



ALCASAR

Application Libre pour le Contrôle d'Accès Sécurisé et
Authentifié au Réseau



INSTALLATION

Projet : ALCASAR	Auteur : Rexy with support of « Alcasar team »
Objet : Installation	Version : 1.8
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : Décembre 2009

Table des matières

Introduction	2
Pré requis matériel	3
Pré requis logiciel	3
Installation du système d'exploitation	3
Installation d'Alcasar	7
Désinstallation et réinstallation d'Alcasar	8
Fiche récapitulative des paramètres d'Alcasar	9

Introduction

ALCASAR est un portail captif authentifiant sécurisé. Ce document décrit la procédure d'installation de ce portail. Il est complété par les trois documents suivant :

- le document de présentation ;
- le document d'exploitation ;
- la documentation technique.

Si vous possédez déjà une version d'Alcasar fonctionnelle et que vous désirez effectuer une mise à jour, reportez-vous sur la documentation d'exploitation (chapitre mise à jour).

Alcasar peut être installé sur un PC bureautique standard dont la totalité du disque dur est utilisée. Ce PC doit posséder deux cartes réseau. La première (eth0) est connectée à l'équipement du Fournisseur d'Accès Internet (FAI). La deuxième (eth1) est connectée à l'Équipement Actif de Réseau (EAR) utilisé pour desservir le réseau des stations de consultation.

Un plan d'adressage par défaut est défini (192.168.182.0/24). Celui-ci peut-être modifier lors de l'installation d'Alcasar. L'ordinateur hébergeant Alcasar possède toujours la première adresse de ce plan (a.b.c.1). Ce plan est divisé en deux :

- la première moitié est dédiée aux équipements dont l'adressage est fixe ;
- la deuxième moitié est affectée aux équipements dont les adresses sont attribuées dynamiquement par Alcasar via le protocole « dhcp ».

Ce découpage permet de connecter sans risque de recouvrement des équipements à adressage dynamique (équipements de consultation) et d'autres à adressage statique comme des imprimantes, des serveurs, des équipements actifs de réseau (points d'accès WiFi, commutateurs, etc.) ou des équipements incompatibles avec l'adressage dynamique. Le réseau de consultation peut exploiter plusieurs technologies d'accès (Ethernet, wifi, CPL, bluetooth, etc.). La seule contrainte consiste à n'utiliser ni routeur ni serveurs DHCP sur ce réseau.

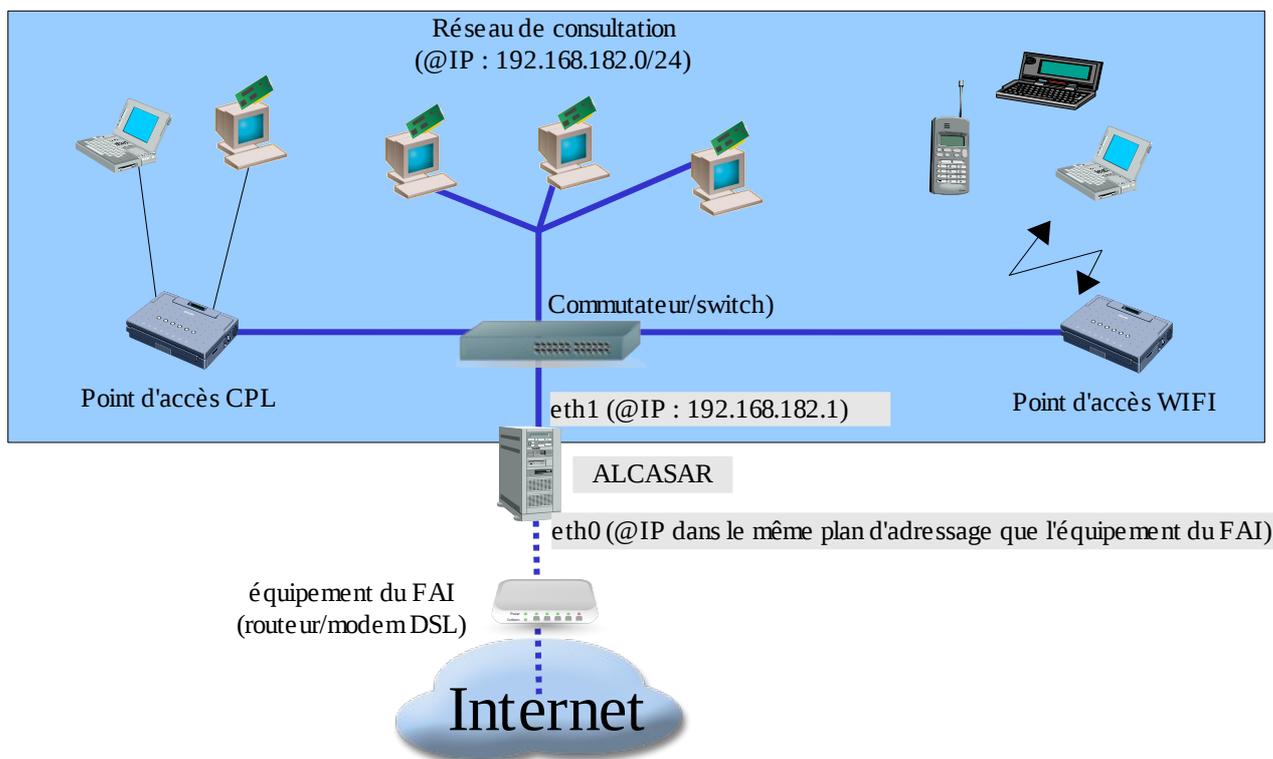
Voici deux exemples de plan d'adressage de classes différentes :

