



PROCÉDURE D'INSTALLATION

Table des matières

Introduction	2
Préalable matériel.....	3
Préalable logiciel.....	3
Installation	3
Installation du système.....	3
Installation d'ALCASAR.....	6
Désinstallation et réinstallation d'ALCASAR	8
Fiche récapitulative des paramètres d'ALCASAR	8

Projet : ALCASAR	Auteur : Rexy with support of « Alcasar team »
Objet : Installation	Version : 2.1
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : avril 2011

Introduction

Ce document décrit la procédure d'installation du portail ALCASAR. Il est complété par trois autres documents : le document de présentation, le document d'exploitation et 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 ordinateur standard équipé de deux cartes réseau Ethernet. La première (eth0) est connectée à l'équipement du Fournisseur d'Accès Internet (FAI). La deuxième (eth1) est connectée au commutateur utilisé pour desservir le réseau des stations de consultation.

Côté réseau de consultation, le plan d'adressage suivant est défini par défaut : 192.168.182.0/24. Ce plan peut être modifié lors de l'installation. La carte réseau eth1 d'ALCASAR possède toujours la première adresse IP de ce plan (ex. 192.168.182.1 pour le plan par défaut). Ce plan est divisé en deux :

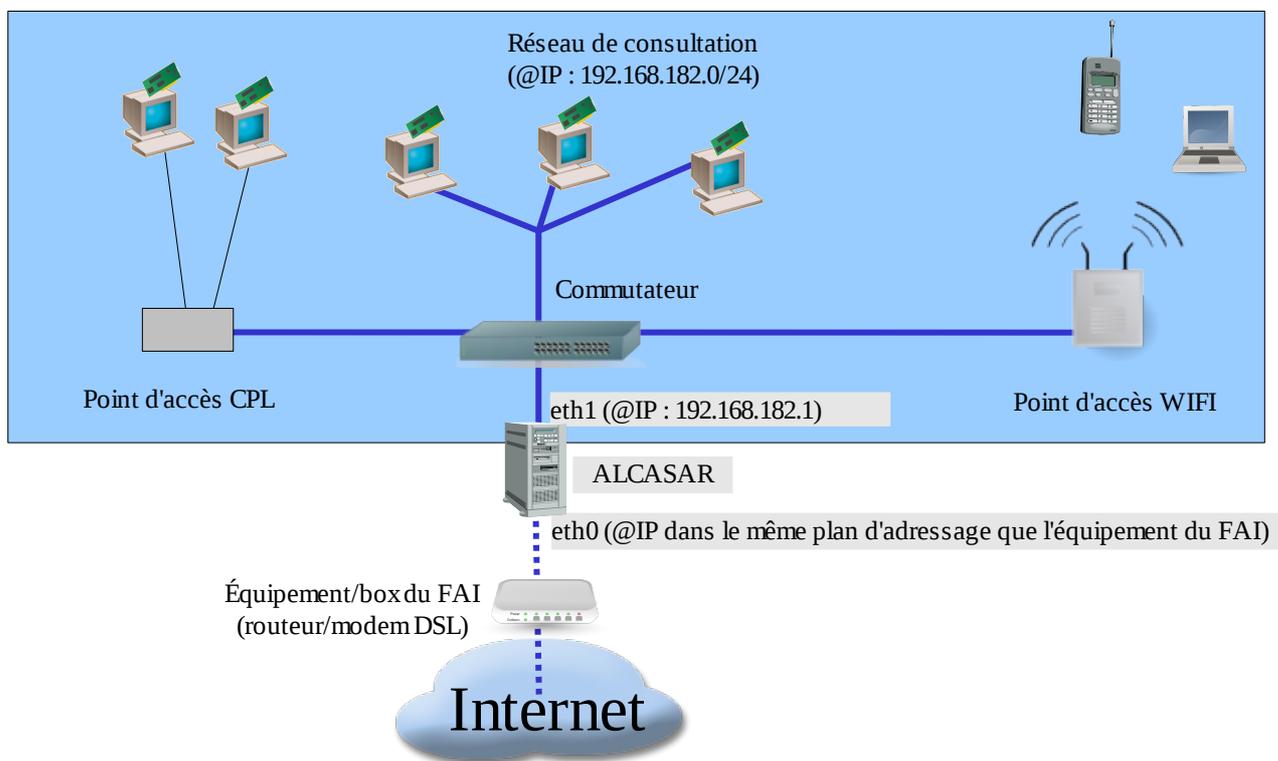
- la première moitié est dédiée aux équipements dont l'adressage IP est fixe ;
- la deuxième moitié est affectée aux équipements dont les adresses IP sont attribuées dynamiquement par ALCASAR via le protocole « dhcp ».

