

Serveur

Le serveur dans Edubuntu joue un rôle central dans la gestion et la distribution des ressources éducatives. Il fournit un espace de stockage centralisé pour les données et les applications, permettant un déploiement efficace des logiciels éducatifs sur les postes de travail des élèves. Le serveur facilite également la gestion des utilisateurs, des autorisations et des politiques de sécurité, assurant ainsi un environnement d'apprentissage sécurisé et collaboratif. En outre, il peut offrir des services de gestion de réseau, de filtrage Internet et de sauvegarde, garantissant un fonctionnement fluide du système et une disponibilité constante des ressources pédagogiques.

- [Bases](#)
- [LTSP](#)
- [ltsp.conf](#)
- [DHCP](#)
- [LDAP](#)
- [LDAP Account Manager](#)
- [Samba](#)
- [Epoptes](#)
- [Veeam](#)
- [Autre](#)

Bases



Présentation

Ubuntu est l'une des distributions Linux les plus populaires et largement utilisées. Fondée en 2004 par Canonical Ltd., Ubuntu est basée sur Debian, une autre distribution Linux bien établie. Voici une présentation rapide de ses caractéristiques :

1. **Facilité d'utilisation** : Ubuntu est réputée pour sa convivialité et son interface utilisateur intuitive. Elle est conçue pour être accessible aux débutants en informatique tout en offrant suffisamment de puissance et de fonctionnalités pour les utilisateurs avancés.
2. **Cycle de publication régulier** : Ubuntu suit un calendrier de publication régulier, avec des versions majeures tous les six mois. Ces versions sont nommées d'après l'année et le mois de leur sortie, par exemple, Ubuntu 20.04 (sortie en avril 2020). Les versions LTS (Long Term Support) sont publiées tous les deux ans et bénéficient d'une prise en charge prolongée, ce qui les rend idéales pour les déploiements à long terme.
3. **Grande communauté et support** : Ubuntu bénéficie d'une communauté active et dynamique d'utilisateurs, de développeurs et de contributeurs. Cette communauté offre un support technique, des forums d'aide, des wikis et des ressources en ligne variées pour aider les utilisateurs à résoudre les problèmes et à tirer le meilleur parti de leur système Ubuntu.
4. **Logiciel libre et open source** : Ubuntu est entièrement basée sur des logiciels libres et open source, ce qui signifie que son code source est disponible pour examen, modification

et redistribution par quiconque le souhaite. Cela garantit également que Ubuntu est exempt de coûts de licence et offre une transparence quant à son fonctionnement interne.

5. **Écosystème logiciel vaste** : Ubuntu offre un vaste écosystème logiciel, avec des milliers d'applications disponibles dans ses référentiels logiciels officiels. De plus, grâce à sa compatibilité avec les paquets Debian, il est possible d'accéder à encore plus de logiciels via d'autres sources.
6. **Prise en charge de matériel étendue** : Ubuntu est compatible avec une large gamme de matériel, ce qui en fait un choix polyvalent pour les ordinateurs de bureau, les serveurs, les ordinateurs portables et même les appareils embarqués.

En résumé, Ubuntu offre une combinaison de convivialité, de stabilité, de sécurité et de liberté, ce qui en fait un choix populaire pour les utilisateurs individuels, les entreprises et les organisations du monde entier.

Site Officiel [Ubuntu](#).

Voici un résumé étape par étape de l'installation de LTSP (Linux Terminal Server Project), la configuration et la création d'un client léger :

1. **Installation de LTSP** :
 - Assurez-vous d'avoir une distribution Linux prise en charge par LTSP, comme Ubuntu, Debian ou Fedora.
 - Installez le paquet LTSP-server sur votre serveur en utilisant le gestionnaire de paquets de votre distribution.
2. **Configuration de LTSP** :
 - Configurez le serveur LTSP en modifiant le fichier de configuration principal, généralement situé dans `/etc/ltsp/ltsp.conf`.
 - Configurez les options réseau telles que l'adresse IP, le masque de sous-réseau et la passerelle par défaut pour le réseau LTSP.
 - Déterminez quels paquets logiciels vous souhaitez inclure dans l'image du client léger et configurez-les en conséquence.
3. **Création de l'image du client léger** :
 - Utilisez la commande `debootstrap` pour créer une image du client léger. Cette commande télécharge et installe les paquets requis dans un environnement `chroot` et configure l'image du client léger.
 - Assurez-vous que votre serveur dispose des ressources nécessaires pour construire l'image du client léger, car cela peut prendre du temps et nécessiter de l'espace disque.
4. **Configuration du démarrage réseau (PXE)** :
 - Configurez le démarrage réseau (PXE) sur les clients légers pour qu'ils puissent démarrer à partir du réseau.
 - Assurez-vous que le BIOS des clients légers est configuré pour démarrer à partir du réseau en premier.

5. Démarrage et connexion des clients légers :

- Démarrez les clients légers et assurez-vous qu'ils se connectent au serveur LTSP via le démarrage réseau (PXE).
- Les clients légers devraient démarrer en utilisant l'image du client léger que vous avez créée et se connecter au serveur LTSP, offrant un environnement de bureau Linux complet.

En suivant ces étapes, vous pouvez installer et configurer avec succès LTSP sur votre serveur Linux, créer une image du client léger et connecter des clients légers pour accéder à des sessions de bureau Linux à partir du serveur.

LTSP



Présentation

LTSP, acronyme de Linux Terminal Server Project, est une solution open source permettant de déployer des clients légers dans un réseau informatique. Voici une présentation de ses principales caractéristiques :

1. **Infrastructure de client léger** : LTSP permet de transformer des ordinateurs peu puissants, appelés clients légers, en terminaux légers qui se connectent à un serveur central pour accéder à un environnement de bureau complet.
2. **Centralisation des ressources** : Avec LTSP, la plupart des ressources de calcul et de stockage sont centralisées sur le serveur, ce qui signifie que les clients légers n'ont besoin que d'une configuration matérielle minimale pour fonctionner. Cela simplifie la maintenance, réduit les coûts et facilite la gestion du parc informatique.
3. **Économique et éco-énergétique** : Les clients légers consomment moins d'énergie et nécessitent moins de maintenance que les ordinateurs traditionnels, ce qui en fait une solution économique et respectueuse de l'environnement pour les environnements informatiques à grande échelle.
4. **Compatibilité multiplateforme** : LTSP est compatible avec une variété de systèmes d'exploitation clients, y compris Linux, Windows, et d'autres systèmes d'exploitation basés sur le protocole de démarrage réseau PXE (Preboot Execution Environment).
5. **Administration centralisée** : LTSP permet une administration centralisée des clients légers à partir du serveur, ce qui facilite la configuration, la surveillance, la gestion des utilisateurs et la distribution de logiciels.
6. **Personnalisation et extensibilité** : LTSP offre des fonctionnalités de personnalisation et d'extensibilité, permettant aux administrateurs de configurer les clients légers selon les besoins spécifiques de leur environnement informatique, en installant des logiciels supplémentaires, en définissant des paramètres système personnalisés, etc.
7. **Utilisation dans l'éducation et les entreprises** : LTSP est largement utilisé dans les écoles, les bibliothèques, les entreprises et d'autres organisations qui ont besoin de déployer et de gérer un grand nombre de postes de travail informatiques de manière efficace et économique.

