

Lucas TARDY

Antoine GIRARDEY

Document de validation de compétences

AP-3 Configuration d'un serveur Nextcloud

20/02/2024 - 26/03/2024

Equipe 4

1. Présentation du contexte d'entreprise

Centrecall est une entreprise d'accueil d'appel et de télémarketing, il y a cinq centres d'appel de télémarketing. Notre mission est d'optimiser la communication entre les différents services en mettant à disposition un service de stockage et de partage cloud tout en restant maître de ses données, le logiciel choisit est "Nextcloud". Un serveur Nextcloud sera donc héberger sur un serveur virtualisé via l'application VirtualBox.

2. Objectifs attendus

Crée un serveur Nextcloud, le configurer, le sécurisé, pouvoir y accéder en local avec une adresse IP ainsi qu'avec un nom de domaine, l'intégrer à un serveur AD DS, et pouvoir y accéder sur téléphone.

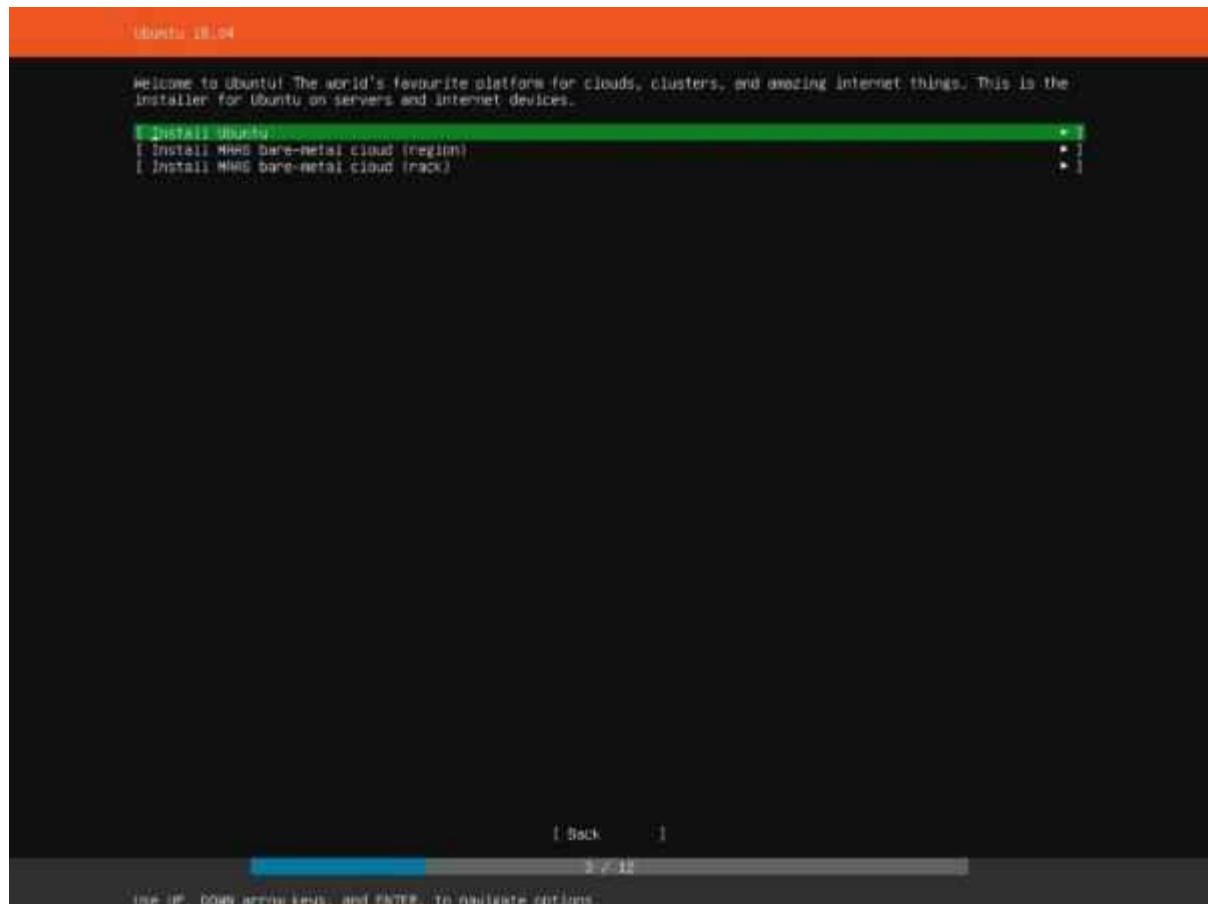
3. Plan de travail

- 1) Installation de l'environnement.
- 2) Paramétrage IP.
- 3) Paramétrage du SSH.
- 4) Installation du serveur Nextcloud.
- 5) Configuration du serveur Nextcloud.
- 6) Sécurisation du serveur Nextcloud.
- 7) Installation de l'application Nextcloud cliente.
- 8) Mise en place de la résolution de nom.
- 9) Intégration du serveur Nextcloud à un serveur AD DS.
- 10) Mise en place de l'accès wifi.

