilisé pour se connecter sur la boîte aux lettres distante.



Cliquez sur le lien « **Changez l'adresse...** » afin de spécifier l'adresse eMail de l'utilisateur local du serveur est destinatrice des messages rapatriés.

Sauvegardez le formulaire.

Une fois le formulaire sauvegardé et au bout de 10Mn (valeur par défaut), des nouveaux messages devraient apparaître dans la boite aux lettre locale stipulée.

Vous pouvez aussi administrer les règles de rapatriement directement dans la section utilisateur.

Cliquez sur l'onglet messagerie du compte utilisateur et sélectionnez l'icône « Fetchmail »

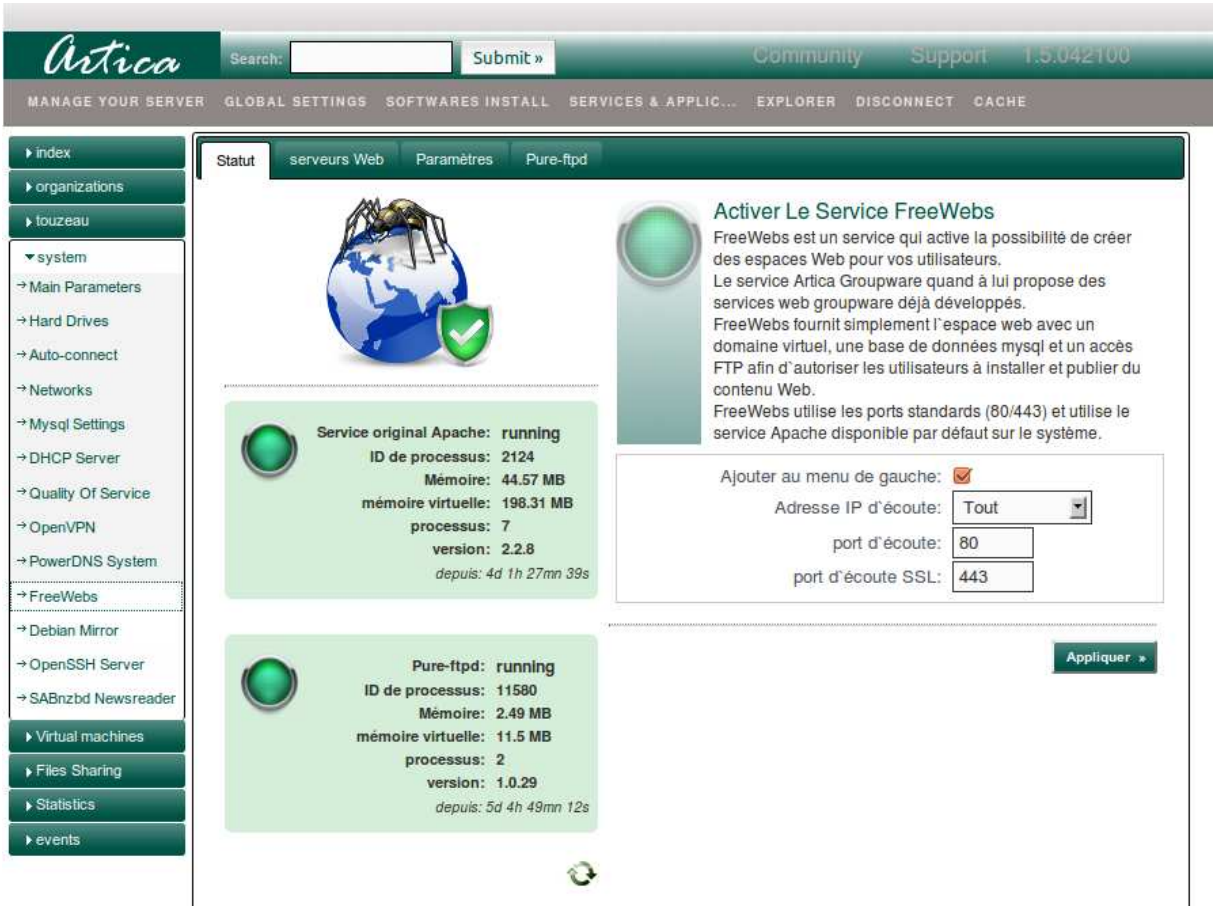
Des sites Internet avec FreeWebs

FreeWebs est une fonctionnalité permettant d'offrir des espaces Web à vos utilisateurs.

Si le serveur Apache est installé Artica vous permet de pouvoir créer des sites Internet pour vos utilisateurs.

Si de surcroit, vous avez installé le service « pure-ftpd », vos utilisateurs auront accès à leur espace Web via FTP

L'accès à l'administration de FreeWebs se trouve dans le menu de gauche, dans « **System** » puis « **FreeWebs** ».



La première page vous permet de modifier les ports d'écoute du moteur web ainsi que l'adresse IP d'écoute.

Par défaut, le serveur Web écoute toutes les adresses réseau sur les ports standards Web

Ajouter un nouveau site web

Cliquez sur l'onglet « **Serveurs Web** » puis sur le bouton « **Ajouter** »

Indiquez le nom du serveur web dans « **Nom d'hôte du serveur web** » que les visiteurs devront taper après le http://

Si vous désirez qu'un utilisateur spécifique puisse paramétrer/Administrer son site web dans son espace réservé, indiquez l'identifiant de l'utilisateur dans « **Membre** »

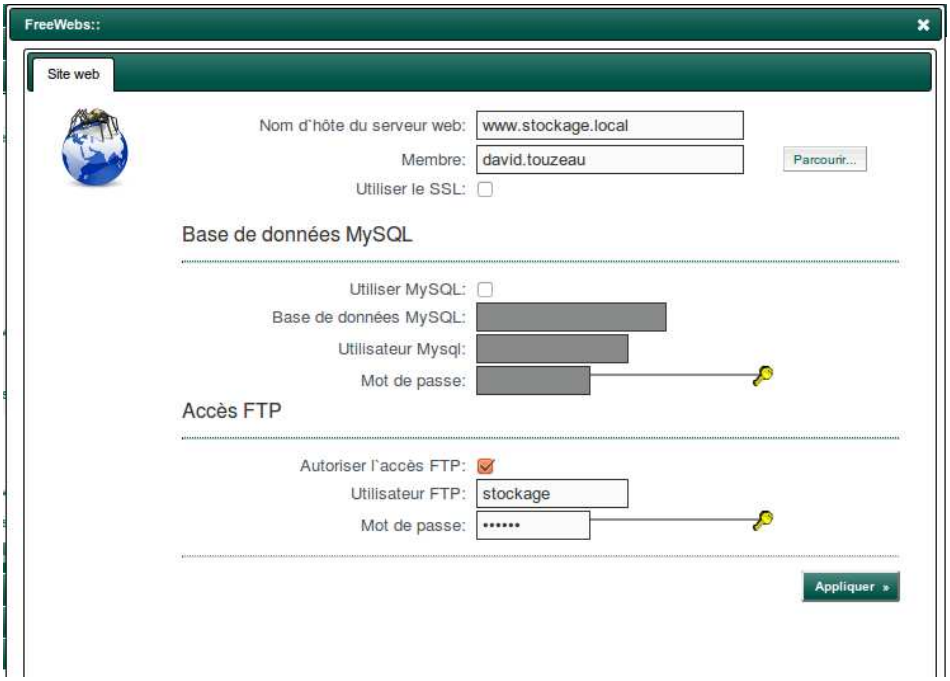
Base de données

Si vous désirez offrir une base de données à l'espace Web, côchez la case « Utiliser Mysql », indiquez le nom de la base de données le compte utilisateur et mot de passe.

Accès FTP

Pour que l'utilisateur puisse avoir accès à l'espace Web via un client FTP, côchez la case « Autoriser l'accès FTP »

indiquez le compte FTP (qui doit être différent du Membre) et le mot de passe



Le site web sera rajouté dans la liste principale des serveurs Web.

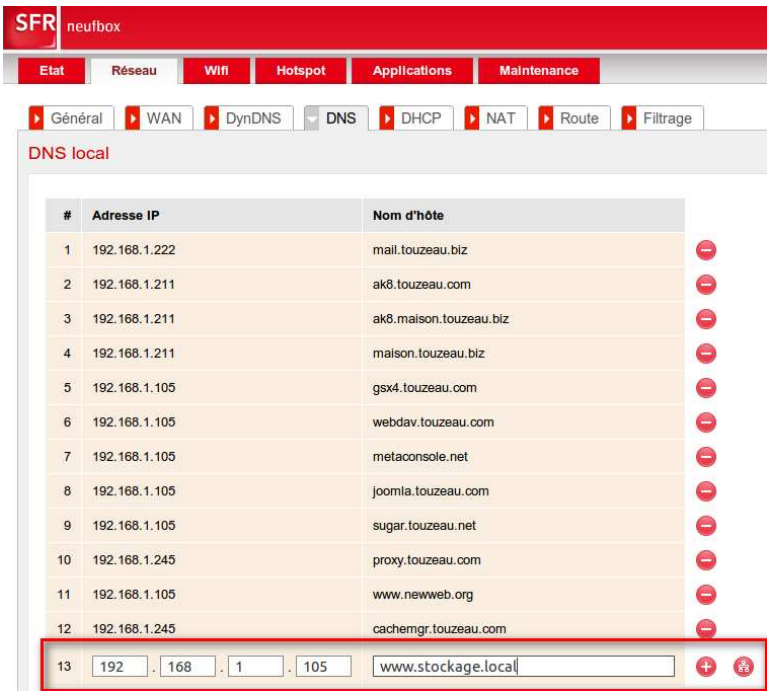
Accès au site web

Artica à construit un « serveur virtuel », ce serveur virtuel nécessite que les visiteurs utilisent le nom du site Web pour pouvoir y accéder.

Vous devez vous assurer que les machines connaissent le le nom du serveur et qu'elle puissent résoudre l'adresse IP du serveur Artica

Vous disposez d'un serveur DNS local ou Internet :

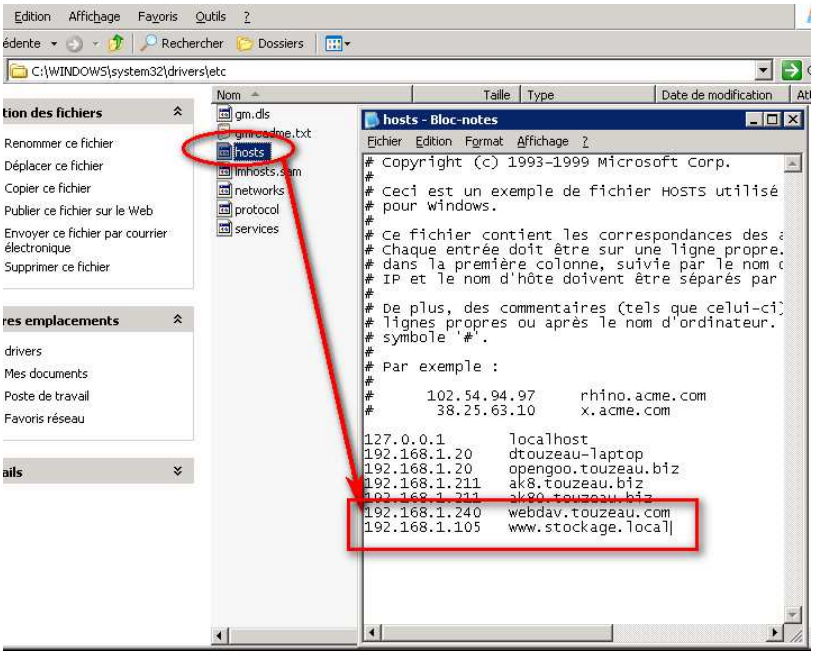
Indiquez alors la correspondance du nom du site web avec l'adresse IP



Modification du fichier hôtes

Si vous voulez simplement tester l'accès au site web, ouvrez le fichier **`C:\windows\system32\drivers\etc\hosts`**

et indiquez la correspondance IP → serveur



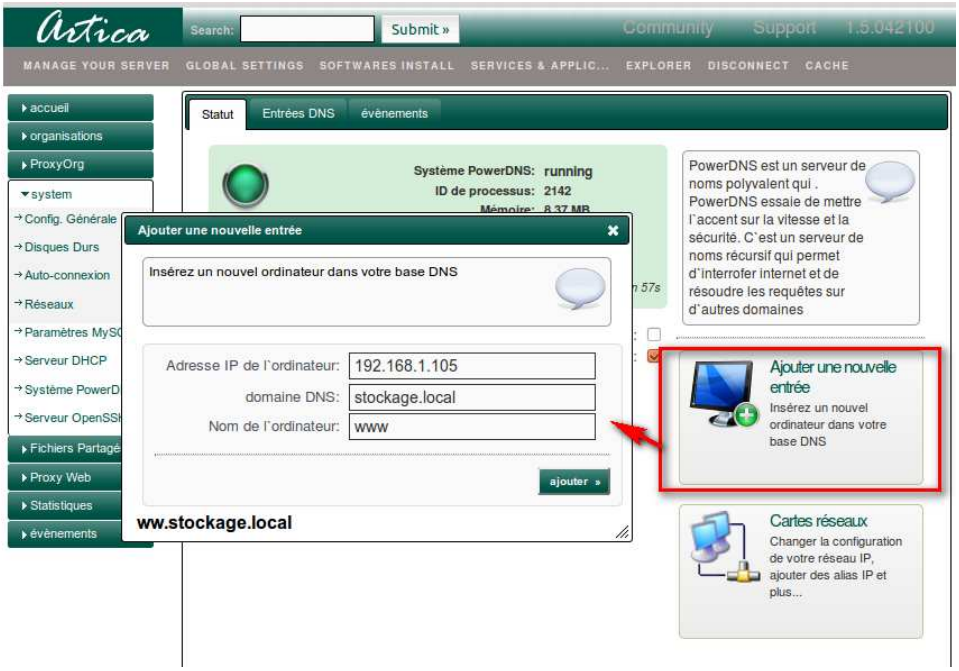
Utilisation d'Artica en serveur DNS (PowerDNS)

Si votre serveur DNS est un serveur Artica utilisant PowerDNS :

Cliquez sur le menu de gauche « **System** » puis « **Système PowerDNS** »

Cliquez sur l'image « **Ajouter une nouvelle entrée** »

Indiquez la correspondance du nouveau serveur web .



