PROCÉDURE D'EXPLOITATION

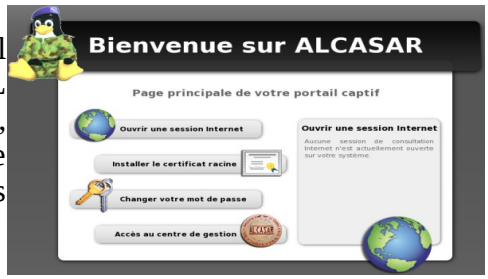
Projet : ALCASAR	Auteur : Rexy with support of « ALCASAR Team »
Objet : Document d'exploitation	Version : 2.3
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : Juillet 2011

Table des matières

Ce document présente les possibilités d'exploitation et d'administration d'ALCASAR à travers le centre de gestion graphique ou au moyen de lignes de commandes Linux (cf. §11).

1. Introduction

ALCASAR est un portail captif authentifiant et sécurisé. Ce document a pour objectif d'expliquer ses différentes possibilités d'exploitation et d'administration.

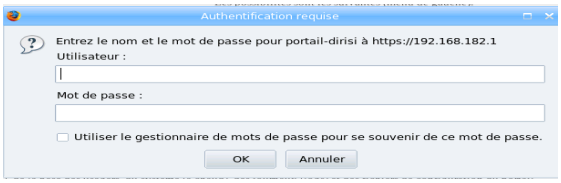


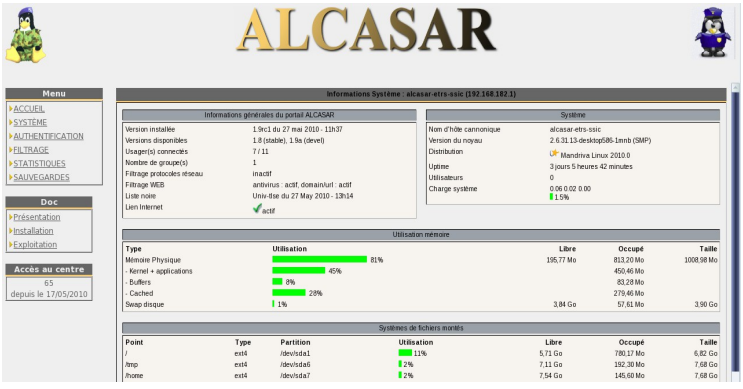
La page d'accueil du portail est consultable à partir de n'importe quel équipement situé sur le réseau de consultation. Elle est située à l'URL http://alcasar. Elle permet aux usagers de se connecter, de se déconnecter, de changer leur mot de passe et d'intégrer rapidement le certificat de sécurité dans leur navigateur. Elle permet aussi aux administrateurs d'accéder au centre de gestion graphique d'ALCASAR.

Concernant les usagers du réseau de consultation, la page d'interception suivante leur est présentée dès que leur navigateur tente de joindre un site Internet. Cette page est présentée dans l'une des 5 langues (anglais, espagnol, allemand, hollandais et français) en fonction de la configuration de leur navigateur. Aucune trame réseau en provenance de leur station ne peut traverser ALCASAR tant que le processus d'authentification n'a pas abouti.

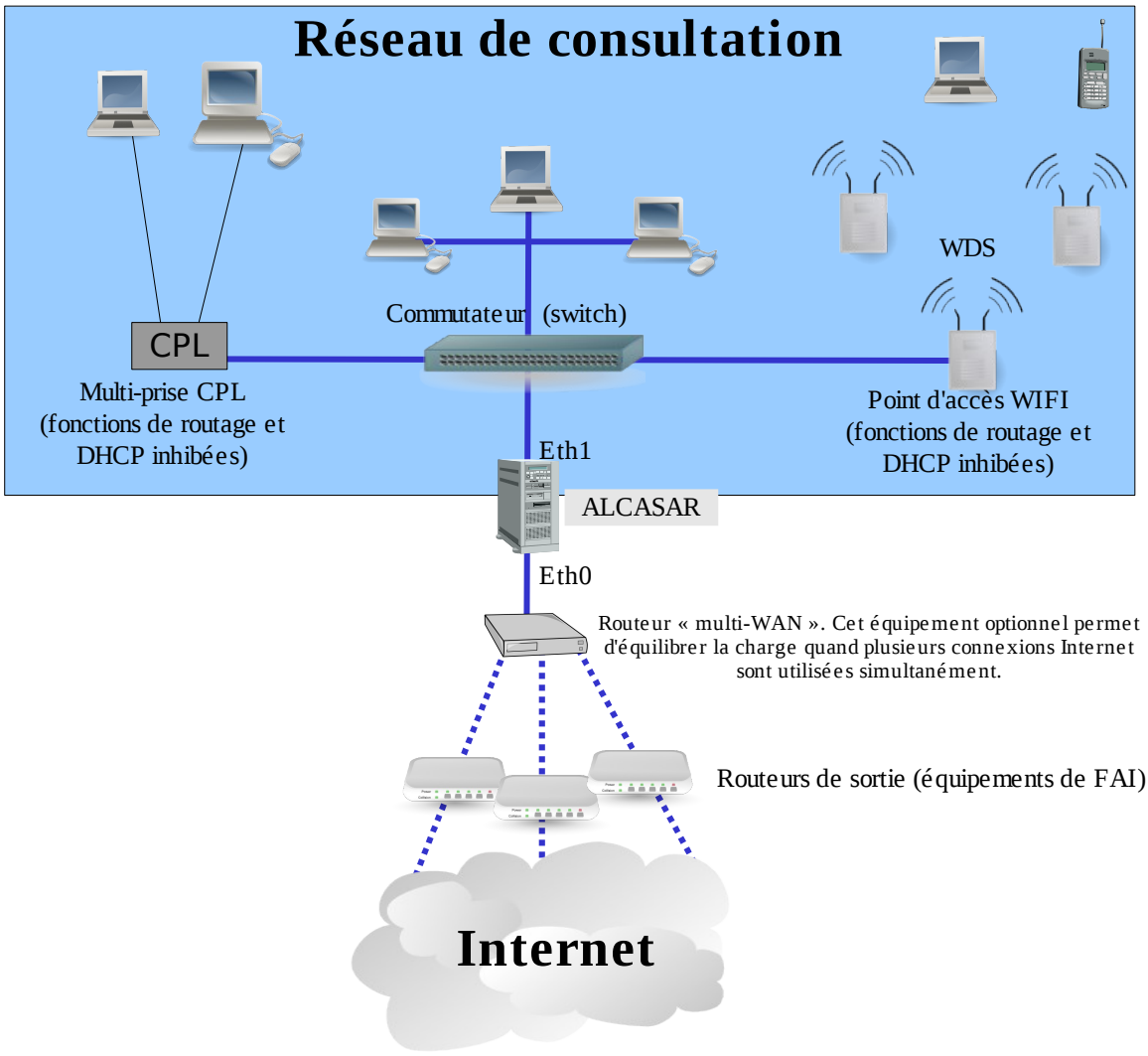
Concernant les administrateurs, le centre de gestion est exploitable de manière chiffrée (https), en deux langues (anglais et français), et après authentification sous un compte d'administration lié à l'un des trois profils suivants (cf. §7.1) :

- profil « admin » permettant d'accéder à toutes les fonctions d'administration du portail ;
- profil « manager » limité aux tâches de gestion des usagers du réseau de consultation ;
- profil « backup » limité aux tâches de sauvegarde et d'archivage des fichiers journaux.





2. Configuration du réseau de consultation



Les équipements de consultation peuvent être connectés sur un réseau local au moyen de différentes technologies (filaire Ethernet, WiFi, CPL, etc.). Ce réseau de consultation est connecté à la carte « eth1 » d'ALCASAR. Pour tous ces équipements, ALCASAR joue le rôle de routeur par défaut (default gateway), de serveur DNS et de serveur DHCP.

ATTENTION : Sur le réseau de consultation, il ne doit y avoir ni routeur ni serveur DHCP supplémentaire (attention aux points d'accès WIFI ou CPL).

2.1. Configuration des équipements des usagers

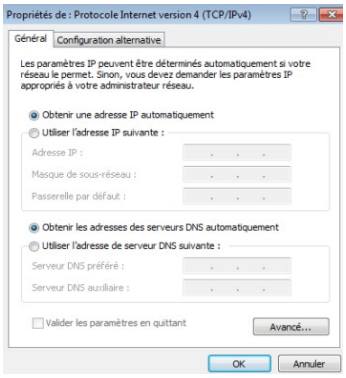
a) configuration réseau

Le plan d'adressage IP du réseau de consultation est défini lors de l'installation d'ALCASAR. Ce plan est divisé en deux : la première moitié est réservée aux équipements dont l'adresse IP est fixe (adressage statique). La deuxième moitié est réservée aux équipements dont l'adresse IP est fournie automatiquement par ALCASAR via le protocole DHCP (adressage dynamique).

Exemple du plan d'adressage de classe C proposé par défaut

- Adresse IP du réseau : 192.168.182.0/24 (masque de réseau : 255.255.255.0)
- Nombre maximum d'équipements sur le réseau de consultation : 251
- Adresse IP de la carte eth1 d'ALCASAR : 192.168.182.1/24
- Paramètres des équipements situés sur le réseau de consultation :
  - adresses IP disponibles : de 192.168.182.2 à 192.168.182.126 (fixes) et de 192.168.182.129 à 192.168.182.254 (dynamiques)
  - adresses des serveurs DNS : 192.168.182.1 (adresse IP d'ALCASAR) – suffixe DNS : localdomain ;
  - adresse du routeur par défaut (default gateway) : 192.168.182.1 (adresse IP d'ALCASAR) ;
  - masque de réseau : 255.255.255.0

Configuration en adressage dynamique (équipement privé d'usager) :

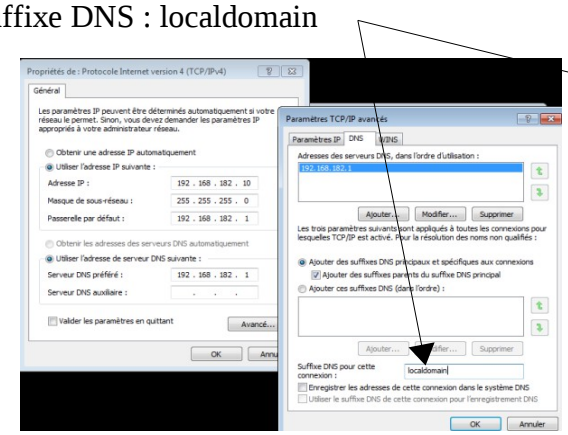


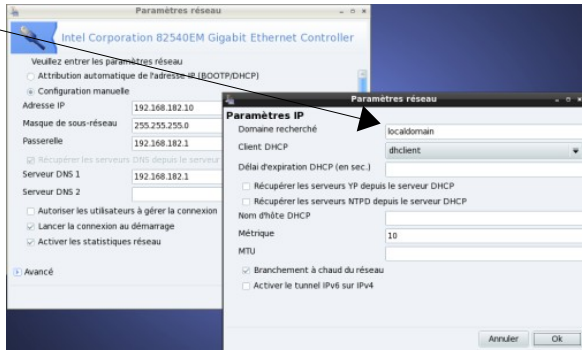
« Windows Seven » **« Mandriva Linux »**

Configuration en adressage statique (serveurs, imprimantes, point d'accès WIFI, etc.) :

Pour ces équipements, les paramètres sont :

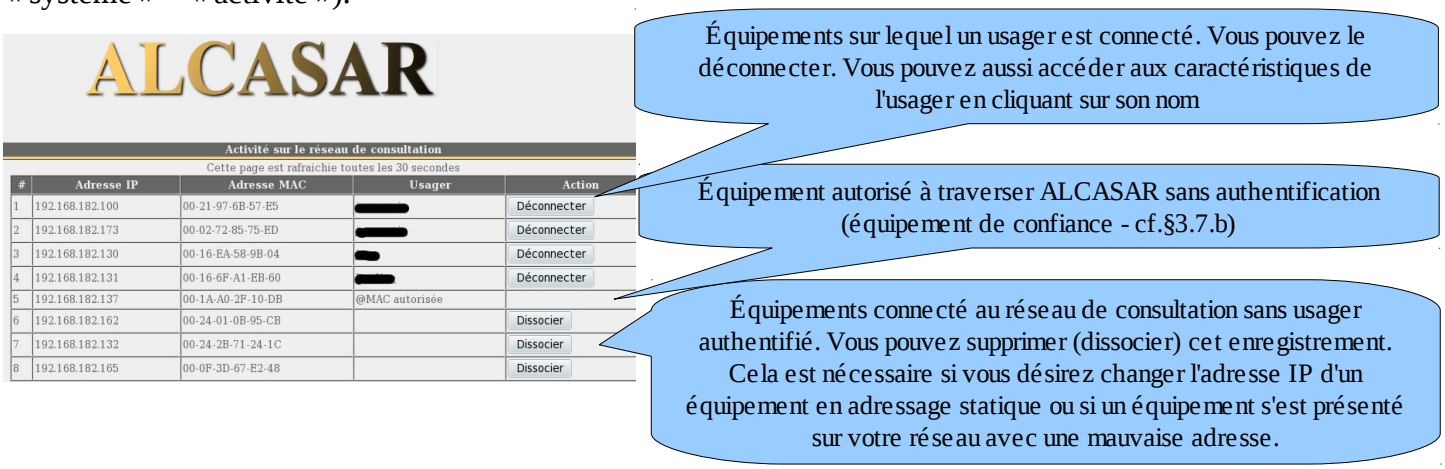
- adresse IP : parmi les adresses situées dans la première moitié du plan d'adressage ;
- routeur par défaut (default gateway) : adresse IP de la carte eth1 d'ALCASAR ;
- serveur DNS : adresse IP de la carte eth1 d'ALCASAR ;
- suffixe DNS : localdomain





« Windows Seven » **« Mandriva Linux »**

Vous pouvez afficher la liste des équipements connectés sur le réseau via le centre de gestion (rubrique « système » + « activité »).



b) Ajout d'un favoris / marque-pages (bookmark)

Les équipements des usagers ne nécessitent qu'un simple navigateur acceptant **le langage « JavaScript » ainsi que les fenêtres « pop-up »**. Pour être intercepté par ALCASAR, le navigateur doit **pointer vers un site situé sur Internet** (page de démarrage). **Les paramètres de proxy doivent être désactivés.**

Sur les navigateurs des stations de consultation, il peut être pratique d'ajouter un favori pointant vers la page d'accueil d'ALCASAR (http://alcasar) afin de permettre aux usagers de changer leur mot de passe, de se déconnecter ou d'intégrer le certificat de sécurité dans leur navigateur (cf. : §suivant).

c) Intégration du certificat de l'Autorité de Certification d'ALCASAR

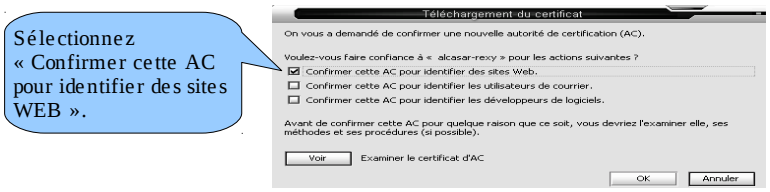
Certaines communications effectuées entre les stations de consultation et ALCASAR sont chiffrées au moyen du protocole SSL (Secure Socket Layer) associé à deux certificats créés lors de l'installation : le certificat d'ALCASAR et le certificat d'une Autorité de Certification locale (A.C.). Par défaut, les navigateurs WEB situés sur le réseau de consultation ne connaissent pas cette autorité. Ils présentent donc les fenêtres d'alerte suivantes lorsqu'ils communiquent pour la première fois avec le portail.