En résumé, LTSP est une solution puissante et économique pour déployer des clients légers dans un environnement informatique, offrant une centralisation des ressources, une administration simplifiée, une compatibilité multiplateforme et une personnalisation flexible.

Site officiel de [LTSP](#).

Configuration minimale

- Processeur : i3
- RAM : 8Go
- Disque : 500Go
- 2 cartes réseau

Installation de LTSP

Dans un premier temps, il faut ajouter les sources LTSP au système :

```
add-apt-repository ppa:ltsp
apt update
```

Une fois cela fait, on peut installer LTSP à proprement parlé :

```
apt install --install-recommends ltsp ltsp-binaries dnsmasq nfs-kernel-server openssh-server
squashfs-tools ethtool net-tools epoptes
```

Epoptes est un logiciel de management et monitoring d'ordinateur, il va nous permettre de voir et prendre la main sur les ordinateurs Edubuntu par la suite.

Pour autoriser le compte du serveur à utiliser epoptes (outil de prise de supervision et controle des clients), il faut l'ajouter au groupe epoptes (ICI le compte est "administrateur") :

```
gpasswd -a administrateur epoptes
```

Création des fichiers de configuration

Une des choses importante est de totalement initialiser LTSP, via ces quelques commandes, qui vont être souvent utilisées pour certaines :

Pour créer le fichier de configuration ltsp.conf :

```
install -m 0660 -g sudo /usr/share/ltsp/common/ltsp/ltsp.conf /etc/ltsp/ltsp.conf
```

Actualiser et faire la prise en compte de la configuration ltsp.conf :

```
ltsp initrd
```

Mettre à jour la configuration IPXE :

```
ltsp ipxe
```

Mettre à jour la configuration NFS :

```
ltsp nfs
```

Actualiser l'image client :

```
ltsp image <nom de l'image>
```

Cette commande remplace la précédemment connue :

```
ltsp-update-image <nom de l'image>
```

ltsp.conf



Présentation

ltsp.conf est un fichier de configuration utilisé par LTSP (Linux Terminal Server Project) pour définir différents paramètres de configuration du serveur LTSP. Ce fichier est généralement situé dans le répertoire `/etc/ltsp/` sur le serveur LTSP. Voici une présentation générale de son contenu et de ses fonctionnalités :

1. Définition des options de démarrage :

- Le fichier ltsp.conf permet de définir les options de démarrage des clients légers. Cela inclut des paramètres tels que l'adresse IP du serveur LTSP, le chemin du noyau Linux à utiliser pour le démarrage, les options de montage NFS pour le système de fichiers racine, etc.

2. Configuration des options réseau :

- Il permet également de configurer les paramètres réseau des clients légers, tels que l'adresse IP du serveur DHCP, le masque de sous-réseau, la passerelle par défaut, les serveurs DNS, etc.

3. Personnalisation de l'environnement utilisateur :

- Le fichier ltsp.conf peut être utilisé pour personnaliser l'environnement utilisateur sur les clients légers. Cela inclut des paramètres tels que la langue par défaut, la disposition du clavier, la résolution d'écran par défaut, les options de bureau, etc.

4. Gestion des périphériques :

- Il offre la possibilité de configurer le support des périphériques sur les clients légers, tels que les imprimantes réseau, les clés USB, les lecteurs de cartes, etc. Cela permet de contrôler quels périphériques sont accessibles aux utilisateurs sur les clients légers.

5. Options de sécurité :

- Le fichier ltsp.conf peut également contenir des options de sécurité pour restreindre l'accès aux clients légers ou limiter les fonctionnalités disponibles aux utilisateurs. Cela peut inclure des configurations de pare-feu, des restrictions d'accès réseau, des politiques d'authentification, etc.

6. Commentaires et documentation :

- En plus des paramètres de configuration, le fichier `ltsp.conf` peut contenir des commentaires et de la documentation pour expliquer l'utilisation des différents paramètres et fournir des exemples de configuration.

En résumé, le fichier `ltsp.conf` est un élément clé de la configuration du serveur LTSP, permettant de définir divers paramètres de démarrage, de réseau, d'environnement utilisateur, de périphériques et de sécurité pour les clients légers. Sa personnalisation permet d'adapter le fonctionnement du serveur LTSP aux besoins spécifiques de chaque déploiement.

Ensemble des infos sur le fichier [*ltsp.conf*](#).

Création du fichier

Pour créer et initialiser le fichier, lancez la commande suivante :

```
install -m 0660 -g sudo /usr/share/ltsp/common/ltsp/ltsp.conf /etc/ltsp/ltsp.conf
```

Fichier modèle pour Edubuntu

La ligne 23 définit la convention de nommage des postes clients, il est donc important de définir une norme pour différencier les postes des différentes écoles, surtout si un agent d'inventaire est installé.

```
# /bin/sh -n
# LTSP configuration file
# Documentation=man:ltsp.conf(5)

# The special [server] section is evaluated only by the ltsp server
[server]
NAT=1
NFS_HOME=1
MENU_TIMEOUT="1"

[common]
TFTP_DIR=/srv/tftp

[clients]
```

```
FSTAB_HOME="server:/home /home nfs defaults,nolock 0 0"
```

```
CUPS_SERVER=192.168.1.1
```

```
LIGHTDM_CONF="greeter-hide-users=true"
```

```
CRONTAB_x="00 20 * * * root poweroff" # Extinction lancée à 20h sur tous les postes
```

```
LOCAL_SWAP=1
```