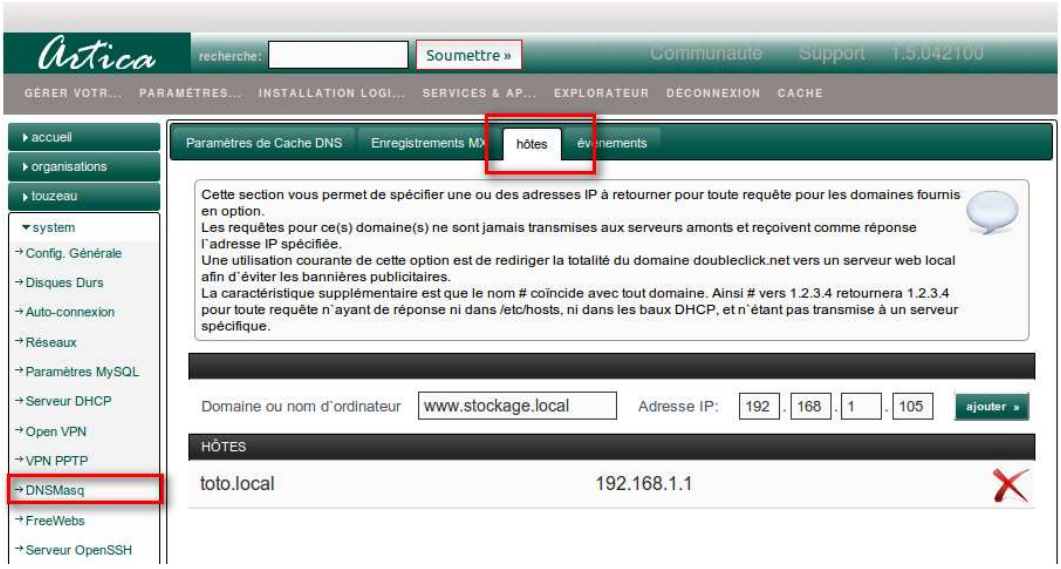
Utilisation d'Artica en serveur DNS (dnsmasq)

Si votre serveur DNS est un serveur Artica utilisant DNSMasq :

Cliquez sur le menu de gauche « **System** » puis « **DNSMasq** »

Cliquez sur l'onglet « **Hôtes** »

Indiquez la correspondance du nouveau serveur web et cliquez sur « **ajouter** »



Tests du site web

si à travers votre navigateur vous visualisez une page « It Works ! » c'est que le site web est prête à être modifié et consulté.

It Works!

HTTP_HOST:www.stockage.local

HTTP_USER_AGENT: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.9.2.16) Gecko/20110323 Ubuntu/10.10 (maverick) Firefox/3.6.16

HTTP_ACCEPT:text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP_ACCEPT_LANGUAGE:fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3

HTTP_ACCEPT_ENCODING:gzip,deflate

HTTP_ACCEPT_CHARSET:ISO-8859-1,utf-8;q=0.7,*;q=0.7

HTTP_KEEP_ALIVE:115

HTTP_CONNECTION:keep-alive

PATH:/usr/local/bin:/usr/bin:/bin

SERVER_SIGNATURE:
Apache/2.2.8 (Ubuntu) mod_ssl/2.2.8 OpenSSL/0.9.8g mod_perl/2.0.3 Perl/v5.8.8 Server at www.stockage.local Port 80

SERVER_SOFTWARE: Apache/2.2.8 (Ubuntu) mod_ssl/2.2.8 OpenSSL/0.9.8g mod_perl/2.0.3 Perl/v5.8.8

SERVER_NAME:www.stockage.local

SERVER_ADDR:192.168.1.105

SERVER_PORT:80

REMOTE_ADDR:192.168.1.101

DOCUMENT_ROOT:/var/www/www.stockage.local

SERVER_ADMIN:david.touzeau@touzeau.com

SCRIPT_FILENAME:/var/www/www.stockage.local/index.php

Partage Web (WebDAV)

Le partage web permet à tout système d'accéder à l'espace dédié au site web à travers une connexion Web (HTTP/HTTPS), tout système Unix ou Windows est capable de monter un répertoire Web.

Cette technique de partage plus communément nommé « Partage WebDAV » propose des avantages :

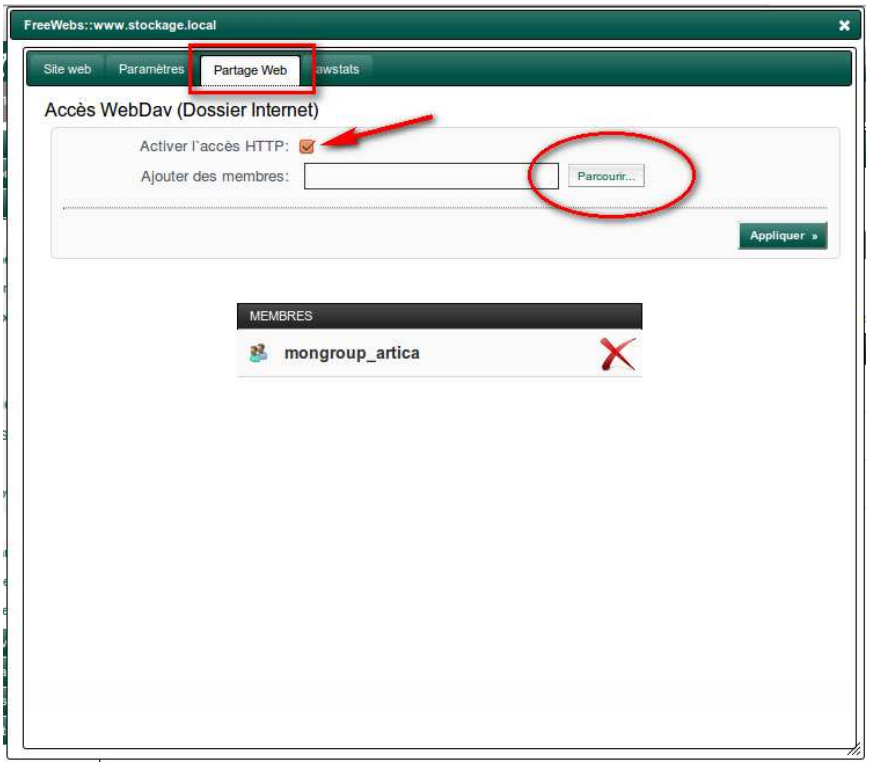
- Assurer l'accès au fichiers nativement à travers l'explorateur Windows du système.
- Aucun client/navigateur spécifique n'est nécessaire.
- Utilise le ports standards Web
- Le partage peut être véhiculé à travers Internet.

Activer un site FreeWebs en partage Webdav

Cliquez sur l'image de gauche dans le tableau des sites web que vous avez créé.

Cliquez sur l'onglet « **Partage Web** »

Activez le partage WebDav en côchant la case « Activer l'accès HTTP »



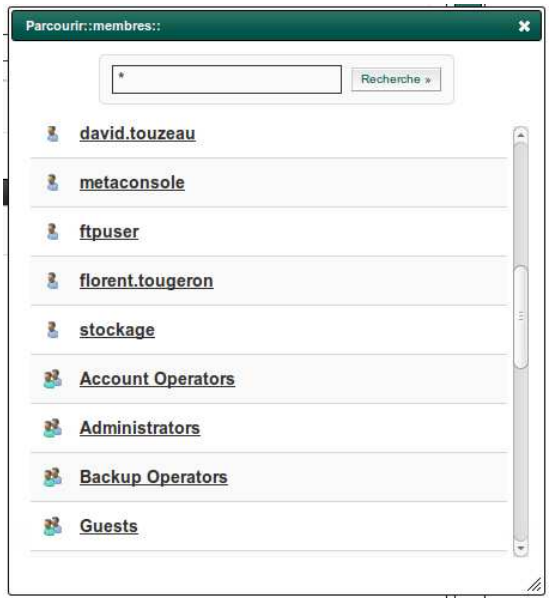
Cet accès partagé nécessite une authentification.

Cette authentification utilise la base LDAP du serveur Artica.

Pour ce faire, cliquez sur le bouton « **Parcourir ...**»

La boîte message « Parcourir » vous permet de choisir à la fois des groupes d'utilisateurs ou des utilisateurs spécifiques.

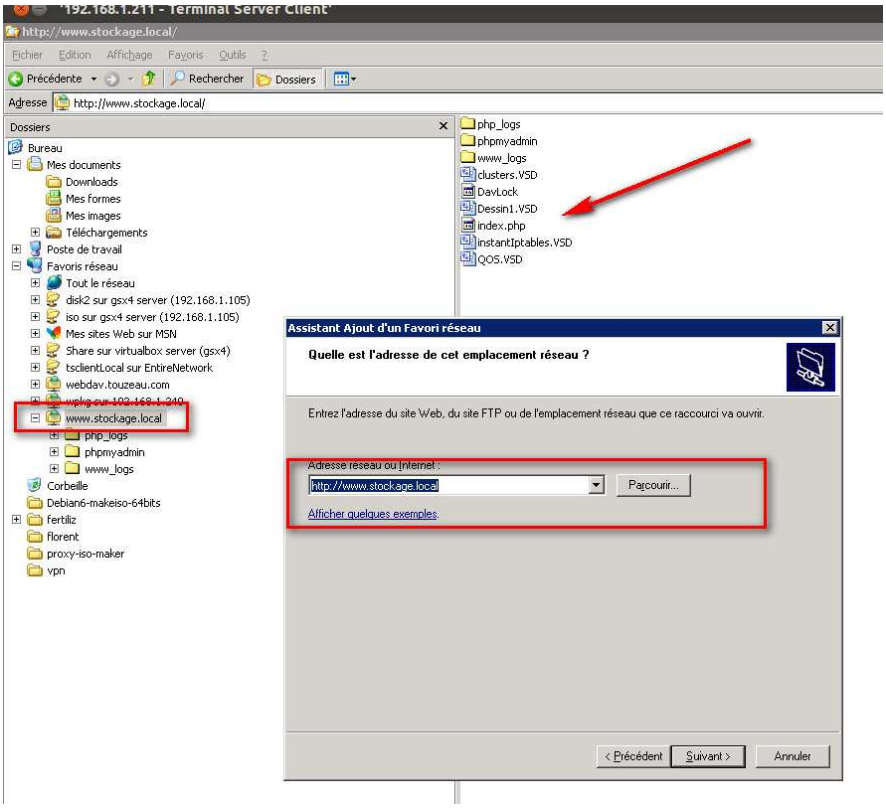
Les groupes et les utilisateurs ajoutés disposeront alors des privilèges pour récupérer, déposer des fichiers dans l'espace web.



Accès au partage Web

L'accès au partage Web s'effectue tout naturellement grâce aux fonctions intégrées à votre système

Sur MS Windows par exemple, il s'effectue à travers l'ajout d'un Favori réseau.



Sécurisation

Authentification du site web

Dans certains cas vous pourriez être amené à forcer l'authentification sur un site web spécifique.

Cette fonctionnalité est très utile lorsque votre application Web ne dispose pas de système d'authentification et lorsque vous désirez utiliser la base de compte LDAP d'Artica pour valider les utilisateurs.

Sélectionnez l'onglet « **Paramètres** » et simplement cochez la case « **Activer l'authentification LDAP** »

Cette opération aura pour but de valider uniquement les utilisateurs stockés dans la base de compte d'Artica.

Vous pouvez aussi changer le texte de la boîte message d'authentification.

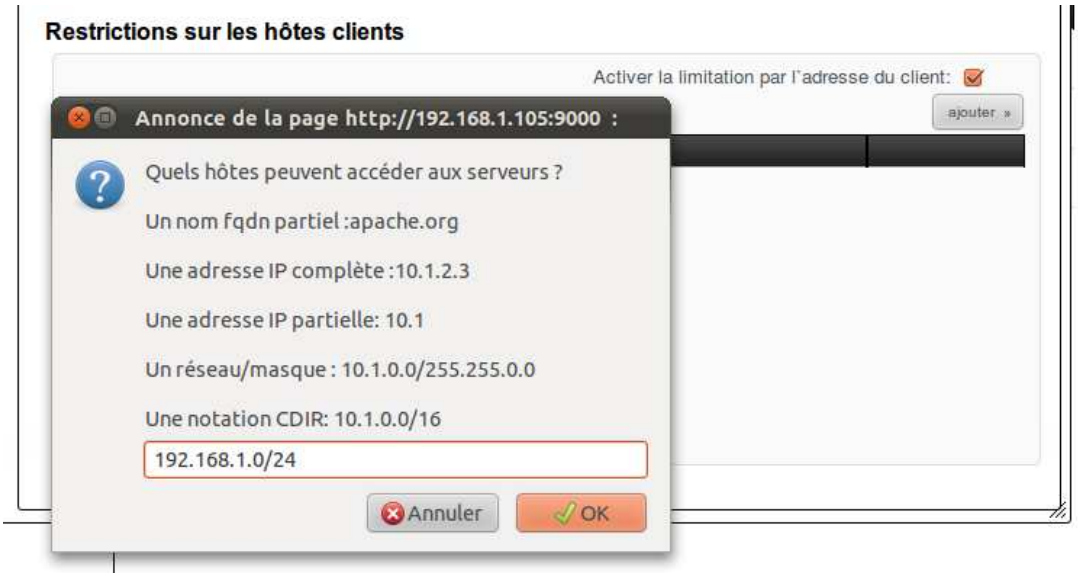
Limitation du site Web par adresses.