« Mozilla-Firefox »

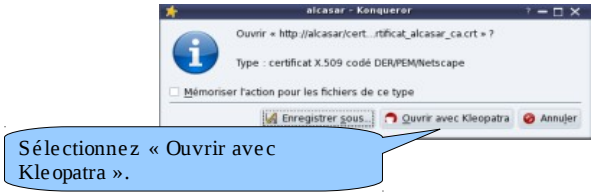
« Microsoft-I.E. »

« Google-chrome »

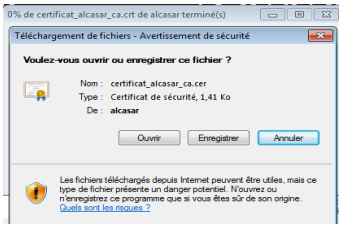
Bien qu'il soit possible de poursuivre la navigation, il est intéressant d'installer le certificat de l'A.C locale (certificat racine) dans les navigateurs afin qu'ils ne présentent plus ces fenêtres d'alerte[1]. Pour cela, cliquez sur la zone « Installer le certificat racine » de la page d'accueil du portail (« http://alcasar »). Pour chaque navigateur, l'installation est la suivante :



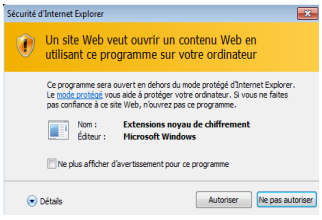
« Mozilla-Firefox »



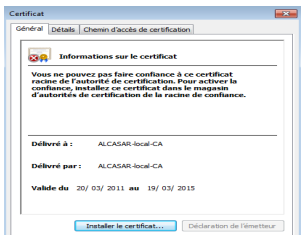
Konqueror



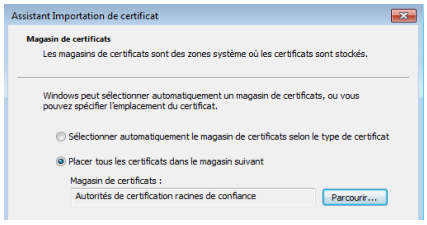
1 – cliquez sur « ouvrir »



2 – cliquez sur « autoriser »



3 – cliquez sur « installer le certificat »



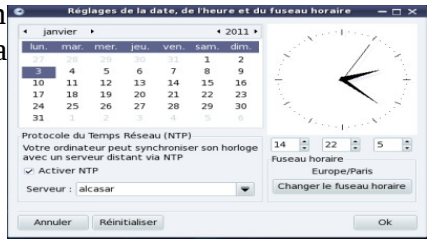
4 – choisissez le magasin « autorité de certification racine de confiance »

« Internet Explorer 8 » et « Safari »

« Google chrome » : Chrome enregistre le certificat localement en tant que fichier (« certificat_alcasar_ca.crt »). Sélectionnez « préférences » dans le menu de configuration, puis « options avancées », puis « gérer les certificats » et enfin « importer » de l'onglet « Autorités ».

d) Synchronisation horaire

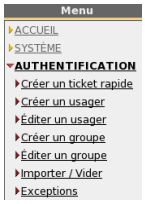
ALCASAR intègre un serveur de temps permettant aux équipements de consultation d'être synchronisés. Il suffit de configurer les horloges des équipements pour exploiter le protocole « NTP » sur le serveur « ALCASAR ». L'exemple suivant illustre cette configuration sur une station de consultation Linux-Mandriva (click droit dans l'horloge puis « Régler la date et l'heure » puis cocher « Activer NTP » + serveur « ALCASAR »).



1 Vous pouvez éviter cette manipulation en achetant et en intégrant à ALCASAR un certificat officiel reconnu par l'ensemble des navigateurs (cf. §7.5).

3. Gérer les usagers

Une fiche explicative à destination des usagers est disponible au §12.
L'interface de gestion des usagers est disponible, après authentification, sur la page de gestion du portail (menus « AUTHENTIFICATION »).
Les possibilités de cette interface sont les suivantes :

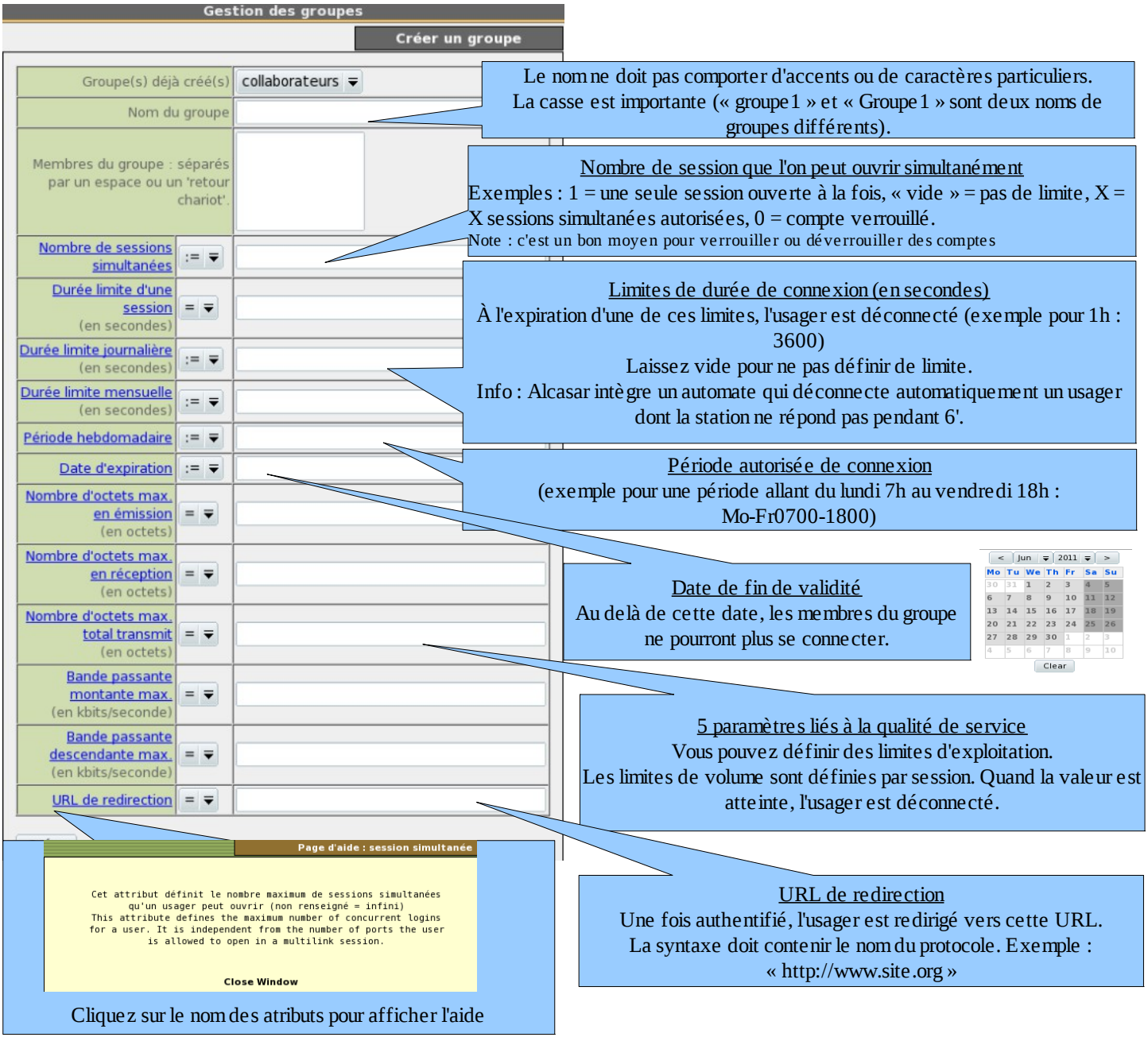


- créer un usager rapidement (ticket ou voucher). Seuls, les attributs principaux apparaissent et sont prérenseignés (exemple : la date d'expiration est fixée à la date du lendemain).
- créer, chercher, modifier et supprimer des usagers ou des groupes d'usagers ;
- importer des noms d'usager via un fichier texte ou via un fichier archive de la base de données ;
- vider la base des usagers ;
- définir des équipements de confiance pouvant joindre Internet sans authentification (exceptions).

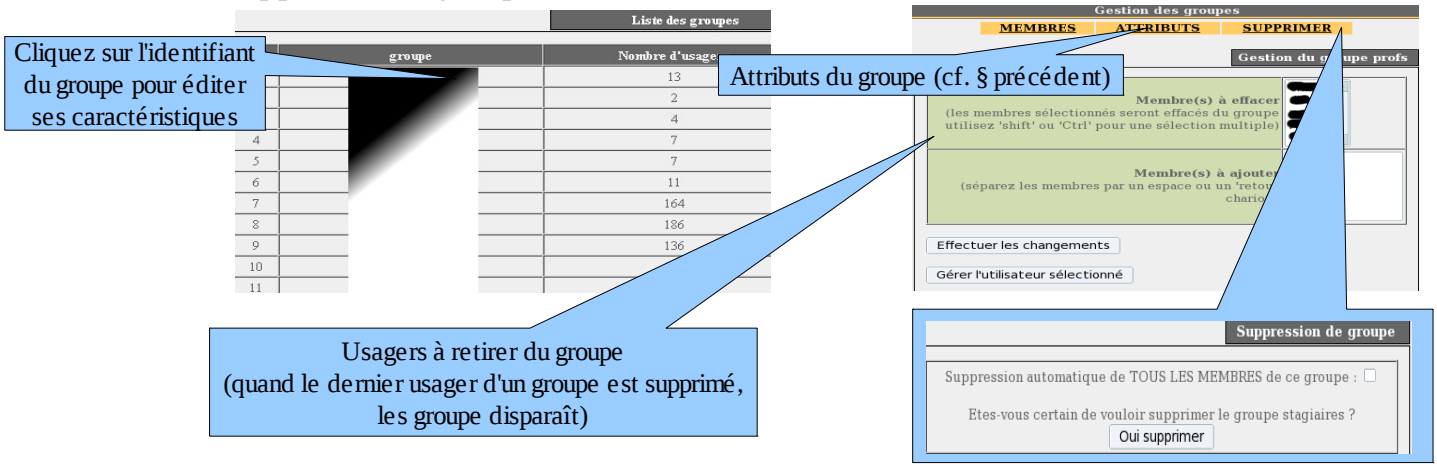
D'une manière générale, et afin de limiter la charge d'administration, il est plus intéressant de gérer les usagers à travers des groupes. À cet effet, la première action à entreprendre est de définir l'organisation (et donc les groupes) que l'on veut mettre en place.

3.1. Créer un groupe

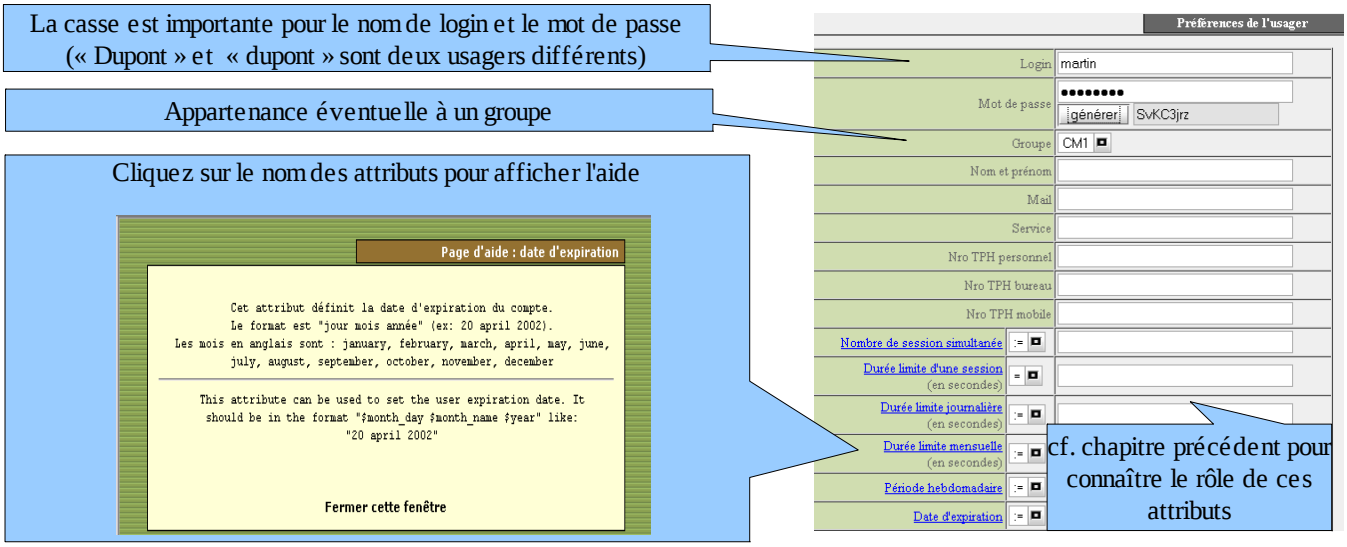
Lors de la création d'un groupe, vous pouvez définir les attributs qui seront affectés à chaque membre.



3.2. Éditer et supprimer un groupe



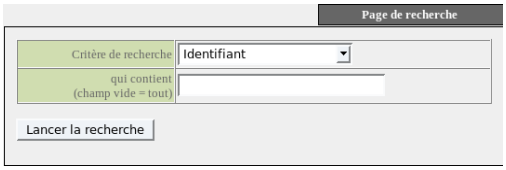
3.3. Créer un usager

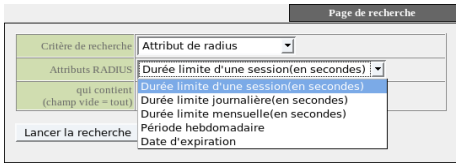


Une fois l'usager créé, un ticket d'impression au format PDF est généré dans la langue de votre choix.
Note1 : quand un paramètre est défini à la fois pour un usager et pour son groupe d'appartenance (exemple : durée d'une session), c'est le paramètre de l'usager qui est pris en compte.
Note2 : quand un usager est membre de plusieurs groupes, le choix de son groupe principal est réalisé dans la fenêtre d'attributs de cet usager (cf. §suivant).
Note3 : lorsqu'un usager est verrouillé par un des ses paramètres, il en est averti par un message situé dans la fenêtre d'authentification (cf. « fiche 'usager' » à la fin de ce document).

