

# Dossier des Ouvrages Exécutés



1. Introduction	2
1.1. Contexte	3
1.2. Objectif du projet	3
2. Architecture système	3
2.1. Choix des systèmes d'exploitation	3
2.2. Dimensionnement	4
2.3. Tableau des machines virtuelles	5
2.4. Rôle de chaque service	5
2.5. Répartition des services	5
3. Conception de l'architecture réseau	6
3.1. Plan d'adressage IP	6
3.2. Choix des VLAN's	6
3.3. Schéma réseau	7
4. Mise en place des environnements	8
4.1. Proxmox	8
4.2. Installation	8
4.3. Configuration réseau	8
4.4. Stockage VM	8
5. Politique de Sécurité du Système d'Information	8
5.1. Modèle d'administration	8
5.2. Comptes "admin" vs "users"	9
5.3. GPO appliquées	9
5.4. Gestion du VPN	9
5.5. Politique de mot de passe	9
6. Active Directory	9
6.1. Installation	9
6.2. Arborescence du domaine	10
6.3. Création utilisateurs	10
6.4. GPO	10
6.5. Tests	10
7. UrBackup	11
7.1 La sauvegarde incrémentielle	11
7.2. La sauvegarde différentielle	12
7.3 Stockage sur le réseau interne	15

7.4 Test de restauration	15
8. GLPI	15
8.1. Fonctionnalités Clés	16
8.2. Architecture Technique	16
8.3. Base utilisateurs	18
8.4 Tests	19
9. Zabbix	19
10. FORTINET (FortiWifi 60D)	20
10.1 Installation	20
10.2 Configuration interface	21
10.3 VPN	21
10.4 Filtrage trafics	21
11. Nextcloud	21
12. Vaultwarden	22
13. High Availability (H.A) via FORTINET	22
14. Sauvegarde et plan de reprise d'activité (PRA)	24
14.1. Analyse des services critiques	24
14.2. Stratégie de sauvegarde	24
14.3. Stockage des backups	24
14.4. Automatisation	24
14.5. Test PRA :	24
15. Tests & validations	24
16. Gestion de projet (obligatoire si vous êtes plusieurs)	24
16.1. Organisation de l'équipe	25
16.2. Rôles et responsabilités	25
16.3. Planning Gantt	25
16.4. Difficultés rencontrées / Solutions apportées	25
16.5. Limites identifiées	25
16.5. Rétrospective	25
17. Annexes	25
Annexe 1 : logos + logiciels utilisés	26
Annexe 2 : Sources	27
Annexe 3 :	27
Annexe 4 : Capture d'écran / configuration du Switch	27
4.1 Création des VLANs	27
2.2 Configuration des ports	28

Annexe 5: Capture d'écrans GLPI	30
Architecture Technique	30

# 1. Introduction

## 1.1. Contexte

Dans le cadre du BTS Services Informatiques aux Organisations (option Solutions d'Infrastructure Système et Réseau), nous devons concevoir une infrastructure réunissant toutes les notions étudiées durant ces deux années.

Afin de pouvoir aborder le projet dans de bonnes conditions, nous avons été rassemblés en groupe (ici de 5 personnes).

**TechNova** est une entreprise de 5 salariés située en milieu urbain. Elle propose des services d'assistance, d'administration et réseaux informatique.

## 1.2. Objectif du projet

L'objectif du projet est de concevoir une solution d'infrastructure réseau, installer, tester et déployer une solution d'infrastructure réseau, exploiter, dépanner et superviser une infrastructure réseau.

# 2. Architecture système

## 2.1. Choix des systèmes d'exploitation

Nous avons choisi globalement les solutions OpenSource pour les raisons suivantes.

Les solutions open-source comme Proxmox, GLPI, Zabbix, OPNsense, Nextcloud, Vaultwarden et UrBackup offrent des avantages majeurs en termes de coût, flexibilité et sécurité pour les environnements IT.

*Elles surpassent souvent les alternatives propriétaires grâce à leur communauté active et leur transparence.*

Coûts Réduits: pas de licences payantes ni de frais récurrents, idéal pour budgets limités en PME ou admin sys. Les économies portent aussi sur les mises à jour et support communautaire gratuit.

Flexibilité Maximale: accès au code source permet personnalisations (ex. scripts Bash pour UrBackup) sans dépendre d'un éditeur. Parfait pour adapter à des besoins spécifiques comme VLAN ou RGD en réseau.