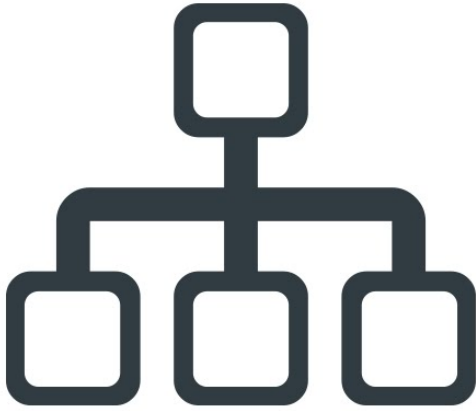
```
HOSTNAME="EDU-ECOLE-%{IP}"#Nom qui sera affiché sur l'écran, dans Eoptes, et dans  
l'inventaire.
```

Service d'impression

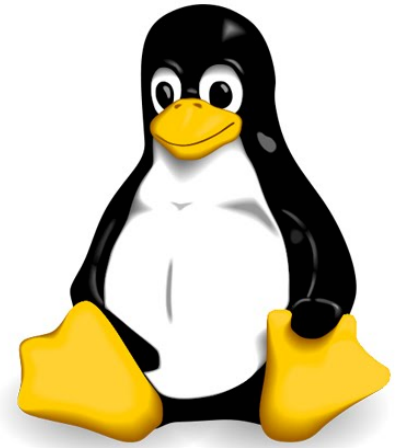
"CUPS_SERVER" permet de définir le serveur CUPS qui sera configuré dans les clients LTSP. Cependant, il faut activer le partage des copieurs depuis le serveur :

```
cupscpl _share_printers=1
```

DHCP



DHCP
SERVER



Présentation

Le paquet ISC-DHCP-Server est une implémentation open source du protocole DHCP (Dynamic Host Configuration Protocol) développée par Internet Systems Consortium (ISC). Voici une présentation de ses caractéristiques principales :

1. **Attribution dynamique des adresses IP** : ISC-DHCP-Server permet d'attribuer dynamiquement des adresses IP aux clients du réseau. Cela signifie que les périphériques connectés au réseau peuvent obtenir automatiquement une adresse IP ainsi que d'autres informations de configuration réseau, comme la passerelle par défaut et les serveurs DNS.
2. **Gestion des baux DHCP** : Le serveur DHCP maintient une table de baux DHCP, qui répertorie les adresses IP attribuées aux clients ainsi que leur durée de validité. Cette table est utilisée pour gérer efficacement l'allocation des adresses IP et éviter les conflits d'adresses.
3. **Prise en charge des options de configuration avancées** : ISC-DHCP-Server prend en charge un large éventail d'options de configuration DHCP, telles que la configuration des serveurs DNS, des serveurs NTP (Network Time Protocol), des serveurs de fichiers, des options de boot PXE (Preboot Execution Environment), etc. Cela permet de fournir aux clients du réseau des informations de configuration supplémentaires selon leurs besoins.

4. **Contrôle d'accès** : Le serveur DHCP permet de définir des règles de contrôle d'accès basées sur des critères tels que les adresses MAC des clients ou les plages d'adresses IP disponibles. Cela permet de restreindre l'accès au réseau aux seuls périphériques autorisés.
5. **Compatibilité avec IPv6** : ISC-DHCP-Server prend en charge à la fois IPv4 et IPv6, ce qui permet de gérer l'attribution des adresses IP dans les environnements réseau prenant en charge les deux protocoles.
6. **Sécurité** : Le paquet ISC-DHCP-Server intègre des fonctionnalités de sécurité telles que l'authentification des clients DHCP pour garantir l'intégrité du processus d'attribution des adresses IP et prévenir les attaques de type "rogue DHCP".

En résumé, ISC-DHCP-Server est un paquet logiciel puissant et flexible pour la gestion des adresses IP dans un réseau informatique, offrant des fonctionnalités avancées de configuration, de contrôle d'accès et de sécurité. Il est largement utilisé dans les environnements réseau pour simplifier et automatiser la configuration des périphériques connectés.

Site officiel de [ISC](#).

Installation du DHCP

Installation du service dhcp :

```
apt install isc-dhcp-server
```

Il faut indiquer au serveur via quelle carte réseau il faut diffuser le DHCP.

Pour se faire on modifie le fichier suivant :

```
nano /etc/default/isc-dhcp-server
```

Comme ceci :

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid
```

```
# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4=""
INTERFACESv6=""
```

```
INTERFACESv4="<nom de l'interface>"
```

Le nom de l'interface est ce qui apparait dans la réponse à la commande :

```
ip a
```

Ajout de la configuration de la plage IP :

```
nano /etc/dhcp/dhcpd.conf
```

```
authoritative;
# option domain-name "e-ecole.org";
option domain-name-servers 192.168.1.1, 1.1.1.1;
option space ipxe;
option ipxe-encap-opts code 175 = encapsulate ipxe;
option ipxe.menu code 39 = unsigned integer 8;
option ipxe.no-pxedhcp code 176 = unsigned integer 8;
option arch code 93 = unsigned integer 16;

# This is the LTSP subnet declaration
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.20 192.168.1.120;
    option ipxe.no-pxedhcp 1;
    option routers 192.168.1.1;
    # On single-NIC setups, usually routers != next-server (=TFTP server)
    # option next-server 192.168.1.1
    if exists ipxe.menu {
        filename "ltsp/ltsp.ipxe";
    } elsif option arch = 00:00 {
        filename "ltsp/undionly.kpxe";
    } elsif option arch = 00:07 {
```

```
filename "ltsp/snponly.efi";
} elsif option arch = 00:09 {
filename "ltsp/snponly.efi";
} else {
filename "ltsp/unmatched-client";
}
}
```

Cependant, pour que le DHCP fonctionne avec LTSP, il faut d'abord taper quelques commande supplémentaires.

En effet, le service DHCP de LTSP (dnsmasq) n'est pas très performant, sauf sur un point, il support le protocole dhcp proxy, utilise si vous avez plusieurs serveurs LTSP sur un même réseau.

Dans le cas contraire, ISC-DHCP-SERVER est mieux indiqué. Il faut alors indiqué à LTSP que le service DHCP c'est pas dnsmasq, mais ISC, via ces commandes :