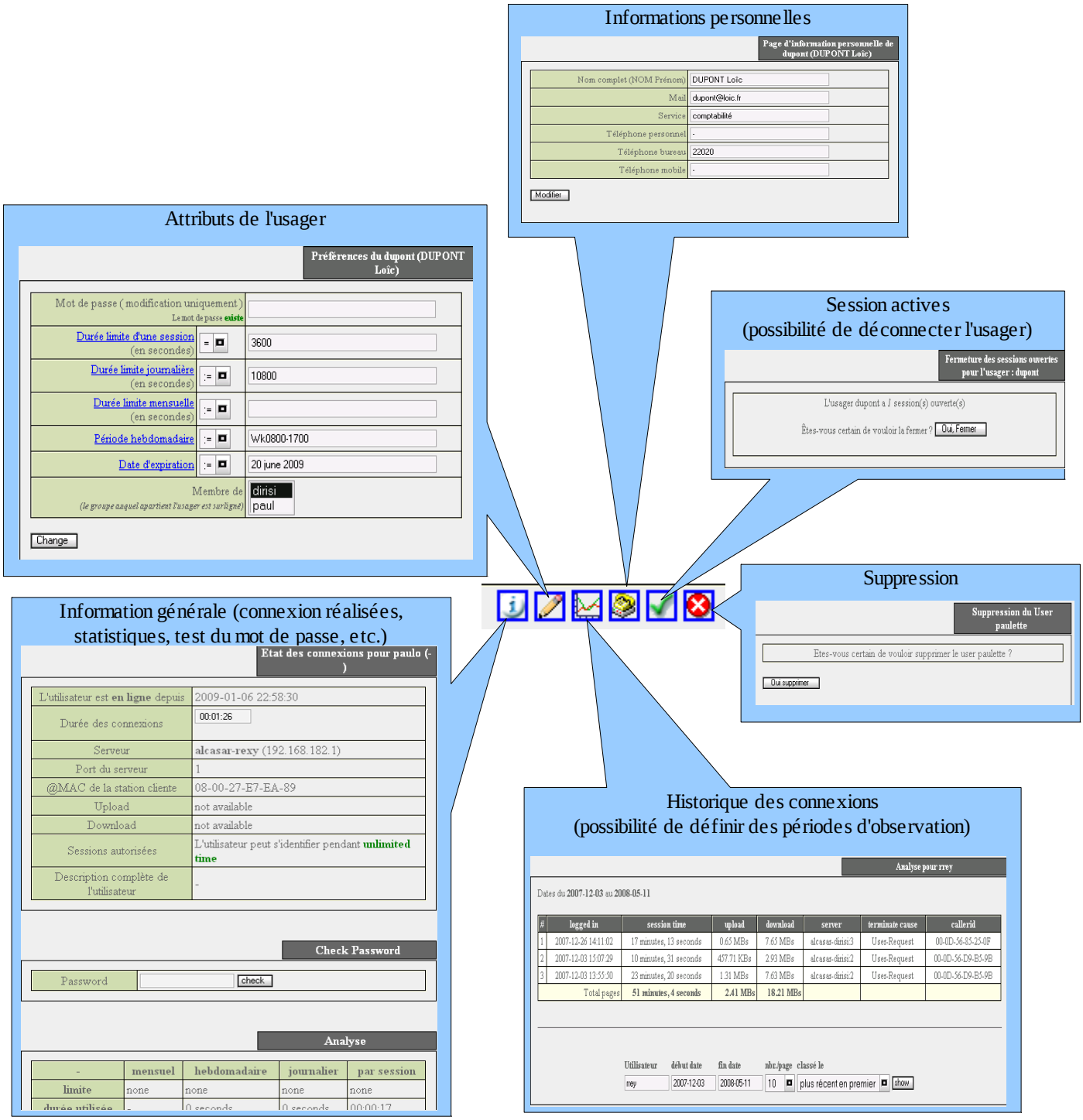
3.4. Chercher et éditer un usager

Il est possible de rechercher des usagers en fonction de différents critères (identifiant, attribut, etc.). Si le critère n'est pas renseigné, tous les usagers seront affichés.





Le résultat est une liste d'usagers correspondant à vos critères de recherche. La barre d'outils associée à chaque usager est composée des fonctions suivantes :



3.5. Importer des usagers

Via l'interface de gestion (menu « AUTHENTIFICATION », « Importer ») :

a) À partir d'une base de données préalablement sauvegardée

Cette importation supprime la base existante. Cette dernière constituant une partie des pièces à fournir en cas d'enquête, effectuez-en une sauvegarde avant de lancer l'importation (cf. §6.2).

b) À partir d'un fichier texte (.txt)

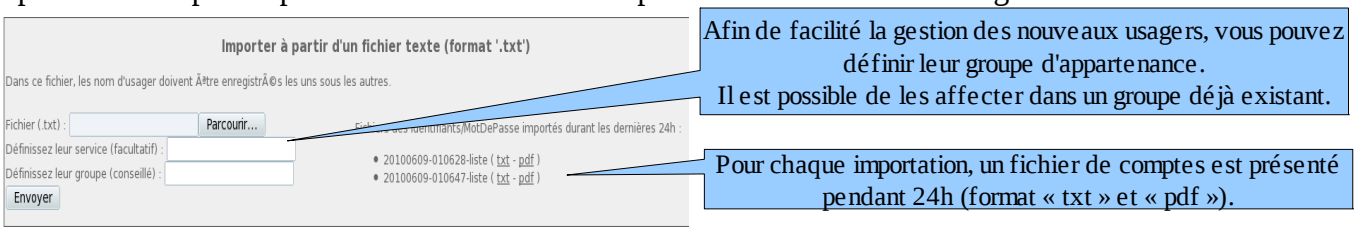
Cette fonction permet d'ajouter rapidement des usagers à la base existante. Ce fichier **texte** ne doit contenir **que les noms de connexion écrits les uns sous les autres**.

Ce fichier peut être issu d'un tableur :

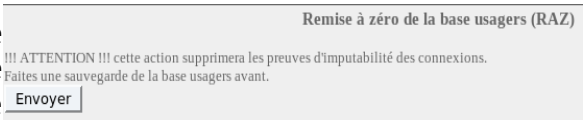
- dans le cas de la suite « Microsoft », enregistrez au format « Texte (DOS) (*.txt) » ;

- dans le cas de « LibreOffice », enregistrez au format « Texte CSV (.csv) » en supprimant les séparateurs (option « éditer les paramètres de filtre »).

Une fois le fichier importé, ALCASAR crée chaque nouveau compte associé à un mot de passe généré aléatoirement. Si des noms de compte existaient déjà, le mot de passe est modifié. Deux fichiers au format « .txt » et « .pdf » contenant les identifiants et les mots de passe sont générés et stockés pendant 24 h dans le répertoire « /tmp » du portail. Ces fichiers sont disponibles dans l'interface de gestion.



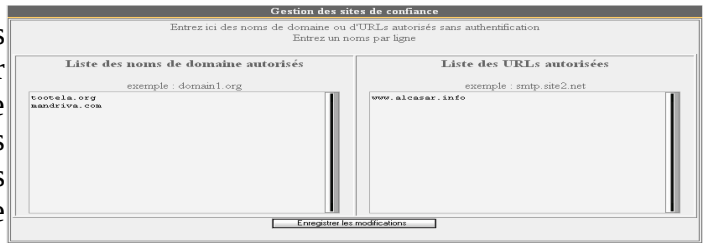
3.6. Vider la base des usagers



Cette fonctionnalité permet de supprimer tous les usagers en une seule opération. Au préalable et avant d'être purgée, une sauvegarde de la base est lancée automatiquement. Pour être certain de disposer d'une sauvegarde, vous pouvez vous en assurer en réalisant manuellement une sauvegarde (cf. §6.2).

3.7. Les exceptions

a) Autoriser des flux vers des sites de confiance

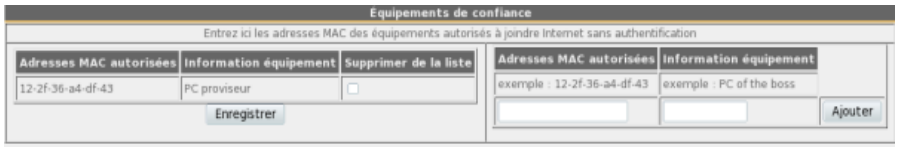


Par défaut, ALCASAR est configuré pour bloquer tous les flux réseau en provenance d'équipement sans usager authentifié. Vous pouvez cependant autoriser le passage de certains flux non authentifiés vers des sites ou des URL spécifiques (sites et URL de confiance). Ces autorisations sont valables quel que soit l'équipement de consultation. Cette possibilité permet par exemple :

- aux logiciels antivirus de se mettre à jour automatiquement ;
- aux systèmes d'exploitation de télécharger automatiquement les rustines de sécurité (patch). À titre d'exemple, voici les noms de domaines liés aux mises à jour Microsoft : .windowsupdate.com, .windowsupdate.microsoft.com, .update.microsoft.com, .windowsupdate.com, .download.microsoft.com, .download.windowsupdate.com

b) Autoriser des équipements de confiance

Il est possible d'autoriser certains équipements à traverser ALCASAR sans être authentifiés (équipements de confiance). Il faut garder à l'esprit que dans ce cas, il devient difficile, voire impossible, d'imputer les traces de ces équipements. Cette opération doit donc être validée par le responsable SSIC de l'organisme. Elle doit rester exceptionnelle.



Les équipements de confiance sont identifiés par leur adresse MAC.

4. Filtrage

ALCASAR possède trois dispositifs de filtrage :

- un filtre de noms de domaine, d'URL et de résultats de moteur de recherche ;
- un filtre de flux réseau permettant de bloquer certains protocoles réseau ;
- un antivirus sur le flux WEB.

Les deux premiers dispositifs de filtrages sont désactivés par défaut. Ils ont été développés pour les organismes susceptibles d'accueillir un jeune public (écoles, collèges, centres de loisirs, etc.).

4.1. Filtrer les noms de domaine, les URL et le résultat des moteurs de recherche

Ce filtre permet d'interdire les noms de domaine et les URL WEB référencées dans des listes noires (blacklists). ALCASAR exploite les deux listes noires suivantes :

- une liste noire principale qui est élaborée par la division des sciences sociales de l'Université de Toulouse-1. Le choix de cette « blacklist » est dicté par le fait qu'elle est diffusée sous licence libre (creative commons) et que son contenu fait référence en France. Dans cette liste, les sites sont gérés par catégories (jeux, astrologie, violence, sectes, etc.). L'interface de gestion vous permet de définir les catégories de sites à bloquer (cf. §4.1.b). Elle vous permet aussi de réhabiliter un site bloqué (cela peut se produire, par exemple, quand un site ayant été interdit a été fermé puis racheté) ;
- une liste noire secondaire qui est laissée à votre disposition. Elle permet de filtrer des sites en fonction de vos besoins spécifiques (alerte CERTA, directives locales, etc.).

Ce filtre active automatiquement pour l'ensemble du réseau de consultation la fonction « Safesearch » des moteurs de recherche les plus connus (google, yahoo, alltheweb, etc.). Cette fonction supprime du résultat des recherches le contenu réservé aux adultes. Attention, le moteur de recherche « bing » n'est pas compatible avec

ce principe.

a) Activer et désactiver le filtrage

Lorsque ce filtrage est activé, ALCASAR bloque aussi l'accès aux sites appelé directement par leur adresse IP (sans nom de domaine). Cela permet de neutraliser certains systèmes de contournement comme les « tunnels HTTP ». Vous pouvez annuler ce comportement particulier en désactivant la catégorie « IP » de la liste noire (cf. §suivant).

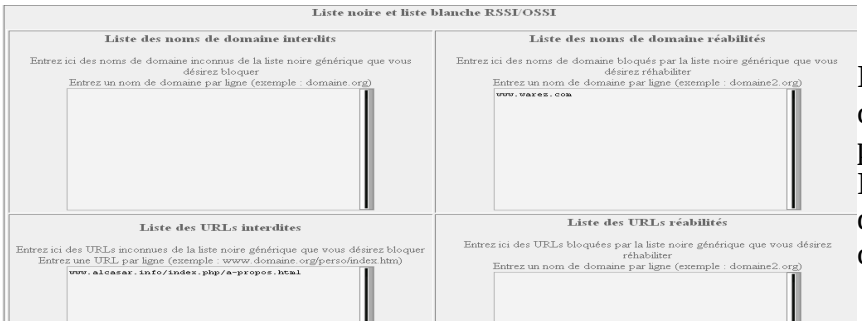
b) Mettre à jour et modifier la liste noire principale

Dans cette liste, les sites sont organisés en différentes catégories. Chaque catégorie contient une liste de noms de domaines (ex. : www.domaine.org) et une liste d'URL (ex. : www.domaine.org/rubrique1/page2.html). Vous pouvez mettre à jour la liste noire de Toulouse et choisir les catégories à filtrer :

En cliquant sur le nom de la catégorie, vous pouvez afficher sa définition ainsi que le nombre de noms de domaine et d'URL filtrés.

Particularités : la catégorie « IP » correspond aux sites WEB appelés directement par leur adresse IP. La catégorie « ossi » correspond à la liste noire secondaire (cf. §suivant).

c) Modifier la « liste noire » secondaire et les sites « réhabilités »



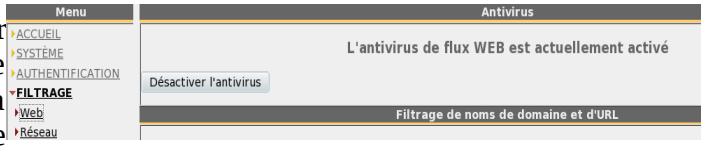
Info : la liste noire secondaire est traitée comme une catégorie de la liste noire principale (catégorie « ossi »).
Info2 : si vous faites des tests de filtrage et de réhabilitation, pensez à vider la mémoire cache des navigateurs.

4.2. Filtrer les flux réseau

ALCASAR intègre un module de filtrage réseau permettant de ne laisser passer que les flux réseau jugés nécessaires. Par défaut, ce module n'est pas activé. Ainsi, un usager authentifié par le portail peut exploiter tous les protocoles imaginables (l'accès à Internet lui est grand ouvert). Toutes les actions des usagers authentifiés sont tracées et enregistrées quel que soit le protocole exploité.
Quand le module de filtrage réseau est activé, seul le protocole HTTP est autorisé. Tous les autres protocoles sont bloqués. Ce mode très restrictif est adapté à la consultation Internet dans les environnements scolaires par exemple. Il est possible, à partir de ce mode restrictif, d'ouvrir, un à un, les protocoles réseau que vous voulez autoriser. Une liste de protocoles par défaut est présentée. Il vous est possible de l'enrichir.

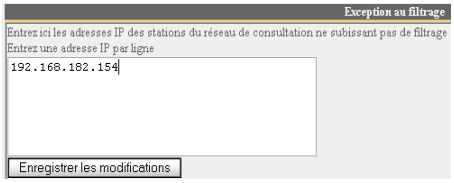
- ICMP : pour autoriser par exemple la commande « ping ».
- SSH (Secure Shell) : pour autoriser des connexions à distance sécurisée.
- SMTP (Simple Mail Tranport Protocol) : pour autoriser l'envoi de mèl à partir d'un client dédié (outlook, thunderbird, etc.).
- POP (Post Office Protocol) : pour autoriser les clients de courrier dédiés à récupérer (relever) le mèl.
- HTTPS (HTTP sécurisé) : pour autoriser la consultation de site WEB sécurisé.

4.3. Antivirus de flux WEB



Cet antivirus exploite le produit libre « clamav » pour analyser et filtrer le flux des pages WEB entrant dans le réseau de consultation. Il est activé par défaut. La mise à jour de la base de connaissance antivirale est effectuée automatiquement toutes les deux heures via le processus « freshclam ». Vous pouvez tester le bon fonctionnement de ce filtre en tentant de récupérer un fichier de test situé à l'URL : http://eicar.org/anti_virus_test_file.htm

4.4. Les exceptions



Le menu « exception » permet de définir les adresses IP du réseau de consultation ne subissant ni le filtrage réseau, ni le filtrage de nom de domaine et d'URL, ni le filtrage des moteurs de recherche (équipements du personnel d'encadrement, d'adultes, d'enseignants, etc.). Le filtrage antivirus reste actif.

