

# **FILINE BANQUE & ASSURANCE**

---

MISE EN PLACE D'UNE APPLICATION COTÉ INFRASTRUCTURE

ANCELIN  
DEQUEANT  
DUCLUZEAUD  
LAVANDEIRA

# SOMMAIRE

- OBJECTIF
- CONTRAINTES ET SOLUTIONS
- COMPETENCES MISES EN ŒUVRES
- REPARTITION DES TÂCHES
- SCHEMA PHYSIQUE ET LOGIQUE
- MISE EN PLACE
- FOURNITURE DE SERVICE / CONTINUITE DE SERVICE / SECURITE

# OBJECTIFS

- Créer l'infrastructure d'hébergement d'une application consultable via web et mobile.
- Niveau de sécurité très élevé : proposer des produits très sécurisés.
- Permettre aux clients de se connecter de n'importe où et d'accéder au service.

# CONTRAINTE ET SOLUTIONS

## CONTRAINTE

CONNEXIONS A DISTANCE SECURISEES & STOCKAGE DES DONNEES

## SOLUTIONS

- VPN : [OpenVPN](#) est gratuit et open source.
  - Autres solutions envisagées : Les VPN [propriétaires](#).
- Cloud : [ownCloud](#) est gratuit, totalement paramétrable, libre et très complet.
  - Autres solutions envisagées : [NextCloud](#) ou [Filezilla Server](#).

