



# INSTALLATION

## Table des matières

1. <a href="#">Introduction</a> .....	2
2. <a href="#">Installation</a> .....	3
2.1. Préalable matériel.....	3
2.2. Installation du système.....	3
2.3. Installation d'ALCASAR.....	6
3. <a href="#">Désinstallation, réinstallation et mise à jour d'ALCASAR</a> .....	8
4. <a href="#">Préparer une installation « hors ligne »</a> .....	8
5. <a href="#">Fiche récapitulative des paramètres d'ALCASAR</a> .....	8

Projet : ALCASAR	Auteur : Rexy with support of « Alcasar team »
Objet : Installation	Version : 2.6
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : Août 2012

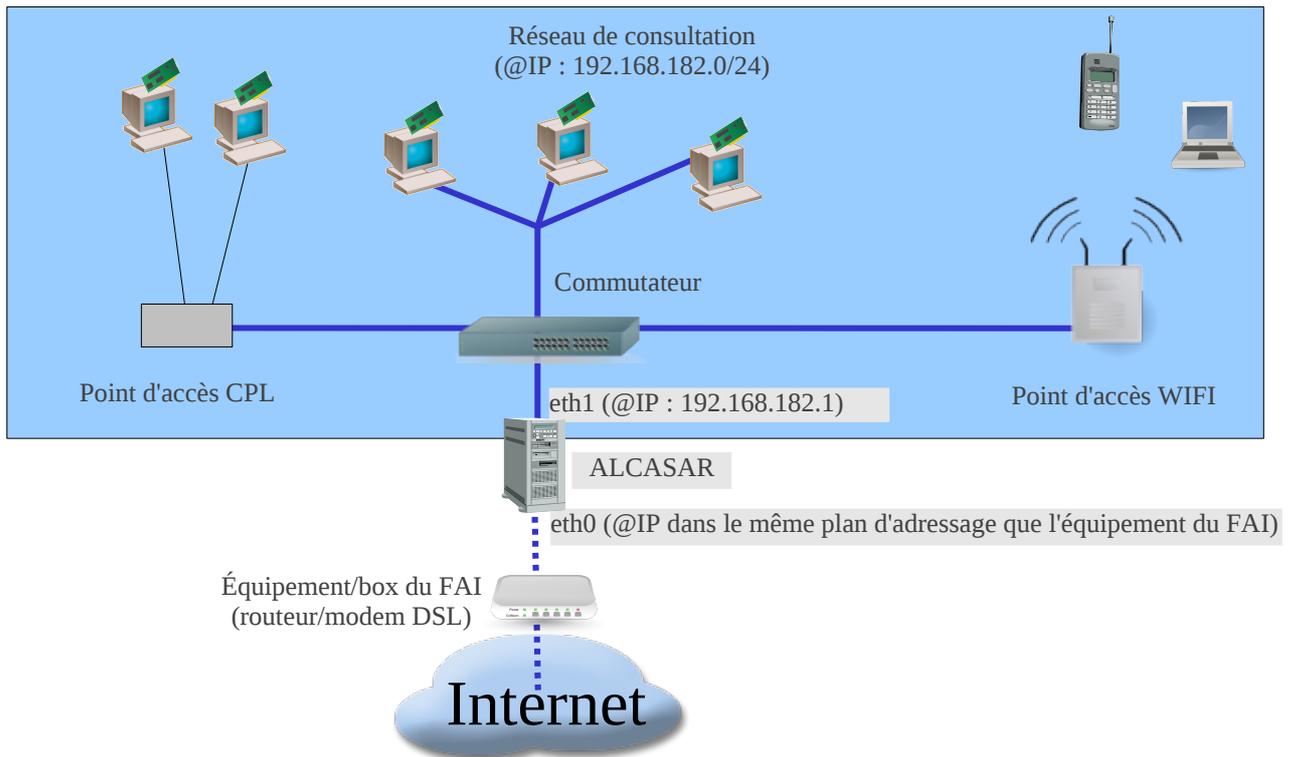
# 1. Introduction

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 à la documentation d'exploitation (chapitre « mise à jour »).

ALCASAR peut être installé sur un 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.

