

SERVEUR ANNUAIRE

LLDAP sur Debian 11

Noah MAILLET Projet-SANDBOX



Table of Contents

1	Preface	
1.1	Presentation LDAP.	
	1.1.1 Protocole LDAP	
	1.1.2 Service LLDAP	
1.2	Configuration minimale	
2	Création du conteneur	
3	Installation LLDAP	
4	Configuration LLDAP.	10
4.1	Base DN for LDAP	10
4.2	Admin username	10
4.3	Admin email	11
4.4	Admin password	11
5	Interface web	



1 Preface

1.1 Presentation LDAP.

1.1.1 Protocole LDAP.

LDAP (Lightweight Directory Access Protocol) est un protocole de communication standard pour accéder et modifier des services d'annuaire à distance. Il est couramment utilisé pour gérer des informations sur les utilisateurs, les groupes, les services et d'autres entités dans un environnement informatique. LDAP simplifie l'accès aux informations en les stockant dans un annuaire centralisé et en offrant une interface de recherche standardisée. Il est souvent utilisé pour l'authentification et l'autorisation des utilisateurs dans les systèmes informatiques et pour stocker des données sensibles telles que des mots de passe de manière sécurisée. LDAP offre également des fonctionnalités de sécurité avancées telles que l'authentification sécurisée et le contrôle d'accès basé sur les rôles et les groupes.

1.1.2 Service LLDAP.

LLDAP (Lightweight LDAP) est un serveur d'authentification léger offrant une interface LDAP simplifiée et intuitive pour l'authentification. Il s'intègre facilement avec divers backends, allant de KeyCloak à Authelia en passant par Nextcloud et bien d'autres encore.

Son interface utilisateur conviviale facilite la gestion des utilisateurs et permet à ces derniers de modifier leurs propres informations ou de réinitialiser leur mot de passe via e-mail.

LLDAP se concentre sur l'auto-hébergement et est spécifiquement conçu pour des serveurs utilisant des logiciels open source tels que Nextcloud, Airsonic, etc., qui ne prennent en charge que LDAP comme source d'authentification externe.

Bien qu'il ne fournisse pas toutes les fonctionnalités d'un serveur LDAP complet comme OpenLDAP, LLDAP est un système de gestion des utilisateurs léger, facile à installer, à gérer et à utiliser. Il est adapté à ceux qui veulent éviter les complexités de LDAP tout en profitant de ses avantages pour l'authentification.

Les données sont stockées par défaut dans une base de données SQLite, mais vous avez la possibilité d'utiliser MySQL/MariaDB ou PostgreSQL comme backend. De plus, si vous recherchez des fonctionnalités avancées telles que le support OAuth/OpenID ou un proxy inverse, vous pouvez installer d'autres composants comme KeyCloak ou Authelia et les configurer pour utiliser LLDAP comme source de vérité pour les utilisateurs via LDAP.

1.2 Configuration minimale.

Annuaire (<u>https://urlz.fr/pyaD</u>) :

- Processeur: 1 cœur
- RAM: 512Mo
- Espace disque : 10Go



2 Création du conteneur.

Dans le cadre du projet sandbox, l'outil de virtualisation qui a été retenue est Proxmox.

Vous pouvez installer LLDAP dans tout autre environnement de virtualisation tant que vous respectez la configuration minimale.

- 1. Je me connecte à mon proxmox.
- 2. Créer un conteneur.



3. Je renseigne le numéro du conteneur, le nom de l'hôte « SRV-LLDAP », le pool de ressource « SANDBOX-TRAINING », configuration du mot de passe. → Suivant.