Dans le cas d'un extranet par exemple vous pourriez être amené à valider les visiteurs uniquement par un tranche ou une liste d'adresse IP.

Dans ce cas de figure, seules les adresses listées seront autorisées à parcourir le site web.

Cochez la case « **Activer la limitation par l'adresse du client** »

Puis indiquez les modèles d'adresses définies dans le formulaire d'ajout.



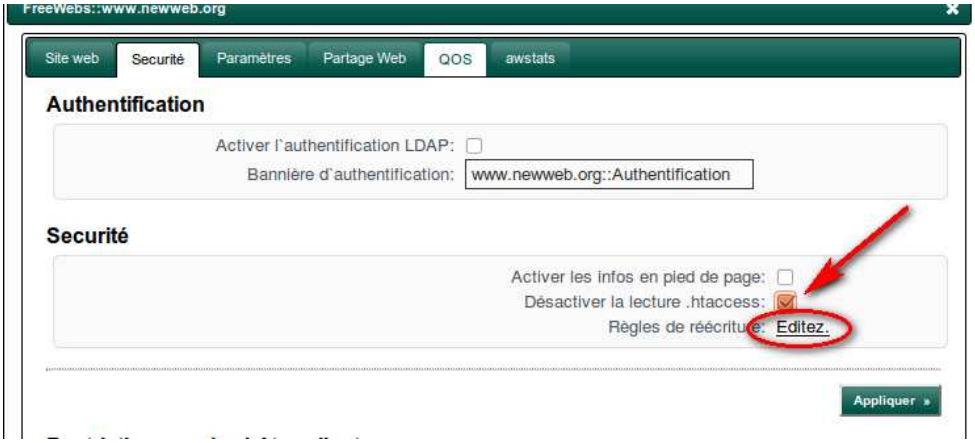
Les règles de réécritures

Les règles de réécritures « mod_rewrite » permettent de modifier le comportement du serveur web en fonction des requêtes des clients.

Si vous désirez interdire l'utilisation des fichiers .htaccess que les utilisateurs peuvent déposer, cochez la case « Désactiver la lecture des .htaccess »

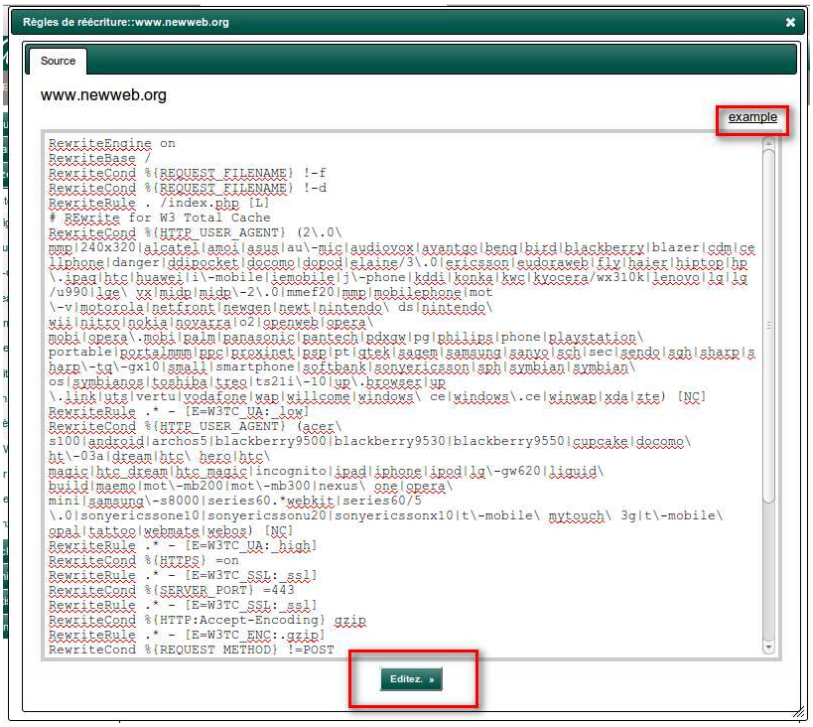
Seules les règles de réécriture que vous indiquez seront prises en compte.

Cliquez sur le lien « Editez » dans règles de réécriture.



Un outil d'édition vous permet de créer vos propres règles.

EN cliquant sur le lien « **example** », vous pouvez visualiser le type de règles qui peut être mise en place.



Permissions sur les dossiers et fichiers

Cette fonctionnalité permet de définir des règles qui assurent que les permissions sur les répertoires et les fichiers sont respectés.

Elle offre un avantage d'exécuter les règles à fréquence régulière.

Ceci vous permettant même en cas d'oubli après le dépôt d'un nouveau fichier, d'assurer la cohérence des permissions.

Dans l'onglet « sécurité », cliquez sur « Editez » dans « Permissions des fichiers et des dossiers »

Dans l'onglet « Paramètres », cochez la case « Activé » afin d'indiquer que vous souhaitez modifier les permissions dans l'espace de votre site web.

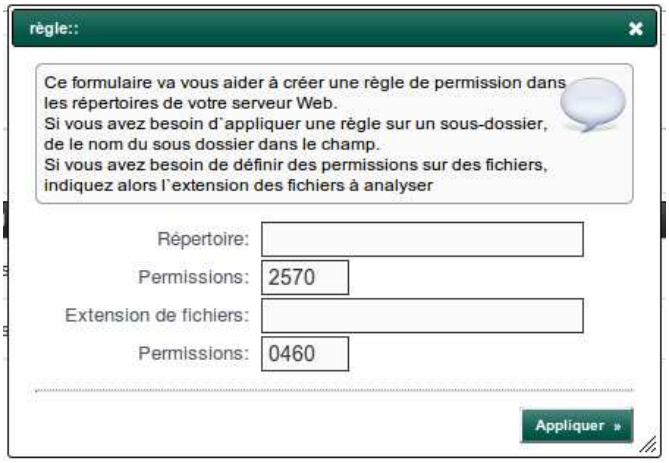
Indiquez la fréquence d'exécution du moteur de permissions.

Pour ajouter une nouvelle règle de permissions, cliquez sur le plus dans le tableau.

Par défaut, le moteur de permissions va s'exécuter dans le répertoire de votre serveur web.

Ne rien mettre dans Répertoire et extension de fichiers correspond à * comme l'exemple indiqué ci-contre.

Le moteur va appliquer les permissions 2570 sur tous les dossiers et sous-dossiers de votre espace web et les permissions 0460 sur tous les fichiers présents dans les dossiers et sous-dossiers de votre site web.

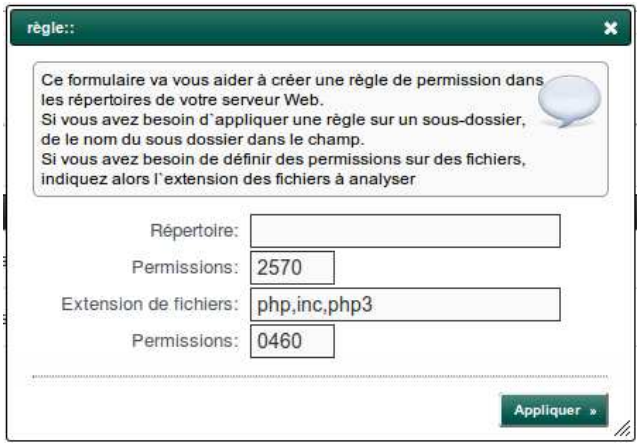


En rajoutant l'extension, nous détaillons les permissions uniquement pour les fichiers dont l'extension est « php »

Le moteur va appliquer les permissions 2570 sur tous les dossiers et sous-dossiers de votre espace web et les permissions 0460 sur tous les fichiers *.php présents dans les dossiers et sous-dossiers de votre site web.

On peut indiquer plusieurs extensions à la fois en les séparant par une virgule.

Le moteur va appliquer les permissions 2570 sur tous les dossiers et sous-dossiers de votre espace web et les permissions 0460 sur tous les fichiers *.php,*.inc,*.php3 présents dans les dossiers et sous-dossiers de votre site web.



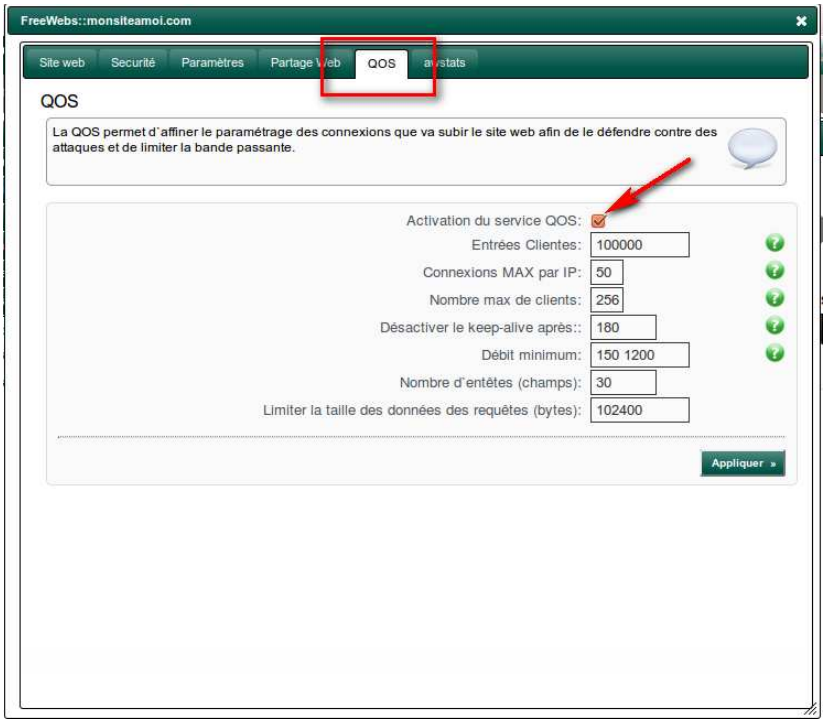
En spécifiant un répertoire on indique que le moteur commence son parcours qu'à partir du sous-répertoire du site web indiqué dans le champ « **Répertoire** ».

Le moteur va appliquer les permissions 2570 sur tous les dossiers et sous-dossiers de /download de votre espace web et les permissions 0460 sur tous les fichiers *.php,*.inc,*.php3 présents dans les dossiers et sous-dossiers de votre site web.

On peut utiliser aussi un chemin tel que /www/download/cache

Le moteur va appliquer les permissions 2570 sur tous les dossiers et sous-dossiers de /www/download/cache de votre espace web

Activation de la QOS



Normalement si Artica détecte le serveur Apache, il va tenter d'installer automatiquement le module QOS (mod_qos) sur votre système.

Si tel est le cas, un nouvel onglet QOS est disponible sur votre site web.

Ce module permet d'éviter des attaques Web et limite de façon intelligente le nombre de connexions sur le site web.

Cochez la case « Activation du service QOS »

Les valeurs par défaut sont les plus courantes, toutefois voici quelques explications :

Entrées Clientes :
C'est le nombre d'addresses IP que le module va gérer en mémoire.

Connexions MAX par IP :
Chaque addresse ne pourra pas se connecter X fois en même temps.

Nombre Max de clients :
Nombre maximum de connexions TCP actives

Désactiver le keep-alive :
Interdire les connexions persistantes lorsque le nombre de connexions TCP actives atteint 180 (70% du Nombre Max de clients)

Débit minimum :
demande minimale / vitesse de réponse (refuser les clients lents qui bloquent le serveur,par exemple. le serveur maintien des connexions ouvertes sans demander quoi que ce soit)

Nombre d'entêtes :
C'est le nombre de champs (clefs) envoyées par le client soit dans un POST, soit dans GET

Gestion du système

Centraliser les évènements systèmes.

Le système écrit ses évènements à travers un service nommé « syslog ».

Ce service écrit par défaut les évènements sur le disque dur.

Artica vous permet soit de définir un serveur centralisateur d'évènements, soit un client qui va envoyer ses évènements sur un autre serveur .

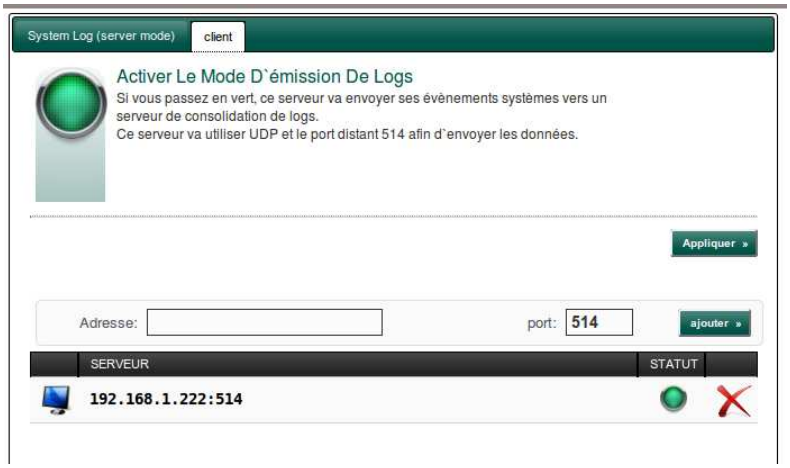
Dans « Système » puis « Config. Générale » dans le menu de gauche, choisissez « Évènements systèmes »

L'option « Activer le mode Réception de logs » transforme le serveur en « centralisateur » de logs.

Il ouvrira un port 514 en UDP afin de recevoir les évènements des autres serveurs.

L'option Activer le mode d'émission de logs indique au serveur d'envoyer ses évènements à un serveur de centralisation SYSLOG

Un formulaire est prévu à cet effet afin de rajouter les différents serveurs SYSLOG qui doivent recevoir les évènements de ce serveur.