Exemple du plan d'adressage de classe C proposé par défaut (252 équipements de consultations)

- Adresse IP du réseau : 192.168.182.0/24 (masque : 255.255.255.0)
- Nombre maximum d'équipements sur le réseau de consultation : 251
- Adresse-IP-Alcasar : 192.168.182.1
- Paramètres des équipements à adressage fixe :
 - adresse IP : de 192.168.182.2 à 192.168.182.126
 - adresses des serveurs DNS : les mêmes adresses que celles définies lors de l'installation d'Alcasar ;
 - adresse du routeur par défaut (default gateway) : adresse IP d'Alcasar (192.168.182.1)
 - masque de réseau : 255.255.255.0
- Paramètres des équipements à adressage dynamique (fournis automatiquement par Alcasar) :
 - adresse IP :de 192.168.182.128 à 192.168.182.254
 - les autres paramètres sont identiques à l'adressage fixe

Exemple d'un plan d'adressage de classe B (65532 équipements de consultation)

- Adresse IP du réseau : 172.16.0.0/16 (masque : 255.255.0.0)
- Nombre maximum d'équipements sur le réseau de consultation : 65531
- Adresse-IP-Alcasar : 172.16.0.1
- Équipements à adressage fixe :
 - adresse IP : de 172.16.0.2 à 172.16.126.254
 - adresses des serveurs DNS : les mêmes adresses que celles définies lors de l'installation d'Alcasar ;
 - adresse du routeur par défaut (default gateway) : adresse IP d'Alcasar (172.16.0.1) ;
 - masque de réseau : 255.255.0.0
- Paramètres des équipement à adressage dynamique (fournis automatiquement par Alcasar) :
 - adresse IP :de 172.16.127.1 à 172.16.255.254
 - les autres paramètres sont identiques à l'adressage fixe



Pré requis matériel

Pour pouvoir fonctionner, Alcasar n'exige qu'un PC bureautique standard possédant 2 cartes réseau Ethernet. Une attention particulière doit être apportée à la capacité du disque dur (≥ 50 Go) afin que celui-ci soit en mesure de stocker les fichiers journaux liés à la traçabilité des connexions. Alcasar intègre un système de filtrage WEB (URL et contenu). Si vous décidez d'activer ce système de filtrage, il est recommandé d'installer au moins 512 MO de mémoire vive afin d'assurer une rapidité de traitement acceptable. À titre d'exemple, un organisme a déployé Alcasar avec plus de 1000 comptes sur un PC dont les caractéristiques sont : Intel P4 3.2Ghz, 2Go de mémoire vive et un disque dur de 80 Go.