```
ltsp dnsmasq --proxy-dhcp=0 --real-dhcp=0
systemctl restart isc-dhcp-server
```

Vérifier que le serveur DHCP est démarré et opérationnel

LDAP



Présentation

OpenLDAP est une implémentation open source du protocole LDAP (Lightweight Directory Access Protocol), un protocole standard utilisé pour accéder et gérer des annuaires d'informations. Voici une présentation de ses caractéristiques principales :

1. **Service d'annuaire** : OpenLDAP fournit un service d'annuaire, qui est une base de données hiérarchique utilisée pour stocker des informations sur les utilisateurs, les groupes, les ressources réseau et d'autres entités dans un réseau informatique.
2. **Protocole LDAP** : OpenLDAP implémente le protocole LDAP, qui permet aux applications et aux clients d'accéder et de manipuler les données stockées dans l'annuaire. LDAP est largement utilisé dans les environnements informatiques pour l'authentification, l'autorisation, la recherche d'informations et d'autres opérations liées à la gestion des identités.
3. **Open Source et Gratuit** : OpenLDAP est distribué sous une licence open source (généralement la licence OpenLDAP Public License) et est gratuit à utiliser et à distribuer. Cela permet aux organisations de déployer des services d'annuaire sans frais de licence.
4. **Sécurité** : OpenLDAP prend en charge divers mécanismes de sécurité pour protéger les données stockées dans l'annuaire, y compris l'authentification des clients, le chiffrement des communications et le contrôle d'accès basé sur des politiques.
5. **Extensibilité** : OpenLDAP est hautement extensible, ce qui signifie qu'il peut être étendu pour prendre en charge de nouveaux schémas de données, des mécanismes d'authentification personnalisés et d'autres fonctionnalités spécifiques aux besoins de l'organisation.
6. **Interopérabilité** : OpenLDAP est compatible avec d'autres implémentations LDAP et peut interagir avec une large gamme d'applications et de services qui prennent en charge le protocole LDAP. Cela permet d'intégrer facilement OpenLDAP dans des environnements informatiques existants.

7. **Administration et Gestion** : OpenLDAP est livré avec des outils d'administration et de gestion qui facilitent la configuration, la surveillance et la maintenance de l'annuaire LDAP.

En résumé, OpenLDAP est une solution puissante et flexible pour la gestion des identités et des ressources dans un réseau informatique. En tant que service d'annuaire open source, il offre une alternative économique et évolutive aux solutions d'annuaire propriétaires.

Installation

Dans le terminal, en superuser :

```
aptitude install slapd ldap-utils
```

Choisir un mot de passe pour l'admin ldap

Ensuite, on va devoir définir le domaine, dans le fichier :

```
nano /etc/ldap/ldap.conf
```

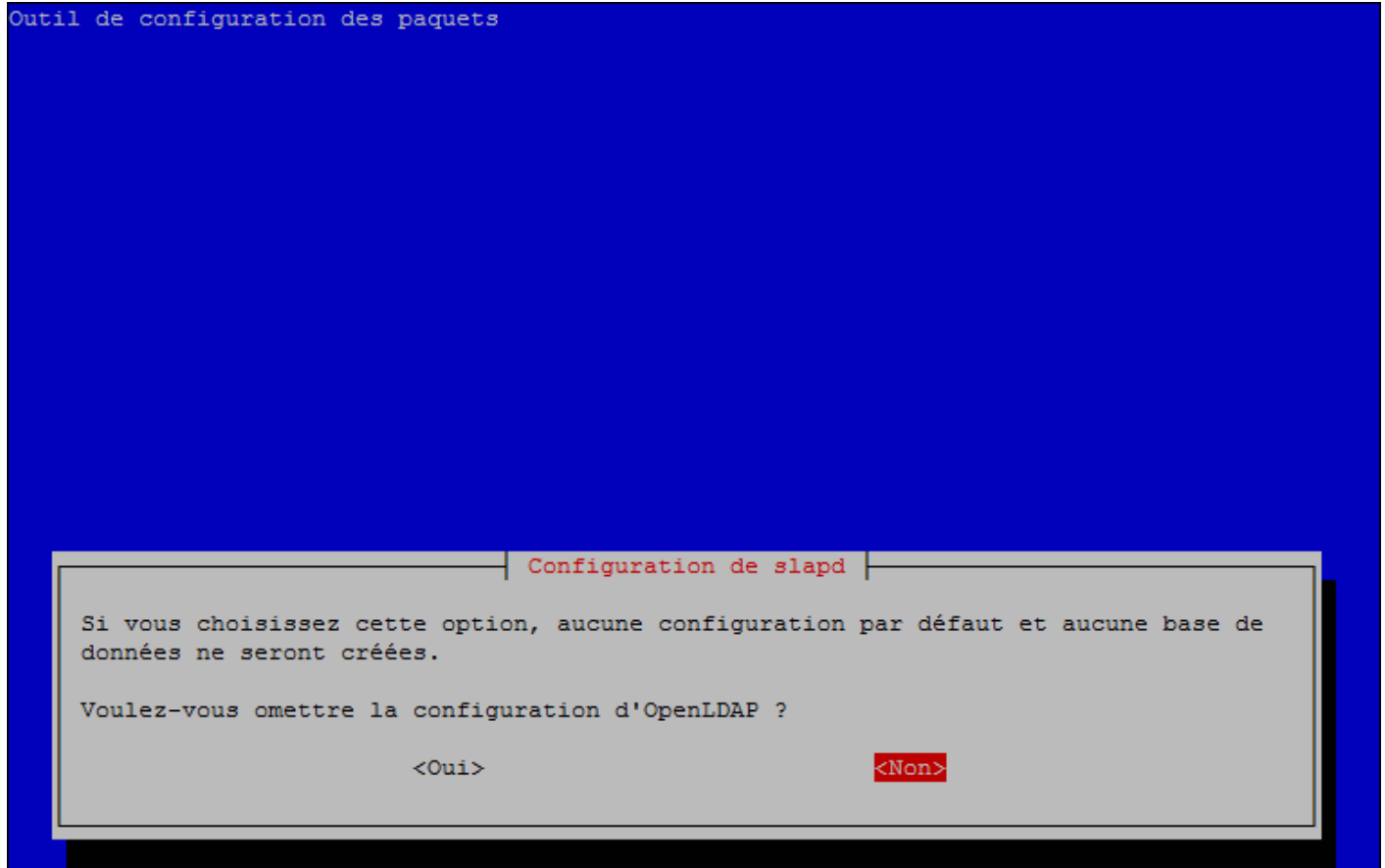
```
#  
# LDAP Defaults  
#  
  