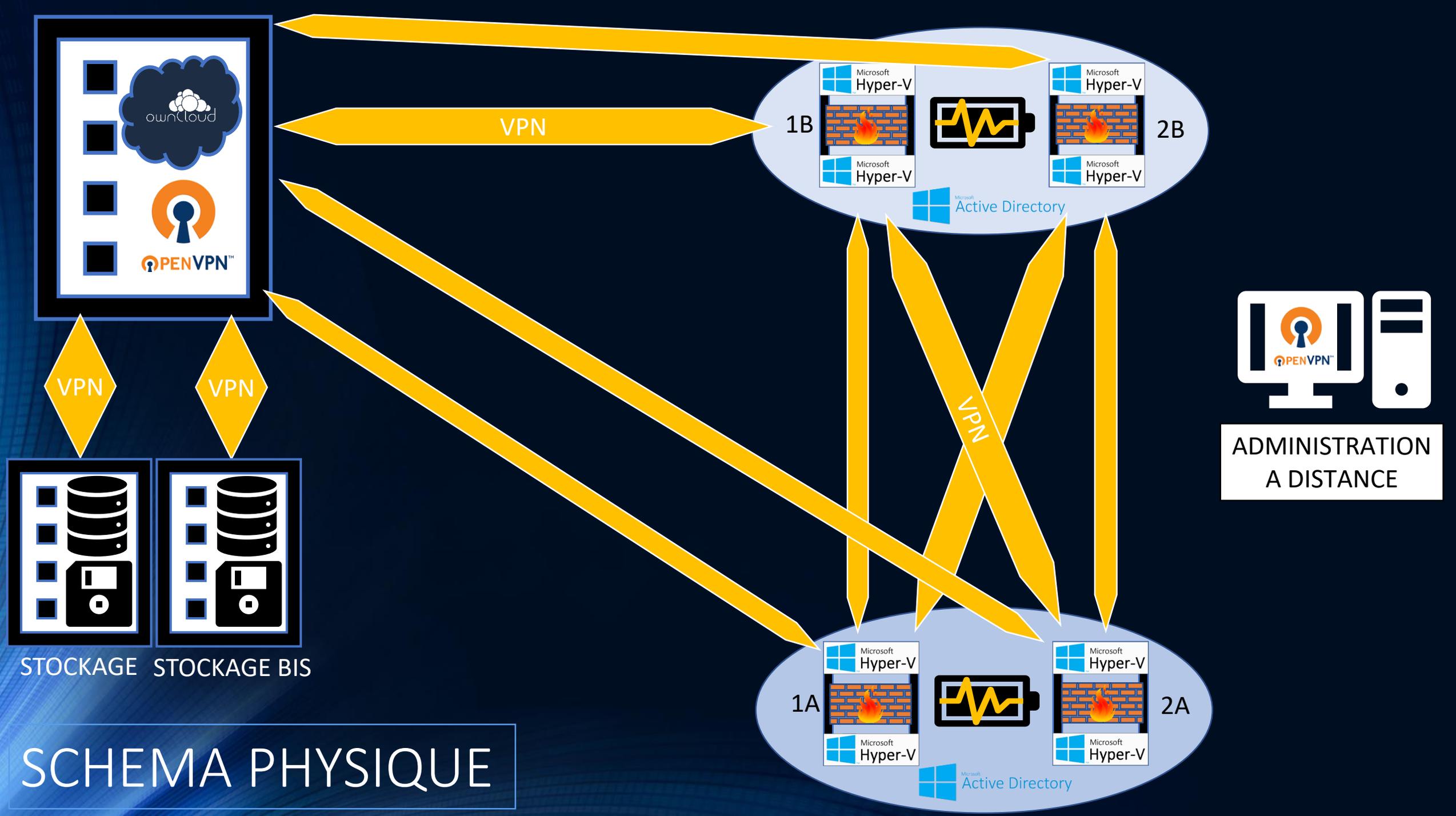
# COMPETENCES MISES EN OEUVRE

- Protocoles FTP / SSH / HTTP dans le cas d'ownCloud.
- Architecture réseau pour la réalisation de l'infrastructure.
- Mise en place de dispositifs de sécurité en coordination avec les applications.
- Gestion de domaine et d'utilisateurs.

# REPARTITION DES TÂCHES

- ANCELIN Maxime : Schéma & architecture du réseau.
- DEQUEANT Logan : Active Directory.
- DUCLUZEAUD Aston : Stockage avec ownCloud.
- LAVANDEIRA Julien : Connexions sécurisées par VPN.