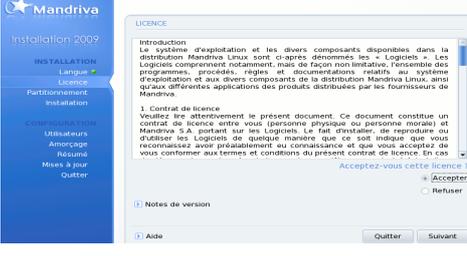
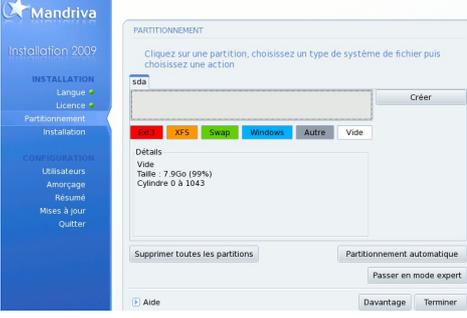
Pré requis logiciel

Alcasar ne s'appuie que sur des logiciels libres. Le système d'exploitation utilisé est « Linux-Mandriva ». Les architectures 32 bits et 64 bits sont supportées.

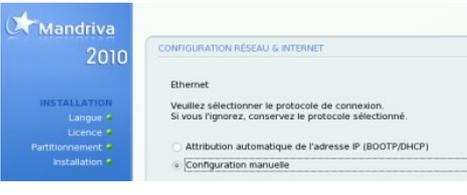
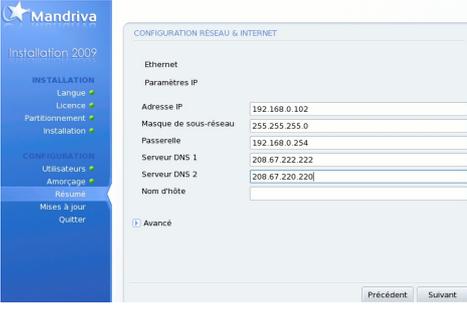
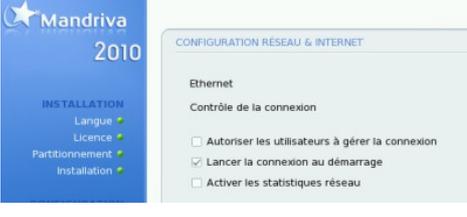
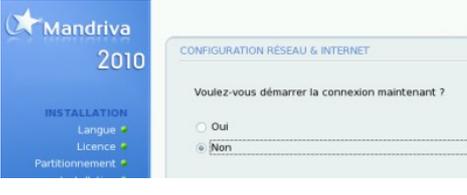
Installation du système d'exploitation

La procédure d'installation de ce système est la suivante (durée estimée : 6') :

- récupérez puis gravez sur un CD-ROM, l'image ISO de la version « free » de Linux Mandriva 2010.0 : fichier « mandriva-linux-free-dual-2010.iso » (698 MB). Cette image ISO est disponible sur le site d'Alcasar ainsi que sur de multiples sites miroirs de Mandriva. Par exemple :
 - ftp://ftp.free.fr/mirrors/Distributions_Linux/MandrivaLinux/official/iso/2010.0/
 - <ftp://ftp.lip6.fr/pub/linux/distributions/Mandrakelinux/official/iso/2010.0/>
 - <ftp://ftp.cru.fr/pub/linux/Mandrakelinux/official/iso/2010.0/>
- modifiez les paramètres BIOS du PC afin de régler la date, l'heure et afin de permettre l'amorçage d'un système à partir du CD-ROM. À la fin de l'installation, modifiez une nouvelle fois les paramètres BIOS pour limiter les possibilités d'amorçage au seul disque dur ;
- insérez le CD-ROM, redémarrez le PC et suivez les instructions suivantes :