Par défaut, l'adresse IP de cette deuxième carte réseau est : 192.168.182.1/24. Cela permet de disposer d'un plan d'adressage de classe C (254 équipements). Ce plan d'adressage est modifiable lors de l'installation. Pour tous les équipements situés sur le réseau de consultation, ALCASAR est le serveur DNS, le serveur de temps et le « routeur par défaut (default gateway) ». **Ainsi, sur ce réseau, il ne doit y avoir aucun autre routeur.** ALCASAR peut aussi servir de serveur DHCP. Assurez-vous, dans ce cas, qu'il soit le seul.



## **Exemple du plan d'adressage de classe C proposé par défaut (254 équipements)**

- Adresse IP d'ALCASAR : 192.168.182.1/24
- Nombre maximum d'équipements sur le réseau de consultation : 253
- Paramètres réseau des équipements de consultation :
  - adresses IP disponibles : de 192.168.182.2 à 192.168.182.254 (statiques ou dynamiques)
  - masque de réseau : 255.255.255.0
  - adresses des serveurs DNS et du routeur par défaut (default gateway) : 192.168.182.1 (adresse IP d'ALCASAR)
  - suffixe DNS pour les équipements en adressage fixe : « localdomain »

## **Exemple d'un plan d'adressage de classe B (65534 équipements)**

- Adresse IP d'ALCASAR : 172.16.0.1/16
- Nombre maximum d'équipements sur le réseau de consultation : 65531
- Paramètre des équipements de consultation :
  - adresses IP disponibles : de 172.16.0.2 à 172.16.255.254 (statiques ou dynamiques)
  - masque de réseau : 255.255.0.0
  - adresses des serveurs DNS et du routeur par défaut (default gateway) : 172.16.0.1 (adresse IP d'ALCASAR)
  - suffixe DNS pour les équipements en adressage fixe : « localdomain »

Bien que cela soit possible, il est déconseillé de définir un réseau de consultation en classe A (ex : 15.0.0.0/8). En effet, le serveur DHCP interne d'ALCASAR devra alors réserver et gérer plus de 16 millions d'adresses IP. La gestion d'un tel volume d'adresses est très gourmande en ressource système et mémoire.

## 2. Installation

L'installation du portail s'effectue en deux étapes. La première étape est l'installation d'un système Linux minimaliste basé sur Linux-Mandriva. La deuxième étape permet d'installer et de configurer les différentes briques logicielles constituant ALCASAR.

### 2.1. Préalable matériel

ALCASAR n'exige qu'un PC bureautique standard possédant 2 cartes réseau et un disque dur d'une capacité de 50 Go au minimum afin d'être en mesure de stocker les fichiers journaux liés à la traçabilité des connexions. Les architectures 32 bits et 64 bits sont supportées et automatiquement prises en compte. ALCASAR intègre plusieurs systèmes optionnels de filtrage (protocoles réseau, adresses IP, URL, noms de domaines et antivirus de flux 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.

### 2.2. Installation du système

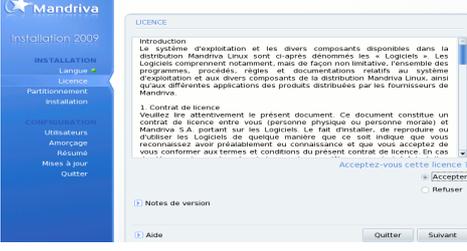
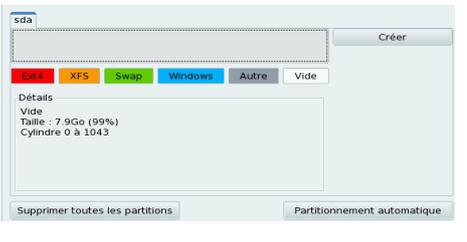
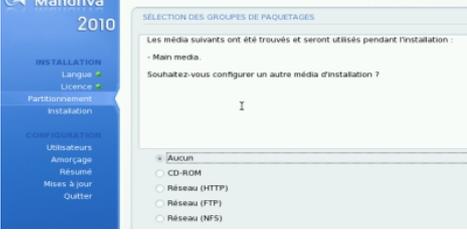
La procédure d'installation de ce système est la suivante (durée estimée : 6') :