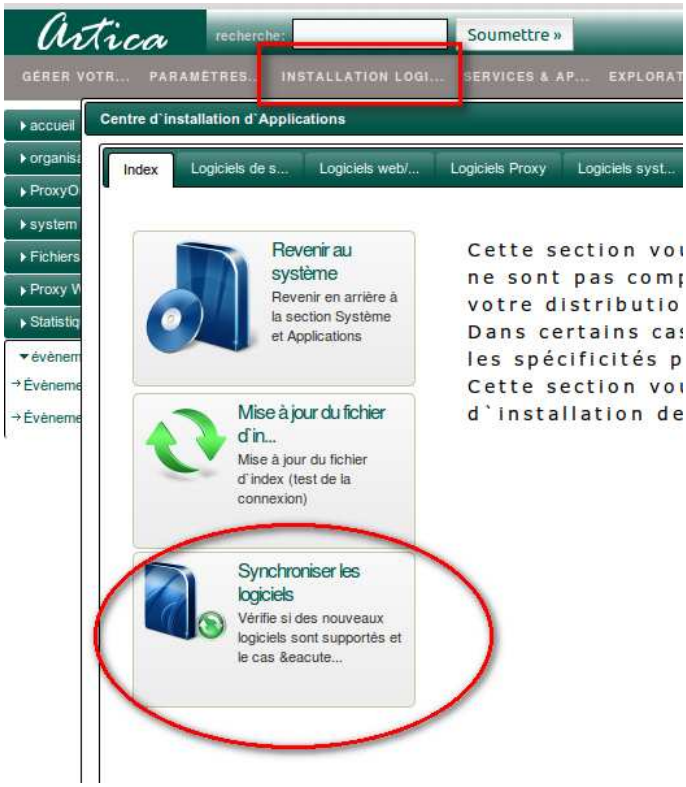
Maintient du système

Synchroniser les paquetages systèmes.

Au fur et à mesure des mises à jour du logiciel Artica, des services et des support de logiciels sont ajoutés.

Principalement, nous essayons au maximum de supporter les logiciels disponibles dans le système d'installation et de mise à jour officiel de la distribution.

De temps, et si vous désirez obtenir de nouveaux services et fonctionnalités, il est nécessaire de synchroniser les logiciels sur votre système.

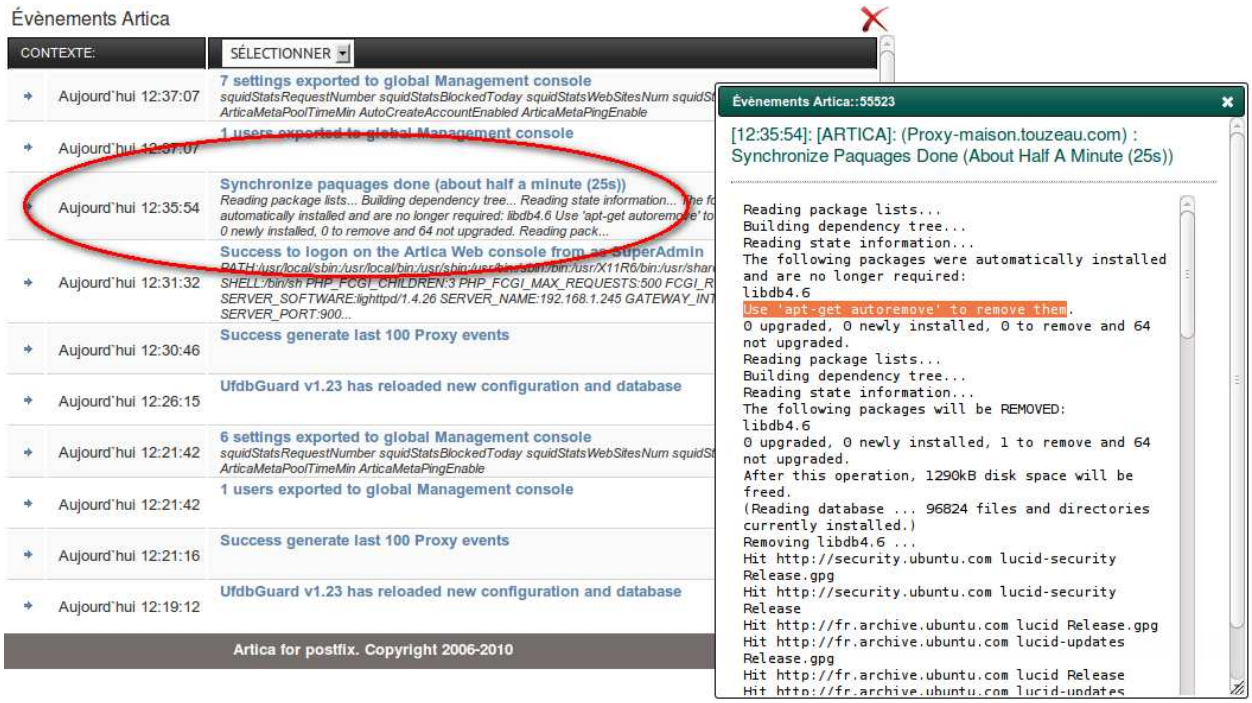


Dans le menu du haut, cliquez sur « **INSTALLATION LOGICELS** »

Dans la nouvelle fenêtre, cliquez sur l'image « **Synchroniser les logiciels** ».

Une boîte message s'affichera vous confirmant la programmation de la tâche en arrière plan.

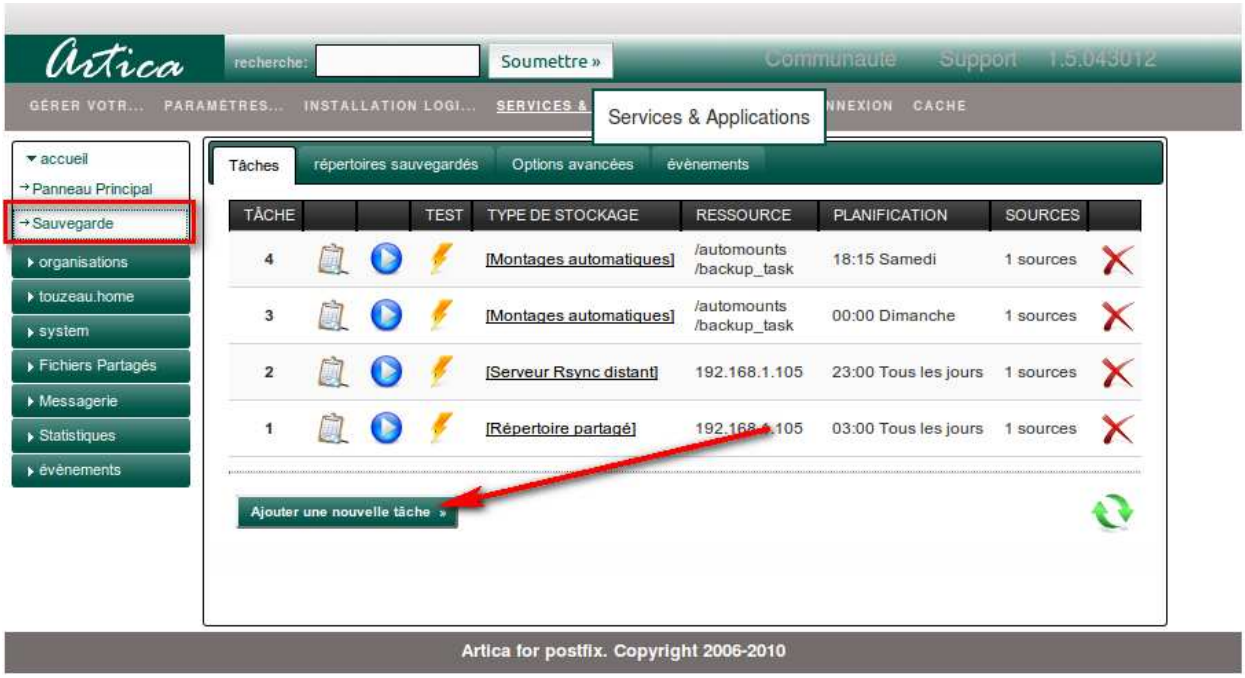
Dans les évènements Artica, vous pourrez visualiser le rapport de la tâche, une fois l'opération terminée.



Sauvegarde des données du système

Il est important de s'assurer que vous disposez de plusieurs sauvegardes afin de pouvoir restaurer le système ou bien de le dupliquer.

L'administration de la sauvegarde se situe par le menu de gauche « **Acceuil** » puis « **Sauvegarde** ».



Le système de sauvegarde s'effectue par tâche qui sont programmées pour être exécutées à une fréquence donnée.

Lorsque vous créez une tâche, par défaut, celle-ci est programmée pour sauvegarder toutes les données d'Artica, les boîtes aux lettre de messagerie, les bases de données nécessaires au fonctionnement du serveur (événements, configurations...).

Avec un jeu de sauvegarde, vous êtes en mesure de reconstruire un nouvel Artica à l'identique.

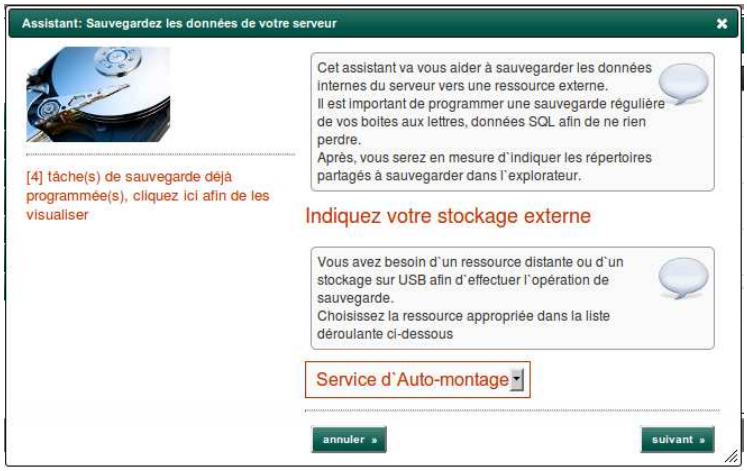
Ajouter une tâche de sauvegarde

Cliquez sur le bouton « A**jouter une nouvelle tâche** »

Une assistant va s'afficher vous proposant de programmer votre tâche de sauvegarde.

Définissez comment le système va accéder à votre ressources de stockage de la sauvegarde.

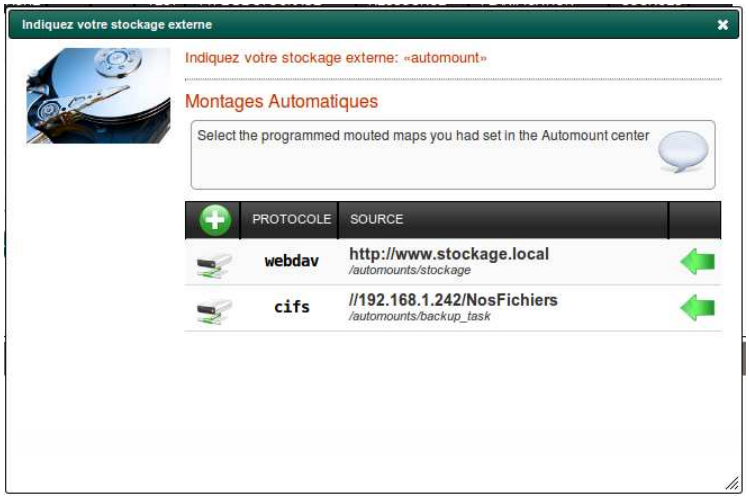
Nous vous conseillons d'utiliser le service d'Auto-montage (voir page 145) qui vous permet d'offrir de multiples protocoles pour copier les sauvegardes sur votre ressource de stockage (iSCSI, FTP, WebDav...)



La deuxième fenêtre vous affiche les ressources que vous avez programmées en tant que connexion de montage.

(Si vous avez pas encore ajouté de ressources, clique sur le plus dans le tableau).

Cliquez sur la flèche verte à droite sur la ressource que vous voulez utilisé comme stockage des jeux de sauvegarde.



La troisième fenêtre vous permet de définir la fréquence par jour et à une heure déterminée d'exécution de la tâche de sauvegarde.

Si vous désirez exécuter la sauvegarde tous les jours de la semaine, créez 7 tâches.

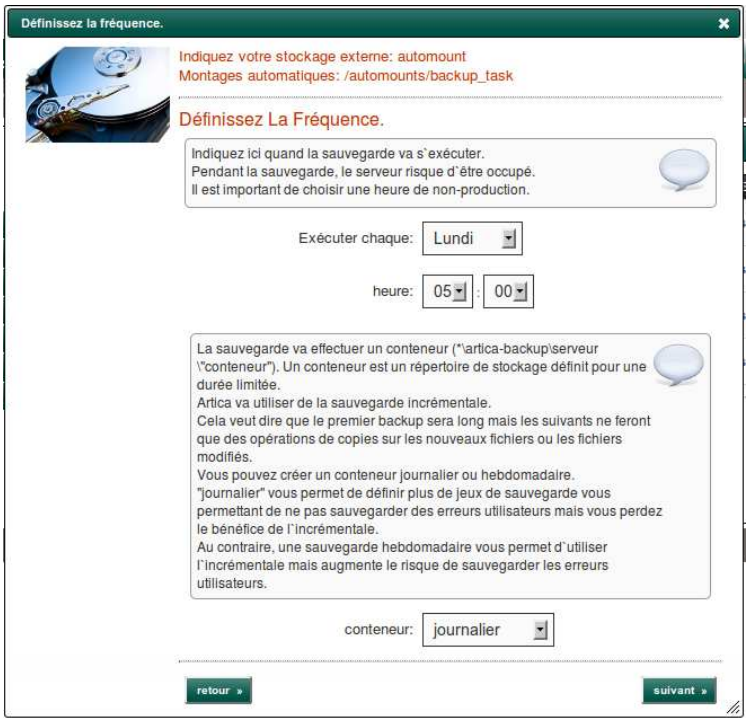
La sauvegarde va effectuer un conteneur (*\artica-backup\serveur\"conteneur").