Messages affichés à l'écran	Commentaires	Actions à réaliser
	<p>Après démarrage du PC, cette page d'accueil est présentée.</p> <p>* si le mode graphique n'apparaît pas, vous devez configurer le BIOS du PC afin d'allouer plus de 2Mo de la mémoire partagée pour la carte graphique.</p>	<p>Sélectionnez « Install Mandriva Linux 2010 ».</p> <p>* Vous pouvez franciser l'installation en sélectionnant « F2 ».</p>
		<p>Sélectionnez la langue française.</p>
		<p>Acceptez le contrat de licence.</p> <p>* ce contrat explique que la plupart des logiciels installés sont des logiciels libres.</p>
		<p>Sélectionnez « Installation ».</p>
		<p>Sélectionnez votre type de clavier (français).</p>
	<p>Le partitionnement du disque dur sera adapté au besoin d'Alcasar (cf. étape suivante).</p>	<p>Sélectionnez « partitionnement de disque personnalisé ».</p> <p>* la copie d'écran montre un disque dur contenant déjà des partitions (celles-ci seront supprimées à l'étape suivante).</p>
	<p>Les 5 partitions suivantes doivent être créées :</p> <ul style="list-style-type: none"> • / : 1Go • swap : gardez la taille proposée (ou 2 fois la taille de la mémoire vive) • /tmp : 1Go • /home : 1Go • /var : le reste du disque dur <p>* à part le « swap », tous les Systèmes de Fichiers (SF) sont du type « Journalized FS : ext4 » (info :EXT4 est le dernier système de fichiers journalisé de Linux).</p>	<p>Le cas échéant, supprimer toutes les partitions existantes. Cliquez ensuite à l'intérieur de la zone grise du disque (sda) pour « créer » chaque nouvelle partition.</p>

Messages affichés à l'écran	Commentaires	Actions à réaliser
	<p>À la fin de cette opération, et en fonction de la taille de votre disque dur, le partitionnement devrait ressembler à cela :</p>	<ul style="list-style-type: none"> - Créez la partition racine (/). Choisissez sa taille (1Go) et son système de fichier (ext4). Recommencez cette étape pour toutes les autres partitions. - Une fois le partitionnement effectué, cliquez sur « terminer ».
	<p>Pour Alcasar, l'installation ne nécessite pas d'autre média.</p>	<p>Sélectionnez « aucun »</p>
	<p>Choix des groupes de paquetages à installer : « Alcasar » ne nécessite qu'une installation minimale du système Linux.</p>	<p>Choisissez uniquement le groupe de paquetages « LSB » (Linux Standard Base). Dé-sélectionnez tous les autres groupes puis cliquez sur « Suivant ». La copie des logiciels (paquetages) sur le disque dur est alors lancée. Durée estimée : 4'</p>
		<p>Affectez le mot de passe au compte « root » puis créez le compte « sysadmin » (et affectez-lui un mot de passe).</p>
	<p>Installation du programme d'amorçage (grub) sur le premier secteur du disque dur (Master Boot Record).</p>	<p>Sélectionnez « Premier secteur du disque (MBR) ».</p>
	<p>Configuration de la première carte réseau</p>	<p>Cliquez sur « Configurer » de la rubrique « Réseau » du groupe « Réseau et Internet ».</p>
		<p>Sélectionnez « Filaire (Ethernet) » .</p>

Messages affichés à l'écran	Commentaires	Actions à réaliser
	<p>On ne configure pour l'instant que la première interface. Celle-ci doit être connectée à l'équipement (routeur DSL) du prestataire de service (FAI). La deuxième interface est connectée au réseau de consultation. Elle sera paramétrée plus tard, lors de l'installation d'Alcasar.</p>	<p>Sélectionnez la première interface.</p>
		<p>Sélectionnez « configuration manuelle ».</p>
	<p>Exemple :</p> <ul style="list-style-type: none"> • Adresse IP : cette adresse doit être dans le même sous-réseau que l'adresse du routeur DSL du FAI. • Masque : 255.255.255.0 • Passerelle : c'est l'adresse du routeur DSL (en général 192.168.1.1 pour une « livebox » et 192.168.0.254 pour une « freebox ») • DNS 1 et DNS 2 :¹ • « nom d'hôte » : laissez ce champ vide 	<p>Entrez les paramètres de cette interface.</p> <p>*Récupérez ces informations auprès de votre FAI afin de les adapter à votre situation.</p>
		<p>Sélectionnez uniquement « Lancer la connexion au démarrage ».</p>
	<p>Il n'est pas nécessaire de lancer cette connexion à ce stade</p>	<p>Sélectionnez « Non »</p>
		<p>Cliquez sur « Terminer ».</p>
		<p>Cliquez sur « Suivant ».</p>