# See ldap.conf(5) for details  
# This file should be world readable but not world writable.  
  
BASE    dc=e-ecole,dc=org  
URI     ldap://192.168.1.1  
  
#SIZELIMIT    12  
#TIMELIMIT    15  
#DEREF        never  
  
# TLS certificates (needed for GnuTLS)  
TLS_CACERT    /etc/ssl/certs/ca-certificates.crt
```

Les deux lignes `BASE` et `URI` sont à décommenter et à remplir comme l'exemple ci-dessus, avec le nom de domaine et l'ip serveur.

On va pouvoir à présent configurer le paquet slapd installé plus tôt :

```
dpkg-reconfigure slapd
```

Lors de la première question "Voulez-vous omettre la configuration [...]", il faut répondre non, auquel cas, la configuration se ferme.



Saisissez votre nom de domaine, dans notre exemple : e-ecole.org, deux fois

Configuration de slapd

Le nom de domaine DNS est utilisé pour établir le nom distinctif de base (« base DN » ou « Distinguished Name ») de l'annuaire LDAP. Par exemple, si vous indiquez « toto.example.org » ici, le nom distinctif de base sera « dc=toto, dc=example, dc=org ».

Nom de domaine :

e-ecole.org

<Ok>

Définissez le nouveau mot de passe de l'administrateur LDAP

Outil de configuration des paquets

Configuration de slapd

Veillez indiquer le mot de passe de l'administrateur de l'annuaire LDAP.

Mot de passe de l'administrateur :

<Ok>

Choisissez de ne pas supprimer la BDD

Outil de configuration des paquets

Configuration de slapd

Faut-il supprimer la base de données lors de la purge du paquet ?

<Oui> <Non>

Choisissez de déplacer l'ancienne base

Outil de configuration des paquets

Configuration de slapd

Des fichiers présents dans /var/lib/ldap vont probablement provoquer l'échec de la procédure de configuration. Si vous choisissez cette option, les scripts de configuration déplaceront les anciens fichiers des bases de données avant de créer une nouvelle base de données.

Faut-il déplacer l'ancienne base de données ?

<Oui>

<Non>

De retour dans le terminal :

```
service slapd restart
```

```
ldapsearch -x
```

Vous devriez avoir un retour similaire à cela :

```
# extended LDIF
#
# LDAPv3
# base <dc=e-ecole,dc=org> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# e-ecole.org
dn: dc=e-ecole,dc=org
objectClass: top
objectClass: dcObject
objectClass: organization
```

```
o: e-ecole.org
dc: e-ecole

# admin, e-ecole.org
dn: cn=admin,dc=e-ecole,dc=org
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

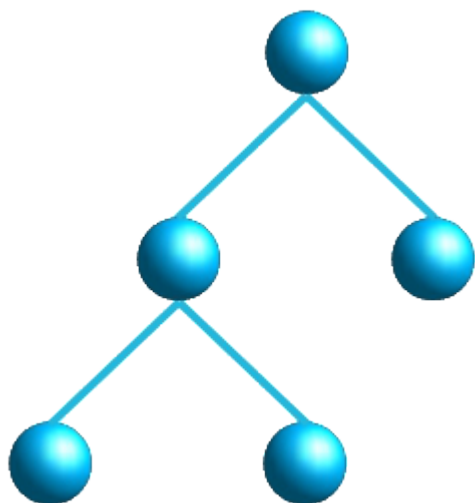
# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

Le LDAP est maintenant configuré !

Il est possible que le compte admin soit invisible sur le résultat, mais qu'il ai été créé malgré tout !

LDAP Account Manager



Présentation

LDAP Account Manager (LAM) est une application web open source qui offre une interface conviviale pour gérer les comptes utilisateurs stockés dans un annuaire LDAP (Lightweight Directory Access Protocol). Il permet aux administrateurs système de gérer facilement les utilisateurs, les groupes, les unités organisationnelles et d'autres objets LDAP à travers une interface web intuitive. Les fonctionnalités typiques de LDAP Account Manager incluent la création, la modification et la suppression des comptes utilisateur, la gestion des mots de passe, la gestion des groupes, la gestion des attributs LDAP, la recherche avancée, ainsi que des fonctionnalités de gestion des droits d'accès et de contrôle des accès. LDAP Account Manager est souvent utilisé dans les environnements où LDAP est utilisé comme service d'annuaire central pour l'authentification et l'autorisation des utilisateurs sur le réseau.

Site officiel [LDAP Account Manager](#).

Installation

Phpldapadmin n'étant compatible qu'avec PHP7.3 maximum, afin de continuer d'évoluer avec les nouveaux OS existant et à venir, le choix à été fait d'utiliser LAM, compatible avec PHP8.

L'installation est simple et se fait via une seule commande :

```
apt install ldap-account-manager
```

Cela va automatiquement installer les dépendances tel que apache ou php.

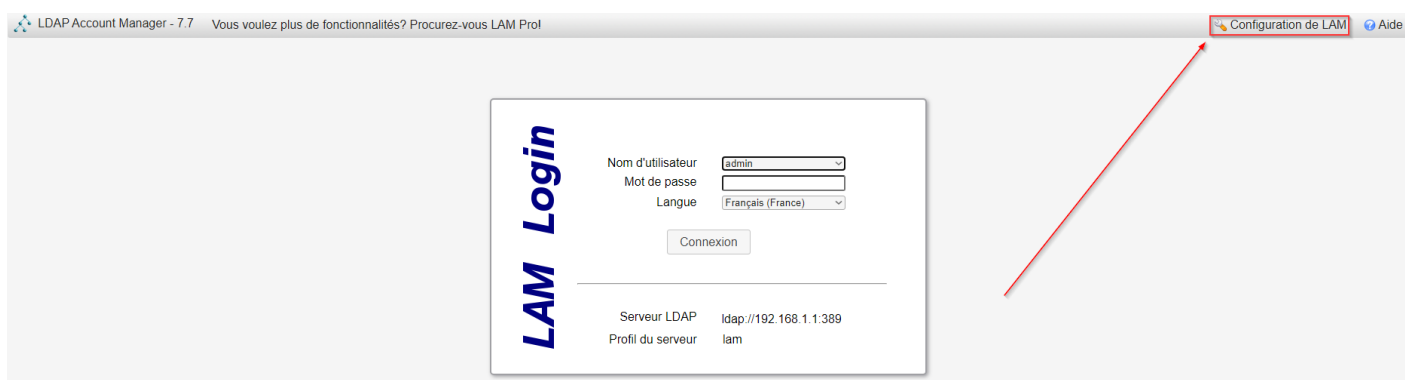
Une fois l'installation du paquet terminée, il suffit de se rendre, via un navigateur, à l'adresse suivante :

```
http://<IP du serveur>/lam
```