ownCloud  
OPENVPN™

VPN

VPN

STOCKAGE STOCKAGE BIS

SCHEMA PHYSIQUE

VPN

1B

2B

Microsoft  
Active Directory

VPN

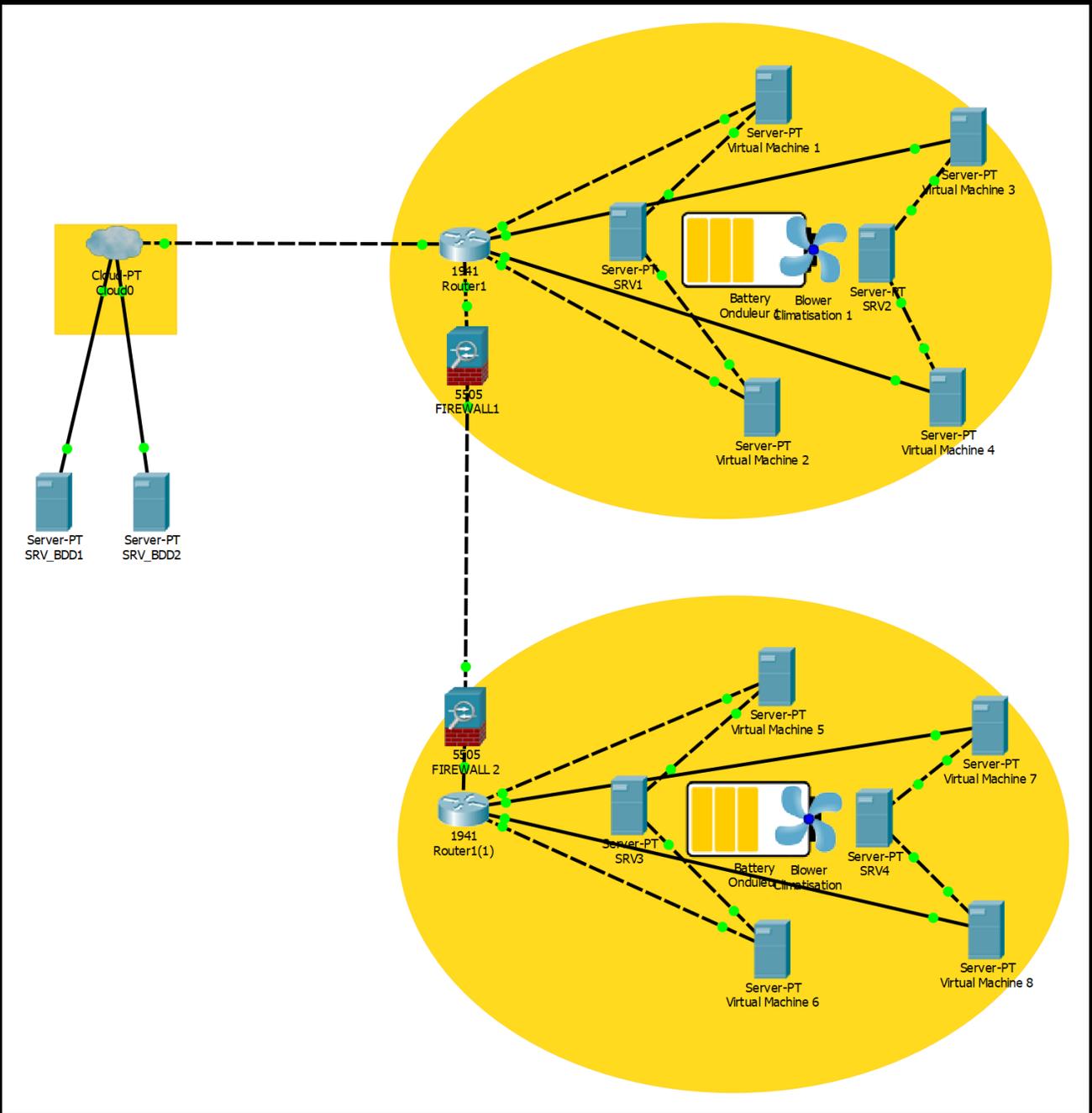
ADMINISTRATION  
A DISTANCE

1A

2A

Microsoft  
Active Directory

# SCHEMA LOGIQUE



# ACTIVE DIRECTORY



The screenshot shows the Active Directory console in Windows Server. The main window is titled "Domaines et approbations Active Directory". It displays a tree view on the left with "Filinebank.lan" expanded. The main pane shows a table of objects in the domain.

Nom	Type
Filinebank.lan	domainDNS

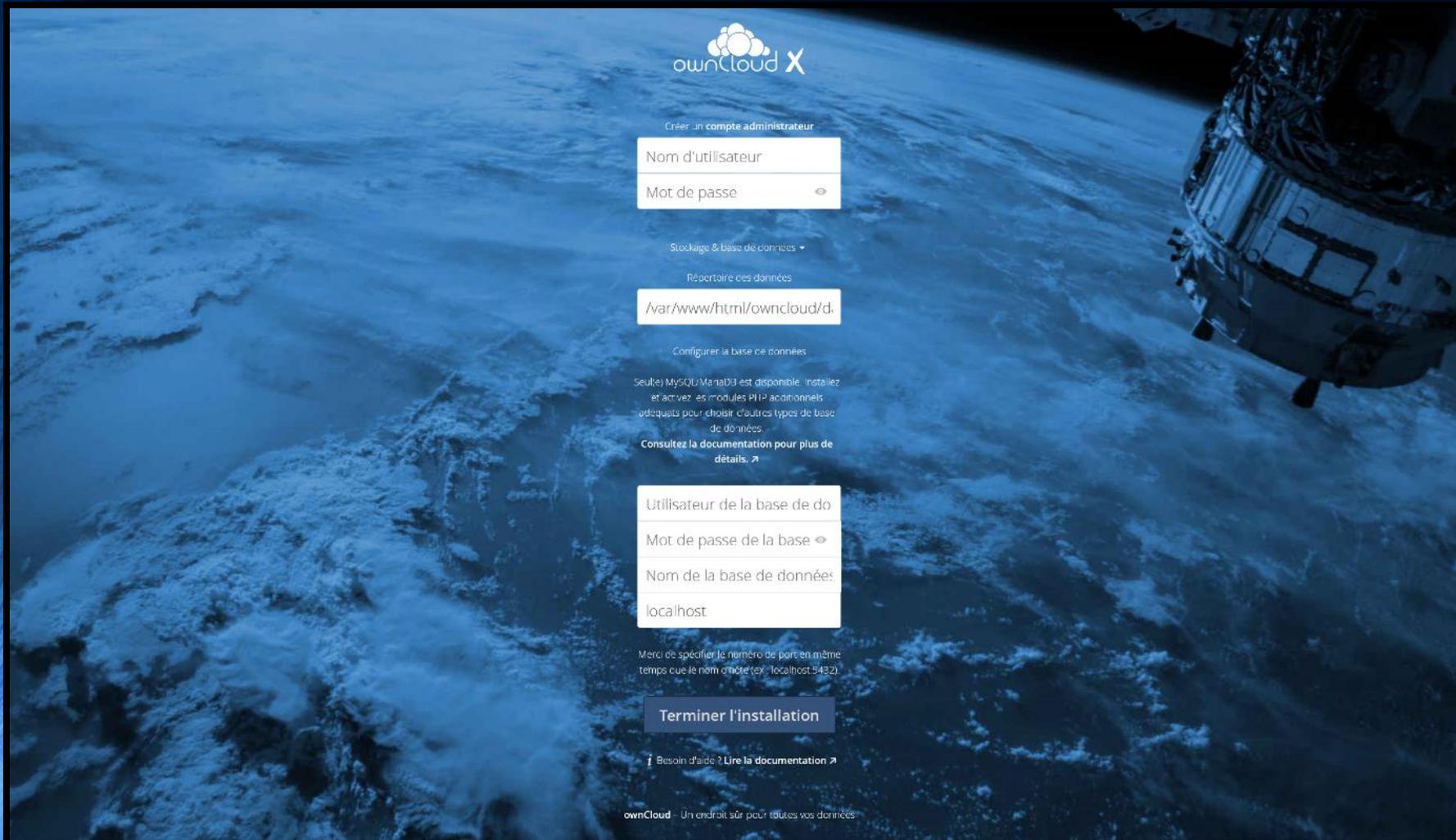
On the right, there is an "Actions" pane with "Autres actions" expanded.