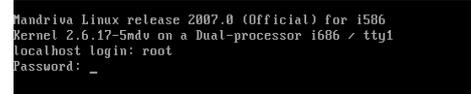
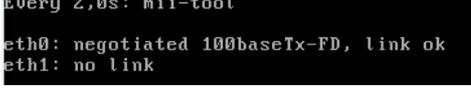
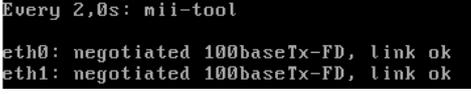
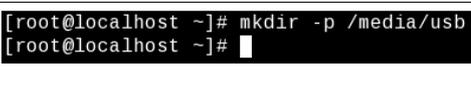
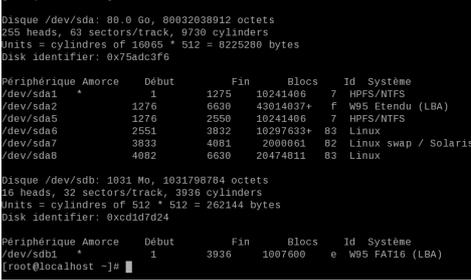
¹ Inscrivez les adresses des serveurs de DNS fournies par votre FAI. Vous pouvez aussi utiliser les serveurs du projet « OpenDNS » (DNS1=208.67.222.222, DNS2=208.67.220.220).

Messages affichés à l'écran	Commentaires	Actions à réaliser
	Les mises à jour de sécurité seront gérées après l'installation d'Alcasar.	Sélectionnez « Non » et cliquez sur « Suivant ».
	L'installation est terminée	<p>Cliquez sur « Redémarrage ».</p> <p>Retirez le CD.</p> <p>Reconfigurez le BIOS afin :</p> <ul style="list-style-type: none"> de limiter les possibilités d'amorçage au seul disque dur ; d'en verrouiller l'accès par mot de passe.

Installation d'Alcasar

Alcasar est constituée d'une archive compressée (alcasar-x.y.tar.gz) et de paquetages additionnels qui seront automatiquement récupérés sur Internet lors de l'installation.

Récupérez la dernière version de cette archive sur le site Internet d'Alcasar et copiez-la sur une clé USB. Suivez la procédure suivante (durée estimée :5').

Messages affichés à l'écran	Commentaires	Actions à réaliser
	- Connectez-vous en tant que « root ».	
	- Déconnectez les câbles des deux cartes réseau est affichez leur état.	watch mii-tool
	- Insérez le câble connecté au routeur du FAI dans la carte « eth0 ».	Si le lien est activé sur «la carte « eth1 », changez le câble de carte
	- Insérez le câble connecté au réseau de consultation dans la carte « eth1 » - Quittez l'affichage d'état des cartes réseau	Info : le changement d'état du lien permet de déterminer la bonne carte (« no link » ou « link ok »). Info : les deux liens réseau doivent être activés (« link ok ») pour poursuivre l'installation
	- Créez un répertoire permettant d'accueillir la clé USB.	Ctrl + c mkdir -p /media/usb
	- Insérez la clé USB - Affichez les informations relatives aux supports de masse afin de récupérer le nom du périphérique associé à votre clé. Dans l'exemple joint, « /dev/sdb1 » correspond à une clé de 1Go.	fdisk -l Info1 : pour les PC à la norme PATA (ancienne génération) la clé sera nommée hd(a-b-c-...)(1-2-3-...). Info2 : vous pouvez aussi afficher le journal système pour récupérer ce nom (tailf /var/log/messages)