Sécurité Renforcée: examen par pairs identifie vite les vulnérabilités ; audits possibles sans portes dérobées. Pour UrBackup, déduplication et backups incrémentiels sécurisent sans interruption.

Innovation Rapide: communauté collabore pour évolutions constantes (ex. support multi-OS UrBackup). Indépendance vis-à-vis fournisseurs, avec interopérabilité native.

Proxmox un système d'exploitation basé sur Linux pour son utilisation optimale ainsi que pour son cout.

*TrueNas pour gérer nos données sur un serveur de stockage.*

10.16.140.1:8006 Serveur Proxmox pour le site distant accueillant un pc, AD,  
[CasaOS](#) (de Mathieu) pour le partage et la modification de fichier.

## 2.2. Dimensionnement

Le dimensionnement d'un projet informatique consiste à évaluer et définir les ressources nécessaires (matériel, humain, financier, temporel) pour répondre aux besoins fonctionnels et aux contraintes techniques, en optimisant coûts et performance.

Pour faire ce dimensionnement, nous avons répertoriés nos ressources disponibles sur nos différents équipements alloués.

Pour ce faire nous avons :

- 1 serveur Proxmox composé de

  - 16 Go de RAM

  - 1.5 To de stockage

  - Windows Server 4 Go RAM

  - Debian 1 (GLPI) 2 Go RAM

  - Windows Server (VEEAM) 8 Go

  - Debian (Zabbix) 2 Go

- 1 serveur : Truenas 10 To – XX Go de RAM

  - RAID 5

  - VaultWarden

  - Nextcloud

  - VM Client Test Windows 11 (WireShark)

  - GLPI

Exemple PPE :

Dimension	Calculé pour ton projet	Justification
Matériel	Serveur Ubuntu : 4 Go RAM, 2 vCPU	10 clients mixtes
Humain	1 élève (lead) + 1 tuteur	Solo labo
Disque	100 Go SSD (quota 50 Go/client)	Incrémentaux + images
Délai	3 semaines (install+tests+doc)	Rétroplanning fin mars

## 2.3. Tableau des machines virtuelles

Proxmox 1	10.16.140.1:8006
Proxmox 2	10.16.140.2:8006
Windows serveur ADDS	10.16.140.10
UrBackup	10.16.140.11
Windows Server de fichier	10.16.140.12
Windows Raccourci	10.16.140.13
Réplication AD	10.16.140.16
Debian Zabbix	10.16.140.30
Debian GLPI	10.16.140.31
Debian WireGuard VPN	10.16.140.51
Nextcloud	10.16.140.40
VaultWarden	10.16.140.41
Windows11-Client	10.16.140.45
Windows11-Client2	10.16.140.46
Docker	10.16.140.50
2eme DEBIAN GLPI	10.16.140.32
C clien	10.16.140.100-200
Passerelle (Fortinet)	10.16.140.254
Switch vlan 1	10.16.140.99

## 2.4. Rôle de chaque service

Texte à écrire ici

## 2.5. Répartition des services

Texte à écrire ici

# 3. Conception de l'architecture réseau

## 3.1. Plan d'adressage IP

<b>Proxmox 1</b>	<b>10.16.140.1:8006</b>
<b>Proxmox 2</b>	10.16.140.2:8006
<b>Windows serveur ADDS</b>	10.16.140.10
<b>UrBackup</b>	10.16.140.11
<b>Windows Server de fichier</b>	10.16.140.12
<b>Windows Raccourci</b>	10.16.140.13
<b>Debian Zabbix</b>	10.16.140.30
<b>Debian GLPI</b>	10.16.140.31
<b>Nextcloud</b>	10.16.140.40
<b>VaultWarden</b>	10.16.140.41
<b>Docker</b>	10.16.140.60
PC client	10.16.140.100-200
Fortinet	172.16.0.1

## 3.2. Choix des VLAN's

Les quatre VLANs suivants sont définis pour segmenter le réseau

VLAN ID	Nom	Réseau IP	Passerelle
100	SRV	10.16.140.0/24	172.16.0.2
20	WIFI	10.16.142.0/24	172.16.0.2
30	ADMIN-SI	10.16.143.0/24	172.16.0.2
40	PROD	10.16.144.0/24	172.16.0.2
50	DMZ	10.16.145.0/24	172.16.0.2