4. Réalisation

Capture d'écran + brèves explications

1) La première étape de cette AP consiste en l'installation de l'environnement qui hébergera notre ubuntu 22.04.



2) Ensuite, nous avons paramétrer l'adresse IP de notre serveur :

Pour ce faire, nous avons modifier le dossier “/etc/netplan/-install-config.yaml” pour intégrer notre serveur au réseau de l’école, en lui donnant une adresse IP étant dans le réseau de l’école, de plus, l’adresse IP de la passerelle est égale à l’adresse IP de la passerelle du BTS. Pour finir ce paramétrage IP, le DNS que j’ai mis est mon serveur AD DS, pour pouvoir ensuite intégrer ce serveur à mon serveur AD DS :

```
# This is the network config written by 'subiquity'
network:
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
        - 172.18.4.3/16
      nameservers:
        addresses: [172.18.200.232]
      routes:
        - to: default
          via: 172.18.255.254
  version: 2
```

"00-installer-config.yaml" [lecture-seule] 13L, 284B

Application des modification réseaux grâce à la commande “netplan apply” puis vérification via la commande “IP a”

```
nextcloud@srv-nextcloud:/etc/netplan$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8d:f3:ea brd ff:ff:ff:ff:ff:ff
    inet 172.18.4.3/16 brd 172.18.255.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe8d:f3ea/64 scope link
        valid_lft forever preferred_lft forever
nextcloud@srv-nextcloud:/etc/netplan$
```

3-4) Durant l'installation deux services nécessaires peuvent être installés, je parle ici en premier lieu du service SSH et du service Nextcloud qui est le cœur de cette activité.

Storage configuration [Help]

FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
[/	11.496G	new ext4	new LVM logical volume ▶]
[/boot	2.000G	new ext4	new partition of local disk ▶]

AVAILABLE DEVICES

DEVICE	TYPE	SIZE
[ubuntu-vg (new)	LVM volume group	22.996G ▶]
free space		11.500G ▶]

[Create software RAID (md) ▶]

[Create volume group (LVM) ▶]

USED DEVICES

DEVICE	TYPE	SIZE
[ubuntu-vg (new)	LVM volume group	22.996G ▶]
ubuntu-lv new, to be formatted as ext4, mounted at /		11.496G ▶]

[VBOX_HARDDISK_VBae7efcd7-cb80b217 local disk 25.000G ▶]

partition 1 new, BIOS grub spacer 1.000M ▶]

partition 2 new, to be formatted as ext4, mounted at /boot 2.000G ▶]

partition 3 new, PV of LVM volume group ubuntu-vg 22.997G ▶]

[Done]

[Reset]

[Back]

Install complete! [Help]

configuring installed system
running 'curtin curthooks'
curtin command curthooks
configuring apt configuring apt
installing missing packages
Installing packages on target system: ['grub-pc']
configuring iscsi service
configuring raid (mdadm) service
installing kernel
setting up swap
apply networking config
writing etc/fstab
configuring multipath
updating packages on target system
configuring pollinate user-agent on target
updating initramfs configuration
configuring target system bootloader
installing grub to target devices
final system configuration
calculating extra packages to install
installing openssh-server
retrieving openssh-server
curtin command system-install
unpacking openssh-server
curtin command system-install
configuring cloud-init
downloading and installing security updates
curtin command in-target]

[View full log]

[Cancel update and reboot]

SSH Setup [Help]

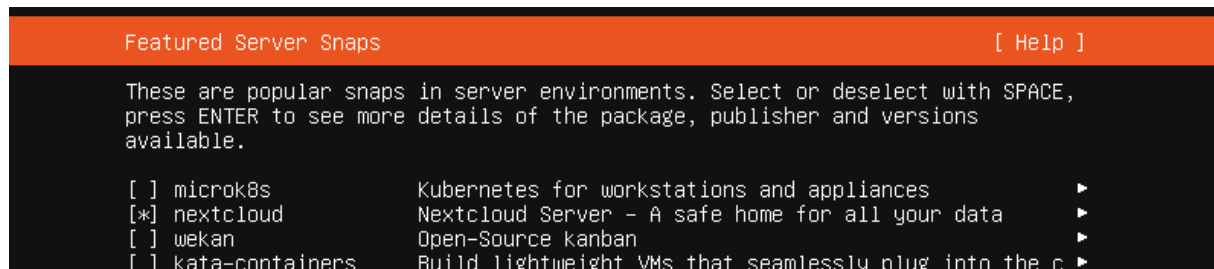
You can choose to install the OpenSSH server package to enable secure remote access to your server.

