

Artica Proxy AD

Proxy Internet couplé à Active Directory
et filtrage de sites web

Révision Du 28 Février 2011 version 1.5.022800



Table des matières

Introduction :	2
Historique du projet :	2
A qui s'adresse Artica ?	2
Licence et support.....	2
Que fait Artica ?	3
Couplage à Active Directory ?.....	4
Gestion des utilisateurs inchangée.....	4
Sécurité de la base de compte.....	4
Partage des équipements.....	4
Mise en place avec Artica.....	5
Installation des modules principaux.....	5
Activation Active Directory.....	6
Activation de l'authentification du proxy	8
Activation du filtrage web.....	9

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 maintien 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, veuillez 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 a 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 **mise 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 **roulage** 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 **cache**s, 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

Couplage à Active Directory ?

Par défaut, Artica offre sa propre base de données, basée sur un serveur LDAP local.

Toutefois, lorsque l'entreprise dispose déjà d'une base de comptes basée sur un serveur Microsoft Active Directory, il est plus simple de connecter le proxy au serveur Microsoft que de répliquer les utilisateurs dans la base d'Artica.

Ce document à été la conclusion de tests effectués sur Microsoft Windows Server 2003 et Microsoft Windows 2008 R2 avec Active Directory et compatibilité Windows 2003.

Gestion des utilisateurs inchangée.

Avec cette méthode, seul le serveur Active Directory est maître des opérations.

Le serveur Artica ne dispose pas des comptes utilisateurs et des mots de passe.

Sécurité de la base de compte.

Un crash du serveur Artica n'entraîne pas une perte des comptes utilisateurs puisqu'ils sont stockés sur le serveur Active Directory.

Partage des équipements.

Plusieurs Proxy Artica peuvent être mis en place. Ils sont alors tous connectés au serveur Active Directory et disposent tous de la même base de comptes utilisateurs.

Mise en place avec Artica

Dans ce document, nous allons construire un Proxy avec authentification d'utilisateurs et avec filtrage de sites web. Le proxy sera connecté à un serveur Active Directory 2008 (Windows 2003 étant aussi compatible).

Pour cela, nous avons besoin de 3 produits principaux que nous allons mettre à jour à travers le centre d'applications.

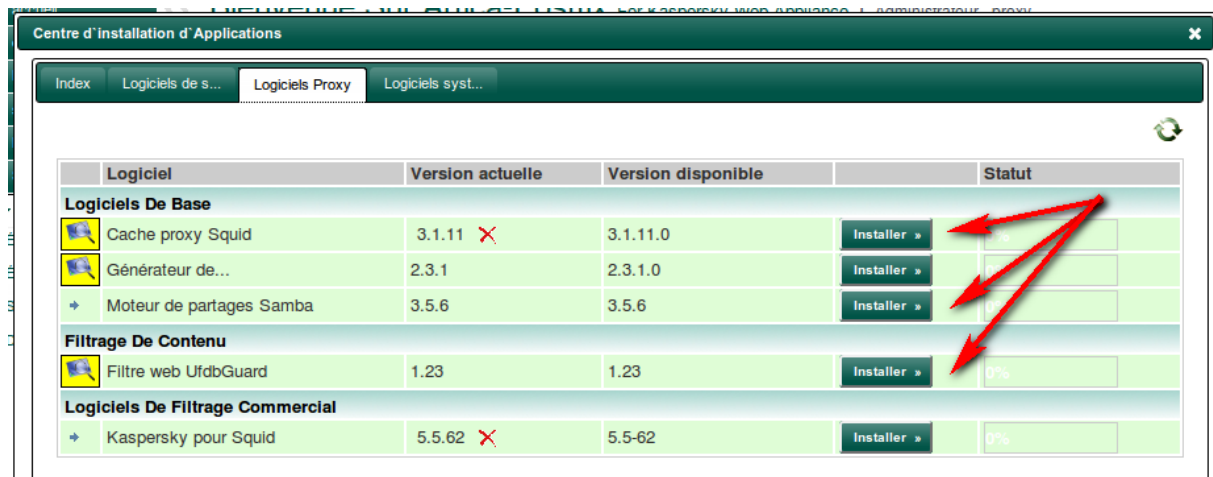
- 1) **Samba** : il servira de lien entre le proxy et le serveur de Domaine Microsoft.
- 2) **Squid** : Moteur de proxy principal. Il sera mis à jour afin de tenir compte de la présence de Samba.
- 3) **Ufdbguard** : Il offrira le filtrage de sites web en se couplant à Squid.