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 ou CPL, commutateurs, etc.) ou des équipements incompatibles avec l'adressage dynamique. Le réseau de consultation peut exploiter toutes les 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 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
- Paramètres des équipements de consultation à adressage fixe :
 - adresses IP disponibles : de 192.168.182.2 à 192.168.182.126
 - adresses des serveurs DNS et du routeur par défaut (default gateway) : 192.168.182.1 (adresse IP d'ALCASAR) ;
 - masque de réseau : 255.255.255.0
- Paramètres des équipements de consultation à adressage dynamique :
 - adresses IP fournies automatiquement par ALCASAR : 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 de la carte eth1 d'ALCASAR : 172.16.0.1
- Paramètre des équipements de consultation à adressage fixe :
 - adresses IP disponibles : de 172.16.0.2 à 172.16.126.254
 - adresses des serveurs DNS et du routeur par défaut (default gateway) : 172.16.0.1 (adresse IP d'ALCASAR) ;
 - masque de réseau : 255.255.0.0
- Paramètres des équipements à adressage dynamique :
 - adresses IP fournies automatiquement par ALCASAR : de 172.16.127.1 à 172.16.255.254
 - les autres paramètres sont identiques à l'adressage fixe

Préalable matériel

Pour pouvoir fonctionner, ALCASAR n'exige qu'un PC bureautique standard possédant 2 cartes réseau Ethernet. Le disque dur doit posséder une capacité de 50 Go au minimum afin d'être en mesure de stocker les fichiers journaux liés à la traçabilité des connexions. ALCASAR intègre plusieurs systèmes optionnels de filtrage (protocoles réseau, URL, antivirus et contenu de page WEB). Si vous décidez d'activer ces systèmes de filtrage, il est recommandé d'installer au moins 1 GO 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. Les architectures 32 bits et 64 bits sont supportées et automatiquement détectées.

Préalable logiciel

ALCASAR ne s'appuie que sur des logiciels libres. Le système d'exploitation utilisé est « Linux-Mandriva ».

Installation

L'installation du portail s'effectue en deux étapes : l'installation du système d'exploitation (Linux-Mandriva) puis l'installation d'ALCASAR.

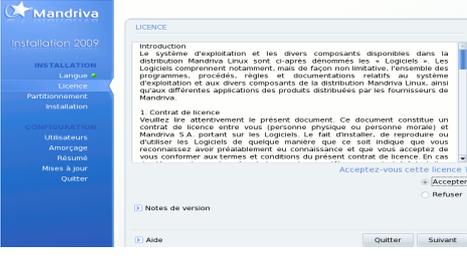
Installation du système

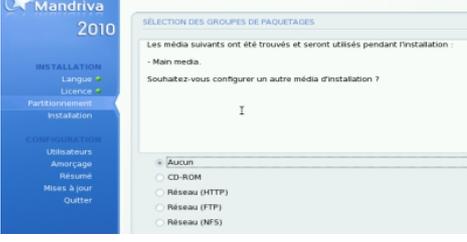
La procédure d'installation de ce système est la suivante (durée estimée : 6') :