Un conteneur est un répertoire de stockage définit pour une durée limitée.

Artica va utiliser de la sauvegarde incrémentale.
Cela veut dire que la première sauvegarde sera longue mais les suivantes ne feront que des opérations de copies sur les nouveaux fichiers ou les fichiers modifiés.

Vous pouvez créer un conteneur journalier ou hebdomadaire.
"**journalier**" vous permet de définir plus de jeux de sauvegarde vous permettant de ne pas sauvegarder des erreurs utilisateurs mais vous perdez le bénéfice de l'incrémentale.

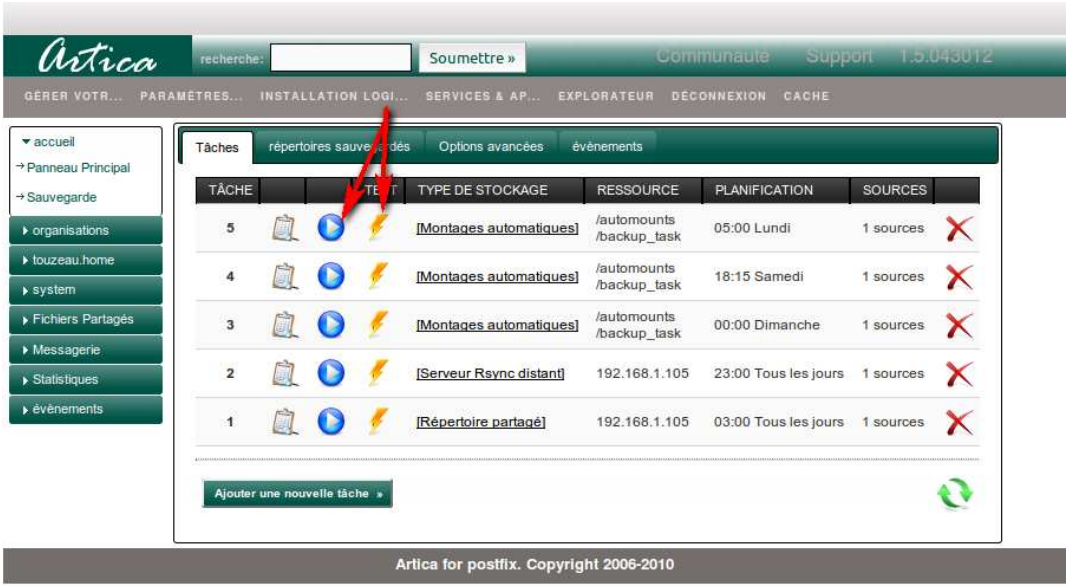
Au contraire, une sauvegarde **hebdomadaire** vous permet d'utiliser l'incrémentale mais augmente le risque de sauvegarder les erreurs utilisateurs.



Une fois la sauvegarde programmée, elle sera listée dans le tableau des tâches.

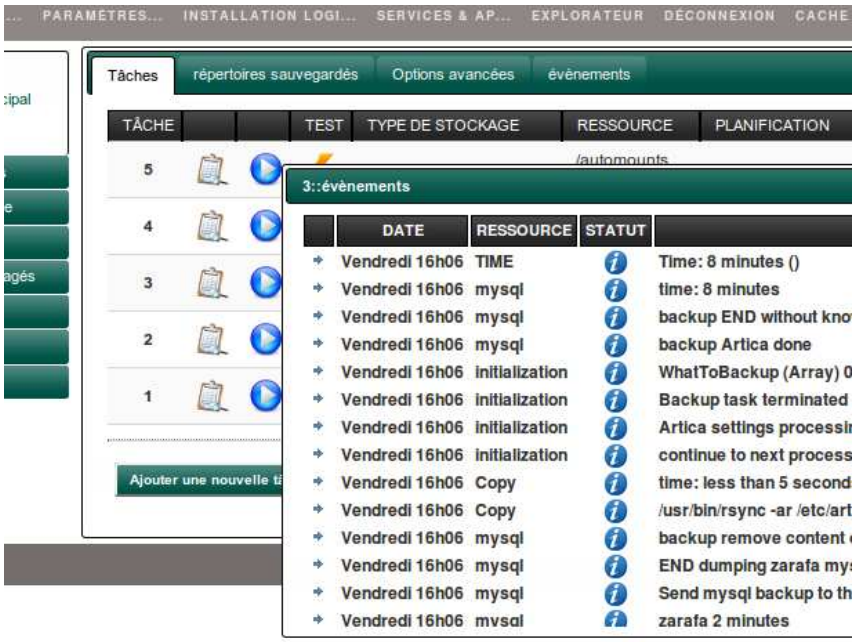
Deux images, une flèche bleue en troisième colonne vous permet de lancer la tâche immédiatement.

Une éclaire en quatrième colonne vous permet de « tester » la connexion avec la ressources utilisée. Ceci pour vous assurer que les droits de copie sont disponibles sur votre ressource.



En cliquant sur l'image de la deuxième colonne, vous accéder aux évènements de la tâche.

Ceci afin de vérifier que les éléments ont correctement été sauvegardés.



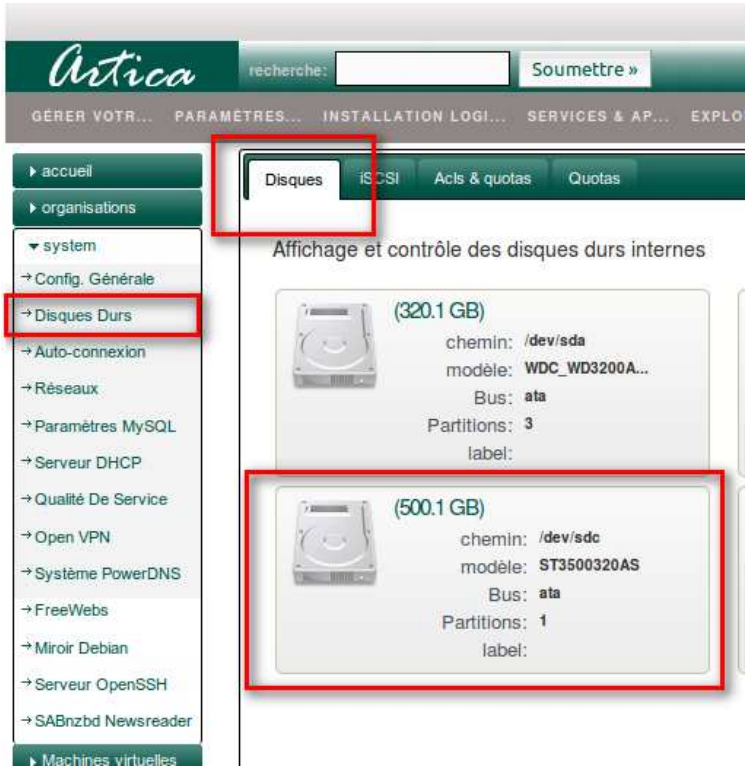
Vérifier la santé de vos disques durs.

SMART, pour Self-Monitoring, Analysis and reporting Technology, désigne un système de surveillance des disques durs.

Grâce aux informations récupérées, ce système permet d'anticiper les défaillances d'un disque (et éventuelle perte de données).

Sur la plupart des systèmes, le support de SMART est assuré.

Accéder aux données SMART dans Artica

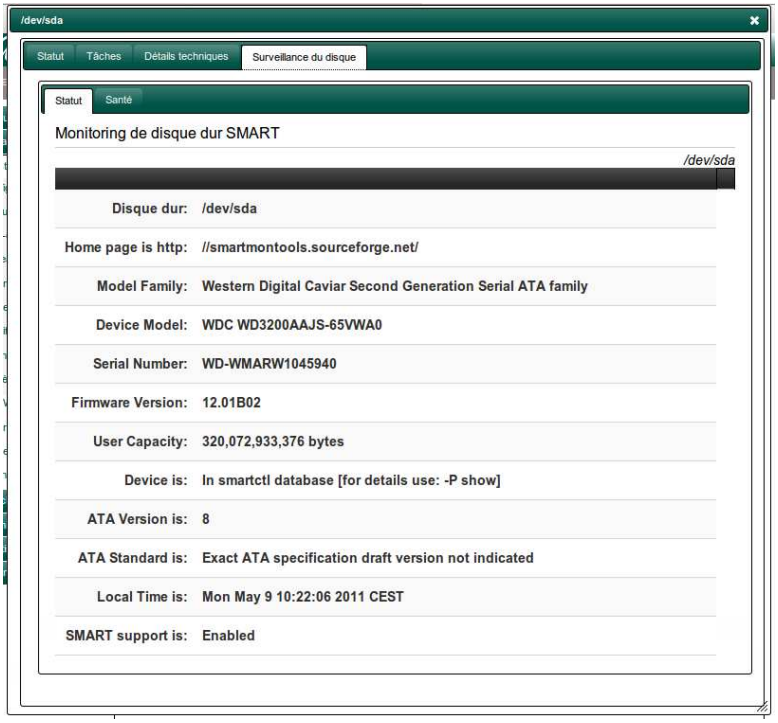


Dans le menu de gauche, sélectionnez « Système » puis « Disques durs »

Vous trouverez la liste de vos disques durs sur la partie droite.

Cliquez sur l'un des disques durs.

Une nouvelle fenêtre s'affiche.



Si le démon SMART est installé, vous devriez visualiser un onglet « **Surveillance du disque** »

En cliquant sur cet onglet, la page vous affiche un premier état des données SMART récupérées sur votre disque dur.

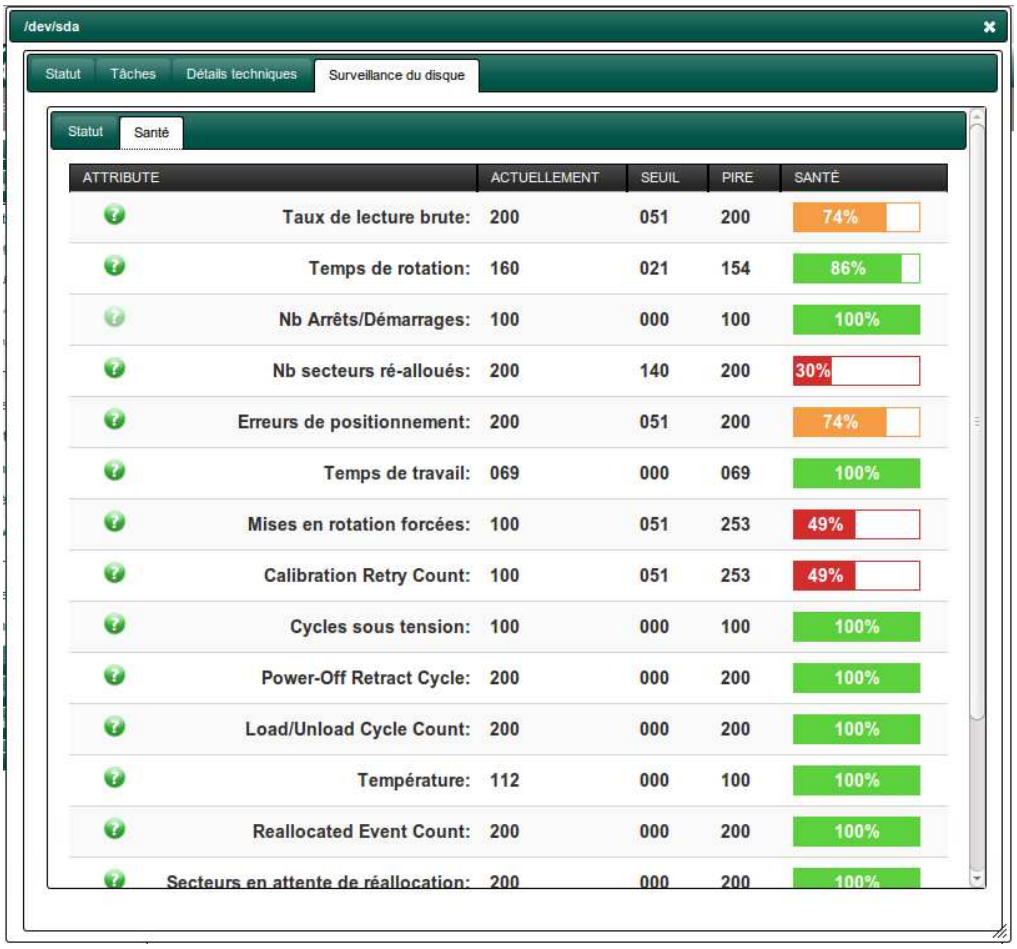
Cliquez sur l'onglet **Santé**.

Vous trouverez un tableau vous permettant de visualiser les points de contrôle de votre disque dur.

- **Actuellement** : Est la note trouvé lors du dernier test effectué automatiquement par SMART.
- **Seuil:** Est la note qu'il ne faut pas dépasser.

Le seuil est inversé dans SMART, plus la valeur est petite plus le disque est mal en point sur le point de contrôle.

> *Il ne faut alors jamais que la note actuelle « **Actuellement** » ne soit en-dessous du **seuil***



« **PIRE** » est la moins bonne valeur enregistrée.

> *Retenez que la variation de la valeur « actuellement » d'un attribut non critique n'affecte pas l'état de santé du disque tant que celle-ci demeure au-dessus du seuil spécifié par le constructeur.*

Vérification RBL (serveurs de listes noires)

Il nécessaire de vérifier la présence de votre adresse IP publique dans les serveurs de listes noires.