Installation des modules principaux.

Dans la console de gestion Artica, cliquez sur le lien en haut « **INSTALLATION LOGICELS** » et sélectionnez l'onglet « **Logiciels Proxy** »

Cliquez sur le bouton installer dans l'ordre suivant

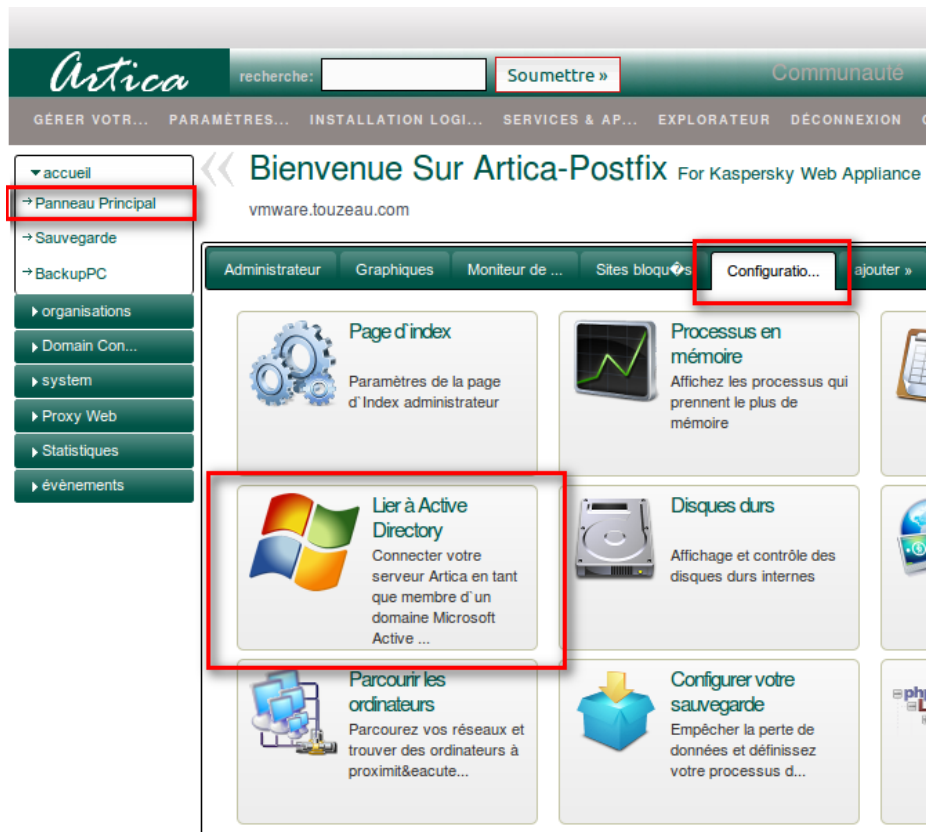
- 1) **Moteur de Partages Samba**
- 2) **Cache Proxy SQUID**
- 3) **Filtre Web UfdBguard.**



Une fois les 3 logiciels installés, cliquez sur le lien en haut « **Cache** » afin de vider le cache de la console web.

Activation Active Directory

Avec le menu de gauche (Accueil/Panneau Principal), revenez sur la page principale et cliquez sur l'onglet « **Configuration** »
Cliquez sur l'image « **Lier à Active Directory** »



Dans notre exemple, nous allons connecter le serveur Artica en tant que membre du domaine Active Directory, spécifier à Artica que sa base de compte est sur le serveur Active Directory et désactiver la fonction de partage de fichier proposée de base par Samba afin de construire un proxy client au serveur Microsoft.

La section « Lier à Active Directory » :

Indiquez le nom complet de l'ordinateur Windows Active Directory dans la champs « **Nom du serveur AD** »

Donnez (optionel) son adresse IP

Indiquez le domaine Active Directory dans le champs « **Domaine Active Directory** »

Indiquer le compte qui va permettre au serveur Artica de se connecter sur le domaine. (Administrateur par exemple)

Indiquez le mot de passe du compte de connexion.