☒ Install OpenSSH server

Import SSH identity: [No ▼]
You can import your SSH keys from GitHub or Launchpad.

Import Username:

☒ Allow password authentication over SSH



Une fois le serveur correctement installé je l'ai correctement mis à jour afin de ne pas avoir de problèmes d'incompatibilité et également pour le sécuriser.

```
root@qsdf:/home/user# apt update
Atteint :1 http://fr.archive.ubuntu.com/ubuntu jammy InRelease
Réception de :2 http://fr.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Réception de :3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Atteint :4 http://fr.archive.ubuntu.com/ubuntu jammy-backports InRelease
Réception de :5 http://fr.archive.ubuntu.com/ubuntu jammy/main Translation-fr [486 kB]
Réception de :6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1 298 kB]
Réception de :7 http://fr.archive.ubuntu.com/ubuntu jammy/restricted Translation-fr [4 760 B]
Réception de :8 http://fr.archive.ubuntu.com/ubuntu jammy/universe Translation-fr [3 564 kB]
Réception de :9 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [292 kB]
Réception de :10 http://fr.archive.ubuntu.com/ubuntu jammy/multiverse Translation-fr [93,5 kB]
Réception de :11 http://fr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1 519 kB]
Réception de :12 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [1 605 kB]
Réception de :13 http://fr.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [293 kB]
Réception de :14 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [270 kB]
Réception de :15 http://fr.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [1 644 kB]
Réception de :16 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [852 kB]
Réception de :17 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [163 kB]
Réception de :18 http://fr.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [274 kB]
Réception de :19 http://fr.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1 060 kB]
Réception de :20 http://fr.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [241 kB]
Réception de :21 http://fr.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [49,6 kB]
Réception de :22 http://fr.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [12,0 kB]
13,9 Mo réceptionnés en 7s (1 947 ko/s)
```

```
106 mis à jour, 3 nouvellement installés, 0 à enlever et 3 non mis à jour.
15 standard security updates
Il est nécessaire de prendre 31,7 Mo dans les archives.
Après cette opération, 425 ko d'espace disque seront libérés.
Souhaitez-vous continuer ? [O/n] _
```

5) La prochaine étape consistait en la configuration du service Nextcloud. C'est-à-dire commencer par y créer un compte Administrateur. Compte qui pourra ensuite créer des comptes utilisateurs et nous permettre de paramétrer les options de sécurité pour ces comptes-ci.

La première commande est donc :

```
root@qsdf:/home/user# nextcloud.manual-install nextcloud_admin @password25
```

Il faut ensuite ajouter le domaine voulus aux domaines de confiance avec la commande suivante :

```
root@qsdf:/home/user# nextcloud.occ config:system:set trusted_domains 1 --value=nextcloud.centrecall.local
```

Ainsi, le domaine a été ajouté aux domaines de confiance ce qui va nous permettre de pouvoir accéder à son interface web.

Ensuite, la prochaine étape consiste à définir des ports à utiliser pour le server nextcloud, chose faites grâce aux commandes suivantes :

```
nextcloud@srv-nextcloud:~$ sudo ufw allow 80,443/tcp  
Rules updated  
Rules updated (v6)
```

6) Une fois la configuration de base effectuée il fallait désormais ajouter une couche de sécurité au serveur, chose qui a été faites en activant l'authentification à deux facteurs pour les utilisateurs, ainsi qu'en appliquant une politique de mots de passe plus stricte.

Authentification à deux facteurs ⓘ

L'authentification à deux facteurs peut être forcée pour tous les utilisateurs et des groupes spécifiques. S'ils n'ont pas un fournisseur à deux facteurs configuré, ils ne seront pas capables de s'authentifier sur le système.

☒ Imposer l'authentification à deux facteurs

Limiter aux groupes

L'authentification à deux facteurs peut être imposée à certains groupes seulement.