Below the main window, a partial view of another window shows a list of objects:

Nom	Type	Description
Invités du d...	Groupe de séc...	Tous les invités du dom...
Logan LD. D...	Utilisateur	
Ordinateurs ...	Groupe de séc...	Toutes les stations de tr...
Propriétaires...	Groupe de séc...	Les membres de ce grou...
Protected Us...	Groupe de séc...	Les membres de ce grou...
Serveurs RA...	Groupe de séc...	Les serveurs de ce group...

# ownCloud | INSTALLATION

<https://download.owncloud.org/community/owncloud-10.0.10.tar.bz2>



The screenshot shows the ownCloud installation wizard interface. At the top, the ownCloud logo is displayed. Below it, the text "Créer un compte administrateur" is visible. The form includes fields for "Nom d'utilisateur" and "Mot de passe" (with a visibility toggle). A dropdown menu for "Stockage & base de données" is set to "Répertoire des données". The "Répertoire des données" field contains the path "/var/www/html/owncloud/d.". Below this, there is a section for "Configurer la base de données" with instructions: "Seule MySQL/MariaDB est disponible. Installez et activez les modules PHP additionnels adéquats pour choisir d'autres types de base de données. Consultez la documentation pour plus de détails." This section includes fields for "Utilisateur de la base de données", "Mot de passe de la base" (with a visibility toggle), and "Nom de la base de données" (containing "localhost"). A note at the bottom of this section says: "Merci de spécifier le numéro de port en même temps que le nom d'hôte (ex: 'localhost5432')." At the bottom of the form, there is a "Terminer l'installation" button and a link for "Besoin d'aide ? Lire la documentation". The footer of the page reads "ownCloud - Un endroit sûr pour toutes vos données".



# ownCloud | SOLUTION FTP

No.	Time	Source	Destination	Protocol	Length	Info
4	0.060630	10.20.144.151	10.20.144.150	FTP	106	Response: 220-QTCP at fran.csg.stercomm.com.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.060630	10.20.144.151	10.20.144.150	FTP	106	Response: 220-QTCP at fran.csg.stercomm.com.
6	0.275760	10.20.144.151	10.20.144.150	FTP	126	Response: 220 Connection will close if idle more than 5 minutes.
8	4.216600	10.20.144.150	10.20.144.151	FTP	81	Request: USER cdts3500
9	4.217350	10.20.144.151	10.20.144.150	FTP	91	Response: 331 Enter password.
11	7.639420	10.20.144.150	10.20.144.151	FTP	81	Request: PASS cdts3500
13	8.184000	10.20.144.151	10.20.144.150	FTP	95	Response: 230 CDTS3500 logged on.