Créer: Contene	eur LXC				\otimes
Général Mo	dèle Disques Processeur	Mémoi	re Réseau DN	IS Confirmation	
Nœud:	pve	\sim	Pool de	SANDBOX-TRAINING ×	~
CT ID:	101	$\hat{}$	ressources:		
Nom d'hôte:	SRV-LLDAP		Mot de passe.		
Conteneur non			de passe:	••••••	
privilégié:			Clef(s) SSH		
Imbriqué:			publique(s):		
			Charger le fichier	de clef SSH	

4. Je sélectionne le modèle de mon conteneur → suivant.

Créer: Co	ntene	ur LX	(C						\otimes
Général	Mod	èle	Disques	Processeur	Mémoire	Réseau	DNS	Confirmation	
Stockage:		stor	age		\sim				
Modèle:		deb	ian-11-stand	lard_11.7-1_am	d64 🗸				



5. J'alloue 10Go de stockage. → Suivant.

er	Créer: Co	nteneur L	хс						\otimes
	Général	Modèle	Disques Proc	cesseur	Mémoire	Réseau	DNS	Confirmation	e
l	rootfs	Û	Stockage:	local-lvr	n	\sim			1
			Taille du disque	10		\bigcirc			0
			(GIO):						g

6. J'alloue 1 cœur de processeur. → Suivant.

Créer: Co	nteneur L)	кс						\otimes
Général	Modèle	Disques	Processeur	Mémoire	Réseau	DNS	Confirmation	e
Cœurs:	1			\bigcirc				ר הייניייייייייייייייייייייייייייייייייי
								c

7. Je laisse la configuration par défaut → suivant.

Créer: Conteneur	LXC						\otimes
Général Modèle	Disques	Processeur	Mémoire	Réseau	DNS	Confirmation	e
Mémoire (MiB):	512		$\hat{}$				1
Espace d'échange (swap) (MiB):	512		\bigcirc				c g

8. Je renseigne le VLAN et les @IP, je décoche l'option pare-feu → Suivant.

Créer: Contene	eur LXC		\otimes
Général Moo	dèle Disques Processeur Mémo	ire Réseau E	ONS Confirmation
Nom:	eth0	IPv4: 💿 Statiq	ue ODHCP
Adresse MAC:	auto	IPv4/CIDR:	10.16.1.1/28
Pont (bridge):	vmbr0 ~	Passerelle (IPv4) [.]	10.16.1.14
Étiquette de VLAN:	1 0	IPv6: Statiq	ue ODHCP OSLAAC
Pare-feu:		IPv6/CIDR:	Aucun
		Passerelle (IPv6):	



9. Je rentre le nom de domaine et le DNS. → Suivant.

Créer: Contene	ur LXC						\otimes
Général Moo	lèle Disques	Processeur	Mémoire	Réseau	DNS	Confirmation	
Domaine DNS:	sandbox.local						ſ
Serveurs DNS:	8.8.8.8						

10. Je vérifie que toutes les informations sont correctes \rightarrow terminer.

Créer: Co	nteneur L	хс					(\otimes
Général	Modèle	Disques	Processeur	Mémoire	Réseau	DNS	Confirmation	
Key \uparrow		Value						
cores		1						
features		nesting	=1					
hostname	Э	SRV-LL	DAP					
memory		512						
nameserv	ver	8.8.8						
net0		name=	eth0,bridge=vm	br0,tag=1,ip=	10.16.1.1/28	3,gw=10	.16.1.14	
nodenam	e	pve						
ostempla	te	storage	vztmpl/debian	11-standard	11.7-1_amd	64.tar.zs	st	
pool		SANDE	30X-TRAINING					
rootfs		local-lv	m:10					
searchdo	main	sandbo	x.local					
ssh-publi	c-keys							
swap		512						
unprivileg	jed	1						-
Démarre	er après cré	ation						
							Avancé 🗌 Retour Termine	er
root@pam		VM 102 -	Détruire					