Configuration

Connexion

Dans votre navigateur, voici ce que vous devez retrouver :



Pour configurer LAM, se rendre dans "configuration de LAM" en haut à droite puis "Modifier les profils"



le mot de passe par défaut est "lam"

Paramètres généraux



Paramètres du serveur

Adresse du serveur *



Activer TLS



Nombre maximum de résultats retournés par la recherche LDAP



DN part to hide



► Options avancées



Paramètres de langue

Langue par défaut



Fuseau horaire



Paramètres de Lmdaemon

Liste de serveurs



Chemin vers le script externe



Nom d'utilisateur



Fichier de clé SSH



Mot de passe de la clé SSH



Droits du répertoire home

Lecture Écrire Exécuter

Propriétaire

Groupe

Autre



Paramètre des outils

Outils cachés

Vue arborescente	<input type="checkbox"/>	Édition multiple	<input type="checkbox"/>	Éditeur de profil	<input type="checkbox"/>
WebAuthn devices	<input type="checkbox"/>	Éditeur PDF	<input type="checkbox"/>	Éditeur d'OU	<input type="checkbox"/>
Tests	<input type="checkbox"/>	Informations serveur	<input type="checkbox"/>	Import / export LDAP	<input type="checkbox"/>
Explorateur de schéma	<input type="checkbox"/>	Chargement de fichier	<input type="checkbox"/>		

Vue arborescente

Suffixe arborescence ?



Paramètres de sécurité

Méthode de connexion ?
Liste des utilisateurs valides * ?



Authentification à 2 facteurs

Fournisseur ?



Mot de passe du profil

Nouveau mot de passe ?
Entrez le mot de passe à nouveau

















Renseigner les champs suivant :

- Adresse du serveur
- Paramètres de langue et régionaux
- suffix de l'arborescence
- méthode de connexion et utilisateur valide
- changer le mot de passe par défaut

Vous pouvez ensuite enregistrer.

Type de compte

Types de compte actifs

 Utilisateurs	Comptes utilisateurs (ex : Unix, Samba et Kolab)  
Suffixe LDAP	<input type="text" value="ou=Classes,dc=e-ecole,dc=org"/> 
Attributs de liste	<input type="text" value="#uid,#givenName,#sn,#uidNumber,#gidNumber"/> 
Libellé personnalisé	<input type="text"/> 
Filtre LDAP supplémentaire	<input type="text"/> 
Caché	<input type="checkbox"/> 
 Groupes	Comptes de groupes (ex : Unix et Samba)  
Suffixe LDAP	<input type="text" value="ou=Groupes,dc=e-ecole,dc=org"/> 
Attributs de liste	<input type="text" value="#cn,#gidNumber,#memberUID,#description"/> 
Libellé personnalisé	<input type="text"/> 
Filtre LDAP supplémentaire	<input type="text"/> 
Caché	<input type="checkbox"/> 

Renseigner les champs suivant :

- Utilisateurs
 - Suffixe LDAP = L'OU qui sera créée contenant les utilisateurs
- Groupes
 - Suffixe LDAP = L'OU qui sera créée contenant les groupes

Paramètres du module

Utilisateurs

Générateur d'UID	Plage fixe
Numéro d'UID minimum *	1100
Numéro d'UID maximum *	2100
Suffixe pour vérification de l'UID/Nom de groupe	
Nom d'utilisateur proposé	@givenname@%sn%

Options cachées ?

Gecos

Mot de passe

Options

Type de hash du mot de passe	MD5
Shells de connexion	/bin/bash
Ajouter l'utilisateur aux membres du groupe principal	<input type="checkbox"/>

Groupes

Générateur de GID	Plage fixe
Numéro de GID minimum *	600
Numéro de GID maximum *	700
Suffixe pour vérification du GID/Nom de groupe	
Désactiver la gestion des appartenances	<input type="checkbox"/>

Renseigner les champs suivant :

- Utilisateurs
 - UID minimum : ici 1100 (UID système commencent à 1000)
 - UID maximum : ici 2100 (1000 users dispo)
- Options
 - Type de hash mot de passe
 - Shell de connexion
- Groupes
 - GID minimum : ici 600 (GID système commencent à 500)
 - GID maximum : ici 700 (100 groupes dispo)

La configuration initiale est terminée.

Samba



Présentation

Samba est une implémentation open source du protocole SMB/CIFS, utilisé pour le partage de fichiers et d'imprimantes entre des systèmes d'exploitation différents, principalement entre des ordinateurs Windows et des ordinateurs Linux. Voici une présentation de ses principales caractéristiques :

1. **Partage de fichiers** : Samba permet de partager des fichiers et des répertoires entre des machines Windows, Linux et macOS au sein d'un même réseau. Il offre la possibilité de définir des autorisations d'accès granulaires pour contrôler qui peut accéder à quels fichiers et répertoires.
2. **Partage d'imprimantes** : En plus du partage de fichiers, Samba permet de partager des imprimantes connectées à un ordinateur Linux avec des ordinateurs Windows sur le réseau. Cela permet aux utilisateurs Windows d'imprimer sur des imprimantes connectées à des serveurs Linux via le protocole SMB/CIFS.
3. **Intégration avec Active Directory** : Samba peut être configuré pour fonctionner comme un contrôleur de domaine compatible avec Active Directory, permettant ainsi aux utilisateurs Linux de s'authentifier et d'accéder aux ressources partagées sur un réseau Windows.
4. **Support multiplateforme** : Samba est compatible avec une large gamme de systèmes d'exploitation, ce qui en fait une solution idéale pour les environnements hétérogènes où des ordinateurs Windows, Linux et macOS coexistent.

5. **Administration via une interface web** : Samba peut être configuré et géré via une interface web conviviale, telle que SWAT (Samba Web Administration Tool), qui simplifie la configuration et la gestion des partages réseau, des utilisateurs et des paramètres de sécurité.
6. **Sécurité** : Samba intègre des fonctionnalités de sécurité avancées pour protéger les données partagées sur le réseau. Cela inclut la prise en charge de l'authentification des utilisateurs, le chiffrement des communications et la gestion des autorisations d'accès.
7. **Support communautaire et documentation abondante** : Samba bénéficie d'une large communauté d'utilisateurs et de développeurs qui fournissent un support technique, des forums d'aide et une documentation exhaustive pour aider les utilisateurs à tirer le meilleur parti de cette solution de partage de fichiers.