### 3.3. Schéma réseau

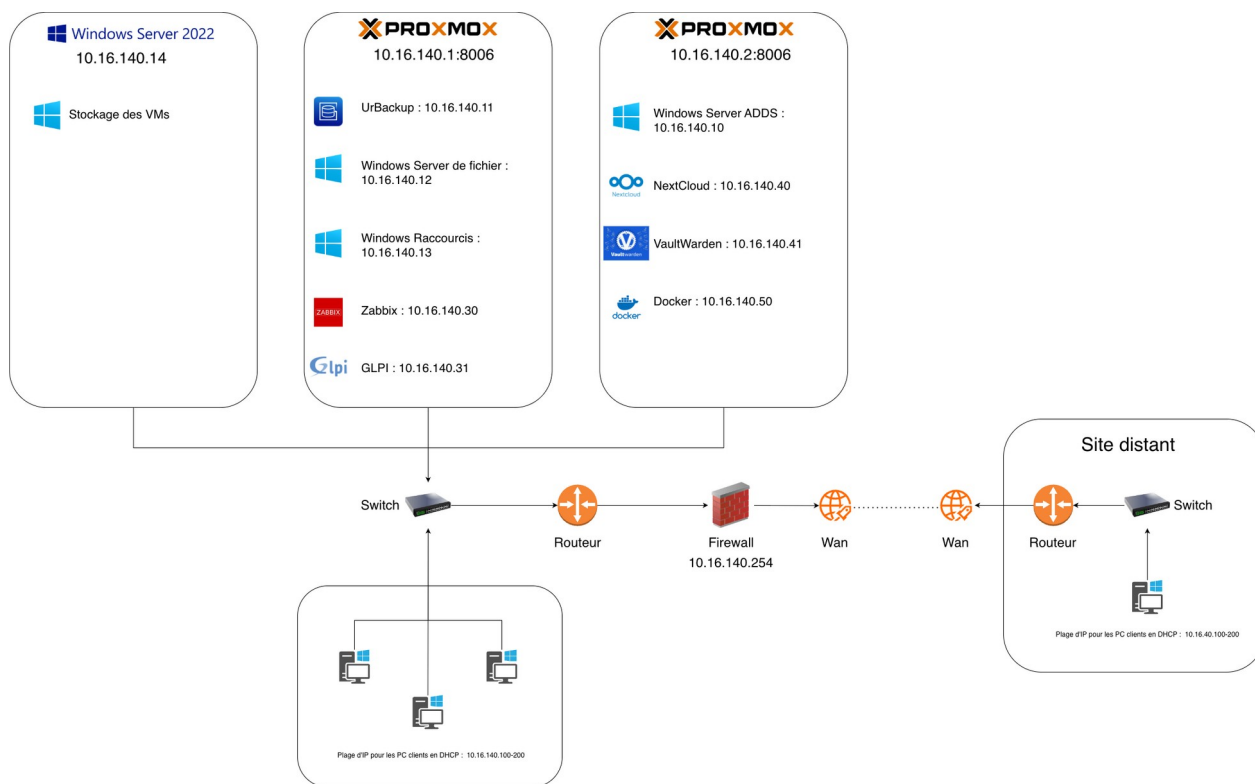


Schéma représentant notre infrastructure fait avec le logiciel draw.io

## 4. Mise en place des environnements

Pour chaque service, tu fais un chapitre clair séparé avec :

- Le rôle du service
- La procédure d'installation
- La configuration clé
- Les tests de validation

### 4.1. Proxmox

## 4.2. Installation

## 4.3. Configuration réseau

## 4.4. Stockage VM

# 5. Politique de Sécurité du Système d'Information

La Politique de Sécurité du Système d'Information (PSSI) est un document stratégique essentiel qui définit les objectifs, règles et moyens pour protéger les systèmes d'information d'une organisation contre les menaces.

Elle reflète la vision de la direction et s'appuie sur une analyse des risques pour assurer la confidentialité, l'intégrité et la disponibilité des données et actifs IT.

Une PSSI couvre généralement trois domaines principaux : organisationnels, de mise en œuvre et techniques:

- **Organisationnels** : Politique globale, organisation de la sécurité (rôles du RSSI), gestion des risques, cycle de vie du logiciel, assurance et certification.
- **Mise en œuvre** : Aspects humains (sensibilisation, formation), continuité d'activité (PCA/PRA), gestion des incidents, exploitation et aspects physiques.
- **Techniques** : Identification/authentification, contrôle d'accès (ACL, VLAN), journalisation, cryptographie (PKI), protection contre les signaux compromettants.