Cliquez sur **Appliquer**.

Nom du serveur AD:	WIN-RSF60G6AS1L.touzeau.com
Adresse IP de l'AD (optionnel):	192.168.1.150
Domaine Active Directory:	touzeau.home
Administrateur Active Directory:	Administrateur
Mot de passe:	[masked]

Au bout de quelques secondes, cliquez sur l'icône de rafraîchissement.

La section du dessous doit vous indiquer les informations de connexion au serveur Active Directory.

Si tel est le cas, votre serveur Artica est alors lié au serveur Microsoft Active Directory.

Cliquez sur l'onglet « **Base utilisateurs** »

Côchez la case « **Utiliser de façon stricte le Domaine AD** »

Cette option à pour but d'indiquer à Artica que les utilisateurs ne sont pas stockés dans la base de son serveur LDAP mais sur le serveur Active Directory.

Côchez la case « **Désactiver le moteur de partage sur le réseau** ».

Cette option modifie le comportement de Samba, celui-ci écoutera l'adresse 127.0.0.1 et ne permettra pas de visualiser les partages samba. (dans notre cas, nous utilisons Samba uniquement pour la relation avec le proxy.)

Indiquez le préfix de connexion de l'utilisateur dans « Connexion DN Bind » qui permettra à Artica de « lire » les informations sur les utilisateurs dans l'Active Directory.

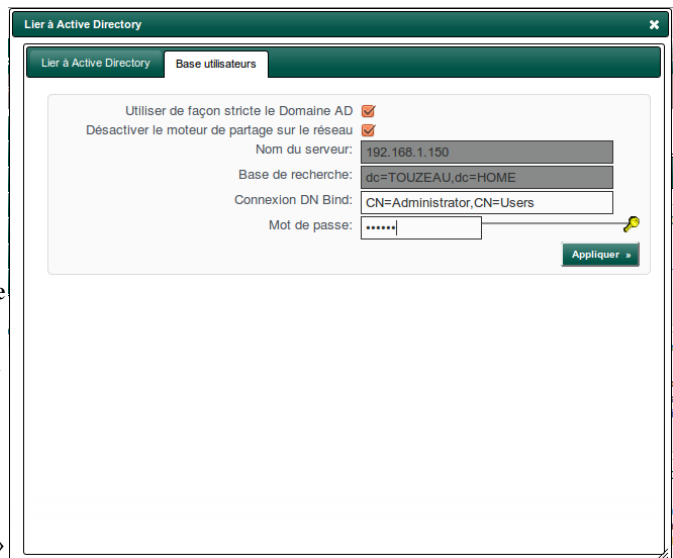
Indiquez le mot de passe de cet utilisateur.



Mot de passe: [masked] [Appliquer]

LDAP server:192.168.1.150, LDAP server name:WIN-RSF60G6AS1L.touzeau.home, Realm:TOUZEAU.HOME, Bind Path:dc=TOUZEAU,dc=HOME, LDAP port:389, Server time:dim., 27 févr. 2011 23:19:59 CET, KDC server:192.168.1.150, Server time offset:1,

[Refresh icon]



Lier à Active Directory

Base utilisateurs

Utiliser de façon stricte le Domaine AD

Désactiver le moteur de partage sur le réseau

Nom du serveur: 192.168.1.150

Base de recherche: dc=TOUZEAU,dc=HOME

Connexion DN Bind: CN=Administrator,CN=Users

Mot de passe: [masked] [Appliquer]

Activation de l'authentification du proxy

Avec le menu de gauche, cliquez sur « **Proxy Web** » puis « **Config. Générale** »

Sélectionnez l'onglet « **Filtres** »

Cliquez sur l'image « **Utilisateurs authentifiés** »



Dans la section « **Base locale** » mettez en vert le rond rouge de l'option « **Authentification Windows Samba** » et cliquez sur Appliquer

En utilisant le port du proxy vous devriez avoir un popup de connexion si votre session Windows n'est pas connectée au domaine.

Si elle est connectée au domaine, vous ne devriez pas avoir de mire d'authentification.



Activation du filtrage web

Cliquez sur l'image « **Activation des plugins Proxy** »



Mettez en vert l'option **Activer le Filtre Web UfdbGuard** et cliquez sur « **Editez** »

Cliquez sur le lien « **Cache** » en Haute afin de détruire le cache pour afficher les nouvelles fonctionnalités de filtrage.