# ownCloud | SOLUTION SSH

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1254 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=1444389 TSecr=0 WS=1
2	0.001690	192.168.0.1	192.168.0.2	TCP	74	23 → 1254 [SYN, ACK] Seq=0 Ack=1 Win=17376 Len=0 MSS=1448 WS=1 TSval=346979 TSecr=1444389
3	0.001741	192.168.0.2	192.168.0.1	TCP	66	1254 → 23 [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSval=1444389 TSecr=346979
4	0.013173	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150283	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150351	192.168.0.2	192.168.0.1	TCP	66	1254 → 23 [ACK] Seq=28 Ack=4 Win=32120 Len=0 TSval=1444404 TSecr=346980

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.1		TCP	74	1254 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=1444389 TSecr=0 WS=1
2	0.001690	192.1		TCP	74	23 → 1254 [SYN, ACK] Seq=0 Ack=1 Win=17376 Len=0 MSS=1448 WS=1 TSval=346979 TSecr=1444389
3	0.001741	192.1		TCP	66	1254 → 23 [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSval=1444389 TSecr=346979
4	0.013173	192.1		TELNET	93	Telnet Data ...
5	0.150283	192.1		TELNET	69	Telnet Data ...
6	0.150351	192.1		TCP	66	1254 → 23 [ACK] Seq=28 Ack=4 Win=32120 Len=0 TSval=1444404 TSecr=346980
7	0.150528	192.1		TELNET	69	Telnet Data ...
8	0.151908	192.1		TCP	66	23 → 1254 [ACK] Seq=4 Ack=31 Win=17376 Len=0 TSval=346980 TSecr=1444404
9	0.153602	192.1		TELNET	91	Telnet Data ...
10	0.153816	192.1		TELNET	130	Telnet Data ...
11	0.154904	192.1		TCP	66	23 → 1254 [ACK] Seq=29 Ack=95 Win=17312 Len=0 TSval=346980 TSecr=1444405
12	0.155418	192.1		TCP	66	23 → 1254 [ACK] Seq=29 Ack=95 Win=17312 Len=0 TSval=346980 TSecr=1444405
13	0.155496	192.1		TCP	66	23 → 1254 [ACK] Seq=29 Ack=95 Win=17312 Len=0 TSval=346980 TSecr=1444405
14	0.156474	192.1		TCP	66	23 → 1254 [ACK] Seq=29 Ack=95 Win=17312 Len=0 TSval=346980 TSecr=1444405
15	0.158758	192.1		TCP	66	23 → 1254 [ACK] Seq=29 Ack=95 Win=17312 Len=0 TSval=346980 TSecr=1444405
16	0.159498	192.168.0.2	192.168.0.1	TCP	66	23 → 1254 [ACK] Seq=29 Ack=95 Win=17312 Len=0 TSval=346980 TSecr=1444405

Display Filters...  
Display Filter Macros...  
Apply as Column Ctrl+Maj+I  
Apply as Filter  
Prepare a Filter  
Conversation Filter  
Enabled Protocols... Ctrl+Maj+E  
Decode As...  
Reload Lua Plugins Ctrl+Maj+L  
SCTP  
Follow  
Show Packet Bytes... Ctrl+Maj+O  
Expert Information

TCP Stream Ctrl+Alt+Maj+T  
UDP Stream Ctrl+Alt+Maj+U  
SSL Stream Ctrl+Alt+Maj+S  
HTTP Stream Ctrl+Alt+Maj+H

# ownCloud | SOLUTION SSH

The image shows a Wireshark interface with a packet capture named 'ch2.pcap'. The left pane shows a list of packets, with packet 14 selected. The right pane shows the 'Follow TCP Stream' view for 'tcp.stream eq 0', displaying the raw data of the selected packet. The data is a terminal session showing an SSH login attempt.