L'authentification à deux facteurs est forcée pour tous les membres des groupes suivants :

user

L'authentification à deux facteurs n'est pas forcée pour les membres des groupes suivants :

admin

Lorsque des groupes sont forcés/exclus, la logique suivante est utilisée pour déterminer si l'authentification à double facteur (A2F) est imposée à un utilisateur. Si aucun groupe n'est forcé, l'authentification à double facteur est activée pour tous sauf pour les membres des groupes exclus. Si des groupes sont forcés, l'authentification à double facteur est exigée pour tous les membres de ces groupes. Si un utilisateur est à la fois dans un groupe forcé et exclu, c'est le groupe forcé qui prime et l'authentification double facteur est imposée.

Politique de mots de passe

- Longueur minimale du mot de passe
- Historique des mots de passe de l'utilisateur
- Nombre de jours avant expiration du mot de passe
- Nombre de tentatives de connexion avant de verrouiller le compte utilisateur (0 pour indiquer aucune limite)

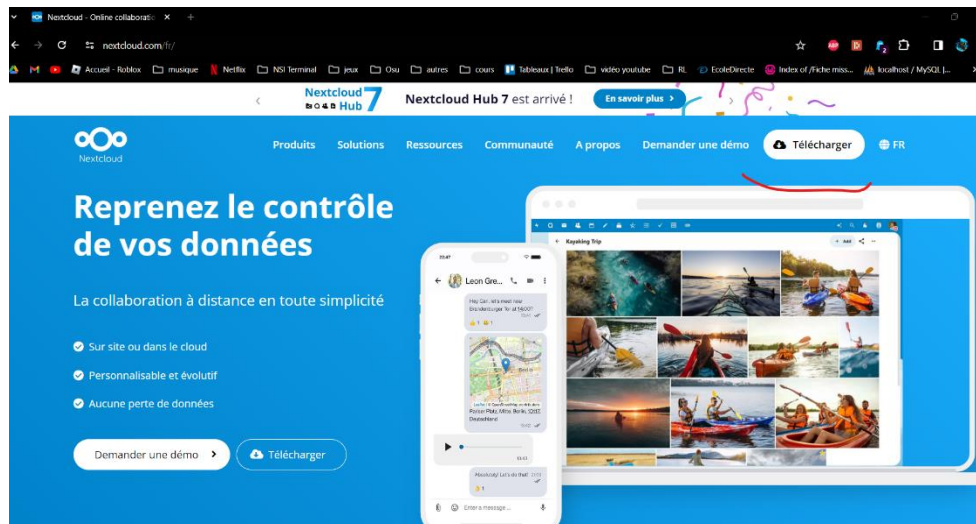
- ☒ Interdire les mots de passe courants
- ☐ Imposer des caractères en majuscules et en minuscules
- ☒ Imposer des chiffres
- ☒ Imposer des caractères spéciaux
- ☒ Vérifier le mot de passe par rapport à la liste des mots de passe compromis sur haveibeenpwned.com

Cette vérification crée un hachage du mot de passe et envoie les 5 premiers caractères de ce hachage à l'API haveibeenpwned.com pour récupérer une liste de tous les hachages qui commencent par ceux-là. Ensuite, il vérifie sur l'instance Nextcloud si le mot de passe est dans le jeu de résultats.

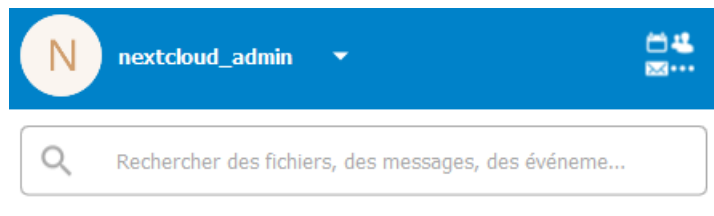


7) Par la suite la prochaine étape consistait en l'installation du logiciel de bureau nextcloud et à se connecter à notre serveur.

Pour installer le logiciel client Nextcloud, il suffit d'écrire "Nextcloud client download" sur internet et suivre les étapes d'installation