En résumé, Samba est un logiciel puissant et polyvalent qui permet le partage de fichiers et d'imprimantes entre des ordinateurs Windows et des ordinateurs Linux dans un environnement réseau, offrant une compatibilité multiplateforme, une sécurité renforcée et une facilité d'administration.

Site officiel [samba](#).

Installation

```
apt update && apt upgrade  
apt install samba
```

Partages

```
[Tablette]  
path = /Serveur/Tablette  
public = yes  
guest only = yes  
writeable = yes  
browseable = yes  
create mask = 777  
directory mask = 777  
  
[Classes]  
path = /Serveur/Classes  
browseable = yes
```

```
guest ok = yes
read only = no
create mask = 777
directory mask = 777
force user = profs
force group = Eleves
```

[Profs]

```
path = /Serveur/Profs
browseable = yes
guest ok = yes
read only = no
create mask = 777
directory mask = 777
force user = direction
force group = Enseignants
```

[Direction]

```
path = /Serveur/Direction
browseable = yes
guest ok = yes
read only = no
create mask = 777
directory mask = 777
force user = direction
force group = Enseignants
```

[Serveur]

```
path = /Serveur
browseable = yes
guest ok = yes
read only = no
create mask = 777
directory mask = 777
force user = direction
force group = Enseignants
```

Eoptes



Présentation

Eoptes est un logiciel open source conçu pour la gestion centralisée des ordinateurs dans un environnement éducatif. Voici une présentation de ses principales caractéristiques :

1. **Gestion des postes de travail** : Eoptes permet aux administrateurs système et aux enseignants de surveiller et de contrôler les ordinateurs des élèves depuis une interface centralisée. Cela inclut la visualisation de l'écran de l'ordinateur, le verrouillage et le déverrouillage de l'écran, ainsi que l'envoi de messages aux utilisateurs.
2. **Contrôle en temps réel** : Les enseignants peuvent surveiller les activités des étudiants en temps réel, ce qui leur permet de détecter les comportements inappropriés, d'offrir une assistance immédiate et de maintenir un environnement d'apprentissage efficace.
3. **Diffusion de contenu** : Eoptes permet aux enseignants de diffuser du contenu sur les ordinateurs des élèves, ce qui facilite la présentation de cours, la démonstration de logiciels ou la distribution de documents et de ressources pédagogiques.
4. **Gestion des applications** : Les administrateurs peuvent contrôler les applications autorisées sur les postes de travail des élèves, ce qui permet de limiter l'accès à des logiciels spécifiques ou d'assurer la conformité avec les politiques de sécurité et d'utilisation des ressources informatiques.
5. **Compatibilité multiplateforme** : Eoptes est compatible avec une variété de systèmes d'exploitation, y compris Linux et certains systèmes d'exploitation basés sur Windows, ce qui en fait une solution polyvalente pour les environnements hétérogènes.
6. **Interface conviviale** : Eoptes offre une interface conviviale et intuitive qui facilite la gestion et le contrôle des postes de travail, même pour les utilisateurs novices.
7. **Sécurité** : Eoptes intègre des fonctionnalités de sécurité telles que l'authentification des utilisateurs et le cryptage des communications pour protéger la confidentialité et

l'intégrité des données.

En résumé, Epopotes est un outil puissant et polyvalent pour la gestion des ordinateurs dans les salles de classe et les environnements éducatifs. En permettant aux enseignants et aux administrateurs de surveiller, contrôler et interagir avec les postes de travail des élèves, il contribue à améliorer l'efficacité de l'enseignement et de l'apprentissage en classe.

Site officiel [Epopotes](#).

Configuration

To do

Utilisation

To do

Veeam

VEEAM

Présentation

Veeam est un leader mondial dans le domaine de la protection des données et de la restauration anti-ransomware. Voici une présentation de ses principales fonctionnalités et avantages :

Fonctionnalités de Veeam :

1. Sauvegarde et restauration :

- **Sauvegarde complète** : Protection de toutes les données, y compris les bases de données, applications et données des utilisateurs.
- **Restauration rapide** : Restauration des données en quelques minutes grâce à des sauvegardes incrémentielles et des snapshots.

2. Protection contre le ransomware :

- **Sauvegardes inaltérables** : Protection contre les ransomwares avec des sauvegardes exemptes de ransomware.
- **Verrouillage des objets** : Protection des objets de sauvegarde pour éviter toute altération.

3. Virtualisation et cloud :

- **Support multi-plateforme** : Sauvegarde et restauration des machines virtuelles sur VMware, Hyper-V et AWS.
- **Protection des données dans le cloud** : Sauvegarde des données dans des environnements cloud comme AWS, Microsoft Azure et Google Cloud.

4. Automatisation et gestion :

- **Automatisation des sauvegardes** : Gestion intelligente et automatisée du cycle de vie des sauvegardes.
- **Rapports et alertes** : Génération de rapports détaillés et alertes pour une meilleure gestion des sauvegardes.

5. Évolutivité et simplicité :

- **Évolutivité** : Solutions évolutives adaptées aux besoins de toutes tailles d'entreprise.

- **Interface intuitive** : Interface utilisateur intuitive et des assistants pour faciliter la gestion des sauvegardes.

Avantages de Veeam :

- **Récupération rapide** : Réduction du temps de récupération grâce à des sauvegardes rapides et efficaces.
- **Coûts réduits** : Réduction des coûts d'investissement et d'exploitation grâce à des solutions économiques et faciles à utiliser.
- **Sécurité renforcée** : Protection robuste contre les ransomwares et autres menaces de sécurité.
- **Flexibilité** : Adaptabilité aux environnements physiques, virtuels et cloud.

Veeam est une solution complète pour la protection des données, offrant sécurité, simplicité et évolutivité.

Installation

Nous devons d'abord télécharger et installer les sources en faisant à la version souhaitée :

```
wget https://kasa.vitrecommunaute.bzh/index.php/s/VEEAM/download?path=%2F&files=veeam-release-deb_1.0.9_amd64.deb&downloadStartSecret=39xfl5i6e8a
wget https://kasa.vitrecommunaute.bzh/index.php/s/VEEAM/download?path=%2F&files=veeam-release-deb_1.0.8_amd64.deb&downloadStartSecret=jn6g3xurbzb

dpkg -i veeam-release-deb_1.0.9_amd64.deb
dpkg -i veeam-release-deb_1.0.8_amd64.deb
```

Une fois les sources installées, on update et on fait l'installation

- Debian 10 / Ubuntu 16-20

```
apt update && apt upgrade && apt full-upgrade
apt install veeam
```

- Debian 11-12 / Ubuntu 22-24

```
apt update && apt upgrade && apt full-upgrade
apt install blksnap veeam
```

Veeam est maintenant installé !