Messages affichés à l'écran	Commentaires	Actions à réaliser
<pre>[root@localhost ~]# mkdir /media/usb [root@localhost ~]# mount /dev/sdb1 /media/usb/ [root@localhost ~]# █</pre>	- « Montez » le périphérique représentant la clé USB sur le répertoire précédemment créé.	mount /dev/sdb1 /media/usb/ Info : remplacez « sda1 » par le nom du périphérique récupéré à l'étape précédente (sdc1, hda1, etc.).
<pre>[root@localhost ~]# cp /mnt/usb/alcasar* .</pre>	- Copiez l'archive d'Alcasar dans le répertoire /root. - Démontez la clé USB. - Retirez-la.	cp /media/usb/alcasar* /root/ umount /media/usb
<pre>[root@localhost ~]# tar -zxvf alcasar.1-5RC4.tar.gz _ [root@localhost ~]# cd alcasar-1.8a [root@localhost alcasar-1.8a]# sh alcasar.sh -install_</pre>	- Décompressez et extrayez cette archive. - Positionnez-vous dans le répertoire d'Alcasar et lancez le script d'installation.	tar -xvf alcasar-x.y.tar.gz cd alcasar-x.y sh alcasar.sh -install
<pre>----- Installation d'ALCASAR 02009.0-rc1 Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau Test de la connexion Internet : veuillez patienter ...</pre>	- Les tests de paramètres réseau sont réalisés.	Info : dans certains cas, le script modifie la configuration des cartes réseau. Il est alors nécessaire de relancer ce script.
<pre>----- Installation d'ALCASAR 02009.0-rc1 Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau Test de la connexion Internet : veuillez patienter ... correct Entrez le nom de votre organisme : _</pre>	- Entrez le nom de votre organisme (sans espace)	Exemple : rassacla Info : ce nom est obligatoire, les seuls caractères acceptés sont : [a-z][A-Z][0-9][_-]
<pre>----- Installation de php-ctype-5.1.6-Indo2007.0.1586.rpm Préparation ... %?100: php-ctype Installation de php-ftp-5.1.6-1-Indo2007.0.1506.rpm Préparation ... warning: php-ftp-5.1.6-1-Indo2007.0: Header U3 DSA signature: NOKEY, key ID 2245 0490 %?100: php-ftp Installation de php-gettext-5.1.6-Indo2007.0.1586.rpm Préparation ...</pre>	L'installation d'une centaine de logiciels (paquetages) est effectuée à partir d'Internet. Durée :2'	
<pre>----- Installation d'ALCASAR 02009.0-rc1 Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau Le plan d'adressage par défaut du réseau de consultation est : 192.168.182.0/24 Voulez-vous utiliser ce plan d'adressage (recommandé) (0/n)? _</pre>	Vous pouvez changer le plan d'adressage par défaut du réseau de consultation (192.168.182.0/24)	Tapez « O » ou « N » Info : le découpage du plan d'adressage effectué par Alcasar peut être consulté dans le fichier « /root/ALCASAR-parametres.txt »
<pre>----- Installation d'ALCASAR 01.8a Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau Pour administrer Alcasar via le centre de gestion WEB, trois profils de comptes ont été définis : - le profil 'admin' capable de réaliser toutes les opérations - le profil 'backups' lié uniquement aux fonctions d'archivage - le profil 'manager' lié uniquement aux fonctions de gestion des usagers Définissez le premier compte du profil 'admin' : nom : _</pre>	Entrez l'identifiant et le mot de passe d'un premier compte d'administration d'Alcasar.	
<pre>===== Fin d'installation d'ALCASAR Application Libre pour le Contrôle Authentifié et Sécurisé des Accès au Réseau (ALCASAR) Projet créé et suivi par l'Alcasar Team (Franck BOUIJOUX, Pascal LEVANT et Richard REY) Merci aux contributeurs et testeurs de la solution ===== - ALCASAR sera fonctionnel après redémarrage du système - Lisez attentivement la documentation - Sécurisez la séquence de démarrage du système et de la station (BIOS) Appuyez sur 'Entrée' pour continuer</pre>	L'installation est terminée. Le système va être relancé afin de synchroniser l'ensemble des constituants d'Alcasar.	Une fois relancé, vous pouvez utiliser le portail en ayant pris soin de créer un premier usager via l'interface de gestion (cf. document « Alcasar-exploitation »).