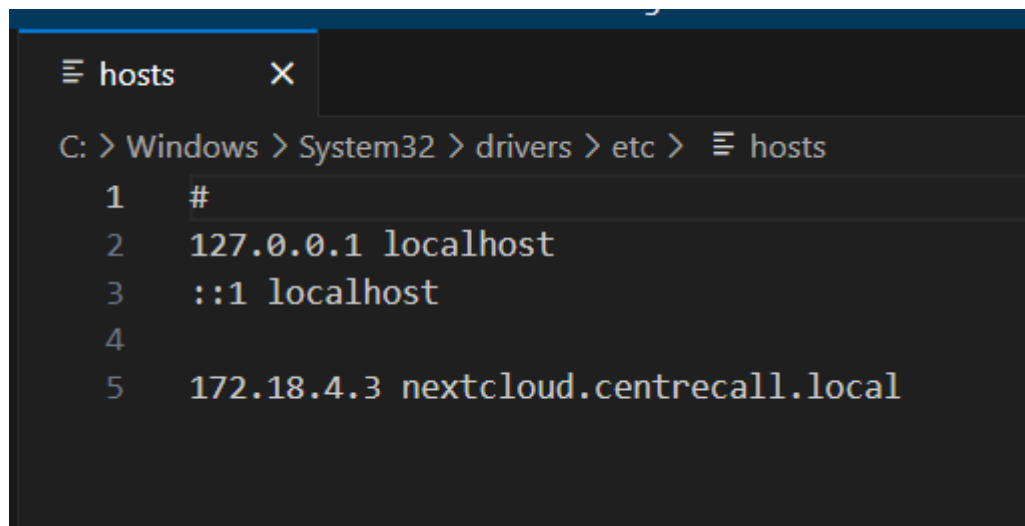


Une fois installer, le menu de base ressemble à cela :



Cela nous permet donc de ne pas avoir nécessairement besoin de se connecter à l'interface web du serveur mais en pouvant simplement se connecter via l'application de bureau qui est plus rapide et simple d'accès. Par ailleurs elle prend également en compte la mémorisation des mots de passe ce qui permet une connexion plus rapide.

8) Ensuite, pour pouvoir traduire l'adresse IP de notre serveur Nextcloud en nom de domaine local, il faut écrire le l'adresse IP de ce serveur accompagner du nom de domaine voulu dans le fichier Host. (Aller dans Windows → système 32 → drivers → etc → hosts ouvert avec visual studio code).

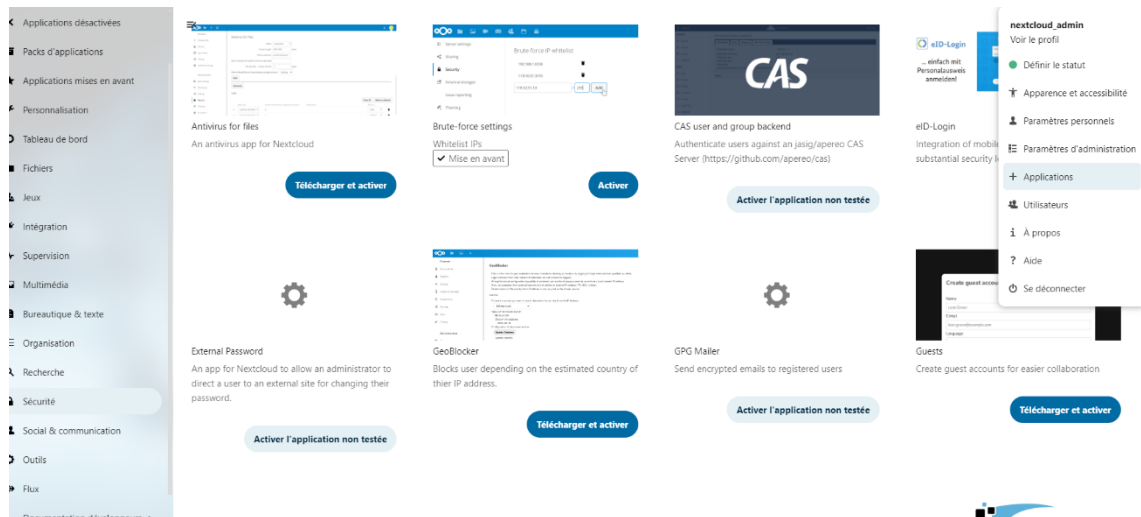


The image shows a Windows File Explorer window titled "hosts" with a close button (X). The address bar displays the path: "C: > Windows > System32 > drivers > etc > hosts". The file contents are listed as follows:

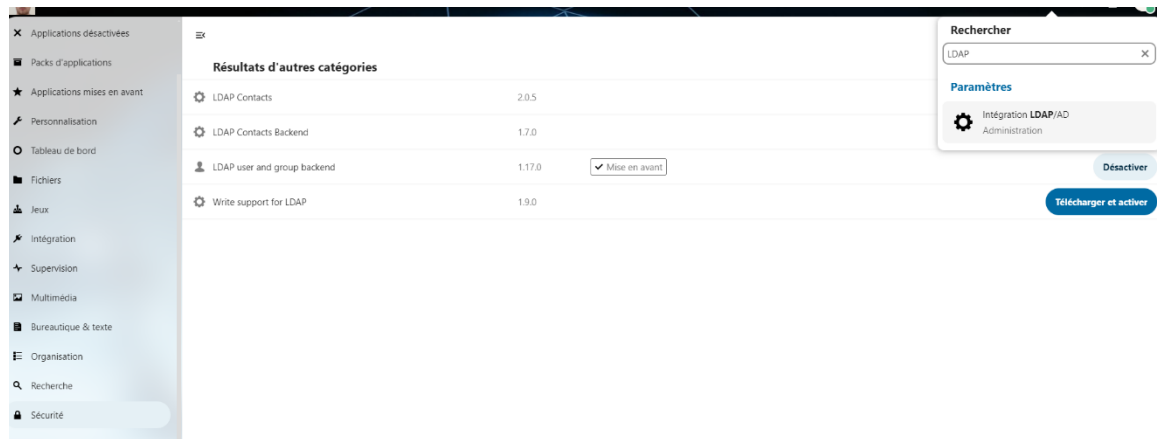
```
1  #
2  127.0.0.1 localhost
3  ::1 localhost
4
5  172.18.4.3 nextcloud.centrecall.local
```

9) Intégration du serveur AD DS à notre serveur Nextcloud:

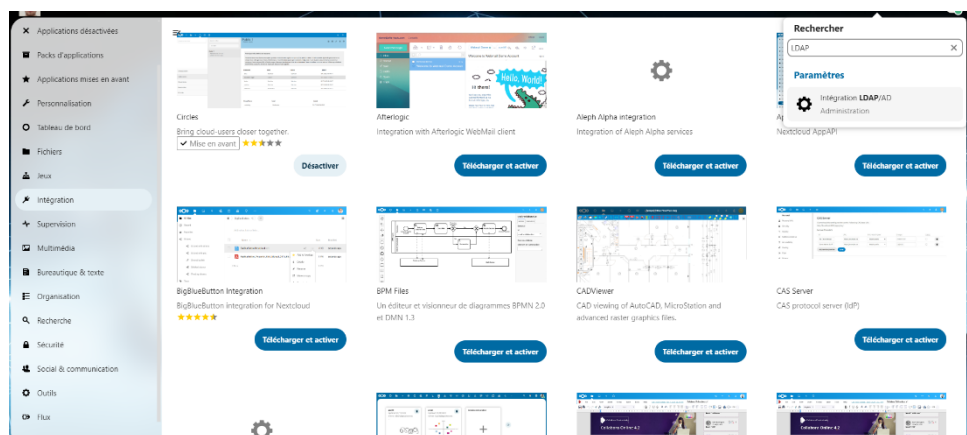
Il faut aller dans le menu d'administration Nextcloud, ensuite on doit aller dans "application", puis dans sécurité (en bas à gauche de l'écran)



Ensuite il faut télécharger et activer “LDAP user and group backend” pour pouvoir intégrer le serveur AD DS



Après, on peut intégrer le serveur AD DS, pour ce faire, nous devons aller dans le menu d’intégration et rechercher “LDAP” :



Ensuite, nous arriverons à ce menu, dans lequel on doit mettre l’adresse IP du serveur AD DS, mettre le port 389 ainsi que le nom de domaine accompagné du nom d’administrateur local avec le mot de passe de ce compte. Pour finir, tout en bas, il faut mettre le nom de l’UO de nos utilisateurs après le “OU=”, le nom de domaine dans “DC=” et le type de domaine dans le deuxième “DC=”.

Intégration LDAP/AD

Serveur

Utilisateurs

Attributs de connexion

Groupes

2. Serveur

+

172.18.200.232

389

Détecter le port

CENTRECALL\Administrateur

Sauvegarder les informations d'identification

OU=UTILISATEURS,DC=centrecall,DC=local

Détecter le DN de base

Tester le DN de base

☐ Saisir les filtres LDAP manuellement (recommandé pour les annuaires de grande ampleur)

Une fois que la configuration est "OK", le serveur AD DS est intégré au serveur Nextcloud:

Voici les groupes d'utilisateurs que l'on peut intégrer au serveur Nextcloud

Intégration LDAP/AD

Serveur

Utilisateurs

Attributs de connexion

Groupes

Rechercher et lister les utilisateurs qui respectent ces critères :

Seulement ces classes d'objets :

person

Les classes d'objets fréquentes pour les utilisateurs sont : organizationalPerson, person, user et inetOrgPerson. Si vous n'êtes pas sûr de la classe à utiliser, demandez à l'administrateur de l'annuaire.