11. Le conteneur a été créé.

Task viewer: CT 1101 - Créer	\otimes
Sortie Statut	
Stopper	📩 Télécharger
WARNING: You have not turned on protection against thin pools running out of space. WARNING: Set activation/thin_pool_autoextend_threshold below 100 to trigger automatic extension of thin pools before they get full. Logical volume "vm-1101-disk-0" created. WARNING: Sum of all thin volume sizes (<1.04 TiB) exceeds the size of thin pool pve/data and the size of whole volume group (<222.57 Gi Creating filesystem with 2621440 4k blocks and 655360 inodes Filesystem UUID: 13e4f3d8-fcde-4ae7-9c5e-5d515a3eb398 Superblock backups stored on blocks: 32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632 extracting archive '/mnt/pve/storage/template/cache/debian-11-standard_11.7-1_amd64.tar.zst' Total bytes read: 490127360 (468MiB, 268MiB/s) Detected container architecture: amd64 Creating SSH host key 'ssh_host_rsa_key' - this may take some time done: SHA256:izlXXHGFYVrxGRhcankLGwksGMwjZO5absQWnddKp0 root@SRV-LLDAP Creating SSH host key 'ssh_host_ecdsa_key' - this may take some time done: SHA256:GfOHP9JXYxmq3GLeCAVVB3ugZlSJmP4a5yH45buPw8 root@SRV-LLDAP Creating SSH host key 'ssh_host_eda_key' - this may take some time done: SHA256:Fybq/YhMYhjKKC7YDEfnGTStvnfRYDKdm/Hm/zNSl8 root@SRV-LLDAP Creating SSH host key 'ssh_host_ed2519_key' - this may take some time done: SHA256:Fybq/YhMYhjKKC7YDEfnGTStvnfRYDKdm/Hm/zNSl8 root@SRV-LLDAP	IB).
TASK OK	

3 Installation LLDAP.

- 1. Je me connecte à ma ferme de serveur Proxmox.
- 2. J'allume le conteneur « SRV-LLDAP ».
- 3. Je me connecte au conteneur.

SRV-LLDAP login: root Password: Linux SRV-LLDAP 6.5.13-1-pve #1 SMP PREEMPT_DYNAMIC PMX 6.5.13-1 (2024-02-05T13:50Z) x86_64

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Thu Mar 7 10:40:12 UTC 2024 on tty1 root@SRV-LLDAP:~#

4. Test de l'accès à internet.

root@SRV-LLDAP:~# ping www.google.fr PING www.google.fr (142.250.179.67) 56(84) bytes of data. 64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=1 ttl=115 time=12.8 ms 64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=2 ttl=115 time=12.5 ms 64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=3 ttl=115 time=12.3 ms 64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=4 ttl=115 time=12.5 ms 64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=4 ttl=115 time=12.5 ms 64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=4 ttl=115 time=12.5 ms 64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=4 ttl=115 time=12.5 ms 64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=4 ttl=115 time=12.5 ms 7C ---- www.google.fr ping statistics ----4 packets transmitted, 4 received, 0% packet loss, time 3004ms rtt min/avg/max/mdev = 12.280/12.520/12.821/0.194 ms root@SRV-LLDAP:~# []

5. Je mets à jour les paquets.

Commande :

apt update && apt upgrade

```
root@SRV-LLDAP:~# apt update && apt upgrade
Hit:1 http://security.debian.org bullseye-security InRelease
Hit:2 http://deb.debian.org/debian bullseye InRelease
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease
Reading package lists... Done
Building dependency tree... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@SRV-LLDAP:~#
```



6. Ajout du dépôt LLDAP.

Commande :

echo 'deb http://download.opensuse.org/repositories/home:/Masgalor:/LLDAP/Debian_11/ /' | sudo tee /etc/apt/sources.list.d/home:Masgalor:LLDAP.list

root@SRV-LLDAP:~# echo 'deb http://download.opensuse.org/repositories/home:/Masgalor:/LLDAP/Debian_11/ /' | sudo t
ee /etc/apt/sources.list.d/home:Masgalor:LLDAP.list
deb http://download.opensuse.org/repositories/home:/Masgalor:/LLDAP/Debian 11/ /

7. Ajout du certificat SSL.

Commande:

curl -fsSL https://download.opensuse.org/repositories/home:Masgalor:LLDAP/Debian_11/Release.key | gpg -dearmor | sudo tee /etc/apt/trusted.gpg.d/home_Masgalor_LLDAP.gpg > /dev/null

root@SRV-LLDAP:~# curl -fsSL https://download.opensuse.org/repositories/home:Masgalor:LLDAP/Debian_11/Release.key
| gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/home Masgalor LLDAP.gpg > /dev/null

8. Je mets à jour les paquets et j'installe LLDAP.

Commande :

apt update && apt install lldap

9. Démarrage et activation du service LLDAP.

Commande :

Systemctl enable lldap

Systemctl start lldap

root@SRV-LLDAP:~# systemctl enable lldap
root@SRV-LLDAP:~# systemctl start lldap



4 Configuration LLDAP.

- 1. Je me connecte à ma ferme de serveur ProxMox.
- 2. J'allume la machine et je me connecte.
- 3. Je me rends dans /etc/lldap.