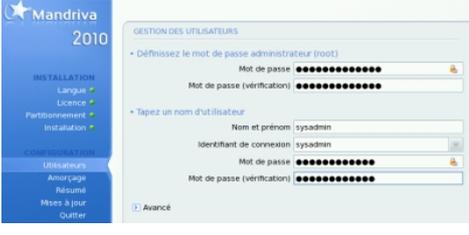
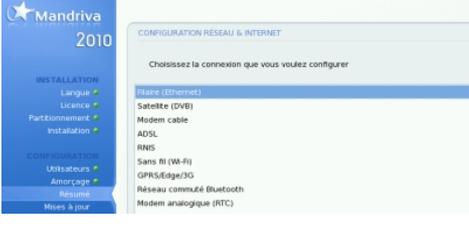
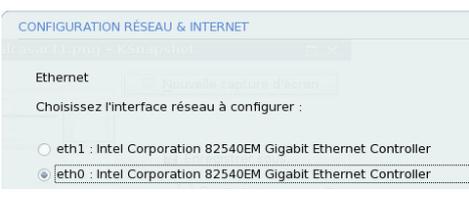
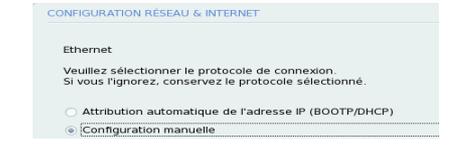
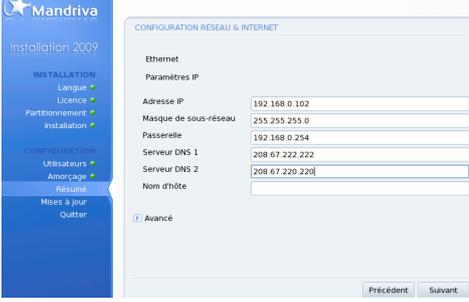
- récupérez l'image ISO de Linux Mandriva 2010.1 en version « free » double architecture (32 et 64 bits) : fichier « mandriva-linux-free-2010-spring-dual.iso » (700MB). Cette image ISO est disponible sur le site d'ALCASAR ainsi que sur de multiples sites miroirs de Mandriva. Par exemple :
  - [ftp://ftp.free.fr/mirrors/Distributions\\_Linux/MandrivaLinux/official/iso/2010.1/](ftp://ftp.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 amorçable<sup>1</sup>
- 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. Supprimez la gestion des lecteurs de disquettes si votre système n'en possède pas. 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 :

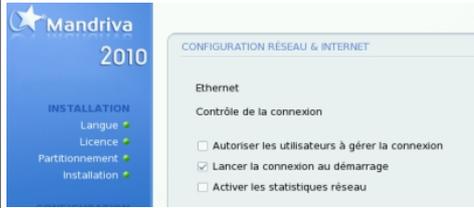
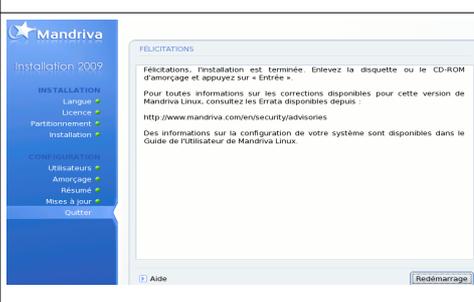
Messages affichés à l'écran	Commentaires	Actions à réaliser
	<p>Après démarrage du PC, cette page d'accueil est présentée.</p> <p>* si le mode graphique n'apparaît pas, vous devez configurer le BIOS du PC afin d'allouer plus de 2Mo de la mémoire partagée pour la carte graphique.</p>	<p>Sélectionnez « Install Mandriva ».</p>

<sup>1</sup> Deux solutions permettent de créer une clé USB amorçable (1 Go minimum **formatée en FAT ou VFAT**) :

- en mode graphique vous pouvez utiliser le logiciel « unetbootin ». Installez-le sous Linux via « urpmi » ou « apt-get ». Sous windows, récupérez-le ici : « <http://unetbootin.sourceforge.net/> ».
- en mode console sous Linux, insérez la clé et récupérez le nom du périphérique associé via 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** ».

Messages affichés à l'écran	Commentaires	Actions à réaliser
		Sélectionnez votre langue.
		Acceptez le contrat de licence.  <b>Info :</b> ce contrat explique que la plupart des logiciels installés sont des logiciels libres.
		Sélectionnez votre type de clavier.
	Le partitionnement du disque dur sera adapté au besoin d'ALCASAR (cf. étape suivante).	Sélectionnez « Partitionnement de disque personnalisé ».
	Les 5 partitions suivantes doivent être créées : <ul style="list-style-type: none"> <li>• / : 2 Go</li> <li>• swap : gardez la taille proposée (ou 2 fois la taille de la mémoire vive)</li> <li>• /tmp : 2 Go</li> <li>• /home : 2 Go</li> <li>• /var : le reste du disque dur</li> </ul>	Cliquez sur « Supprimer toutes les partitions ». Cliquez ensuite à l'intérieur de la zone grise du disque (sda) pour créer chaque nouvelle partition.  <b>Info :</b> 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).
	À la fin de cette opération, et en fonction de la taille de votre disque dur, le partitionnement devrait ressembler à cela : 	- Créez la partition racine (/). Choisissez sa taille (2 Go) ainsi que son système de fichier (ext4). Recommencez cette étape pour toutes les autres partitions. - Une fois le partitionnement effectué, cliquez sur « Terminer ».
	Pour ALCASAR, l'installation ne nécessite pas d'autre média.	Sélectionnez « Aucun »