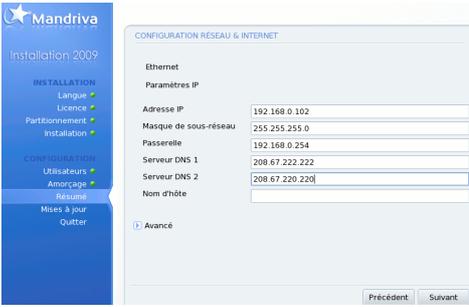
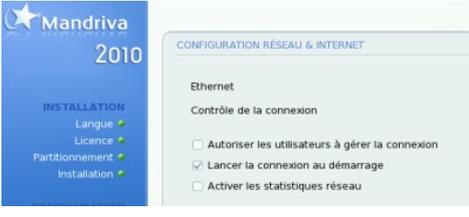
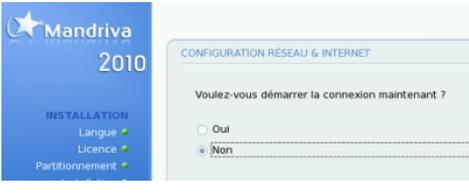
- récupérez l'image ISO de Linux Mandriva 2010.1 en version « free » double architecture (32 et 64 bits) : fichier « mandriva-linux-free-2010-spring-dual.iso » (700MB). Cette image ISO est disponible sur le site d'ALCASAR ainsi que sur de multiples sites miroirs de Mandriva. Par exemple :
 - ftp://ftp.free.fr/mirrors/Distributions_Linux/MandrivaLinux/official/iso/2010.1/
 - <ftp://ftp.lip6.fr/pub/linux/distributions/Mandrakelinux/official/iso/2010.1/>
 - <ftp://ftp.cru.fr/pub/linux/Mandrakelinux/official/iso/2010.1/>
- gravez cette image sur un CDROM ou créez une clé USB amorçable¹
- modifiez les paramètres BIOS du PC afin de régler la date, l'heure et afin de permettre l'amorçage du PC à partir d'un CD-ROM ou d'une clé USB. À la fin de l'installation, modifiez une nouvelle fois les paramètres BIOS pour limiter les possibilités d'amorçage du PC au seul disque dur ;
- insérez le CD-ROM ou la clé USB, redémarrez le PC et suivez les instructions suivantes :

¹ Deux solutions permettent de créer une clé USB amorçable (taille de la clé : 1 Go minimum) :

- en mode console sous Linux, insérez une clé et récupérez le nom du périphérique associé par la commande « `fdisk -l` » (une clé USB est souvent associée au périphérique « `/dev/sdb` » ou « `/dev/sdc` »). Lancez la commande : « `dd if=<nom_de_l'image_iso> of=<nom_du_périphérique_usb> bs=8M` ».
- en mode graphique sous linux ou windows, utilisez l'outil « mandriva-seed » disponible ici : <http://www.mandrivalinux-online.org/download/category-4+mandriva-seed-la-cle-usb-bootable.php>

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 ».</p>
		<p>Sélectionnez votre langue.</p>
		<p>Acceptez le contrat de licence.</p> <p><u>Info</u> : ce contrat explique que la plupart des logiciels installés sont des logiciels libres.</p>
		<p>Sélectionnez votre type de clavier.</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>Les 5 partitions suivantes doivent être créées :</p> <ul style="list-style-type: none"> / : 2 Go swap : gardez la taille proposée (ou 2 fois la taille de la mémoire vive) /tmp : 2 Go /home : 2 Go /var : le reste du disque dur 	<p>Cliquez sur « Supprimer toutes les partitions ».</p> <p>Cliquez ensuite à l'intérieur de la zone grise du disque (sda) pour créer chaque nouvelle partition.</p> <p><u>Info</u> : à part le « swap », tous les Systèmes de Fichiers (SF) sont du type « Journalized FS : ext4 » (ext4 est un système de fichiers journalisé pour Linux).</p>
	<p>À la fin de cette opération, et en fonction de la taille de votre disque dur, le partitionnement devrait ressembler à cela :</p> 	<p>- Créez la partition racine (/). Choisissez sa taille (2 Go) ainsi que son système de fichier (ext4). Recommencez cette étape pour toutes les autres partitions.</p> <p>- Une fois le partitionnement effectué, cliquez sur « Terminer ».</p>