Seulement dans ces groupes :

Groupe Commercial, Groupe de Comptabilite, Groupe de Developpement,

Modifier la requête LDAP

Filtre LDAP :

(&(|(objectclass=person))(|(|(memberof=CN=Groupe Commercial,OU=Commercial,OU=UTILISATEURS,DC=centrecall,DC=local)(primaryGroupID=1117))(|(|(memberof=CN=Groupe de Comptabilite,OU=Comptabilite,OU=UTILISATEURS,DC=centrecall,DC=local)(primaryGroupID=1116))(|(|(memberof=CN=Groupe de Developpement,OU=Developpement,OU=UTILISATEURS,DC=centrecall,DC=local)(primaryGroupID=1115))(|(|(memberof=CN=Groupe de Direction,OU=Direction,OU=UTILISATEURS,DC=centrecall,DC=local)(primaryGroupID=1114))(|(|(memberof=CN=Groupe

Voici leurs attributs de connexion :

Serveur

Utilisateurs

Attributs de connexion

Groupes

À la connexion, Nextcloud cherchera l'utilisateur sur la base des attributs suivant :

Nom d'utilisateur LDAP/AD : ☒

Adresse électronique LDAP/AD : ☐

Autres attributs : Sélectionner les attributs

[Modifier la requête LDAP](#)

Filtre LDAP : (&(&((objectclass=person))((memberof=CN=Groupe Commercial,OU=Commercial,OU=UTILISATEURS,DC=centrecall,DC=local)(primaryGroupID=1117))((memberof=CN=Groupe de Comptabilite,OU=Comptabilite,OU=UTILISATEURS,DC=centrecall,DC=local)(primaryGroupID=1116))((memberof=CN=Groupe de Developpement,OU=Developpement,OU=UTILISATEURS,DC=centrecall,DC=local)(primaryGroupID=1115))((memberof=CN=Groupe de Direction,OU=Direction,OU=UTILISATEURS,DC=centrecall,DC=local)(primaryGroupID=1114))((memberof=CN=Groupe utilisateurs,OU=UTILISATEURS,DC=centrecall,DC=local)(primaryGroupID=1111))))(samaccountname=%uid))

Voici les différents groupes d'utilisateurs sélectionner :

Serveur

Utilisateurs

Attributs de connexion

Groupes

Les groupes respectant ces critères sont disponibles dans Nextcloud :

Seulement ces classes d'objets : Sélectionner les classes d'objet

Seulement dans ces groupes : Groupe Commercial, Groupe de Comptabilite, Groupe de Developpement, Groupe de Direction, Groupe utilisateurs