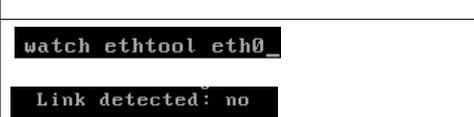
Messages affichés à l'écran	Commentaires	Actions à réaliser
	<p>Choix des groupes de paquetages à installer : « ALCASAR » ne nécessite qu'une installation minimale du système Linux-Mandriva.</p>	<p>Choisissez uniquement le groupe de paquetages « LSB » (Linux Standard Base). Désélectionnez <b>tous</b> les autres groupes puis cliquez sur « Suivant ». La copie des paquetages sur le disque dur est alors lancée. Durée estimée : 4'</p> <p><b>Info :</b> 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-ethernet » 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><b>Info :</b> Aucun test n'a encore été effectué sur ALCASAR concernant les accès à Internet par d'autres types 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><b>Info :</b> si les interfaces ne sont pas identifiées (eth0, eth1, etc.), sélectionnez la première interface.</p>
		<p>Sélectionnez « configuration manuelle ».</p> <p><b>Info :</b> 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>
	<p>Exemple :</p> <ul style="list-style-type: none"> <li>• Adresse IP : cette adresse doit être dans le même sous-réseau que l'adresse du routeur DSL du FAI (box).</li> <li>• Masque : 255.255.255.0</li> <li>• Passerelle : c'est l'adresse de la box (en général 192.168.1.1 pour une « livebox » et 192.168.0.254 pour une « freebox »)</li> <li>• DNS 1 et DNS 2 :*</li> <li>• « nom d'hôte » : laissez ce champ vide</li> </ul>	<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 DNS du projet « OpenDNS » (DNS1=208.67.222.222, DNS2=208.67.220.220) ou les serveurs DNS publics de google (DNS1=8.8.8.8, DNS2=8.8.4.4).</p>

Messages affichés à l'écran	Commentaires	Actions à réaliser
		Sélectionnez uniquement « Lancer la connexion au démarrage ».
	Il n'est pas nécessaire de lancer cette connexion à ce stade	Sélectionnez « Non »
		Cliquez sur « Terminer ».
		Cliquez sur « Suivant ».
	Les mises à jour de sécurité seront gérées pendant l'installation d'ALCASAR.	Sélectionnez « Non » et cliquez sur « Suivant ».
	L'installation est terminée	Cliquez sur « Redémarrage ». Retirez le CDROM ou la clé USB. Reconfigurez le BIOS afin : <ul style="list-style-type: none"> <li>de limiter les possibilités d'amorçage au seul disque dur ;</li> <li>d'en verrouiller l'accès par mot de passe.</li> </ul>

### 2.3. Installation d'ALCASAR

ALCASAR est constitué d'une archive compressée (alcasar-x.y.tar.gz) et de paquetages additionnels qui seront automatiquement téléchargés sur Internet.

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
		Connectez-vous en tant que « root ».
	- Déconnectez les câbles des deux cartes réseau et affichez l'état de la première carte (eth0).	<code>watch ethtool eth0</code> <i>Info : la dernière ligne affichée présente l'état du lien sur la carte (Link detected &lt;yes/no&gt;)</i>