Messages affichés à l'écran	Commentaires	Actions à réaliser
	<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-Mandriva.</p>	<p>Choisissez uniquement le groupe de paquetages « LSB » (Linux Standard Base). Désélectionnez tous les autres groupes puis cliquez sur « Suivant ». La copie des paquetages sur le disque dur est alors lancée. Durée estimée : 4'</p> <p><u>Info</u> : sous Linux, un paquetage est un fichier archive contenant tout les constituants d'un logiciel (binaires, fichiers d'aide, fichiers de configuration, etc.).</p>
		<p>Affectez le mot de passe au compte « root » puis créez le compte « sysadmin » et affectez-lui un mot de passe.</p>
	<p>Configuration de l'accès à Internet</p>	<p>Cliquez sur « Configurer » de la rubrique « Réseau » du groupe « Réseau et Internet ».</p>
		<p>Sélectionnez le type de connexion à Internet. Dans le cas d'une « box », choisissez « Filaire (Ethernet) ».</p> <p><u>Info</u> : Aucun test n'a encore été effectué sur ALCASAR concernant les accès à Internet par d'autres type de connexion.</p>
	<p>On ne configure pour l'instant que l'interface connectée à la « box » du FAI. La deuxième interface qui est connectée au réseau de consultation sera paramétrée plus tard, lors de l'installation d'ALCASAR.</p>	<p>Sélectionnez l'interface identifiée « eth0 ».</p> <p><u>Info</u> : si les interfaces ne sont pas identifiées (eth0, eth1, etc.), sélectionnez la première interface.</p>
		<p>Sélectionnez « configuration manuelle ».</p> <p><u>Info</u> : bien que cela soit possible, il est déconseillé de configurer cette interface en mode dynamique (bootp/dhcp) car l'équipement n'a pas vocation à être nomade.</p>

Messages affichés à l'écran	Commentaires	Actions à réaliser
	<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 (box). • 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 :* • « nom d'hôte » : laissez ce champ vide 	<p>Entrez les paramètres de cette interface.</p> <p>* 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).</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>
	<p>Les mises à jour de sécurité seront gérées pendant l'installation d'ALCASAR.</p>	<p>Sélectionnez « Non » et cliquez sur « Suivant ».</p>
	<p>L'installation est terminée</p>	<p>Cliquez sur « Redémarrage ». Retirez le CD-ROM ou la clé USB. 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 constitué d'une archive compressée (alcasar-x.y.tar.gz) et de paquetages additionnels qui sont automatiquement téléchargés sur Internet pendant la phase d'installation.

Récupérez la dernière version de l'archive compressée 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
<pre>Mandriva Linux release 2007.0 (Official) for i586 Kernel 2.6.17-5mdv on a Dual-processor i686 / tty1 localhost login: root Password: _</pre>	- Connectez-vous en tant que « root ».	
<pre>Every 2,0s: mii-tool eth0: no link eth1: no link</pre>	- Déconnectez les câbles des deux cartes réseau et affichez leur état.	watch mii-tool
<pre>Every 2,0s: mii-tool eth0: negotiated 100baseTx-FD, link ok eth1: no link</pre>	- Insérez le câble connecté à l'équipement du FAI dans la carte « eth0 ».	Si le lien est activé sur « la carte « eth1 », changez le câble de carte. Info : le changement d'état du lien permet de déterminer la bonne carte (« no link » ou « link ok »).
<pre>Every 2,0s: mii-tool eth0: negotiated 100baseTx-FD, link ok eth1: negotiated 100baseTx-FD, link ok</pre>	- Insérez le câble connecté au réseau de consultation dans la carte « eth1 » - Sortez du programme actif	Info : côté réseau de consultation, connectez un équipement actif de réseau (switch, AP WIFI, commutateur CPL, etc.) afin d'être assuré de la permanence du lien. <Ctrl> + c
<pre>[root@localhost ~]# mkdir -p /media/usb [root@localhost ~]# █</pre>	- Créez un répertoire permettant d'accueillir la clé USB.	mkdir -p /media/usb
<pre>[root@localhost ~]# fdisk -l Disque /dev/sda: 80.0 Go, 80032038912 octets 255 heads, 63 sectors/track, 9730 cylinders Units = cylinders of 16065 * 512 = 8225280 bytes Disk identifier: 0x5ad53f6 Périphérique Amorces Début Fin Blocs Id Système /dev/sda1 1 1275 10241406 7 HPFS/NTFS /dev/sda2 1275 6630 43914037+ f W95 Etendu (LBA) /dev/sda3 1275 2330 10241406 7 HPFS/NTFS /dev/sda6 2551 3832 10297633+ 83 Linux /dev/sda7 3833 4681 2080661 82 Linux swap / Solaris /dev/sda8 4682 6630 20474611 83 Linux Disque /dev/sdb: 1031 Mo, 1031709784 octets 16 heads, 32 sectors/track, 3996 cylinders Units = cylinders of 512 * 512 = 262144 bytes Disk identifier: 0xcd1d7d24 Périphérique Amorces Début Fin Blocs Id Système /dev/sdb1 1 3936 1007600 0 W95 FAT16 (LBA) [root@localhost ~]# █</pre>	- 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-...). Pour les PC à la norme SATA, elle prendra le nom sd(a-b-c-...)(1-2-3-...). Info2 : vous pouvez aussi afficher le journal système pour récupérer ce nom (tailf /var/log/messages)
<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 ... agereet Entrez le nom de votre organisme : _</pre>	- Entrez le nom de votre organisme (sans espace)	Exemple : rascal Info : ce nom est obligatoire, les seuls caractères acceptés sont : [a-z][A-Z][0-9][-]
<pre>Installation de php-ctype-5.1.6-Indu2007.0.i586.rpm Préparation ... 75/100: php-ctype Installation de php-ftp-5.1.6-1-Indu2007.0.i586.rpm Préparation ... using: php-ftp-5.1.6-1-Indu2007.0: Header 03 DSN signature: NOKEY, key ID 2245 84/99 76/100: php-ftp Installation de php-gettext-5.1.6-Indu2007.0.i586.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) (O/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-parameters.txt »
<pre>Installation d'ALCASAR 01.0a 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 'backup' 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.	