Sauvegarde

To do

Autre

Mettre en place NAT

Pour que les postes Edubuntu puissent accéder à Internet, il faut créer une règle NAT.

Dans la version précédente de Edubuntu, nous faisons l'appel des règles via le fichier de configuration interfaces.

Cela ne peut plus se faire avec la nouvelle version, j'ai donc choisis de passer par crontab :

```
crontab -e
```

On ajout ensuite la ligne suivante :

```
@reboot iptables --table nat --append POSTROUTING --jump MASQUERADE --source 192.168.1.0/24
```

Scripts

Vider sessions

Un script mis en place sur cette nouvelle version est de supprimé le contenu des sessions utilisateurs.

Decision prise après la quantité de problèmes survenus à cause des sessions trop volumineuses.

Le fichier bash est à placé dans le répertoire cron.daily:

```
nano /etc/cron.daily/vider-sessions.sh
```

```
for user in $(ls /home/users/)
do
    rm -rf /home/users/$user/Documents/*
    rm -rf /home/users/$user/Images/*
    rm -rf /home/users/$user/Musique/*
    rm -rf /home/users/$user/Téléchargements/*
    rm -rf /home/users/$user/Vidéos/*
    rm -rf /home/users/$user/.config/dolphinrc
done
rm -rf /Serveur/.Trash*
```

Il faut ensuite définir qu'il s'agit d'un fichier exécutable :

```
chmod +x /etc/cron.daily/vider-sessions.sh
```

Copier menu démarrer modèle

Un autre script utile permet de mettre à jour le menu KDE depuis la session modèle vers l'ensemble des sessions de façon journalière.

Cela permet de modifier la session modèle sans se soucier de devoir mettre à jour le skel ou les sessions manuellement.

Le fichier bash est à placer dans le répertoire cron.daily :

```
nano /etc/cron.daily/dupliquer-menu.sh
```

```
#!/bin/bash

for user in $(ls /home/users/); do
    cp -R /home/users/info20/.config/menus/* /home/users/$user/.config/menus/;
    cp -R /home/users/info20/.local/share/applications/*
/home/users/$user/.local/share/applications/;
    cp -R /home/users/info20/.config/plasma-org.kde.plasma.desktop-appletsrc
/home/users/$user/.config/plasma-org.kde.plasma.desktop-appletsrc
    $groupe = "groups $user";
    chown -R $user:$groupe /home/users/$user/
    echo "Le fichier a été copié sur le bureau de \"$user\" !"
done

cp -R /home/users/info20/.config/menus/* /etc/skel/.config/menus/;
cp -R /home/users/info20/.local/share/applications/* /etc/skel/.local/share/applications/;
cp -R /home/users/info20/.config/plasma-org.kde.plasma.desktop-appletsrc
/etc/skel/.config/plasma-org.kde.plasma.desktop-appletsrc

echo "Les fichiers ont été copiés dans le skel"
```

Il faut ensuite définir qu'il s'agit d'un fichier exécutable :

```
chmod +x /etc/cron.daily/dupliquer-menu.sh
```

Actualiser les droits du partage Serveur

Un script qui permettra de toujours avoir les droits des fichiers à jour, malgré la multitude d'utilisateurs.

Ceci afin d'éviter les soucis liés à la quantité d'utilisateurs différents sur le partage.

Le fichier bash est à placé dans le répertoire cron.min :

```
mkdir /etc/cron.min
```

```
nano /etc/cron.min/Droits-montage.sh
```

```
#!/bin/bash
for COUNT in `seq 5`; do
    NOW=$(date +"%m-%d-%Y %H:%M:%S")
    echo $NOW >/tmp/perm.txt
    chown root:root /Serveur
    chmod 755 /Serveur
    chown -R mnteleve:Eleves /Serveur/Tablette
    chmod -R 777 /Serveur/Tablette
    chown -R mtenseignants:Enseignants /Serveur/Profs
    chmod -R 770 /Serveur/Profs
    chown -R mtenseignants:Enseignants /Serveur/Direction
    chmod -R 770 /Serveur/Direction
    chown -R mnteleve:Eleves /Serveur/Classes
    chmod -R 777 /Serveur/Classes
    chmod -R 755 /Serveur/CDs
    sleep 10
done
```

Il faut ensuite définir qu'il s'agit d'un fichier executable :

```
chmod +x /etc/cron.min/Droits-montage.sh
```

Copier documentation bureau

Un autre script utile permet de mettre à jour le menu KDE depuis la session modèle vers l'ensemble des sessions de façon journalière.

Cela permet de modifier la session modèle sans se soucier de devoir mettre à jour le skel ou les sessions manuellement.

Le fichier bash est à placé dans le répertoire cron.daily :

```
nano /etc/cron.daily/dupliquer-doc.sh
```

```
#!/bin/bash

wget -O /home/users/info20/Bureau/Presentation\ Edubuntu\ 2.0.pdf
https://kasa.vitrecommunaute.bzh/index.php/s/doc-edubuntu/download/Presentation%

for user in $(ls /home/users/); do
    cp "/home/users/info20/Bureau/Presentation Edubuntu 2.0.pdf"
"/home/users/"$user"/Bureau/Presentation Edubuntu 2.0.pdf"
    echo "Le fichier a été copié sur le bureau de "$user" !"
done

cp "$file_to_copy" /etc/skel/Bureau/
echo "Le fichier a été copié dans le skel"
```

Il faut ensuite définir qu'il s'agit d'un fichier exécutable :

```
chmod +x /etc/cron.daily/dupliquer-doc.sh
```

Mise à jour auto de l'image

Au vu du nombre d'écoles infogérées par le service, et afin de simplifier la gestion, un script qui update upgrade l'image a été mis en place.

Le fichier bash est à placé dans le répertoire cron.monthly :

```
nano /etc/cron.monthly/update-chroot.sh
```

```
#!/bin/bash

#Changement de la banniere en cas de connexion pendant la mise à jour
cp /etc/motd-maintenance /etc/motd
update-motd

# Chemin du chroot
chroot_path="/srv/ltsp/edubuntu/"

# Montage des systèmes de fichiers nécessaires
mount --bind /proc "$chroot_path/proc"
mount --bind /sys "$chroot_path/sys"
mount --bind /dev "$chroot_path/dev"
```