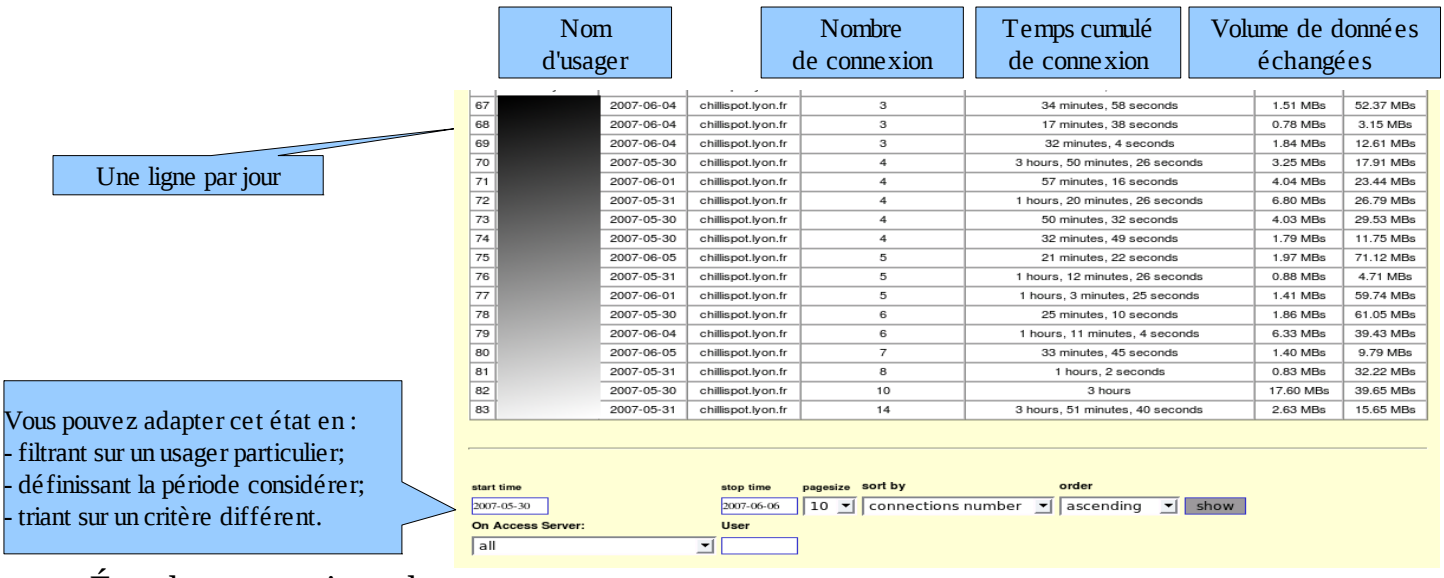
5. Accès aux statistiques

L'interface des statistiques est disponible, après authentification, sur la page de gestion du portail (menu « statistiques ».
Cette interface permet d'accéder aux informations suivantes ;

- nombre de connexion par usager et par jour (mise à jour toutes les nuits à minuit) ;
- état des connexions des usagers (mise à jour en temps réel)
- charge journalière du portail (mise à jour toutes les nuits à minuit) ;
- statistiques de la consultation WEB (mise à jour toutes les 30 minutes) ;
- réaction du pare-feu (mise à jour en temps réel).

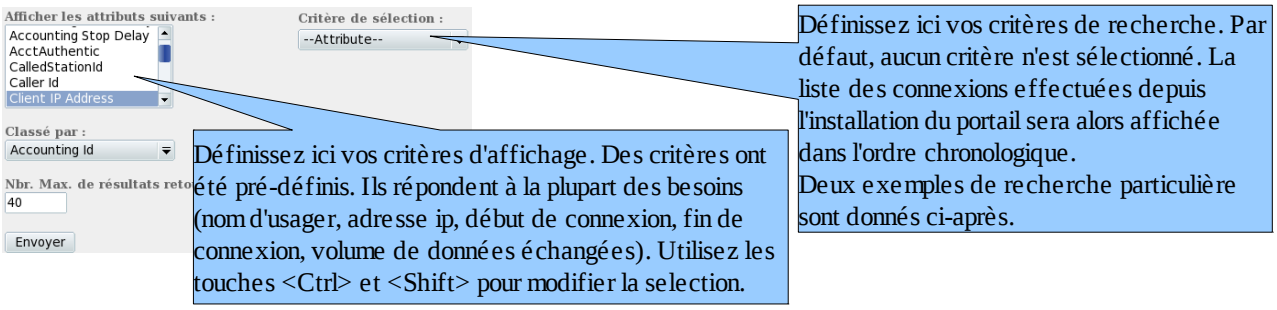
5.1. Nombre de connexions par usager et par jour

Cette page affiche, par jour et par usager, le nombre et le temps de connexion ainsi que les volumes de données échangées. Attention : le volume de données échangées correspond à ce qu'ALCASAR a transmis à l'usager (upload) ou reçu de l'usager (download).

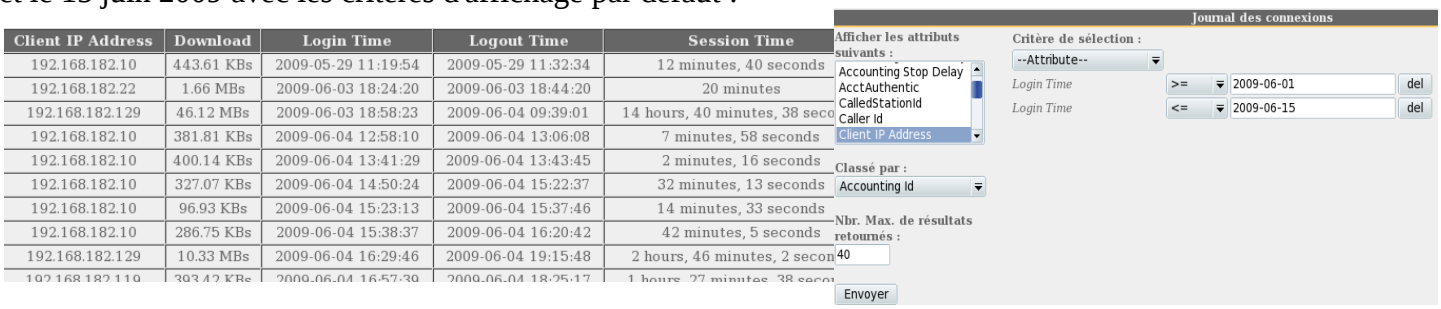


5.2. État des connexions des usagers

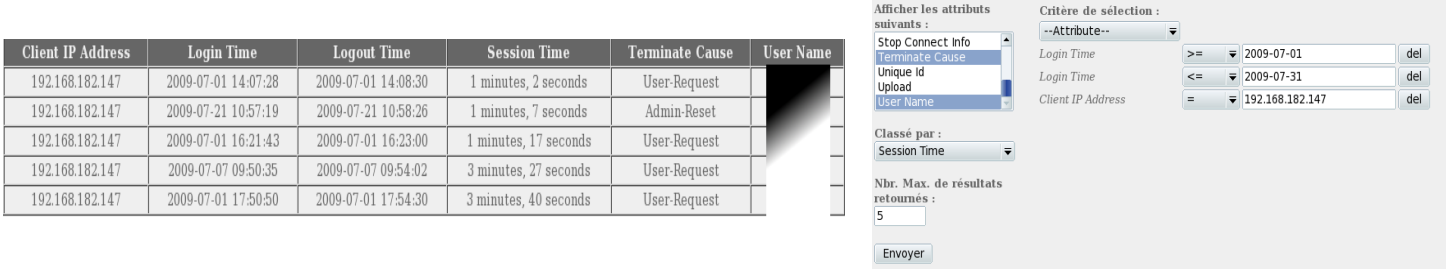
Cette page permet de lister les ouvertures et fermetures de session effectuées sur le portail. Une zone de saisie permet de préciser vos critères de recherche et d'affichage :
Sans critère de recherche particulier, la liste chronologique des connexions est affichée (depuis l'installation du portail). Attention : le volume de données échangées correspond à ce qu'ALCASAR a transmis à l'usager (upload) ou reçu de l'usager (download).



- Exemple de recherche N°1 : affichage dans l'ordre chronologique des connexions effectuées entre le 1er juin et le 15 juin 2009 avec les critères d'affichage par défaut :

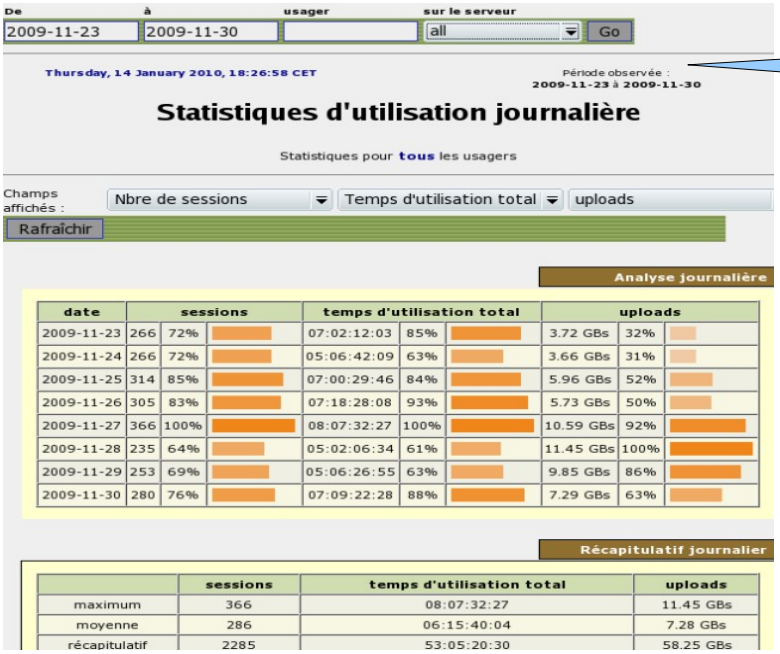


- Exemple de recherche N°2 : affichage des 5 connexions les plus courtes effectuées pendant le mois de juillet 2009 sur la station dont l'adresse IP est « 192.168.182.129 ». Les critères d'affichage intègrent la cause de déconnexion et ne prennent pas en compte le volume de données échangées :



5.3. Usage journalier

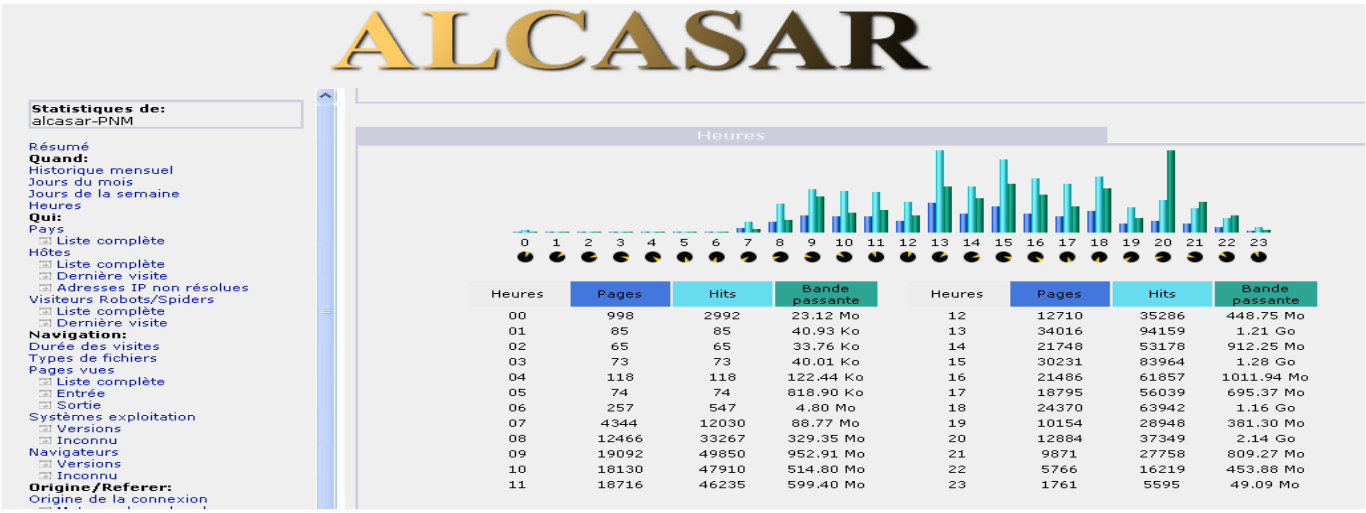
Cette page permet de connaître la charge journalière du portail.



Définissez ici la période observée. Vous pouvez définir un usager particulier (laissez ce champs vide pour prendre en compte tous les usagers.

5.4. Consultation WEB

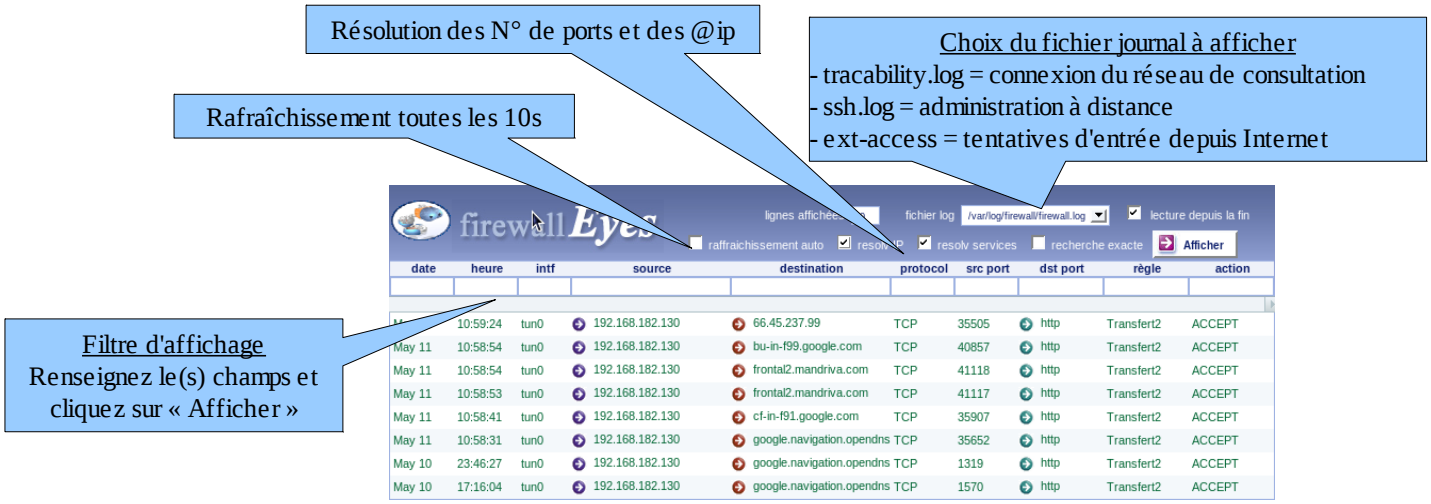
Cette page permet d'afficher les statistiques de la consultation WEB globale effectuée par les équipements situés sur le réseau de consultation. Cet état statistique est recalculé toutes les 30 minutes à partir de fichiers



journaux ne contenant ni les adresses IP source ni le nom des usagers.

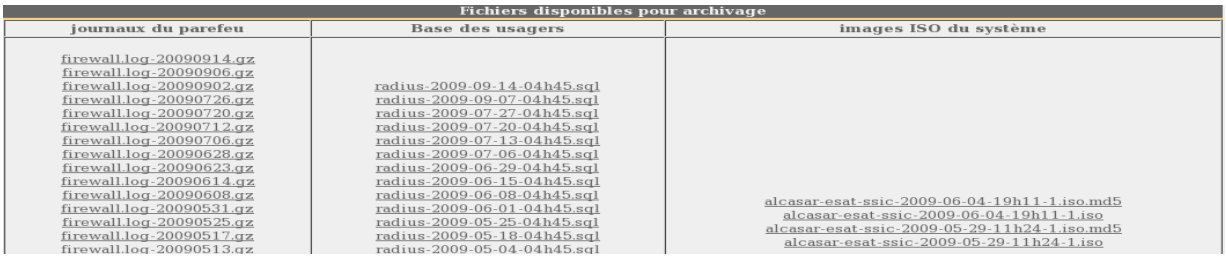
5.5. Pare-feu

Cette page permet d'afficher les fichiers journaux du pare-feu d'ALCASAR (fichiers log.). Trois familles de fichiers sont visualisables : les traces de connexion du réseau de consultation (fichiers « tracability.log »), les traces liées à l'administration à distance (fichier « ssh.log ») et les traces des tentatives d'entrée dans le réseau de consultation depuis Internet (fichiers « ext_acces.log »). Chaque fichier journal représente la semaine en cours. Les semaines écoulées sont aussi visualisables en choisissant les fichiers archivés de manière compressée.



6. Gestion des sauvegardes

Le menu « Sauvegardes » de l'interface de gestion présente les fichiers de traces produits par ALCASAR afin de permettre leur archivage (« clic droit » sur le nom du fichier, puis « enregistrer la cible sous »).