Le fichier « /root/ALCASAR-parameters.txt » contient les paramètres du portail. Le fichier « /root/ALCASAR-passwords.txt » contient les mots de passe exploités en interne par les différents modules d'Alcasar. Ces fichiers peuvent être consultés via la commande (cat <nom_de_fichier>).

Désinstallation et réinstallation d'Alcasar

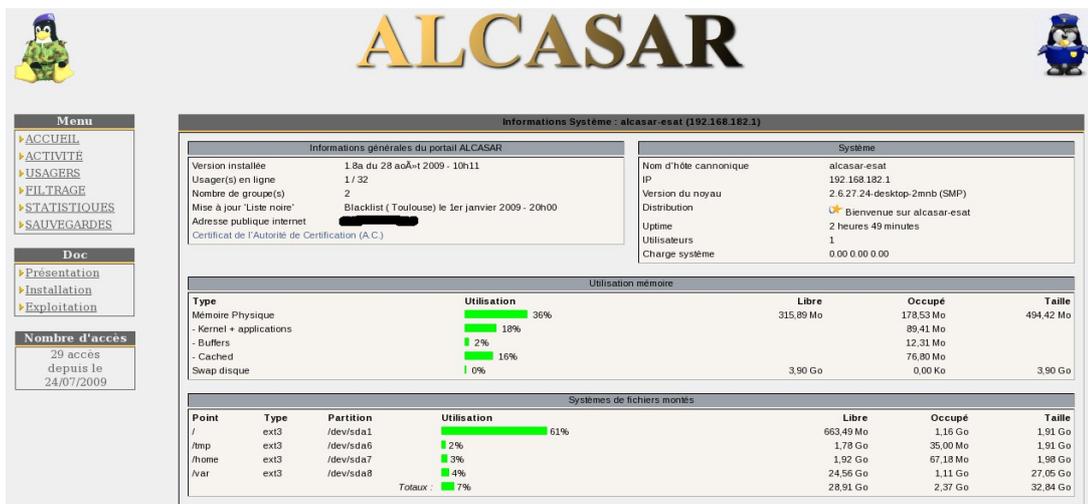
Il est possible de désinstaller le portail via la commande « sh alcasar.sh -uninstall ». Vous pouvez alors lancer une nouvelle installation en suivant la procédure décrite précédemment.

Si vous voulez réinstaller le portail tout en gardant vos paramètres de filtrage et les certificats, lancer la commande « sh alcasar.sh -update ». Cela peut vous être utile, par exemple, si vous désirez changer le plan d'adressage de votre réseau de consultation.

Pour une mise à jour de version du portail, lisez le chapitre adéquat de la documentation d'exploitation.

Fiche récapitulative des paramètres d'Alcasar

Le centre de gestion sécurisée est consultable à partir de n'importe quel équipement situé sur le réseau de consultation à l'adresse : [https://.....\(adresse-ip-alcasar\)](https://.....(adresse-ip-alcasar)). Les possibilités de cette interface sont décrites dans le document « Alcasar-exploitation ».



Nom d'organisme :		
Page d'authentification des usagers	Cette page est présentée automatiquement quand le navigateur d'une station de consultation tente de joindre un site Internet.	
Page de déconnexion des usagers	http://adresse-ip-alcasar:3990/logoff	
Page de changement de mot de passe usager ²	https://adresse-ip-alcasar/pass/	
Comptes du système Linux	root sysadmin
1er compte de gestion d'Alcasar
Paramètre du Système de Gestion de Bases de données (SGBD)	<ul style="list-style-type: none"> Nom de la base : radius Administrateur du SGBD : root Utilisateur de la base : radius
Plan d'adressage IP	<ul style="list-style-type: none"> Alcasar (côté WAN/Internet) : Alcasar (côté réseau de consultation) : Réseau de consultation : <ul style="list-style-type: none"> adresses fixes : adresses dynamiques : 	<ul style="list-style-type: none">1/.. de à de à
DNS déclarés	

² : le '/' à la fin du lien est important. 'http' n'est pas équivalent à 'https'