Messages affichés à l'écran	Commentaires	Actions à réaliser
<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 BOUJOUX, 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>	<p>L'installation est terminée. Le système va être relancé afin de synchroniser l'ensemble des constituants d'ALCASAR.</p>	<p>Une fois le système relancé, démarrez un équipement de consultation et connectez-vous sur l'interface de gestion du portail afin de créer vos premiers usagers (« http://alcasar »). Lisez attentivement la documentation d'exploitation (« Alcasar-exploitation.pdf »).</p>

Désinstallation et réinstallation d'ALCASAR

Il est possible de réinstaller le portail en utilisant la même commande que précédemment (« `sh alcasar.sh --install` »). Le script vous demandera alors si vous voulez garder les paramètres de la version déjà en place. Cela peut être utile pour faire des tests ou pour modifier le plan d'adressage du réseau de consultation par exemple. Vous pouvez désinstaller le portail avec la commande « `sh alcasar.sh --uninstall` ». Pour effectuer une mise à jour, lisez la documentation d'exploitation.

Fiche récapitulative des paramètres d'ALCASAR

Le fichier « `/root/ALCASAR-parameters.txt` » rappelle les paramètres réseau et système du portail. Le fichier « `/root/ALCASAR-passwords.txt` » rappelle les mots de passe exploités en interne par les différents modules d'ALCASAR (dont le mot de passe de protection du chargeur système (bootloader « GRUB »)). Ces fichiers peuvent être consultés via la commande (`cat <nom_de_fichier>`).

Nom d'organisme :	
Page d'authentification des usagers	Cette page est présentée quand un navigateur tente de joindre un site Internet.
Page d'accueil du portail permettant : - l'accès au centre de gestion graphique - la déconnexion d'un usager authentifié - le changement du mot de passe usager	<code>http://alcasar</code> Info: les possibilités du centre de gestion sont décrites dans le document « Alcasar-exploitation ».
Comptes du système Linux	root mot de passe : sysadmin mot de passe :
1er compte d'administration d'Alcasar (profil 'admin') mot de passe :
<u>Paramètres réseau</u> <ul style="list-style-type: none"> • @IP de l'équipement FAI (routeur) • @IP des serveurs DNS • @IP d'Alcasar (côté WAN/Internet) : • @IP d'Alcasar (côté réseau de consultation) : • Réseau de consultation : <ul style="list-style-type: none"> ○ @IP fixes : ○ @IP dynamiques : 	<ul style="list-style-type: none"> •_....._....._..... • DNS1 :_....._....._..... • DNS2 :_....._....._..... •_....._....._..... •_....._....._......1 •_....._....._......0/_..... • de_....._....._..... à_....._....._..... • de_....._....._..... à_....._....._.....