6.1. Les journaux du pare-feu

Trois familles de fichiers sont disponibles : les traces de connexion du réseau de consultation (fichiers « tracability.log »), les traces liées à l'administration à distance (fichier « ssh.log ») et les traces des tentatives d'entrée dans le réseau de consultation depuis Internet (fichiers « ext_acces.log »). Ces fichiers sont générés automatiquement une fois par semaine dans le répertoire « */var/Save/logs/firewall/* » du portail. Les fichiers de plus d'un an sont supprimés. Ces fichiers ne contiennent pas le nom des usagers.
Il est possible d'effectuer des recherches automatiques dans ces fichiers. À titre d'exemple, pour savoir si l'adresse IP Internet « 10.10.10.10 » a été contactée par un poste usager, exécutez la ligne : « *for i in /var/Save/logs/firewall/tracability*;do gunzip -c $i|grep 10.10.10.10; done* ».

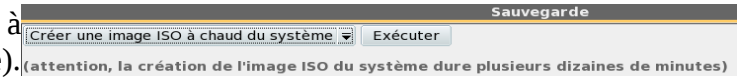
6.2. La base des usagers

Ces fichiers au format « SQL » contiennent l'ensemble des données relatives aux usagers (identifiants, mots de passe chiffrés, attributs, etc.). Ils contiennent également l'historique des ouvertures et fermetures de session sur le portail. Ils sont générés une fois par semaine dans le répertoire « */var/Save/base/* » du portail. Les fichiers de plus d'un an sont supprimés. Ils couvrent les deux objectifs suivants :

- associés aux journaux de traçabilité du pare-feu (cf. §précédent), ils constituent les traces que le responsable d'un réseau de consultation doit fournir aux autorités judiciaires en cas d'enquête (cf. annexe 1 du document de présentation). C'est en agrégeant les informations de ces deux types de fichiers que l'imputabilité des traces est assurée. Ainsi, il est conseillé d'archiver ces deux types de fichiers ;
- ils constituent une sauvegarde de la base des usagers qu'il est possible de réinjecter dans ALCASAR dans le cas d'une réinstallation, d'une mise à jour ou d'une panne majeure.

Vous pouvez effectuer une sauvegarde de cette base au moment où vous le souhaitez. Vous pouvez importer une base via le menu « usagers » + « import ».

6.3. Le système complet (ISO)



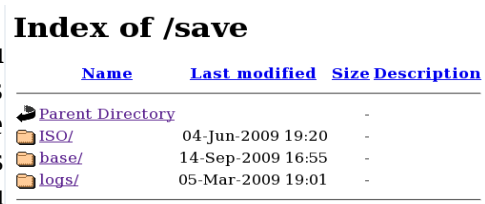
Il est possible de réaliser une image complète et « à chaud » du portail au format ISO (CD-ROM bootable).
La réalisation de cette image dure plusieurs dizaines de minutes. Lancez cette opération lorsque le système est peu chargé (pause méridienne, soir, etc.).
Pour restaurer l'image du système, il est nécessaire de démarrer (booter) le PC à l'aide du CDROM. Au prompt, taper « *nuke* » pour lancer la restauration automatique (si rien n'est tapé, le système lance une restauration interactive). La restauration suit les étapes suivantes :

- comparaison de la capacité des partitions du disque dur
- partitionnement automatique du disque dur
- « formatage » et montage des partitions
- restauration des données
- redémarrage du gestionnaire d'amorçage
- redémarrage après avoir tapé la commande « exit »

Cette procédure de sauvegarde/restauration du système exploite les outils « MondoArchive » et « Mindi ». Plusieurs documentations traitent du fonctionnement et de l'utilisation de ces outils.
Note : si vous restaurez votre système sur un PC ne comportant pas les mêmes cartes réseau que celui d'origine (ou si vous changez les cartes réseau), vous devrez modifier le fichier « */etc/udev/rules.d/*persistent-net.rule* » afin de supprimer les références aux anciennes cartes et afin d'affecter les noms « eth0 » et « eth1 » aux nouvelles. Relancez le système pour prendre en compte cette nouvelle affectation.

6.4. Les autres fichiers journaux

ALCASAR propose une autre interface permettant de récupérer les sauvegardes (https://alcasar/save/). Cette interface permet d'accéder à d'autres fichiers journaux :



- dans le répertoire « logs/squid/ », sont stockés les journaux du serveur mandataire (proxy). Ces journaux contiennent les traces détaillées du seul trafic WEB effectuées par les stations de consultation (détails des appels d'URL). Ces fichiers sont générés une fois par semaine dans le répertoire « */var/Save/logs/proxy/* » du portail. Ils ne contiennent aucun nom d'usager ni aucune adresse IP source. Ces fichiers servent à créer les statistiques de consultation Web du réseau de consultation. Sans être indispensables, ils peuvent apporter un complément d'information lors d'une enquête ;
- dans le répertoire « /logs/httpd/ », sont stockés les journaux d'accès au centre de gestion graphique d'ALCASAR. Ces journaux permettent de connaître la date, l'heure, et l'équipement s'étant connecté au centre de gestion.

7. Fonctions avancées

7.1. Gestion des comptes d'administration

Votre PC ALCASAR comporte deux « comptes système » (ou comptes Linux) qui ont été créés lors de l'installation :

- « root » : c'est le compte d'administration du système ;
- « sysadmin » : ce compte permet de se connecter à distance sur le portail de manière sécurisée (cf. § suivant).

Parallèlement à ces comptes systèmes, il a été décidé de mettre en place des « comptes de gestion » d'ALCASAR. Ces comptes ne servent qu'à l'administration des fonctions d'ALCASAR à travers le centre de gestion graphique. Ils peuvent appartenir aux trois profils suivant :

- « admin » : les comptes liés à ce profil peuvent accéder à toutes les fonctions du centre de gestion. Un premier compte lié à ce profil a été créé lors de l'installation du portail (cf. doc d'installation) ;
- « manager »: les comptes liés à ce profil n'ont accès qu'aux fonctions de gestion des usagers du réseau de consultation (présentées au §3) ;
- « backup » : les comptes liés à ce profil n'ont accès qu'aux fonctions de sauvegarde et d'archivage des fichiers journaux (présentées au §6).

Vous pouvez créer autant de comptes de gestion que vous voulez dans chaque profil. Pour gérer ces comptes de gestion, utilisez la commande « *alcasar-profil.sh* » en tant que « root » :

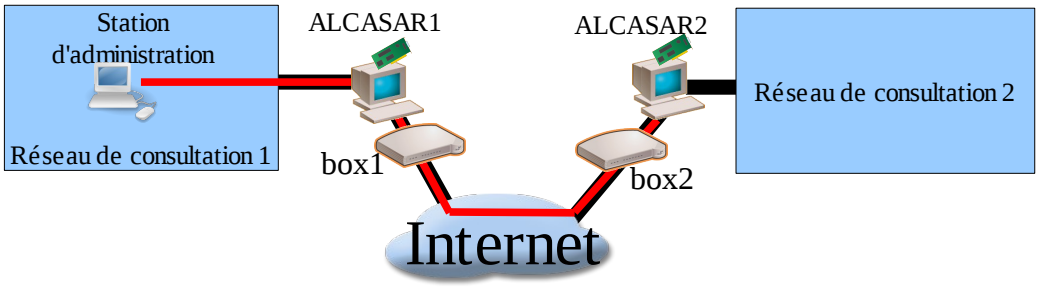
- *alcasar-profil.sh --list* : pour lister tous les comptes de chaque profil
- *alcasar-profil.sh --add* : pour ajouter un compte à un profil
- *alcasar-profil.sh --del* : pour supprimer un compte
- *alcasar-profil.sh --pass* : pour changer le mot de passe d'un compte existant

7.2. Administration distante sécurisée

Il est possible de se connecter à distance sur ALCASAR au moyen d'un flux chiffré (protocole SSH). Seul le compte Linux « sysadmin » créé lors de l'installation du système est autorisé à se connecter par ce moyen. Dans un premier temps, activez le service « ssh » via l'interface de gestion (menu « système » puis « réseau »).
Pour vous connecter à distance, utilisez la commande « *slogin sysadmin@adresse-ip-alcasar* » sous Linux. Utilisez l'utilitaire « putty » sous Windows. Une fois connecté, vous pouvez devenir « root » via la commande « su ».

a) administration graphique à travers Internet

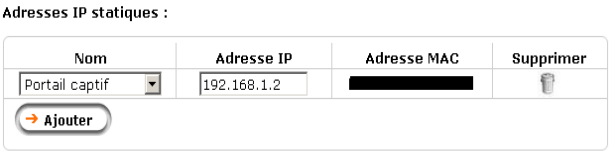
Ce chapitre explique comment exploiter le centre de contrôle graphique d'ALCASAR à travers Internet via un tunnel ssh (secure shell). Dans l'exemple suivant, l'administrateur est situé dans le réseau de consultation N°1. Il cherche à administrer graphiquement l'ALCASAR2 (dont le service SSH est activé) à travers Internet en « anonymisant » le flux dans le N° de port « 52222 » (vous pourrez choisir le N° de port que vous voudrez).



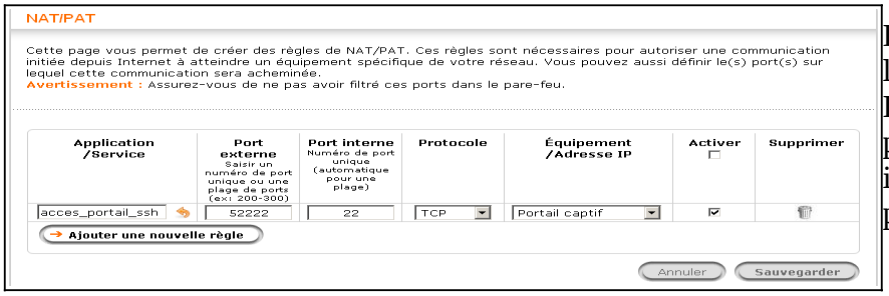
Configuration de la BOX2

Objectif : transférer le protocole SSH en provenance de la station d'administration vers eth0 d'ALCASAR2.

- Cas d'une « livebox »

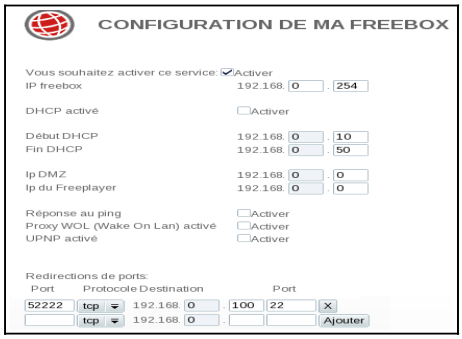


Dans le menu « paramètres avancés », créez une entrée pour l'adresse IP d'eth0 d'ALCASAR2 (côté Internet).



Dans le menu « NAT/PAT », renseignez les champs suivants et sauvegardez :
Le port externe en 52222 correspond au port sur lequel les trames ssh arriveront. En interne, ALCASAR2 écoute SSH sur le port 22 (port par défaut de ce protocole),

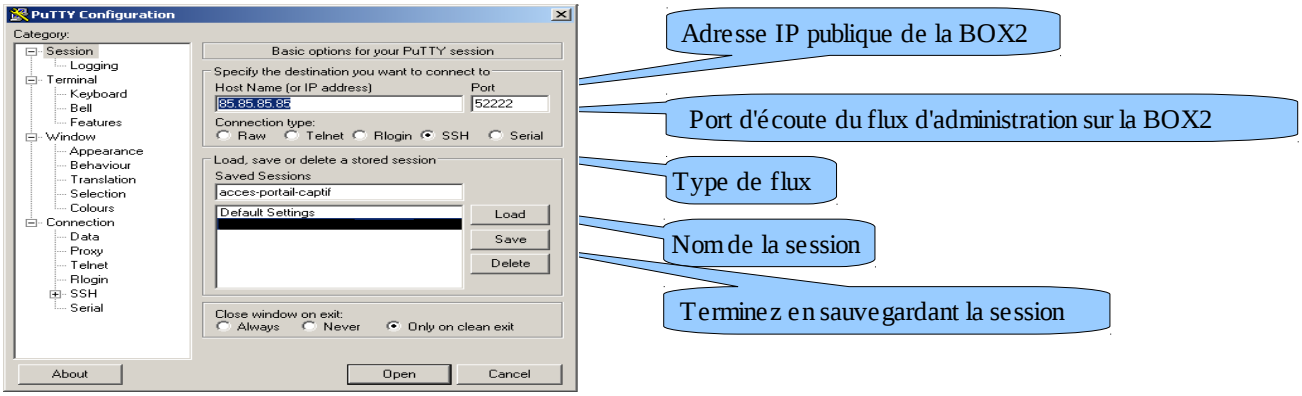
- cas d'une « freebox »



Dans le menu « routeur », configurez une redirection de port.

Activation du tunnel SSH à partir de la station d'administration

- Installez un client SSH :
  - Sous Linux, installez « openssh-client » (il est aussi possible d'installer « putty ») ;
  - Sous Windows, installez « Putty » ou « putty-portable » ou « kitty » et créez une nouvelle session :



- Lancez une première connexion :
  - Sous Linux, lancez la commande « *slogin -p port_externe sysadmin@w.x.y.z* » ou « *ssh -p port_externe sysadmin@w.x.y.z* » (remplacez w.x.y.z par l'adresse IP publique de la BOX2 et port_externe par la valeur configurée dans le PAT du routeur : 52222 dans notre exemple).
  - Sous Windows, cliquez sur *« Open »*, acceptez la clé du serveur et connectez-vous avec le compte « sysadmin ».
- Vous êtes connecté en mode console. Vous pouvez devenir « root » via la commande « su ».

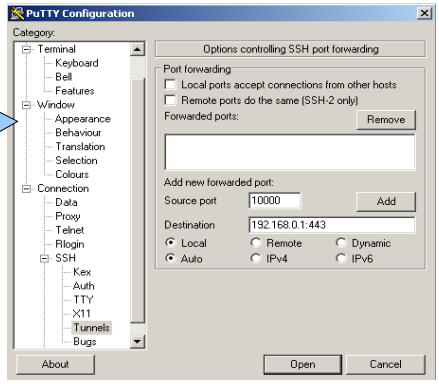
Rappel : « sysadmin » est le nom du compte Linux créé pendant la phase d'installation de Mandriva-Linux sur ALCASAR 2.

Exploitation du tunnel pour l'administration graphique

L'objectif est de rediriger le flux du navigateur WEB de la station d'administration dans le tunnel SSH afin de pouvoir administrer graphiquement l'ALCASAR distant (ALCASAR 2).