Messages affichés à l'écran	Commentaires	Actions à réaliser
<pre>Link detected: yes</pre>	- connectez le câble allant à l'équipement du FAI sur la première carte.	Attendez quelques secondes que le lien soit monté. Dans le cas contraire, connectez le câble sur l'autre carte. Dès que le lien est monté, stoppez la commande à l'aide de la séquence de touches : <b>&lt;Ctrl&gt; + c</b>
<pre>[root@localhost ~]# fdisk -l</pre> Disque /dev/sda: 80 0 Go, 80032038912 octets 255 heads, 63 sectors/track, 9730 cylinders Units = cylinders of 16065 * 512 = 8225280 bytes Disk identifier: 0x35a6c3f6  Périphérique Amorçé Début Fin Blocs Id Système /dev/sda1 1 1275 10241406 7 HPFS/NTFS /dev/sda2 1276 6630 49314037+ f W95 Etendu (LBA) /dev/sda3 1276 2530 10241406 7 HPFS/NTFS /dev/sda6 2551 3832 10297633+ 83 Linux /dev/sda7 3833 4081 2080061 82 Linux swap / Solaris /dev/sda8 4082 6630 20474612 83 Linux  Disque /dev/sdb: 1031 Mo, 1031798784 octets 16 heads, 32 sectors/track, 3936 cylinders Units = cylinders of 512 * 512 = 262144 bytes Disk identifier: 0xcd1d7d24  Périphérique Amorçé Début Fin Blocs Id Système /dev/sdb1 1 3936 1007600 0 W95 FAT16 (LBA) [root@localhost ~]#	- Effectuez la même opération avec la deuxième carte (eth1) et le câble provenant du réseau de consultation.  - 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.	<b>watch ethtool eth1</b> Info : côté réseau de consultation, connectez un équipement actif de réseau (commutateur Ethernet, CPL, AP WIFI, etc.) afin d'être assuré de la permanence du lien même si les stations sont éteintes.  <b>fdisk -l</b>  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 avant d'insérer la clé pour récupérer ce nom (tailf /var/log/messages)
<pre>[root@localhost ~]# mkdir /media/usb</pre> <pre>[root@localhost ~]# mount /dev/sdb1 /media/usb/</pre> <pre>[root@localhost ~]# cp /media/usb/alcasar-* .</pre> <pre>[root@localhost ~]# umount /media/usb/</pre> <pre>[root@localhost ~]# md5sum alcasar-2.5.tar.gz</pre> 311f0884be511e8205d22e04d0d1528d alcasar-2.5.tar.gz  	- Créez un répertoire permettant d'accueillir la clé USB. - « Montez » le périphérique représentant la clé USB sur ce répertoire. - Copiez l'archive d'ALCASAR dans le répertoire /root. - Démontez la clé USB. - Retirez-la. - Calculez l'empreinte numérique 'MD5' de cette archive et comparez-la avec celle du site WEB.	<b>mkdir -p /media/usb</b> <b>mount /dev/sdb1 /media/usb/</b> <b>cp /media/usb/alcasar-* /root/</b> <b>umount /media/usb</b> <b>md5sum alcasar-x.y.tar.gz</b>  Info : remplacez « sdb1 » par le nom du périphérique récupéré à l'étape précédente (sdc1, hda1, etc.).  Info2 : si l'empreinte numérique ne correspond pas, téléchargez à nouveau l'archive sur le site WEB. En cas de nouveau problème, prévenez l'équipe de développement via le forum.
<pre>[root@localhost ~]# tar -zxvf alcasar-1.5RC4.tar.gz</pre>  <pre>[root@localhost ~]# cd alcasar-1.8a</pre> <pre>[root@localhost alcasar-1.8a]# sh alcasar.sh -i</pre>	- Décompressez et extrayez cette archive. - Positionnez-vous dans le répertoire d'ALCASAR et lancez le script d'installation.	<b>tar -zxvf alcasar-x.y.tar.gz</b> <b>cd alcasar-x.y</b> <b>sh alcasar.sh -i</b>
<pre>ALCASAR UZ.2 Installation</pre> Application Libre pour le Contrôle d'accès Sécurisé et Authentifié au Réseau Tests des paramètres réseau : ....	- 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 de php-ctype-5.1.6-1.mdu2007.0.i586.rpm</pre> Préparation ... 75/100: php-ctype  Installation de php-ftp-5.1.6-1.mdu2007.0.i586.rpm Préparation ... Warning: php-ftp-5.1.6-1.mdu2007.0: Header 03 USR signature: NOKEY, key ID 2245639B 76/100: php-ftp  Installation de php-gettext-5.1.6-1.mdu2007.0.i586.rpm Préparation ...	L'installation d'une centaine de logiciels (paquetages) est effectuée à partir d'Internet. Durée : 2'	
<pre>ALCASAR UZ.2 Installation</pre> Application Libre pour le Contrôle d'accès Sécurisé et Authentifié au Réseau Entrez le nom de votre organisme :	- 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>ALCASAR UZ.2 Installation</pre> Application Libre pour le Contrôle d'accès Sécurisé et Authentifié au Réseau Par défaut, l'adresse IP d'ALCASAR sur le réseau de consultation est : 192.168.102.1/24 Voulez-vous utiliser cette adresse et ce plan d'adressage (recommandé) (O/n)? :	Vous pouvez changer l'adresse IP d'ALCASAR et le plan d'adressage par défaut du réseau de consultation	Tapez « O » ou « N »  Info : si vous tapez « n », le script vous demandera l'adresse IP d'ALCASAR et le masque de réseau au format CIDR (ex : 172.16.0.1/16).
<pre>ALCASAR UZ.2 Installation</pre> Application Libre pour le Contrôle d'accès Sécurisé et Authentifié au Réseau Définissez un premier compte d'administration du portail : Nom : _	- Entrez l'identifiant et le mot de passe d'un premier compte d'administration d'ALCASAR.	Info : Ce compte sert à administrer ALCASAR au moyen de l'interface graphique située à l'URL http://alcasar. Ce n'est pas un compte usager permettant de se connecter à Internet.