Ceci afin de pouvoir effectuer les opérations de dégagement sans quoi vous ne pourrez plus communiquer avec les autres serveurs de messagerie.

Bien entendu, cette fonctionnalité est surtout intéressante lorsque vous utilisez Artica comme serveur de messagerie. Toutefois, elle est activée par défaut.

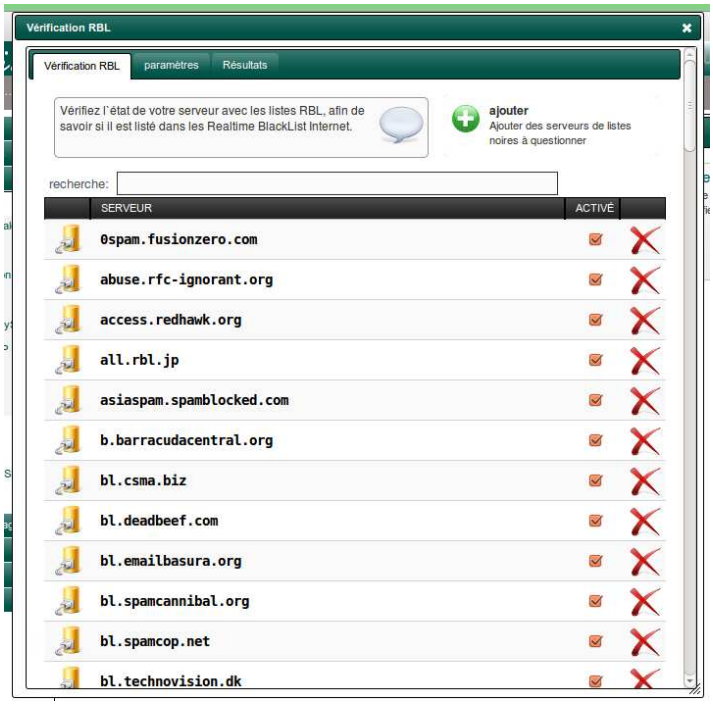
En effet, même si Artica n'est pas un serveur de messagerie, cette fonctionnalité va tester l'adresse IP publique de votre réseau.

Les paramètres de pilotage de cette fonctionnalité se trouvent par le menu de gauche « **System** » puis « **Config. Générale** »

Cliquez sur l'onglet « **DNS & Résolution** »

Liste des serveurs RBLS

Puis cliquez sur l'image « **Vérification RBL** »

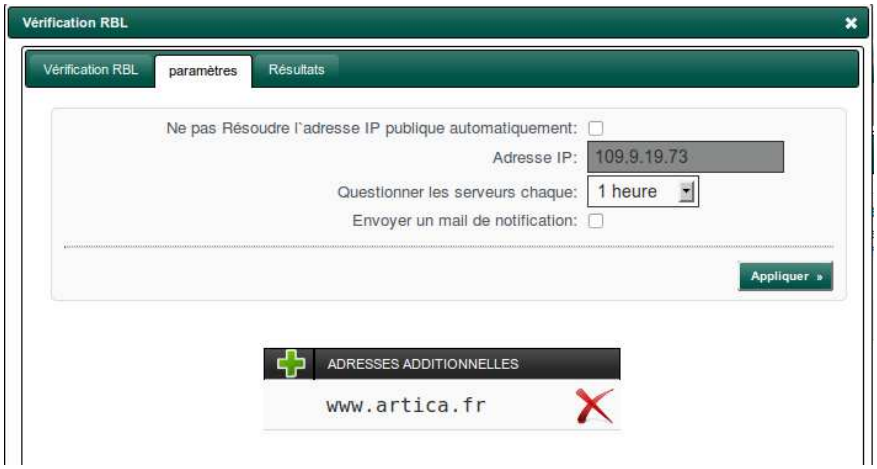


Le premier onglet « **Vérification RBL** » vous permet d'ajouter ou de retirer des serveurs de liste que Artica va consulter afin de savoir si votre adresse est listée.

Dès qu'un des serveurs à répondu, Artica va arrêter le traitement et vous émettre une notification (par email et à travers l'interface).

Paramètres

L'onglet « **paramètres** » vous permet de personnaliser le moteur.



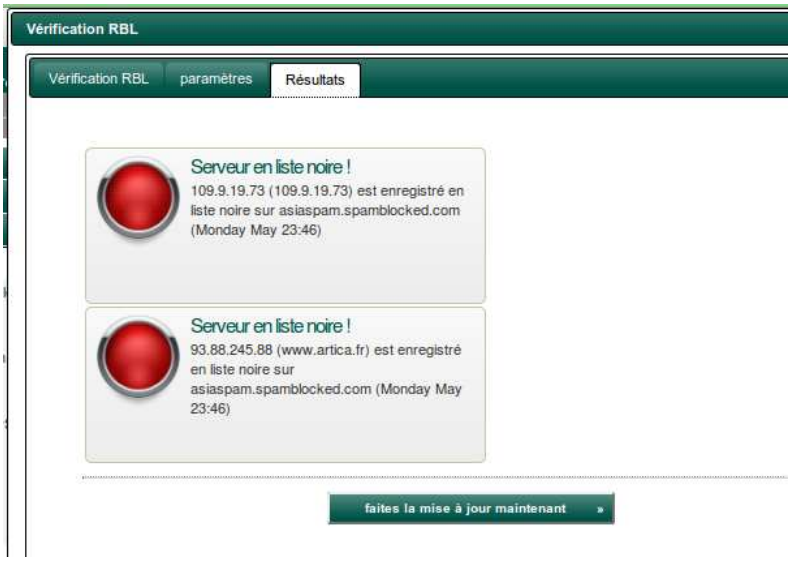
- « **Ne pas résoudre l'adresse IP publique automatiquement** » : Permet de désactiver la fonctionnalité permettant à Artica de détecter l'adresse de votre retour sur Internet.
  Si cochée, le champs « **Adresse IP** » vous invite à indiquer l'adresse de votre choix.
- « **Questionner les serveurs chaque** »: Vous permet de définir la fréquence des requêtes vers les serveurs de liste noire.
- « **Envoyer un mail de notification** » : Vous informe par email si une liste noire à référencé l'adresse de votre serveur.
- Un tableau « **Adresses additionnelles** » vous permet d'ajouter de nouvelles adresses à vérifier.
  Cliquez sur la croix verte afin de rajouter une entrée.
  Vous pouvez ajouter un nom de machine ou bien un adresse IP.

Affichage des résultats

Cliquez sur l'onglet « **Résultats** »

Vous y trouverez les résultats des précédentes vérifications.

Vous pouvez lancer une vérification forcée en cliquant sur « **faites la mise à jour maintenant** »



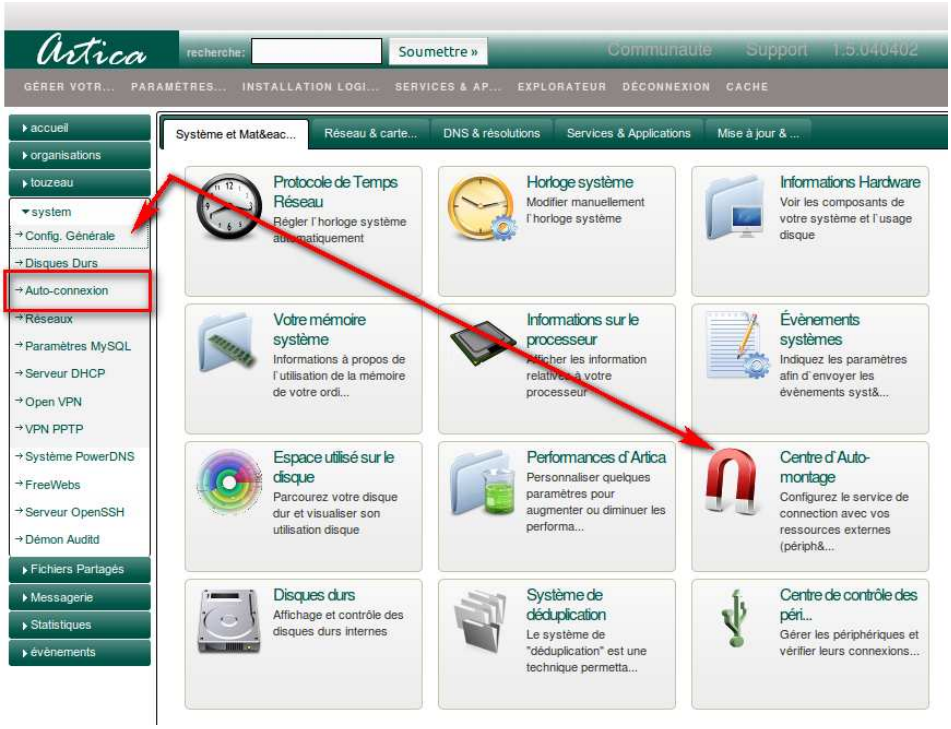
Gestion automatique des points de montage

Un point de pontage est un lien virtuel vers une autre ressource.

Cette autre ressource peut être un répertoire FTP, un répertoire distant partagé en Windows, NFS...

La technique de point de montage permet au serveur d'accéder à la ressource partagée comme un répertoire local voir même « partager » à nouveau ce répertoire.

Cette technique est très connue dans le monde Microsoft, où on « Mappe » un lecteur réseau T:///, y:// ou Z:// par exemple



Dans Artica, la gestion des points de montage se nomme « **Auto-connexion** » ou l'icône « **Centre d'Auto-montage** »

L'avantage d'utiliser ce service est que les connections s'effectuent uniquement à la demande.
Une déconnexion automatique est effectuée au bout d'un certain temps.

Contrairement à la méthode de « Mappage » Microsoft, où, lorsque vous « mappez » un lecteur, la connexion est tenue continuellement jusqu'à une déconnexion manuelle du lecteur.

En effet, les liaisons NFS/Partages Windows utilisent de la bande passante tout au long de la connexion.
Cette méthode permet d'utiliser uniquement un connexion distante qui si il y en a le besoin.

D'autre part, il vous est permis de connecter une ressource autre que celle d'un partage distant Microsoft.

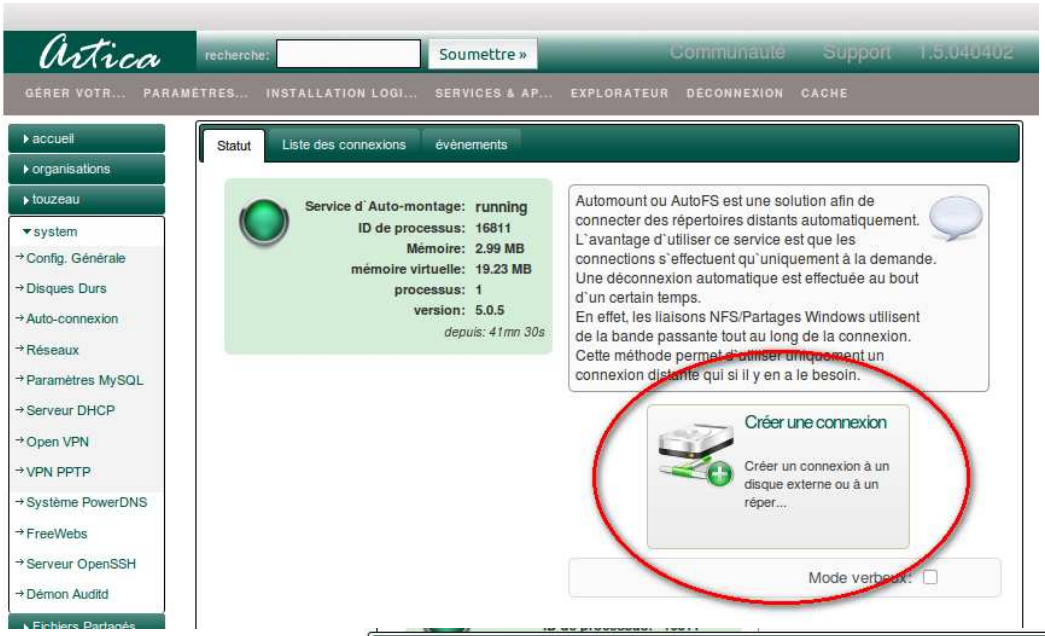
On y retrouvera les clefs USB mais aussi des répertoires distants FTP ou NFS

D'autres options d'Artica font références à cette fonctionnalité. Notamment pour y effectuer des sauvegardes.

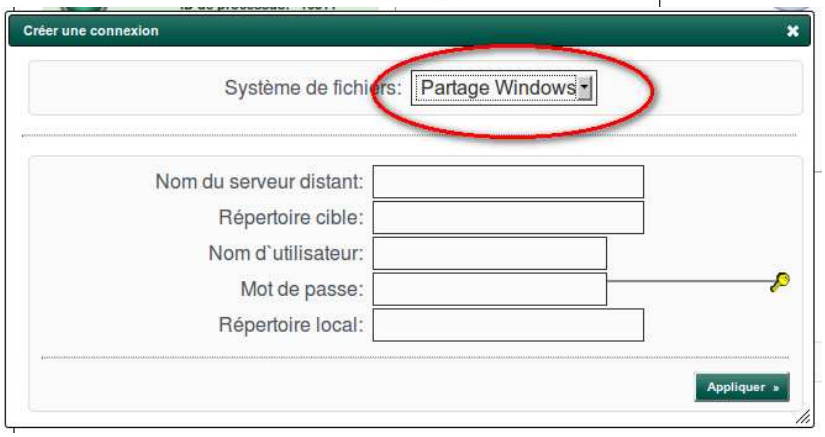
Créer une connexion vers un répertoire distant.

La création d'une connexion est assez simple en soi.

Cliquez sur l'image « **Créer une connexion** »



Une nouvelle boîte de dialogue s'affiche.