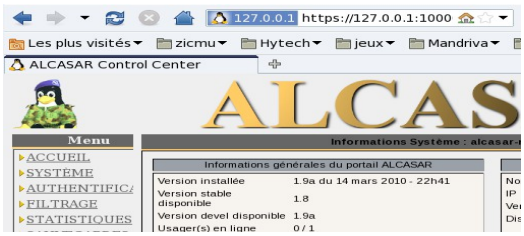
- Sous Window, configurez putty de la manière suivante :

- chargez la session précédente
- sélectionner dans la partie gauche « Connection/SSH/Tunnels »
- dans « Source port », entrez le port d'entrée local du tunnel (supérieur à 1024 (ici 10000))
- dans « Destination », entrez l'adresse IP de eth1 d'alcasar1 suivis du port 443 (ici 192.168.0.1:443)
- cliquez sur « Add »
- sélectionner « Session » dans la partie gauche
- cliquer sur « Save » pour sauvegarder vos modification
- cliquer sur « Open » pour ouvrir le tunnel
- entrer le nom d'utilisateur et son mot de passe



- Sous Linux, lancez la commande :
  « *slogin -L 10000:@IP_eth1_alcasar2:443 -p 52222 sysadmin@ip_publique_box1* »

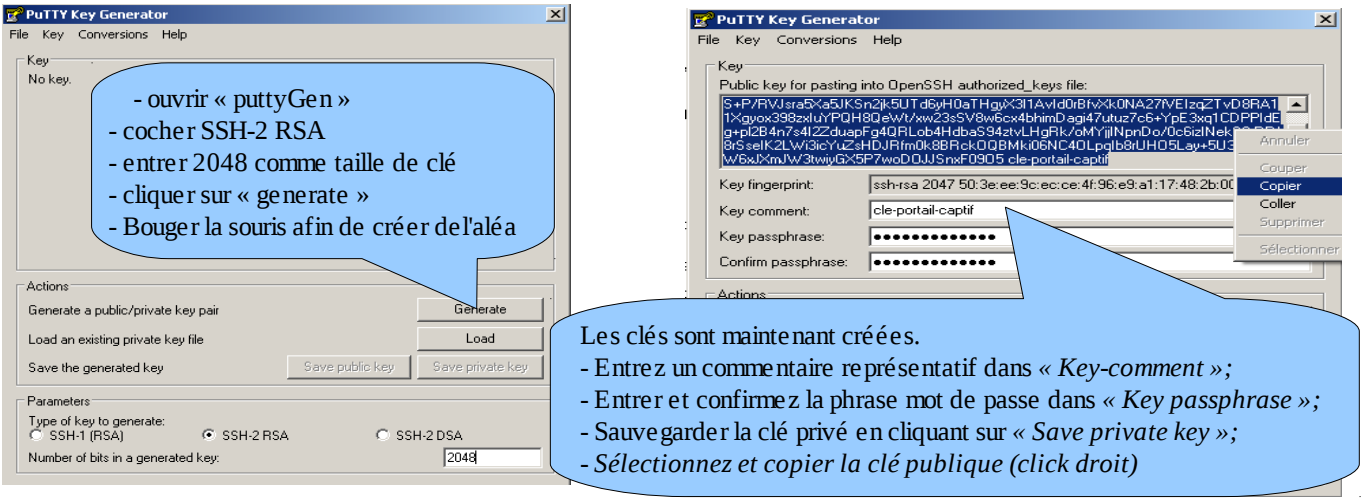
Lancez votre navigateur avec l'URL :
https://localhost :10000/acc/



b) Exploitation du tunnel SSH au moyen d'une biclé (clé publique/clé privée)

Ce paragraphe, bien que non indispensable, permet d'augmenter la sécurité du tunnel d'administration à travers l'authentification de l'administrateur par sa clé privée.

- générez une biclé (clé publique/clé privée)
  - Sous Windows avec « puttygen »



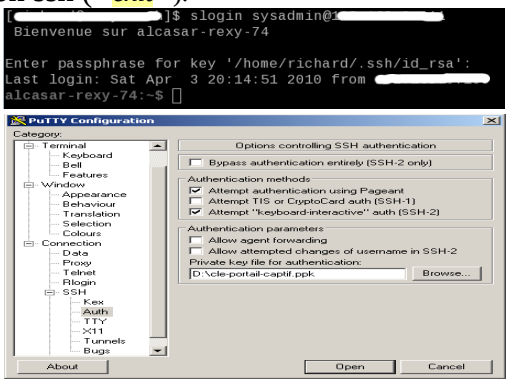
- ou sous Linux avec « *ssh-keygen* »

Dans votre répertoire personnel, créez le répertoire « *.ssh* » s'il n'existe pas. À partir de celui-ci, générez votre biclé (« *ssh-keygen -t rsa -b 2048 -f id_rsa* »). la commande « *cat id_rsa.pub* » permet de voir (et de copier) votre clé publique.

```
[richard@rexy ~]$ mkdir .ssh
[richard@rexy ~]$ cd .ssh/
[richard@rexy .ssh]$ ssh-keygen -t rsa -b 2048 -f id_rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
```

```
[ .ssh]$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyL4yMM8BO18Quusv1Iq/V
3kF2wvhuHzmNmH9ITFTALwHPHA9lWnxlcDPE9DPR7FPqrEZf/uT84C2G
o7d/IX+/JyPlVXoUdXaZ9wjtusU3SVWSr6o9NXmbZqoOgzrGpjN7Vfu5
npCrDQGfuq6PImO6AQCJQkySmOXDIGFVr4r5Zbw== [redacted]
```

- Copiez la clé publique sur le portail distant :
  - dans la fenêtre de connexion « ssh » en tant que « sysadmin », exécutez les commandes suivantes : « *mkdir .ssh* » puis « *cat >.ssh/authorized_keys* » ;
  - copier le contenu de la clé publique provenant du presse papier (« Ctrl V » pour Windows, bouton central de la souris pour Linux) ;
  - tapez « Entrée » puis « Ctrl+D » ;
  - protégez le fichier : « *chmod 700 .ssh* » puis « *chmod 600 .ssh/authorized_keys* » ;
  - vérifiez : « *cat .ssh/authorized_keys* ».
- Si vous souhaitez vous connecter uniquement par certificat, configurez le serveur sshd :
  - passez root (*su -*) et dé-commentez les options suivantes du fichier « */etc/ssh/sshd_config* »:
    PasswordAuthentication no
  - relancez le serveur sshd (« *service sshd restart* ») et fermez la session ssh (« *exit* »).
- Test de connexion à partir de Linux : « slogin sysadmin@w.x.y.z »
- Test de connexion à partir de Windows :
  - chargez la session précédente de putty ;
  - dans la partie gauche, sélectionnez « Connection/SSH/Auth » ;
  - cliquez sur « browse » pour sélectionner le fichier de clé ;
  - sélectionnez dans la partie gauche Session ;
  - cliquez sur « Save » puis « Open » ;
  - entrez l'utilisateur « sysadmin » ;
  - la clé est reconnue, il ne reste plus qu'à entrer la phrase de passe.



7.3. Contournement du portail (By-pass)

Pour des raisons de maintenance ou d'urgence, une procédure de contournement du portail a été créée. Elle permet de supprimer l'authentification des usagers ainsi que le filtrage. La journalisation de l'activité du réseau reste néanmoins active. L'imputabilité des connexions n'est plus assurée.
Pour lancer le contournement du portail, lancez le script « *alcasar-bypass.sh --on* ». Pour le supprimer, lancez le script « *alcasar-bypass.sh --off* ». À noter que cette commande fonctionne encore avec '-on' et '-off' dans la version 2.0.x

7.4. Mise en place du logo de l'organisme

Il est possible de mettre en place le logo de votre organisme en cliquant sur le logo situé en haut et à droite de l'interface de gestion. Votre logo sera inséré

dans la page d'authentification ainsi que dans le bandeau supérieur de l'interface de gestion. Votre logo doit être au format libre « png » et il ne doit pas dépasser la taille de 100Ko. Il est nécessaire de rafraîchir la page du navigateur pour voir le résultat.

7.5. Installation d'un certificat serveur officiel

Depuis la version 2.0, il est possible d'installer un certificat officiel de type « intranet » proposé par certains fournisseurs. L'intégration d'un tel certificat évite les fenêtres d'alerte de sécurité sur les navigateurs n'ayant pas intégré le certificat racine d'ALCASAR (cf. §2.2.b). Contrairement aux certificats « Internet » qui certifient un nom de domaine déposé auprès d'un bureau d'enregistrement (registrar), un certificat « intranet », peut certifier une adresse IP privée ou un nom simple de serveur (hostname).

Le « hostname » de tout les portails ALCASAR est : « alcasar ». Pour acquérir votre certificat, suivez les instructions données sur le site du fournisseur sachant que le serveur WEB exploité par ALCASAR est un serveur « APACHE » avec module SSL. L'exemple qui suit permet d'intégrer un certificat « intranet » généré par le fournisseur « Digitalix ».

Dans un premier temps, vous devrez lancer la commande suivante sur ALCASAR en tant que « root » : *openssl req -newkey rsa:2048 -new -nodes -keyout my_private.key -out my_server.csr* Cette commande permet de générer deux fichiers : la clé privé (my_private.key) et la demande de certificat (my_server.csr). Copiez le fichier de demande de certificat sur clé USB afin de pouvoir copier son contenu sur le site du fournisseur. Celui-ci doit vous retourner un fichier contenant votre certificat serveur officiel (my_certificate.crt). Le cas échéant, vous devez aussi récupérer le certificat d'autorité intermédiaire de votre fournisseur (pour Digitalix, il est disponible ici : http://www.digitalix.fr/certs/HACert-bundle.crt).

En tant que « root », copiez les trois fichiers « my_private.key », my_certificate.crt » et « HACert-bundle.crt » dans votre répertoire. Effectuez alors les manipulations suivantes :

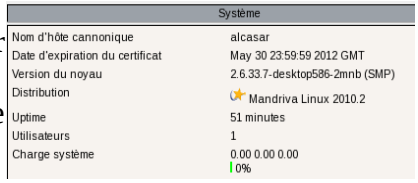
1. *cd /etc/pki/tls* (déplacement dans le répertoire des certificats)
2. *mv certs/alcasar.crt certs/alcasar.crt.old* puis *mv certs/server-chain.crt certs/server-chain.crt.old* et enfin *mv private/alcasar.key private/alcasar.key.old* (copie de sauvegarde des anciens certificats)
3. *cp /root/my_certificate.crt certs/alcasar.crt* et *cp /root/my_private.key private/alcasar.key* (copie du certificat officiel et de sa clé privée)
4. si votre fournisseur a un certificat d'autorité intermédiaire : *cp /root/HACert-bundle.crt certs/server-chain.crt* sinon : *cp certs/alcasar.crt certs/server-chain.crt*
5. Relancez le serveur WEB Apache via la commande « *service httpd restart* ».

En cas de problème :

- soit vous revenez en arrière en inversant les opérations de la 2ème ligne ; soit vous recréez des certificats « tout neufs » via la commande « alcasar-CA.sh » ;
- relançez le serveur WEB Apache via la commande « *service httpd restart* ».

Particularités :

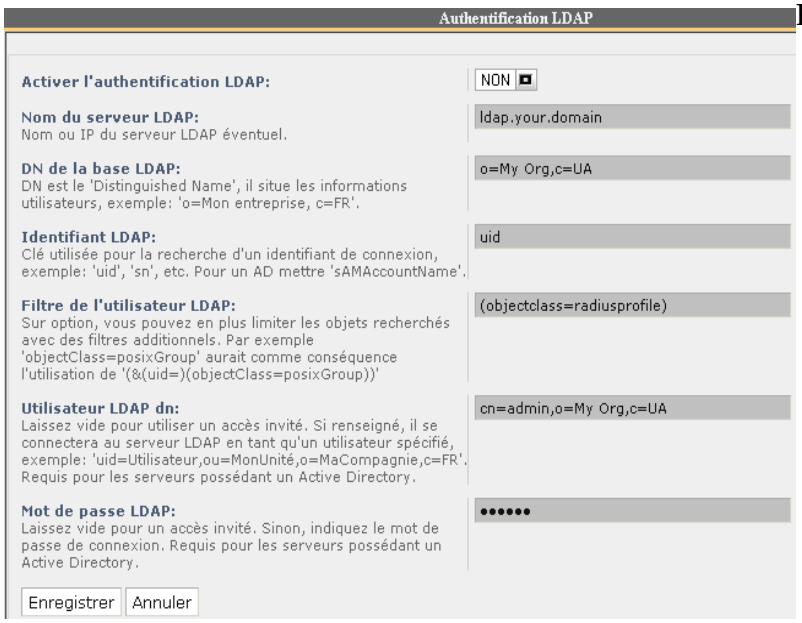
- Si vous administrez plusieurs portails ALCASAR, vous pouvez exploiter le même certificat officiel sur l'ensemble de votre parc.
- La date d'expiration du certificat (qu'il soit officiel ou non) est affichée dans la page d'accueil du portail.



7.6. Utilisation d'un serveur d'annuaire externe (LDAP ou A.D.)

ALCASAR intègre un module lui permettant d'interroger un serveur d'annuaire externe (LDAP ou A.D) situé indifféremment côté LAN ou WAN. Quand ce module est activé, ALCASAR utilise en premier lieu l'annuaire externe puis, en cas d'échec, la base locale pour authentifier un usager[2]. Dans tous les cas, les fichiers journaux relatifs aux évènements des usagers (log) restent traités dans la base locale d'ALCASAR. L'interface graphique de gestion de ce module est la suivante :

2 Quand un compte est géré sur un serveur LDAP/A.D externe, il est possible d'enrichir ses attributs par les attributs spécifiques d'ALCASAR (nombre de session simultanée, créneaux horaires autorisés, etc.). Pour cela, créez un compte usager dans la base locale portant le même nom que celui défini dans l'annuaire externe. Cela permettra, de plus, d'améliorer la lisibilité des rapports statistiques.

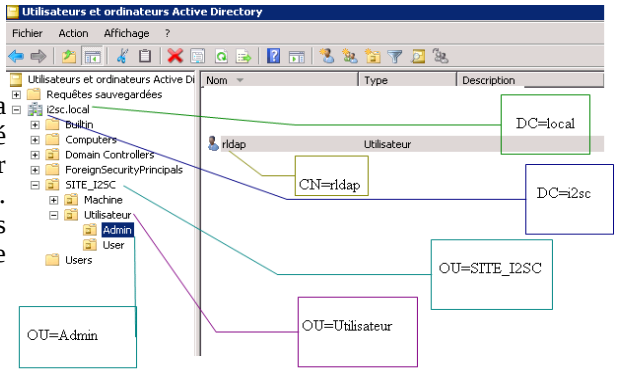


Remarque :

- les attributs des usagers situés dans l'annuaire externe ne peuvent pas être modifiés via l'interface de gestion d'ALCASAR ;
- l'utilisation du protocole sécurisé « ldaps » n'est pas disponible pour le moment. Le segment réseau entre ALCASAR et l'annuaire doit donc être maîtrisé, pour des raisons évidentes de sécurité (cf. §10) ;
- les annuaires externes ne gèrent pas la casse contrairement à la base locale d'ALCASAR.

Exemple :

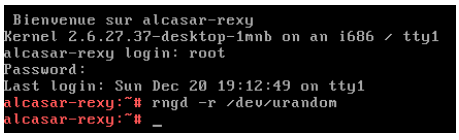
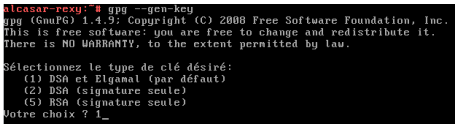
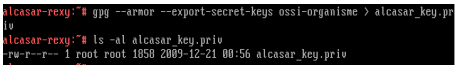
Cette copie d'écran montre le schéma d'un annuaire A.D. organisé de la manière suivante : les usagers standards sont placés dans l'Unité Organisationnelle (O.U.) « User ». Le compte utilisé par ALCASAR pour consulter l'annuaire à distance est le compte « rldap » situé dans l'O.U. « Admin ». Ce compte est un compte standard qui n'a pas besoin de droits particuliers. Les deux O.U. « Admin » et « User » sont situées elles-même dans une O.U. « Utilisateur ».

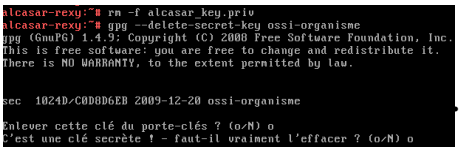
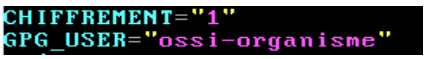


- DN de la base : « ou=User,ou=Utilisateur,ou=SITE_I2SC,dc=i2sc,dc=local »
- Identifiant LDAP : « sAMAccountName »
- Filtre : vide
- Utilisateur LDAP : « cn=rldap,ou=Admin,ou=Utilisateur,ou=SITE_ISC,dc=i2sc,dc=local »
- Mot de passe : mot de passe de l'utilisateur « rldap »

7.7. Chiffrement des fichiers journaux

Il est possible de chiffrer automatiquement les fichiers journaux du parefeu, de squid et de l'accès à l'interface de gestion à l'aide d'un algorithme asymétrique (clé publique + clé privée). En fournissant la clé privée à un responsable de votre organisme pour séquestre, vous protégez les administrateurs d'accusations de modification de ces fichiers. En cas d'enquête, il suffira de fournir les fichiers journaux chiffrés ainsi que la clé privée de déchiffrement. La procédure est la suivante :

Messages affichés à l'écran	Commentaires	Actions à réaliser
	- Connectez-vous en tant que « root ». - Lancez le générateur d'entropie (d'aléa).	*rngd -r /dev/urandom*
	- Générez la biclé (clé publique + clé privée). - Choisissez l'algorithme, la taille ainsi que la longévité des clés (sans expiration). - Choisissez un nom d'utilisateur et une phrase de passe.	*gpg --gen-key* info : le nom d'utilisateur ne doit pas comporter d'espace. Ce nom est repris sous le terme <nom_utilisateur> dans la suite du document.
	- Arrêtez le générateur d'entropie.	*killall rngd*
	- Exportez la clé privée. Copiez là sur un support externe. - Fournissez-la (avec la phrase passe et le <nom_utilisateur>) à un responsable de votre organisme (pour séquestre).	*gpg --armor –export-secret-key \ <nom_utilisateur> > alcasar_key.priv* info : cf. doc d'installation pour la gestion USB.