No.	Time	Source
1	0.000000	192.168
2	0.001690	192.168
3	0.001741	192.168
4	0.013173	192.168
5	0.150283	192.168
6	0.150351	192.168
7	0.150528	192.168
8	0.151908	192.168
9	0.153602	192.168
10	0.153816	192.168
11	0.154904	192.168
12	0.155418	192.168
13	0.155496	192.168
14	0.156474	192.168

```
.....!.."..'.....#..%..%.....!..".....P. ....".....b.....b.... B.  
.....".....'.....#..&..&..$..&..&..$.....#.....'.....9600,9600....#.bam.zing.org:  
0.0....'..DISPLAY.bam.zing.org:0.0.....xterm-color.....!....."  
OpenBSD/i386 (oof) (tty1)  
  
login: .."....."ffaakkee  
.  
Password:user  
.  
Last login: Thu Dec  2 21:32:59 on tty1 from bam.zing.org  
Warning: no Kerberos tickets issued.  
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999  
  
Welcome to OpenBSD: The proactively secure Unix-like operating system.  
  
Please use the sendbug(1) utility to report bugs in the system.  
Before reporting a bug, please try to reproduce it with the latest  
version of the code.  With bug reports, please try to ensure that  
enough information to reproduce the problem is enclosed, and if a  
known fix for it exists, include that as well.
```

# ownCloud | SOLUTION HTTP

```
Frame 1: 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits)
Ethernet II, Src: Apple_94:b1:0e (00:1b:63:94:b1:0e), Dst: Cisco_eb:e0:80 (00:d0:bc:eb:e0:80)
Internet Protocol Version 4, Src: 128.222.228.85, Dst: 128.121.146.100
Transmission Control Protocol, Src Port: 55872, Dst Port: 80, Seq: 1, Ack: 1, Len: 452
Hypertext Transfer Protocol
> GET /statuses/replies.xml HTTP/1.1\r\n
  User-Agent: CFNetwork/330\r\n
> Cookie: _twitter_sess=BAh7CDoJdXNlcjA6B2lkIiVmZGQ2ODc5MTMwMWFhOTFhMWExZDViZmQwMGEz%250A0WNkMyIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc2g6OQZsYXNo%250ASGFzaHsABjoKQHVzZWR7AA...
  Accept: */*\r\n
  Accept-Language: en-us\r\n
  Accept-Encoding: gzip, deflate\r\n
▼ Authorization: Basic dXNlcjRlc3Q6cGFzc3dvcmQ=\r\n
  Credentials: usertest:password
```

# OpenVPN | CONFIGURATION

```
root@vps634017:~# sudo wget http://swupdate.openvpn.org/as/openvpn-as-2.6.1-Debian9.amd_64.deb
--2019-01-07 14:53:25-- http://swupdate.openvpn.org/as/openvpn-as-2.6.1-Debian9.amd_64.deb
Resolving swupdate.openvpn.org (swupdate.openvpn.org)... 104.18.249.114, 104.18.252.114, 104.18.251.1
14, ...
Connecting to swupdate.openvpn.org (swupdate.openvpn.org)[104.18.249.114]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 35274332 (34M) [application/x-www-form-urlencoded]
Saving to: 'openvpn-as-2.6.1-Debian9.amd_64.deb'
```

```
openvpn-as-2.6.1-Debian9. 100%[=====>] 33.64M 11.8MB/s in 2.8s
```

```
2019-01-07 14:53:28 (11.8 MB/s) - 'openvpn-as-2.6.1-Debian9.amd_64.deb' saved [35274332/35274332]
```

```
root@vps634017:~# dpkg -i openvpn-as-2.6.1-Debian9.amd_64.deb
Selecting previously unselected package openvpn-as.
(Reading database ... 27242 files and directories currently installed.)
Preparing to unpack openvpn-as-2.6.1-Debian9.amd_64.deb ...
Unpacking openvpn-as (2.6.1-Debian9) ...
Setting up openvpn-as (2.6.1-Debian9) ...
```

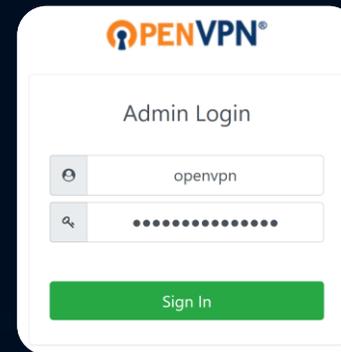
The Access Server has been successfully installed in /usr/local/openvpn\_as  
Configuration log file has been written to /usr/local/openvpn\_as/init.log

Please enter "passwd openvpn" to set the initial administrative password, then login as "openvpn" to continue configuration here: <https://51.77.156.126:943/admin>

To reconfigure manually, use the /usr/local/openvpn\_as/bin/ovpn-init tool.

```
+++++
Access Server Web UIs are available here:
Admin UI: https://51. . . :943/admin
Client UI: https://51. . . :943/
+++++
```

Beginning with OpenVPN AS 2.6.0 compression is disabled by default and on upgrades as security patch.