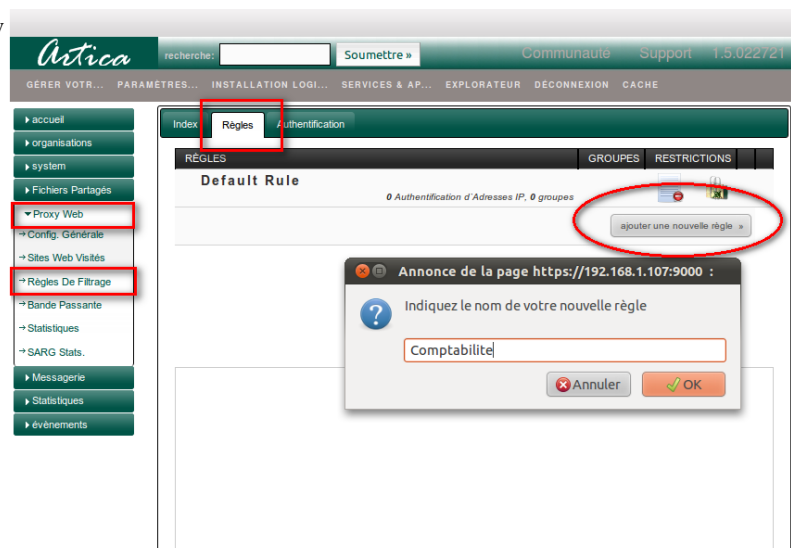


Dans le menu de gauche, sélectionnez « **Proxy Web** » puis « **Règles de Filtrage** »

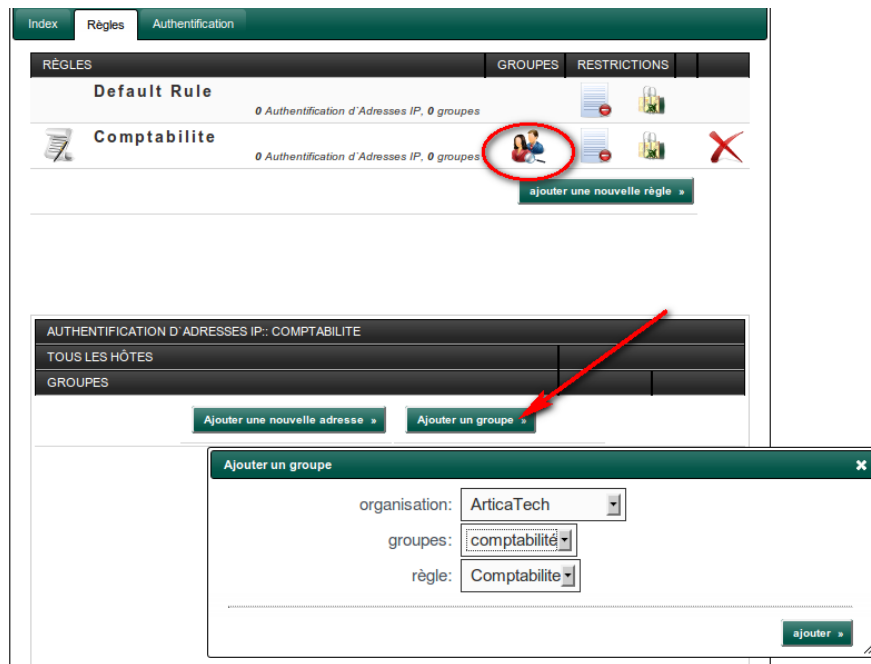
Cliquez sur l'onglet « **Règles** »

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

Indiquez le nom de votre règle (évités les accents, les espaces...)



Cliquez sur l'image représentant un groupe dans votre nouvelle règle créée. Dans le tableau, en dessous, cliquez sur le bouton « **Ajouter un groupe** ». Si les informations de connexion à votre serveur Active Directory sont correctes, le formulaire va vous afficher les organisations et les groupes de votre domaine active Directory.