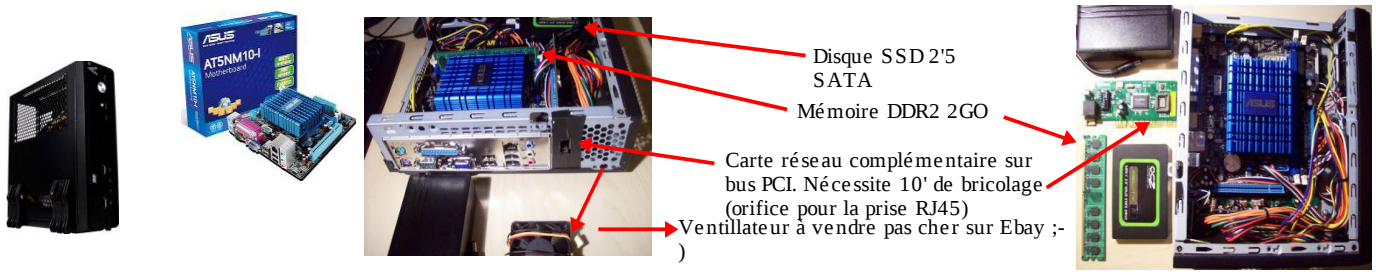
Messages affichés à l'écran	Commentaires	Actions à réaliser
	- supprimez le fichier généré précédemment - supprimez la clé privée du trousseau GPG	*rm -f alcasar_key.priv* *gpg --delete-secret-key <nom_utilisateur>*
	- Activer le chiffrement en modifiant les variables « chiffrement » et « gpg_user » du fichier « /usr/local/bin/alcasar-log-export.sh ».	*vi /usr/local/bin/alcasar-log-export.sh* info : affectez le « nom_utilisateur » à la variable « gpg_user »

Infos :

- ALCASAR utilise le trousseau de clés de « root » situé dans le répertoire « */root/.gnupg* » ;
- '*gpg –list-key*' : permets de lister toutes les biclés contenues dans ce trousseau ;
- '*gpg --delete-key <nom_utilisateur>* ' : efface une clé publique du trousseau de clés ;
- '*gpg --delete-secret-key <nom_utilisateur>*' : efface une clé privée du trousseau de clés ;
- Vous pouvez copier le répertoire « */root/.gnupg* » sur un autre serveur ALCASAR. Ainsi, vous pourrez utiliser le même <nom_utilisateur> et les mêmes clés ;
- Pour déchiffrer une archive chiffrée : '*gpg –decrypt <nom_archive_chiffrée>*'

7.8. Créer son boîtier dédié ALCASAR

Ce chapitre présente un exemple de réalisation d'un boîtier dédié (appliance) ALCASAR économique dont les contraintes sont : format miniature (mini-itx), sans bruit (noiseless), sans ventilateur (fanless) et faible consommation d'énergie. La configuration est la suivante : boîtier A+Case CS160 (alimentation 12V intégrée), carte mère AT5NM-10 (processeur Intel D525 intégré), 2GO de mémoire DDR2 (PC2-6400), disque dur 2,5' sata 200Go, carte PCI réseau Ethernet complémentaire. Le remplacement du disque dur par un disque SSD 2,5' de 40GO permet de diminuer la chaleur dégagée, de supprimer le ventilateur du boîtier et ainsi de diminuer la consommation de 28W à 20W. Le coût de cette configuration avoisine les 210€ TTC (frais de port compris). Le coût lié à la consommation électrique annuelle est de 20,53€ (20*24*365/1000*0,1152). ALCASAR est installé via une clé USB selon la procédure habituelle. Une fois déployé, le boîtier ne nécessite ni clavier, ni souris, ni moniteur.



8. Mises à jour et arrêt

8.1. Mises à jour du système d'exploitation

Mandriva-Linux propose un excellent mécanisme permettant d'appliquer les correctifs (patchs) sur le système. ALCASAR a été développé afin d'être entièrement compatible avec ce mécanisme. Ainsi, pour mettre à jour le système, il suffit de lancer la commande « *urpmi –auto --auto-update* » en tant que « root ».
Une fois la mise à jour terminée, un message peut vous avertir qu'un redémarrage système est nécessaire. Ce message n'apparaît que si un nouveau noyau (kernel) a été installé.

8.2. Mise à jour d'ALCASAR

Vous pouvez savoir si une mise à jour d'ALCASAR est disponible en regardant la page de garde de votre interface de gestion ou en lançant la commande « *alcasar-version.sh* ». Il est possible d'effectuer une mise à jour automatique de la version en cours d'exploitation. Les paramètres suivants sont alors repris :

- le nom et le logo de l'organisme ;
- les identifiants et les mots de passe des comptes d'administration du portail ;
- la base des usagers et des groupes ;
- les listes noires principales et secondaires ;

- la liste des sites et des adresses MAC de confiance ;
- la configuration du filtrage réseau
- les certificats de l'Autorité de Certification (A.C.) et du serveur.

La mise à jour d'ALCASAR lance automatiquement la mise à jour du système d'exploitation (Mandriva-Linux).
Procédure de mise à jour automatique : récupérez et décompressez l'archive de la nouvelle version du portail. Positionnez-vous dans son répertoire et lancez le script d'installation « *sh alcasar.sh --install* ».
Le script détectera automatiquement la mise à jour à effectuer. En cas d'échec, vous pouvez suivre la procédure manuelle décrite ci-après.
Procédure de mise à jour manuelle : lancez la commande « *alcasar-conf.sh --create* » pour générer le fichier de configuration de la version en cours d'exploitation (« */tmp/alcasar-conf.tar.gz* »). Récupérez ce fichier sur une clé USB. Installez le nouveau système d'exploitation comme lors d'une première installation. Connectez votre clé USB et copiez le fichier « *alcasar-conf.tar.gz* » dans le répertoire /tmp. Récupérez et décompressez l'archive de la nouvelle version d'ALCASAR. Positionnez-vous dans son répertoire et lancez le script d'installation « *sh alcasar.sh --install* ».

8.3. Arrêt du système

Deux possibilités permettent d'arrêter « proprement » le PC ALCASAR :

- en appuyant brièvement sur le bouton d'alimentation de l'équipement ;
- en se connectant sur la console en tant que root et en lançant la commande « init 0 ».

Lors du redémarrage du PC ALCASAR, une procédure supprime toutes les connexions qui n'auraient pas été fermées suite à un arrêt non désiré (panne, coupure électrique, etc.).

9. Diagnostics

Ce chapitre présente diverses procédures de diagnostic en fonction des situations ou des interrogations rencontrées. Les commandes (*italique* sur fond jaune) sont lancées dans une console en tant que « root ».

9.1. Connectivité réseau

- test de l'état des cartes réseau : lancez la commande « *mii-tool* » afin de vérifier l'état des deux cartes réseaux. Le résultat « *100baseTx–FD, link ok* » est correct (100Mb/s - full duplex – lien activé) ;
- test de connexion vers le routeur de sortie : lancez un « *ping* » vers l'@IP du routeur de sortie (Box F.A.I). En cas d'échec, vérifiez les câbles réseau, la configuration de l'interface eth0 (*ifconfig eth0*) et l'état du routeur ;
- test de connexion vers les serveurs DNS externes : lancez un « *ping* » vers les @IP des serveurs DNS. En cas d'échec, changez de serveurs.
- test du serveur DNS interne (dnsmasq) : lancez une demande de résolution de nom (ex. : *dig www.google.fr*). En cas d'échec, vérifiez le fichier de configuration de « dnsmasq » (*cat /etc/dnsmasq.conf*) ;
- test de connectivité Internet : lancer la commande « *wget www.google.fr* ». En cas de réussite la page de garde de Google est téléchargée et stockée localement (index.html). Le menu « système/service » de l'interface de gestion rend compte de ce test :

- test de connectivité vers un équipement de consultation : vous pouvez tester la présence d'un équipement situé sur le réseau de consultation via la commande « *arping -I eth1 @ip_équipement* ».

Vous pouvez afficher l'ensemble des équipements situés sur le réseau de consultation en lançant la commande « *arpscan eth1* » ;

```
00:1C:25:CB:BA:7B 192.168.182.1
00:11:25:B5:FC:41 192.168.182.25
00:15:77:A2:6D:E9 192.168.182.129
```

Vous pouvez afficher les trames réseau provenant du réseau de consultation en installant l'outil « tcpdump » (urpmi tcpdump) et en lançant la commande « tcpdump -i eth1 ».

9.2. Espace disque disponible

Si l'espace disque disponible n'est plus suffisant, certains modules peuvent ne plus fonctionner. À titre d'exemple, et par principe de sécurité, le serveur mandataire « Squid » s'arrêtera dès qu'il ne pourra plus alimenter ses fichiers journaux. Vous pouvez vérifier l'espace disque disponible (surtout la partition */var*) :

Systèmes de fichiers montés

Point	Type	Partition	Utilisation	Libre	Occupé	Taille
/	ext3	/dev/sda1	56% (1%)	383,34 Mo	547,34 Mo	980,49 Mo
/tmp	ext3	/dev/sda6	3% (1%)	1,03 Go	33,77 Mo	1,12 Go
/home	ext3	/dev/sda7	3% (1%)	1,07 Go	33,46 Mo	1,10 Go
/var	ext3	/dev/sda8	0%	62,74 Go	251,01 Mo	66,35 Go
		Totaux :	1%	65,21 Go	865,59 Mo	69,53 Go

- en mode graphique, via la page d'accueil du centre de gestion

- en mode texte, via la commande « *df* »

En cas de diminution trop importante de cet espace, supprimez les anciens fichiers journaux et autres images ISO du système après les avoir archivés (répertoire */var/Save/**).

9.3. Services serveur ALCASAR

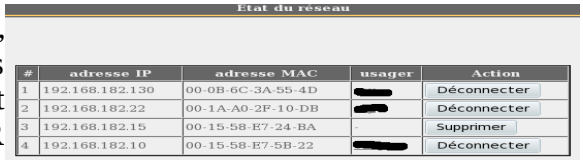
Afin de remplir ces différentes tâches, ALCASAR exploite plusieurs services serveur. L'arrêt de l'un d'entre eux peut empêcher ALCASAR de fonctionner. Il est alors utile de savoir diagnostiquer la raison pour laquelle un service s'est arrêté. Lancez la commande « *ps fax* » et vérifiez que le serveur WEB 'apache' (« httpd ») est bien lancé. Le cas échéant, lancez-le via la commande « *service httpd start* ». En cas d'échec, visualiser son journal de rapport d'erreur via la commande « *tail /var/log/httpd/error.log* ».
L'état de fonctionnement des autres services est affiché dans l'interface de gestion (menu « système/services ») :

Status	Nom du services	Actions		
✔	radiusd	---	Arrêter	Redémarrer
✔	chilli	---	Arrêter	Redémarrer
✔	dansguardian	---	Arrêter	Redémarrer
✔	mysqld	---	Arrêter	Redémarrer
✔	squid	---	Arrêter	Redémarrer

Vous pouvez les arrêter ou les relancer via l'interface de gestion ou via la commande « service nom_du_service start/stop/restart ». En cas d'échec, vérifiez dans le fichier journal système (*tail /var/log/messages*) la raison pour laquelle, ils n'arrivent pas à se lancer.

9.4. Connectivité des équipements de consultation

Dans l'interface de gestion (rubrique « SYSTÈME/Activité »), vérifiez que vos équipements de consultation possèdent des paramètres réseau corrects (adresse MAC / adresse IP). Si ce n'est pas le cas, supprimez l'ancienne adresse enregistrée par ALCASAR et reconfigurez l'équipement.



Sur les équipements de consultation :

- vérifiez les paramètres réseau : lancez « *ipconfig /all* » sous Windows, « */sbin/ifconfig* » sous Linux ;
- s'il ne sont pas corrects, modifiez-les. Pour les équipements en mode dynamique, relancez une demande d'adresse : « *ipconfig /renew* » sous Windows, « *dhclient eth0* » sous Linux.

Si l'interface n'est pas configurée, vérifiez les câbles et assurez-vous que les trames DHCP de l'équipement transitent bien sur le réseau (à l'aide de l'analyseur de trames « wireshark » par exemple). Sur ALCASAR, vous pouvez voir arriver les demandes d'adressage des équipements en lançant la commande « *tailf /var/log/messages* » ou en affichant le terminal N°12 (<Alt> + F12).

```
Dec 29 22:31:27 alcasar      coova-chilli[2299]: chilli.c: 2694: New DHCP reques
t from MAC=08-00-27-E7-EA-89
Dec 29 22:31:27 alcasar      coova-chilli[2299]: chilli.c: 2661: Client MAC=08-0
0-27-E7-EA-89 assigned IP 192.168.182.129
```

- Test de connexion vers le portail : lancez un ping vers l'adresse IP d'ALCASAR. En cas d'échec, vérifiez les câbles et la configuration de l'interface réseau.
- Test de la résolution de nom : Sous Windows, lancez « *nslookup alcasar* ». sous Linux, lancez « *dig alcasar* ». Le résultat doit être l'@IP d'ALCASAR. En cas d'échec, vérifiez qu'ALCASAR soit bien le serveur DNS des équipements de consultation
- l'interface de gestion : lancez un navigateur sur un équipement de consultation et tentez de vous connecter sur ALCASAR (http://alcasar).
- Test de connexion Internet : Testez la connexion vers un site Internet. ALCASAR doit vous intercepter et présenter la fenêtre d'authentification.

9.5. Problèmes déjà rencontrés

Ce chapitre présente le retour d'expérience d'organismes ayant trouvé la solution à des problèmes identifiés.

a) Les images ne s'affichent pas sur certains sites

Quand le filtrage de domaines et d'URLs est activé, ALCASAR filtre par défaut les liens WEB sans nom de domaine (vers des adresses IP pures). Ainsi, les pages WEB contenant ce type de lien ne s'affichent que partiellement. Deux solutions permettent d'éviter ce comportement : supprimer la catégorie « IP » de la liste noire (cf. §4.1.b) ou enregistrer les adresses IP contenus dans ces liens WEB comme « domaines réhabilités » (cf. §4.1.c). À titre d'exemple, le site « leboncoin.fr » référence toutes ses images vers les adresses IP suivantes : 193.164.196.30, .40, .50 et .60 ainsi que 193.164.197.30, .40 et .50.

b) Navigation impossible avec certains antivirus

Désactivez la fonction « proxy-web » intégrée à certains antivirus (cas de trend-micro).

c) Stations Windows précédemment connectées sur un Hotspot public

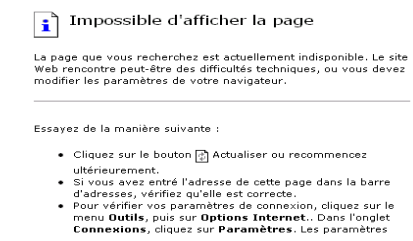
Lorsqu'un système se connecte à un « Hotspot public », celui-ci fournit les paramètres réseau ainsi qu'un « bail » qui détermine le temps de validité de ces paramètres. Les stations Windows XP ne réinitialisent pas ces paramètres lors d'un redémarrage. Ainsi, même si elles changent de réseau, elles se présenteront avec les paramètres du Hotspot précédent. Ce problème est reconnu par Microsoft qui propose la solution suivante : forcer 'à la main' la demande de renouvellement des paramètres réseau via la commande « ipconfig /renew ».