## 5.1. Modèle d'administration

En cours de création

## 5.2. Comptes “admin” vs “users”

En cours de création

## 5.3. GPO appliquées

En cours de création

## 5.4. Gestion du VPN

En cours de création

## 5.5. Politique de mot de passe

Mot de passe long: 12 caractères + chiffres

Réinitialisation de mot de passe: 90 jours

## 5.6. Cloisonnement réseau

## 5.7. Sécurisation des sauvegardes

## 5.8. Log et audit

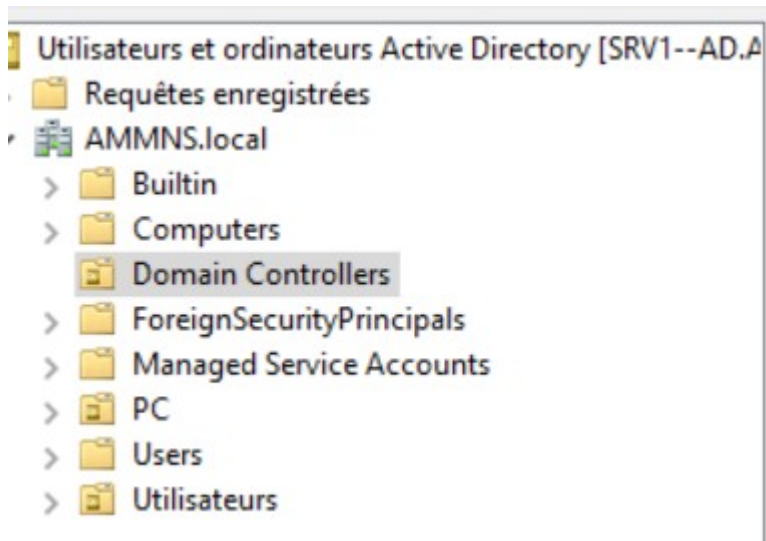
## 5.9. Politique de mise à jour

# 6. Active Directory

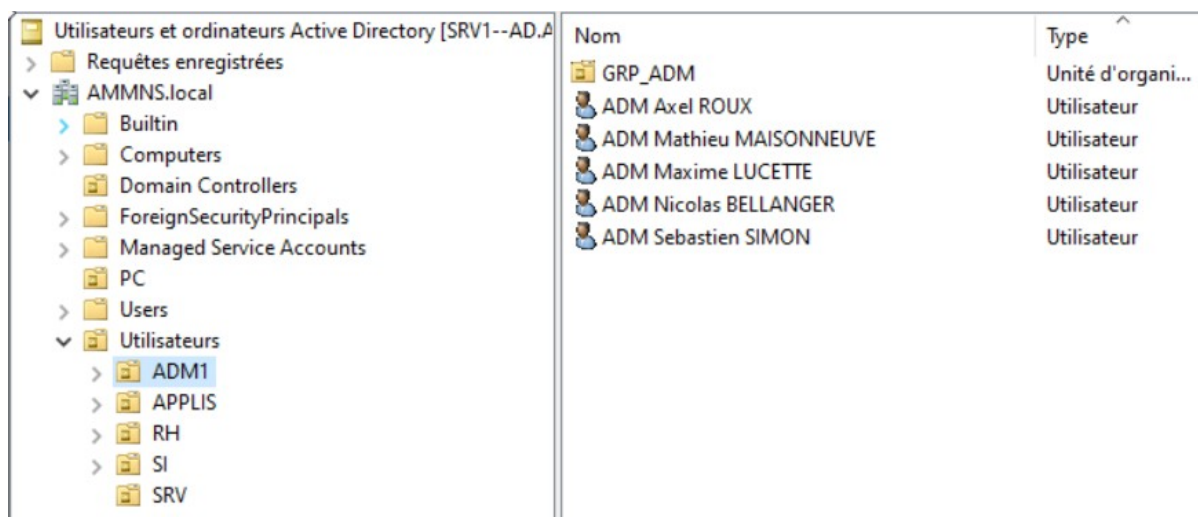
Active Directory (AD) est un service d'annuaire centralisé de Microsoft, intégré à Windows Server, qui gère les identités, authentifications et autorisations sur un réseau d'entreprise. Il stocke des informations sur les objets comme les utilisateurs, ordinateurs et ressources partagées, facilitant l'administration centralisée et la sécurité.