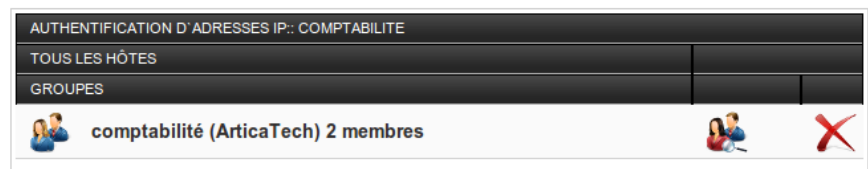


Sélectionnez le groupe Active Directory que vous désirez filtrer.

Cliquez sur « **Ajouter** »



Le tableau doit vous afficher le groupe choisi ainsi que le nombre de membres qu'héberge votre groupe Active Directory.



Cliquez sur l'image qui représente un sens interdit et une page.

Puis, cliquez sur l'image « **Catégories** »



Côchez les cases correspondantes aux catégories que vous désirez interdire au groupe que vous avez sélectionné précédemment.

Catégories ✕

Indiquez ici les catégories de sites web interdits. C'est la liste noire.

CATÉGORIE	ACTIVÉ
Site érotique à pornographie dure.	<input type="checkbox"/> adult
Sites de vente de lingerie qui présentent cette lingerie de façon sexy	<input type="checkbox"/> sex/lingerie
Les sites Web qui contiennent des sections adultes peu structurées	<input type="checkbox"/> mixed_adult
Sites Web parlant d'éducation sexuelle, pouvant être mal détectés en tant que Porno	<input type="checkbox"/> sexual_education
Sites de rencontres pour célibataires	<input type="checkbox"/> dating
Sites agressifs.	<input type="checkbox"/> agressif
Sites agressifs. (2)	<input type="checkbox"/> aggressive
Sites sur le meurtre ou permettant de blesser les gens	<input type="checkbox"/> violence
Tout ce qui parle des motos, incluant les sites marchands de fans, de passions, scooters inclus	<input type="checkbox"/> automobile/bikes
Tout ce qui concerne les bateaux à moteurs incluant les sites marchands, de passions, fans, non inclus les sites de voyages	<input type="checkbox"/> automobile/boats
Tout ce qui concerne l'automobile, constructeurs et revendeurs	<input type="checkbox"/> automobile/cars
Tout ce qui concerne les avions, hélicoptères, aéroports non inclus	<input type="checkbox"/> automobile/planes
Publicité	<input type="checkbox"/> publicite
Publicité (2)	<input type="checkbox"/> adv
Sites pour désinfecter, mettre à jour ou protéger les ordinateurs.	<input type="checkbox"/> cleaning
Sites décrivant comment fabriquer une bombe ou tout autre matière dangereuse.	<input type="checkbox"/> dangerous_material
Couvre le partage de fichiers, perr-to-peer et sites web torrent et autres sites de téléchargement aussi	<input type="checkbox"/> downloads
Sites web fournissant la messagerie instantanée, les dialogues en direct.	<input type="checkbox"/> chat
Sites web de stockage de mots de passe et d'informations sécurisées	<input type="checkbox"/> passwords
Sites parlants de drogues.	<input type="checkbox"/> drogue
Sites parlants de drogues. (2)	<input type="checkbox"/> drugs
Tous les domaines permettant aux utilisateurs d'obtenir des adresses IP dynamiques	<input type="checkbox"/> dynamic
Parent de sites d'informations financières.	<input type="checkbox"/> financial
Page de garde des sites de sociétés de banque	<input type="checkbox"/> finance/banking
Sites sur les assurances, informations relatives	<input type="checkbox"/> finance/insurance
Sites de prêts et hypothèques ou informations relatives	<input type="checkbox"/> finance/moneylending
Site d'achats et vente de immobilier, trouver des appartements à louer et à vendre	<input type="checkbox"/> finance/realstate
Tout ce qui concerne la finance qui ne correspond pas aux autres catégories	<input type="checkbox"/> finance/other
Site de Forums.	<input type="checkbox"/> forums
Site de Forums. (2)	<input type="checkbox"/> forum
Sites permettant de rassembler les internautes (sociales) pour des relations amicales	<input type="checkbox"/> socialnet

Votre filtrage Web avec authentification et groupes Active Directory est désormais en production.

Si vous venez d'installer le serveur Artica, attendez au minimum 5 heures pour que celui-ci télécharge automatiquement les bases de filtrages disponibles sur le serveur de mise à jour Artica.