Active Configuration	
Access Server version:	2.6.1
Server Name:	51.
License Status:	2 devices
Current Active Users:	0
Authenticate users with:	local
Accepting VPN client connections on IP address:	ens3: 51.
Port for VPN client connections:	tcp/443, udp/1194
OSI Layer:	3 (routing/NAT)
Server Cipher:	AES-256-CBC
Clients access private subnets using:	NAT
Node:	vps63401

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
user1	No Default Group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
New Username	No Default Group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Require user permissions record for VPN access  Off

Save Settings

# OpenVPN | INTERFACE UTILISATEUR



**OPENVPN®**

Username  
user1

Password  
●●●●●●●●

Login

**OPENVPN®**

To download the OpenVPN Connect app, please choose a platform below:

- [OpenVPN Connect for Windows](#)
- [OpenVPN Connect for Mac OS X](#)
- [OpenVPN Connect for Android](#)
- [OpenVPN Connect for iOS](#)
- [OpenVPN for Linux](#)

Connection profiles can be downloaded for:

- [Yourself \(user-locked profile\)](#)

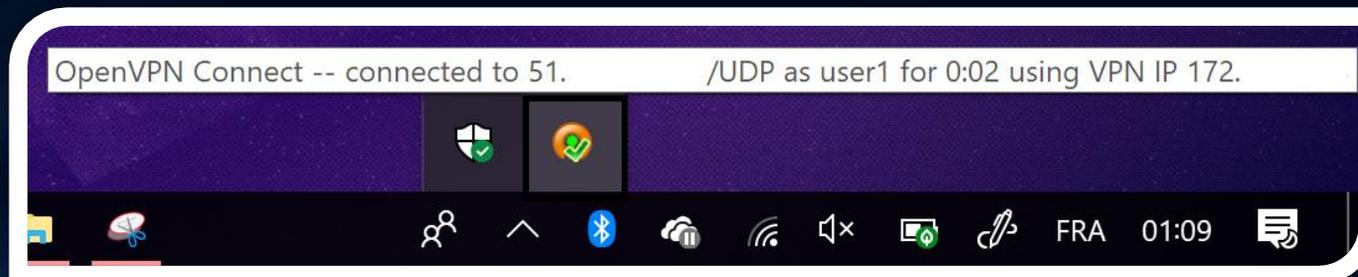
Connect

**OPENVPN™**

Server: 51.77.156.126

Username: user1

Password: ●●●●●●●●



# FOURNITURE DE SERVICE

- Point d'accès sur serveur web applicatif.
- Service de stockage des données (ownCloud).
- Connection à distance sécurisée avec OpenVPN.

# CONTINUITE DE SERVICE

- 2 VM par serveur.
- 4 Serveurs (en redondance).
- NAS pour éviter une perte de données (sauvegarde différentielle).
- Équilibrage de la charge serveur.
- 2 serveurs de stockage.
- Multiples pare-feu.
- Onduleur & batteries pour anticiper les pannes électriques.

# SECURITE | SOLUTIONS

- Filtrage par liste blanche de domaines sur ownCloud.
- Fail2Ban / Anti-Bruteforce pour éviter de deviner le mot de passe des comptes.
- Obliger l'utilisation d'un VPN pour accéder au service..
- Possibilité de relier ownCloud à son AD pour l'authentification.
- Ajout d'une politique des mots de passe.
- Utilisation de protocoles sécurisés (~~FTP/SSH~~ -> HTTPS).
- Sauvegardes différentielles des données.
- Chiffrement AES des données sur ownCloud.
- 2FA (2 Factor Auth) activable sur le cloud.
- Antivirus intégré au cloud.

MERCI DE VOTRE ATTENTION

—

DES QUESTIONS ?