Commande :

cd /etc/lldap

4. J'ouvre le fichier de configuration : lldap_config.toml

Commande :

nano lldap_config.toml

4.1 Base DN for LDAP.

Cette section permet de modifier la racine du serveur LLDAP.

Par défaut la valeur est : ldap_base_dn = « dc=example,dc=com »

Je modifie la valeur par : ldap_base_dn = « dc=sandbox,dc=local »

```
## Base DN for LDAP.
## This is usually your domain name, and is used as a
## namespace for your users. The choice is arbitrary, but will be needed
## to configure the LDAP integration with other services.
## The sample value is for "example.com", but you can extend it with as
## many "dc" as you want, and you don't actually need to own the domain
## name.
Idap base dn = "dc=sandbox,dc=local"
```

4.2 Admin username.

Cette section permet de modifier le nom de l'utilisateur.

Dans notre cas de figure, nous n'avons pas besoin de le modifier.

Nous le décommentons juste pour assurer le bon nom de notre admin.

```
## Admin username.
## For the LDAP interface, a value of "admin" here will create the LDAP
## user "cn=admin,ou=people,dc=example,dc=com" (with the base DN above).
## For the administration interface, this is the username.
ldap_user_dn = "admin"
```



4.3 Admin email.

Cette section permet de modifier le mail administrateur.

Nous allons juste changer le FQDN (Full qualified Domain) pour qu'il corresponde à celui de notre domaine.



4.4 Admin password.

Cette section permet de modifier le mot de passe du compte administrateur.

Si vous souhaitez la valeur du mot de passe administrateur vous aurez juste à décommenter la ligne « ldap_user_pass » et remplacer la valeur de « Remplace_with_password ».



Une fois les modifications effectuer vous devez sauvegarder le fichier et redémarrer le service.

Commande : systemctl restart lldap.service



5 Interface web.

- 1. Je me connecte à une machine dans le même réseau local que mon Serveur LLDAP.
- 2. Je tape l'URL du serveur AD avec le port 1710.

http://@IP-SRV-AD:17170/login

LLDAP Username -Password も Login Forgot your password? 3. Je me connecte avec le compte « admin ». LLDAP 🕮 Users 📋 Groups 👤 admin 👻 💽 Dark mode User ID Email **Display name** First name **Creation date** Delete Last name admin Administrator 2024-03-07 \otimes ≗+ Create a user

4. Je créer un utilisateur à mon nom.

Create a user	
User name*:	nmaillet
Email*:	noah.maillet@sandbox.local
Display name:	Noah MAILLET
First name:	Noah
Last name:	MAILLET
Password:	
Confirm password:	



5. J'ajoute le compte que j'ai créé dans le groupe administrateur.

lldap_admin			
Group:	lldap_admin		
Creation date:	2024-03-07		
UUID:	b3e395e9-c260-35e9-8f98-6829938e9bc1		
Members			
User Id	Display name		
admin	Administrator	8	
nmaillet			

6. Je me déconnecte du compte administrateur et je me connecte avec mon nouveau compte.

LLDAP	忽 Users				nmaillet 👻 💽) Dark mode
User ID	Email	Display name	First name	Last name	Creation date	Delete
admin		Administrator			2024-03-07	8
nmaillet	noah.maillet@sandbox.local	Noah MAILLET	Noah	MAILLET	2024-03-07	8
온 Create a user						

Si vous avez suivi la procédure jusqu'au bout, vous devriez avoir ce résultat.



About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | <u>www.capgemini.com</u>



This document contains information that may be privileged or confidential and is the property of the Capgemini Group.

Company Confidential. Copyright © 2023 Capgemini. All rights reserved.