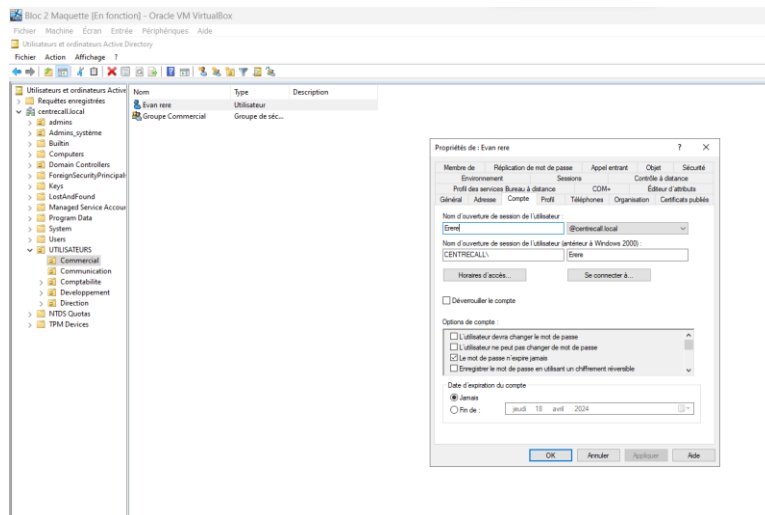
>

<

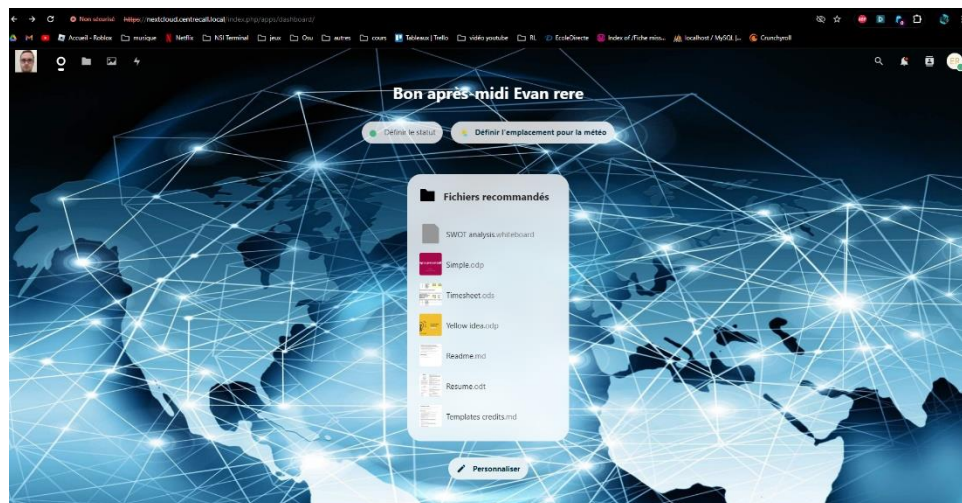
[Modifier la requête LDAP](#)

Filtre LDAP : ((cn=Groupe Commercial)(cn=Groupe de Comptabilite)(cn=Groupe de Developpement)(cn=Groupe de Direction)(cn=Groupe utilisateurs))

On peut voir un utilisateur de notre serveur AD DS :



Et si on essaie de se connecter à notre serveur Nextcloud avec ses identifiants, on peut en effet s'y connecter :



10) Enfin il fallait configurer une borne wifi Cisco. Le modèle est Cisco aironet 700 series. Cette borne devait permettre de se connecter au serveur nextcloud depuis notre téléphone ou n'importe quel appareil.

Il a donc fallu la réinitialiser en accédant à son interface console via câble serial et taper les commandes suivantes :

```
ap: delete flash:private-multiple-fs
Are you sure you want to delete "flash:private-multiple-fs" (y/n)?y
File "flash:private-multiple-fs" deleted
```

Au prochain redémarrage la borne avait été réinitialisée.

Une fois la borne réinitialisée, je m'y suis connecté grâce à son IP à l'interface web et j'ai ensuite accédé au Dashboard de configuration afin de paramétrer la diffusion radio 2.4ghz comme ci-dessous :

Radio 2.4GHz

SSID :	<input type="text" value="AP_Antoine_Lucas"/>
	<input type="checkbox"/> Broadcast SSID in Beacon
VLAN :	<input checked="" type="radio"/> No VLAN <input type="radio"/> Enable VLAN ID:
	<input type="text" value="(1-4094)"/> <input type="checkbox"/> Native VLAN
Security :	<input type="text" value="No Security"/>
Role in Radio Network :	<input type="text" value="Access Point"/>
Optimize Radio Network :	<input type="text" value="Default"/>
Aironet Extensions:	<input type="text" value="Enable"/>
Channel:	<input type="text" value="Least-Congested"/>
Power:	<input type="text" value="Maximum"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

J'ai ici choisi de configurer le 2.4ghz et non le 5Ghz car certains vieux appareils ne prennent pas en compte le 5Ghz. J'y ai donc configuré un SSID ainsi que son rôle (ici Access point).

Une fois ces options configurées, il a fallu les activer sur la borne je me suis donc rendu dans un autre menu pour y attribuer les options précédemment configurées comme ci-dessous :

Guest Mode/Infrastructure SSID Settings



Radio0-802.11N^{2.4GHz}:

Set Beacon Mode:	<input checked="" type="radio"/> Single BSSID	Set Single Guest Mode SSID: <input type="text" value="AP_Antoine_Lucas"/>
	<input type="radio"/> Multiple BSSID	
Set Infrastructure SSID:	<input type="text" value="< NONE >"/>	<input type="checkbox"/> Force Infrastructure Devices to associate only to this SSID

Radio1-802.11N^{5GHz}:

Set Beacon Mode:	<input checked="" type="radio"/> Single BSSID	Set Single Guest Mode SSID: <input type="text" value="< NONE >"/>
	<input type="radio"/> Multiple BSSID	
Set Infrastructure SSID:	<input type="text" value="< NONE >"/>	<input type="checkbox"/> Force Infrastructure Devices to associate only to this SSID

Enfin pour finir cette partie sur la borne wifi la dernière étape consistait à mettre en ligne la partie 2.4Ghz de la borne comme suivant :

Interface	MAC Address	Transmission Rate
 GigabitEthernet	547c.6921.edaa	1Gbps
 Radio0-802.11N^{2.4GHz}	1ce8.5db8.9ca0	Mcs Index 15

On peut maintenant voir le wifi et s'y connecter à notre guise :