En fonction de votre système et de ce qu'il peut comprendre en type de système de fichiers, vous aurez la possibilité de choisir entre :

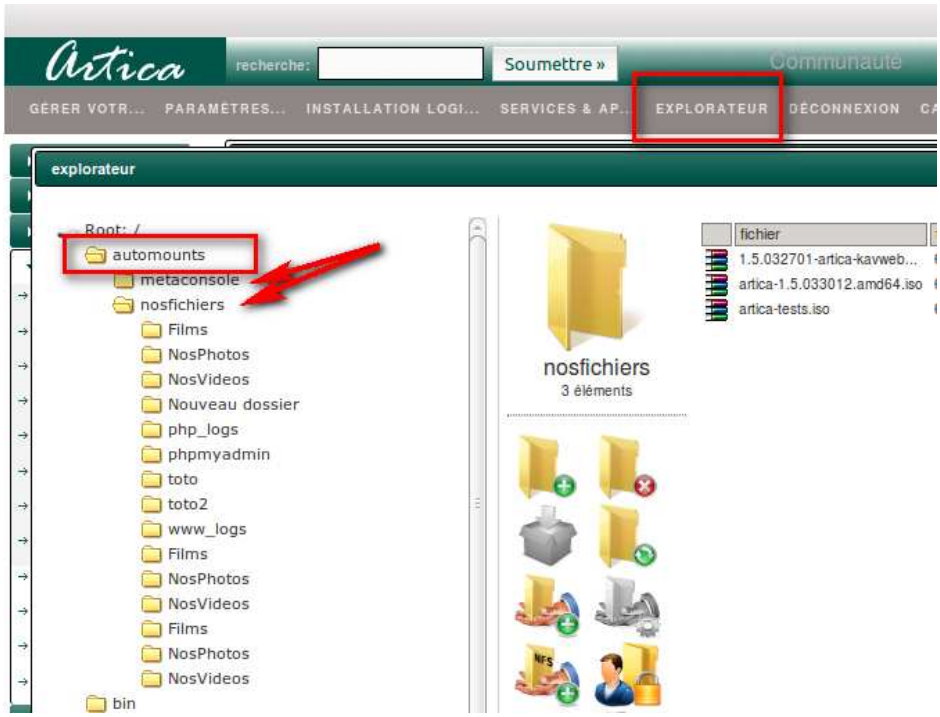
- Un disque USB externe.
- Un partage distant FTP
- Un Partage distant NFS
- Un Partage distant Windows.
- Un répertoire Web (WebDav)

Lorsque vous choisissez le système de fichier, le formulaire du dessous se modifie et vous permet de définir les paramètres de connexion.

À chaque fois vous devez indiquer le nom du point de montage local dans le champs **répertoire local**.

Ce répertoire se situe dans le répertoire principale `/automounts`.

Cela veut dire que si vous avez défini le nom du répertoire local comme « disque-500go », vous pourrez parcourir la ressource distante dans `/automounts/disque-500go`



Si les connexions sont correctement paramétrées, dans l'Explorateur d'Artica,

vous servez en mesure de visualiser le contenu des répertoires distants.

L'onglet « Liste des connexions » vous permet de visualiser l'ensemble des points de montage que vous avez programmé sur le serveur.

Artica Client ou fournisseur iCSCI

iSCSI permet d'exporter un périphérique au travers d'un réseau en le présentant comme un périphérique SCSI.

Outre le fait que le protocole SCSI est un standard de l'industrie déployé massivement en production, le fait de passer par un réseau IP classique permet de réduire les coûts de mise en œuvre par rapport au déploiement de solutions de stockage basées sur la technologie Fibre Channel.

Par ailleurs, la sauvegarde des données peut se faire au niveau du serveur iSCSI, ce qui limite le coût de la solution de sauvegarde.

L'utilisation du iCSCI est intéressant du fait que le client « croît » que le disque dur est un disque dur local.

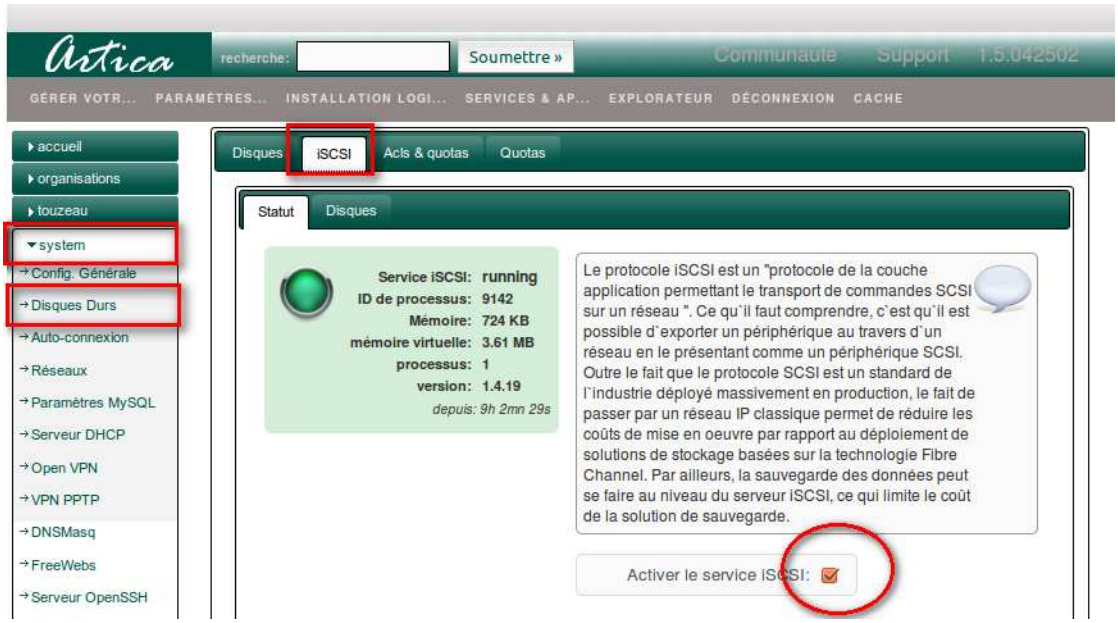
Par rapport à un partage réseau classique le iCSCI offre des performances supérieures quand à l'accès aux données 400% en lecture et 20% en plus en écriture.

Cette technique est donc très intéressante lorsqu'il s'agit par exemple de rajouter des disques durs dans un environnement virtuel afin de partager des éléments entre deux machines virtuelles installées sur le même hôte (réseau local) . Voir pour effectuer des sauvegardes du serveur Artica.

Artica fournisseur iCSCI

Dans cette section, nous allons procéder à la création et le partage des disque iCSCI sur un serveur Artica.

Dans le menu de gauche, cliquez sur **System** puis « **Disques Durs** »



Cochez la case « **Activer le service iCSCI** »

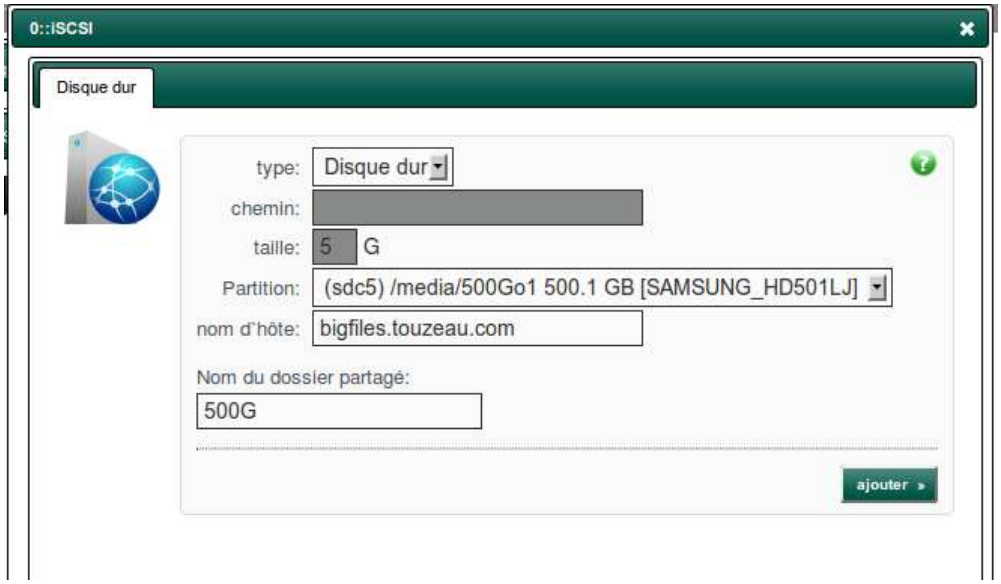
Cliquez sur l'onglet « **Disques** » puis sur l'image « **plus** » située dans le tableau.

Le formulaire d'ajout va vous proposer deux choix en « type » de disque dur iSCSI :

Le mode « **Disque dur** » qui vous permettra de sélectionner un disque dur (matériels USB compris). Vous pouvez utiliser un disque dur déjà utilisé par le système ; le système iSCSI est prévut pour ne pas « écraser » les données existantes et fournir un « Disque virtuel »

Le mode « **Fichier** » indique à Artica de créer un fichier « plat » dans le chemin stipulé dans le champ « Chemin » avec une « **Taille** » donnée.

Ce fichier sera alors vu comme un « Disque dur » par les clients iCSCI.

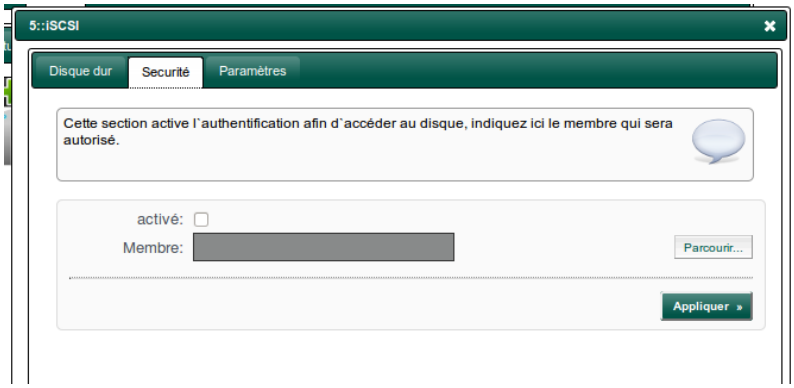


Indiquez le nom du dossier partagé que les clients vont visualiser par le réseau, ce nom de dossier sera alors « Le disque Dur » iCSCI.

La liste principale sera incrémentée par ce nouveau Disque.

Cliquez sur l'image du disque dur dans la liste.

De nouveaux onglets apparaissent vous permettant de personnaliser le Disque iCSCI dans l'ongelt « **Paramètres** » mais aussi d'assurer une authentification pour se connecter au disque dans l'onglet « **Sécurité** »



Client iCSCI sous MS Windows

Windows 7 et Windows 2008 disposent nativement du support iCSCI

Dans Windows Server 2008 R2 :

vous pouvez accéder à l'interface de l'initiateur Microsoft iSCSI de l'une des manières suivantes :

- Cliquez sur **Démarrer**, **Panneau de configuration**, **Affichage classique,** puis sur **Initiateur iSCSI**.
- Cliquez sur **Démarrer**, sur **Outils d'administration**, puis sur **Initiateur iSCSI**.
- Cliquez sur **Démarrer**, dans **Rechercher**, tapez **iSCSI**, puis dans Programmes, cliquez sur **Initiateur iSCSI**.
- Cliquez sur **Démarrer**, sur **Panneau de configuration**, dans le champ de recherche, tapez **iSCSI**, puis dans Outils d'administration, cliquez sur **Initiateur iSCSI**.

Dans Windows 7 :

vous pouvez accéder à l'interface de l'initiateur Microsoft iSCSI de l'une des manières suivantes :

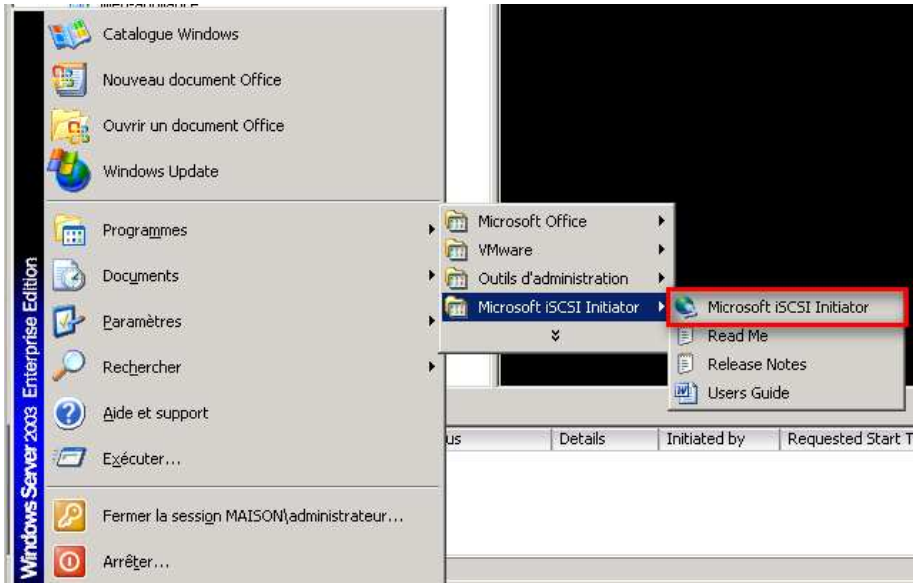
- Cliquez sur **Démarrer**, dans **Rechercher**, tapez **iSCSI**, puis dans **Programmes**, cliquez sur **Initiateur iSCSI**.
- Cliquez sur **Démarrer**, cliquez sur **Panneau de configuration**, dans le champ de recherche, tapez iSCSI, puis dans **Outils d'administration**, cliquez sur **Initiateur iSCSI**.