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 (« <a href="http://alcasar">http://alcasar</a> »). Lisez attentivement la documentation d'exploitation (« <a href="#">alcasar-exploitation.pdf</a> »).</p>

### 3. Désinstallation, réinstallation et mise à jour d'ALCASAR

Vous pouvez désinstaller le portail avec la commande « `sh alcasar.sh --uninstall` ». Vous vous retrouvez alors comme si vous veniez d'installer uniquement le système d'exploitation.

Vous pouvez réinstaller ou mettre à jour le ALCASAR avec la même commande que précédemment (« `sh alcasar.sh --install` »). Le script vous demandera si vous voulez garder les paramètres de la version déjà en place.

### 4. Préparer une installation « hors ligne »

La procédure suivante permet d'installer ALCASAR en mode « hors ligne ». Cela peut être utile quand on prévoit d'installer des machines ALCASAR dans une zone où l'accès Internet n'est pas encore disponible (clin d'oeil MINDEF/BTAC) ou que cet accès sera de débit très faible (clin d'oeil MINDEF/OPEX). Dans ce cas, il faut pouvoir générer à l'avance un fichier archive contenant la totalité des paquetages (RPMS). Ce fichier sera exploité en lieu et place du téléchargement Internet. La procédure est la suivante :

- préparation de l'archive des RPM : sur une machine vierge connectée à Internet, installez le système Linux Mandriva comme indiqué au §2.2 puis récupérez et décompressez l'archive d'ALCASAR. Déplacez-vous dans le répertoire des scripts « `cd alcasar-x.y/scripts/sbin` » et lancez le script « `./alcasar-rpm-download.sh` ». Ce script va générer l'archive des RPM correspondant à l'architecture de la machine (32 ou 64 bits). Récupérez cette archive sur clé USB.
- Installation hors ligne : après avoir installé le système, récupérez votre archive de RPM. Décompressez-la et positionnez-vous dedans. Installez la totalité des RPM (`urpmi --no-verify-rpm *`). Procédez ensuite à l'installation d'ALCASAR comme indiqué au §2.3.

### 5. Fiche récapitulative des paramètres d'ALCASAR

Le fichier « `/root/ALCASAR-passwords.txt` » contient les mots de passe exploités en interne par les différents modules d'ALCASAR. Il contient notamment le mot de passe de protection du chargeur système (bootloader « GRUB »). Il peut être consulté via la commande (`cat /root/ALCASAR-passwords.txt`).

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 ; - l'installation du certificat de l'Autorité de Certification (A.C.) dans les navigateurs.	<a href="http://alcasar">http://alcasar</a>  Info : les possibilités du centre de gestion sont décrites dans le document « <a href="#">alcasar-exploitation</a> ».
Comptes Linux	root                    mot de passe : ..... sysadmin                mot de passe : .....
1er compte d'administration graphique d'ALCASAR	..... mot de passe : .....
<u>Paramètres réseau</u> • @IP de l'équipement FAI (routeur) • @IP des serveurs DNS • @IP d'ALCASAR (côté WAN/Internet) : • @IP d'ALCASAR (côté réseau de consultation) :	• _____ • DNS1 : _____ DNS2 : _____ • _____/_____ • _____/_____