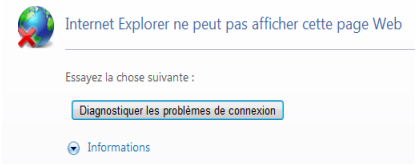
d) Stations Windows à adressage fixe

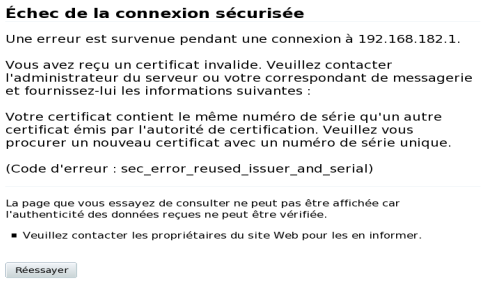
Il est nécessaire d'ajouter le suffixe DNS « localdomain » (configuration réseau + « avancé + rubrique « dns »).

e) Navigation impossible alors que l'on accède à la page du portail (http://alcasar)

Ce phénomène peut apparaître après une réinstallation complète du portail ou après une mise à jour avec changement du certificat serveur. Les navigateurs présentent alors les pages suivantes quand ils tentent de joindre un site Internet :







Sous IE6 Sous IE 7 - 8 et 9 Sous Mozilla

Ce phénomène est dû au fait que les navigateurs essaient d'authentifier le portail ALCASAR à l'aide d'un ancien certificat. Sur les navigateurs, il faut donc supprimer l'ancien certificat d'ALCASAR (« outils » + « options Internet », onglet « contenu », bouton « certificats », onglet « autorités de certification racine ») pour le remplacer par le dernier comme indiqué au §2.3.1.

f) Navigation impossible après avoir renseigné la rubrique « sites de confiance »

ALCASAR vérifie la validité des noms de domaine renseignés dans cette rubrique (cf. §3.7.a). Si un nom de domaine n'est pas valide, le service 'chilli' ne peut plus se lancer. Modifiez alors le nom de domaine posant un problème et relancez le service 'chilli' via la commande « *service chilli restart* ».

g) Surcharge mémoire et système

Le système Linux essaie toujours d'exploiter le maximum de mémoire vive. Sur la page d'accueil du centre de gestion, le bargraph indiquant l'utilisation de la mémoire physique peut ainsi régulièrement se trouver au-delà de 80% et apparaître en rouge. Cela est normal.
Si le système a besoin de mémoire supplémentaire, il exploitera le swap. Ce swap est une zone du disque dur exploitée comme mémoire vive (mais 1000 fois plus lente). Si vous vous apercevez que le système utilise cette zone de swap (> 1%), vous pouvez envisager d'augmenter la mémoire vive afin d'améliorer grandement la réactivité du système surtout quand le module de filtrage de domaines et d'URL est activé.
Vous pouvez visualiser la charge du système sur la page d'accueil du centre de gestion dans la partie 'Système/Charge système' ou en mode console à l'aide de la commande « *top* » ou « *uptime* » :

- les 3 valeurs affichées représentent la charge moyenne du système pendant la dernière, les 5 dernières et les 15 dernières minutes. Cette charge moyenne correspond au nombre de processus en attente d'utilisation du processeur.
  Ces valeurs sont normalement inférieures à 1. Une valeur supérieure à '1.00' traduit un sous-dimensionnement du serveur (surtout si elle se répercute sur les 3 valeurs (charge inscrite dans la durée).
- Chercher le processus qui monopolise un grand pourcentage de la charge (commande « *top* »).

10. Sécurisation

Sur le réseau de consultation, ALCASAR constitue le moyen de contrôle des accès à Internet. Il permet aussi de protéger le réseau vis-à-vis de l'extérieur ou vis-à-vis d'un pirate interne. À cet effet, il intègre :

- une protection contre le vol d'identifiants. Les flux d'authentification entre les équipements des usagers et ALCASAR sont chiffrés. Les mots de passe sont stockés chiffrés dans la base ;
- une protection contre les oublis de déconnexion. L'attribut « durée limite d'une session » (cf. §3.1) permet de déconnecter automatiquement un usager après un temps défini ;
- une protection contre les pannes (réseau ou équipements de consultation). Les usagers dont l'équipement de consultation ne répond plus depuis 6 minutes sont automatiquement déconnectés ;
- une protection contre le vol de session par usurpation des paramètres réseau. Cette technique d'usurpation exploite les faiblesses des protocoles « Ethernet » et WIFI. Afin de diminuer ce risque, ALCASAR intègre un processus d'autoprotection lancé toutes les 3 minutes (alcasar-watchdog.sh) ;
- une protection du chargeur de démarrage du portail (GRUB) par mot de passe. Ce mot de passe est stocké dans le fichier « */root/ALCASAR-passwords.txt* ».

La seule présence d'ALCASAR ne garantit pas la sécurité absolue contre toutes les menaces informatiques et notamment la menace interne (pirate situé dans votre organisme).
Dans la majorité des cas, cette menace reste très faible. Sans faire preuve de paranoïa et si votre besoin en sécurité est élevé, les mesures suivantes permettent d'améliorer la sécurité globale de votre système :

10.1. Sur ALCASAR

Choisissez un mot de passe « root » robuste (vous pouvez le changer en lançant la commande « *passwd* »).
Protégez le PC « ALCASAR » et l'équipement du FAI afin d'éviter :
- l'accès et le vol des équipements (locaux fermés, cadenas, etc.) ;
- le démarrage du PC au moyen d'un support amovible (configurez le BIOS afin que seul le disque dur interne soit amorçable) ;
- la mise en place d'un équipement entre ALCASAR et l'équipement du FAI.

10.2. Sur le réseau de consultation

Les postes doivent être protégés par des mesures garantissant leurs intégrités physiques.
L'accès physique au réseau de consultation doit être maîtrisé :
- déconnectez (débrassez) les prises réseau inutilisées ;
- activez le « verrouillage par port » (fonction « *Port Security* ») sur les commutateurs (switch) du réseau de consultation. Pour usurper un équipement de consultation, un pirate interne sera alors obligé d'introduire physiquement un concentrateur (hub) sur le réseau ;
- camouflez le SSID et activez le chiffrement WPA2 sur les points d'accès WIFI.

Les équipements de consultation peuvent (doivent) intégrer plusieurs autres éléments de sécurité tels que le verrouillage de la configuration du BIOS et du bureau, un antivirus, la mise à jour automatique de rustines de sécurité (patch), etc. Afin de faciliter le déploiement de ces éléments, ALCASAR peut autoriser les équipements du réseau de consultation à se connecter automatiquement et sans authentification préalable sur des sites spécialement identifiés afin de télécharger des rustines de sécurité ou afin de mettre à jour les antivirus (cf. §7).
Si vous désirez mettre en place des stations de consultation en accès libre, il peut être intéressant de vous appuyer sur des produits garantissant à la fois la protection de la vie privée et la sécurisation de la station de consultation (stations de type « cybercafé »). Ces produits permettent de cloisonner l'usager dans un environnement étanche. À la fin d'une session, l'environnement de l'usager est complètement nettoyé.
- Pour des stations sous Linux, vous pouvez installer le produit « xguest » (il est fourni nativement dans le cas de la distribution Mandriva, Fedora et RedHat)
- Pour les stations sous Windows, suivez ce lien sur le TechNet ©Microsoft : « http://technet.microsoft.com/fr-fr/library/gg176676%28WS.10%29.aspx »

Sensibilisez les usagers afin qu'ils changent leur mot de passe et afin qu'ils ne divulguent pas leurs identifiants (ils sont responsables des sessions d'un « ami » à qui ils les auraient fournis).

11. Commandes et fichiers utiles

11.1. Pour ALCASAR

L'administration d'ALCASAR est directement exploitable dans un terminal par ligne de commande (en tant que 'root'). Ces commandes commencent toutes par « alcasar-... ». Certaines d'entre elles s'appuient sur le fichier

central de configuration d'ALCASAR (« /usr/local/etc/alcasar.conf »). Avec l'argument « -h », chaque commande fournit la liste des options qu'elle possède.

- alcasar-conf -apply : applique les paramètres réseau conformément au fichier de configuration ;
- alcasar-bl.sh [-on/-off] : active/désactive le filtrage de domaines et d'URL ;
- alcasar-bl.sh -download : télécharge et applique la dernière version de la BlackList de Toulouse ;
- alcasar-safesearch.sh [-on/-off] : active/désactive le filtrage du résultat des principaux moteurs de recherche ;
- alcasar-dg-pureip.sh [-on/-off] : active/désactive le filtrage des urls contenant des adresses IP (sans nom de domaine) ;
- alcasar-nf.sh [-on/-off] : active/désactive le filtrage de protocoles réseau ;
- alcasar-havp.sh [-on/-off] : active/désactive le filtrage d'antivirus sur les flux WEB ;
- alcasar-havp.sh -update : mets à jour la base de connaissance de l'antivirus (clamav) ;
- alcasar-mysql.sh -import fichier_sql.sql : importe une base d'usagers (écrase l'existante) ;
- alcasar-mysql.sh -raz : remise à zéro de la base des usagers ;
- alcasar-mysql.sh -dump : crée une archive de la base d'usagers actuelle dans « /var/Save/base » ;
- alcasar-mysql.sh -acct_stop : stop les sessions de comptabilité ouvertes ;
- alcasar-logout.sh <username> : déconnecte l'usager <username> (toute ses sessions) ;
- alcasar-logout.sh all : déconnecte tous les usagers connectés ;
- alcasar-version.sh : compare la version d'ALCASAR active avec la dernière version disponible ;
- alcasar-bypass.sh [-on/-off] : active/désactive le mode « BYPASS » ;
- alcasar-mondo.sh : crée une image ISO « à chaud » du système (!!! processus pouvant durée plus d'une heure) ;
- alcasar-CA.sh : crée une autorité de certification locale et un certificat serveur. Nécessite de relancer le serveur WEB Apache (service httpd restart).

Chaque service rendu par le serveur est pris en charge par un « daemon », dont le démarrage est géré automatiquement :

- Voir l'état d'un démon particulier (fonctionne pour la majorité des démons)
  /etc/init.d/<nom du service> status
- Relancer/stopper un démon :
  /etc/init.d/<nom du service> {start|stop|restart|reload}

11.2. Éditeur de texte vi

Ce résumé des commandes usuelles de vi est extrait du site : http://wiki.linux-france.org/wiki/Utilisation_de_vi
Auteur : Jérôme Desmoulins (septembre 1999) Wikisé par Nat - Récupérée de « http://wiki.linux-france.org/wiki/Utilisation_de_vi »

Présentation

« vi » offre deux modes de fonctionnement: le mode « *commande* » et le mode « *insertion* ».
Au démarrage il est en mode commande, ce qui permet de déplacer le curseur, de parcourir le document et de copier-coller. On le quitte, en entrant du même coup en mode insertion, en utilisant une commande d'insertion ou de modification.
En mode insertion il est possible de saisir du texte. Appuyer sur la touche [ESC] pour revenir en mode commande.
De nombreuses commandes peuvent être préfixées du nombre de répétitions souhaitées : par exemple *5Y* permet de copier 5 lignes à partir du curseur.

Commandes et combinaisons de touches

Saisir les combinaisons, proposées ci-après, telles quelles ; seuls les éléments en *italiques* y sont à interpréter. La première combinaison proposée, par exemple, est **:w** donc implique de taper sur la touche ':' puis sur la touche 'w'.
Pour lancer vi en lui demandant de charger (ouvrir) un fichier: ***vi <nom_du_fichier>***

Sauvegarder un fichier - quitter vi

:w	sauvegarde le fichier (penser à *write*)
:wq	sauvegarde le fichier et quitte vi (*write* and *quit*) équivalent à :x
:q	quitte vi sans sauvegarder les modifications (*quit*)
:q!	quitte immédiatement, sans rien faire d'autre
:w <*nom_de_fichier*>	sauvegarde le fichier sous le nom <*nom_de_fichier*>
:w	*sauvegarde le fichier (penser à write)*
:wq	sauvegarde le fichier et quitte vi (*write* and *quit*) équivalent à :x
:q	quitte vi sans sauvegarder les modifications (*quit*)
:q!	quitte immédiatement, sans rien faire d'autre
:w <*nom_de_fichier*>	sauvegarde le fichier sous le nom <*nom_de_fichier*>

Rechercher et remplacer

/motif	recherche motif en allant vers la fin du document
n	répète la dernière recherche (*n*ext, suivant)
N	retourne au résultat de la précédente recherche effectuée
:%s/*motif*/*motif2*/g	recherche le *motif* et la remplace par *motif2*

Copier-Coller

Y	copie une ligne, donc la place dans un tampon, pour pouvoir ensuite la coller (*y*ank, tirer)
*n*Y	copie *n* lignes
p	colle les lignes après le curseur (*p*aste, coller)

Annuler ou répéter des modifications

u	annule la dernière modification (*u*ndo, défaire)
.	(un point) répète les dernières modifications

Insérer du texte

i	active le mode insertion

Supprimer du texte

x	supprime un caractère (« faire une croix dessus »)
dd	supprime une ligne
*n*dd	supprime *n* lignes

11.3. Manipulation de fichiers et répertoires

- *cd <directory>* : *aller dans un répertoire*
- *cd /* : *retourner à la racine*
- *ls <directory>* : *afficher le contenu d'un répertoire*
- *ls* : *afficher le contenu du répertoire courant*
- *cat <file>* : *afficher le contenu d'un fichier*
- *mv <source> <destination>* : *déplacer ou renommer un fichier*
- *cp <source> <destination>* : *copier un fichier*
- *rm <file>* : *efface un fichier*
- *rm -rf <directory>* : *efface un répertoire et ses sous-répertoires sans demander de confirmation*
- *tar –zxvf <fichier_archive.tar.gz>* : *décompresser et désarchiver dans le répertoire courant*

12. Fiche « usager »

Un contrôle d'accès Internet a été mis en place dans votre organisme au moyen d'un portail ALCASAR. Quand votre navigateur tente de se connecter sur Internet, la fenêtre de connexion suivante permet de vous identifier. La casse est prise en compte (« dupont » et « Dupont » sont deux usagers différents).

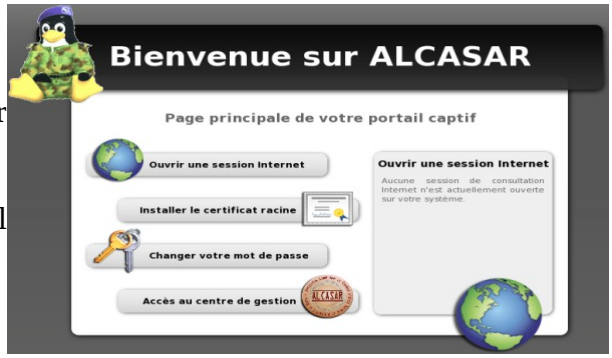
Quand l'authentification a réussi, la fenêtre « pop-up » suivante est présentée. Elle permet de vous déconnecter du portail (fermeture de session). Vous serez automatiquement déconnecté si vous la fermez. Cette fenêtre fournit les informations relatives aux droits accordés à votre compte (expirations, limites de téléchargement, etc.). Dans certains cas, cette fenêtre n'est plus visible, alors que vous êtes toujours connecté. Pour vous déconnecter, entrez le lien « http://alcasar » dans votre navigateur.

En cas d'échec de connexion, un message permet d'en connaître la cause :

Sans information particulière, votre identifiant et/ou votre mot de sont erronés.

Vous avez la possibilité de vous déconnecter ou de changer votre mot de passe via le lien suivant : http://alcasar

Ce lien permet aussi d'intégrer le certificat de sécurité du portail dans votre navigateur.



Le portail possède un antivirus protégeant les flux WEB. Il intègre un dispositif de filtrage des sites dont le contenu peut être répréhensible. Il permet aussi de savoir quand la connexion à Internet est inopérante (panne d'un équipement ou lien opérateur défectueux). Les pages suivantes sont alors affichées :