Dans Windows 2003 et XP

Téléchargez et installez l'Initiateur iSCSI en utilisant ce lien

http://www.microsoft.com/downloads/en/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en

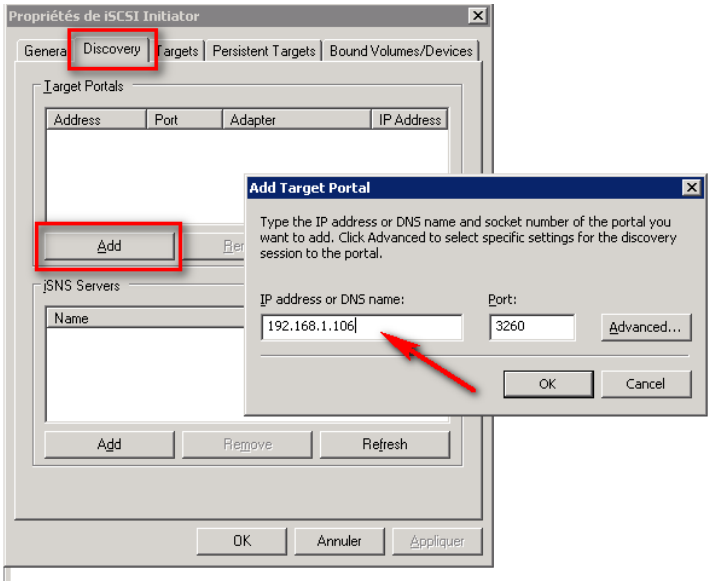
Cliquez sur « **Menu démarrer** » puis « **Programmes** » , « **Microsoft iSCSI Initiator** », « **Microsoft iSCSI Initiator** »



Cliquez sur l'onglet « **Discovery** »

Dans « **Target Portals** », cliquez sur le bouton « **Add** »

Dans « **IP address ou DNS name** » , indiquez l'adresse de votre serveur Artica qui héberge vos disques iSCSI

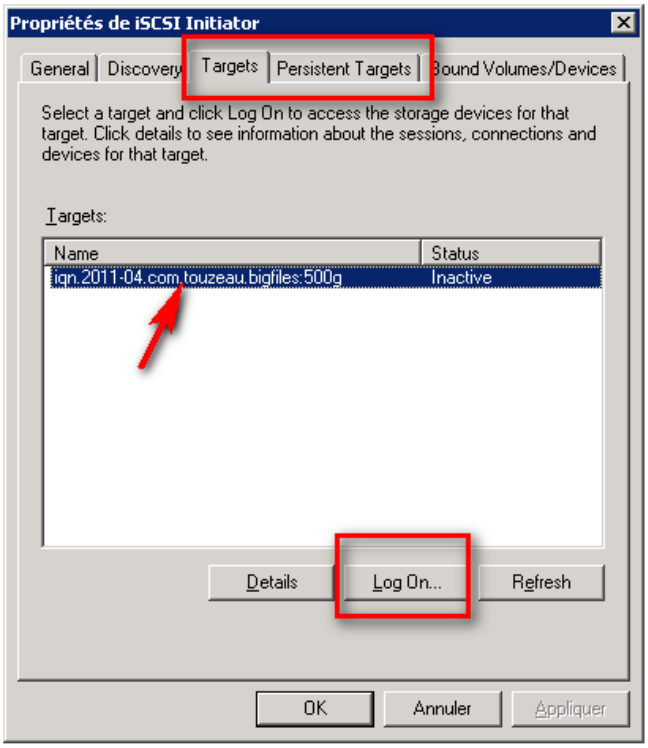


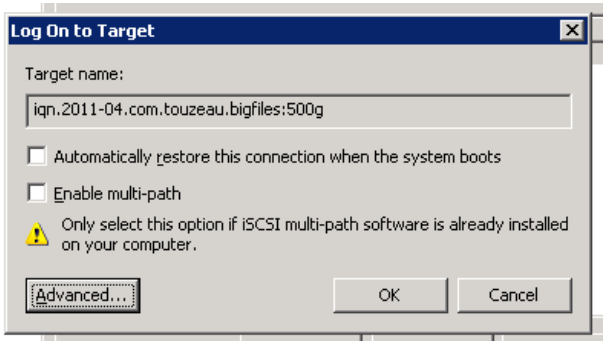
Cliquez sur l'onglet « **Targets** ».

Vous devriez retrouver le disque iSCSI partagé sur votre serveur Artica.

Sélectionnez le disque iSCSI, puis cliquez dur le bouton « **Log On..** »

Si vous désirez que le disque soit toujours présent après le redémarrage de la machine Windows, cliquez sur la case à côcher « **Automatically restore this connection when the system boots** »

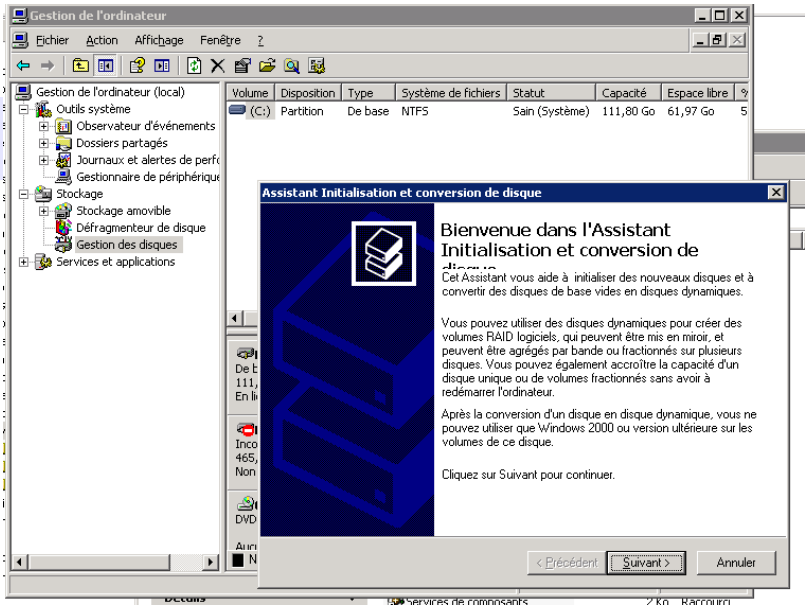




L'état doit passer en mode « Active ».

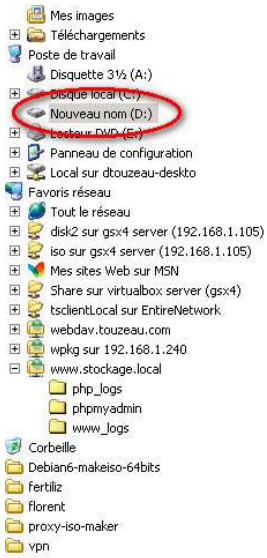
> *A partir de ce moment, c'est comme si un nouveau disque « physique » à été rajouté dans l'ordinateur.*

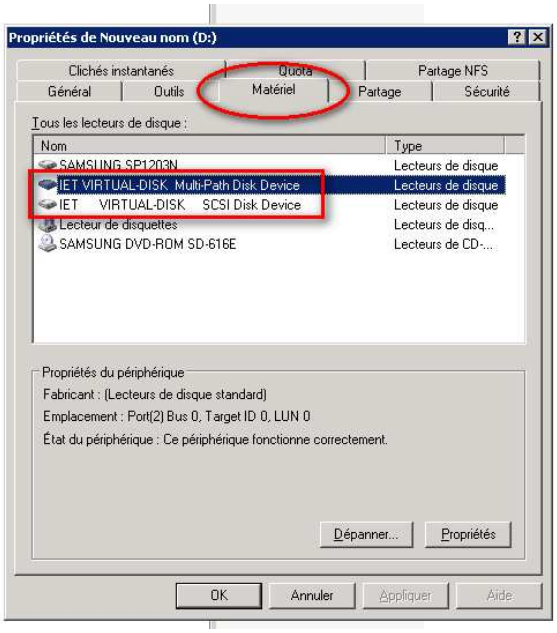
Tout comme nouveau disque, vous devez l'initialiser à travers l'outil de « **gestion de l'ordinateur** »



Dans les propriétés du nouveau lecteur, cliquez sur l'onglet « **Matériel** ».

Vous pourrez constater que le disque dispose comme constructeur. « **IET VIRTUAL DISK** »





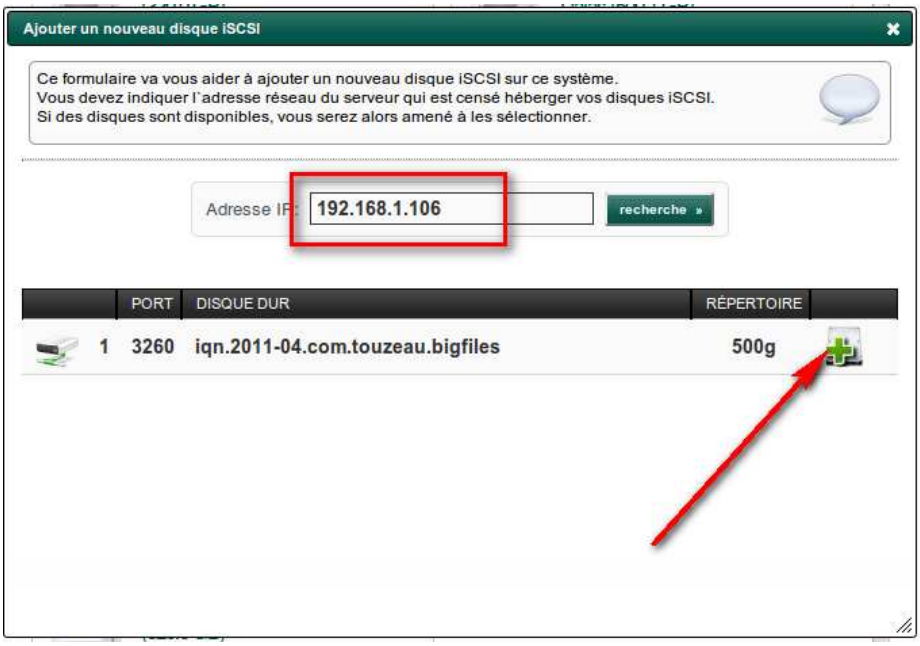
Client iCSCI sous Artica

Dans le menu de gauche, cliquez sur « **System** » puis « **Disques Durs** »

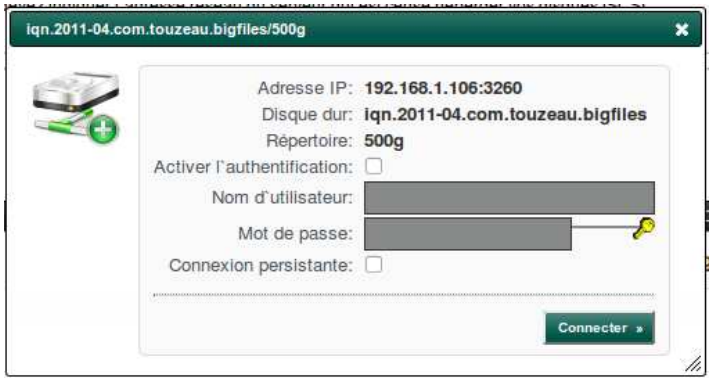
Cliquez sur l'icône avec un plus en haut à droite de la liste des disques durs.

Dans le formulaire, indiquez l'adresse IP du fournisseur de disques iSCSI

Une liste va s'afficher, vous proposant les différents disques disponibles.



Cliquez sur l'image avec un plus au niveau du disque que vous souhaitez connecter.



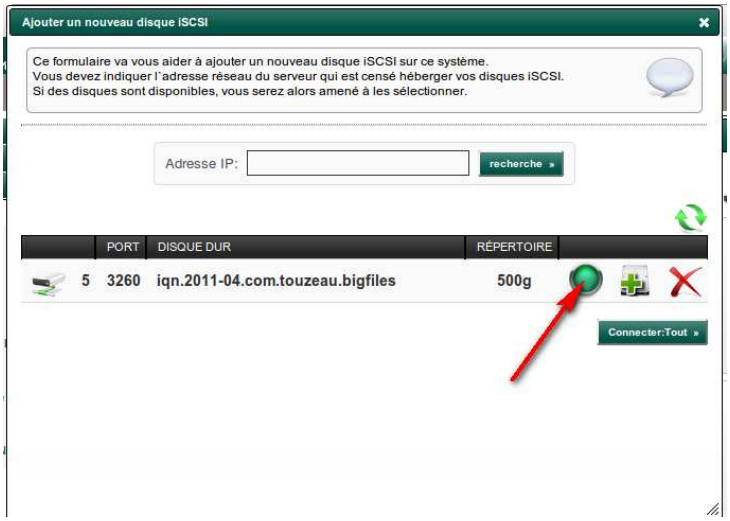
Une nouvelle boîte message apparaît vous permettant de préciser si la connexion nécessite une authentification.

Si vous désirez que le disque soit toujours présent après le redémarrage de la machine Windows, cliquez sur la case à côcher

« **Connexion persistante** »

Cliquez sur le bouton « **Connecter** »

Si le disque iSCSI est correctement connecté, un rond vert devrait s'afficher sur la ligne du disque sélectionné.



Dans la liste des disques durs, cliquez sur l'icône d'un disque du avec un « I » bleu.

Cela aura pour effet de forcer Artica à redécouvrir les disques et de régénérer la liste.

Si un disque iSCSI est présent sur le système, Artica vous affichera une icône de disque différente (avec une terre) et dans le modèle, vous pourrez constater « VIRTUAL-DISK » comme attribut.

Cliquez sur l'icône du disque dur afin de le formater ou bien de le connecter à votre système à travers le centre d'auto-montage ou bien avec le système.