## 6.1. Installation

## 6.2. Arborescence du domaine



## 6.3. Création utilisateurs



## 6.4. GPO

Nom	État GPO	Filtre WMI	Modifié le	Propriétaire
Default Domain Controllers Policy	Activé	Aucun(e)	06/12/2025 10:54:02	Admins du domaine (AM...
Default Domain Policy	Activé	Aucun(e)	16/12/2025 13:31:28	Admins du domaine (AM...
GPO_LECTEUR_ADM	Activé	Aucun(e)	22/01/2026 16:51:52	Admins du domaine (AM...
GPO_SSL_ammns.local	Activé	Aucun(e)	24/01/2026 11:57:28	Admins du domaine (AM...
PSSI-CLEANING	Activé	Aucun(e)	16/12/2025 11:36:44	Admins du domaine (AM...
PSSI-SESSION	Activé	Aucun(e)	16/12/2025 11:29:24	Admins du domaine (AM...

## 6.5.

## Tests

## 7. UrBackup

UrBackup est la solution de sauvegarde client-serveur open-source que nous avons déployée.

Fonctionnalités Principales de la solution UrBackup.

UrBackup effectue des *sauvegardes complètes et incrémentielles* ultra-rapides (seuls secteurs/changements transmis), sur images disque (VHD/raw pour btrfs/ZFS) et fichiers, même en live sans Volume Shadow Copy sur Windows/Linux/macOS/FreeBSD. Les clients surveillent les changements en continu, assurant cohérence (PST Outlook, bases actives) et métadonnées préservées, avec filtres et exclusions personnalisables. Restauration facile via web, client, Explorer Windows ou USB bootable pour images, avec alertes email si backup manquant.

Interface et Administration

L'interface web (port 55414) montre le status clients, activités, statistiques, et permet des configurations (fréquences, groupes clients pour niveaux backup différents).

Également de gérer des archives (ex: garder 3 mois après 4 semaines), nettoyage auto espace disque, et backups distants sécurisés (chiffrés TLS/HTTPS). Notifications SMTP pour admins/users.

Installation Serveur/Client:

Sur Ubuntu/Debian: ajoutez PPA `ppa:uroni/urbackup`, `apt install urbackup-server`, définissez dossier backup (ex: `/mnt/backup`), démarrez via `systemd`. Clients: Windows (MSI auto-détection serveur), Linux (`apt install urbackup-client`), configurez via web ou CLI (`urbackupclientctl add-backupdir -x /etc`). Docker possible avec Traefik pour remote, testez régulièrement restaurations pour PRA.

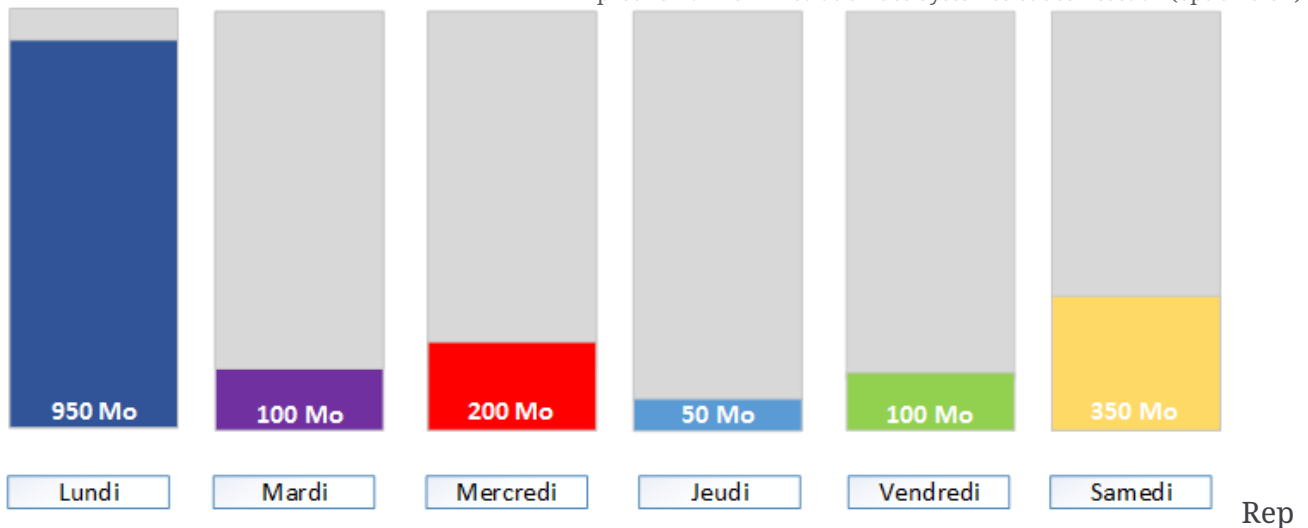
Intégration et Sécurité:

Flux locaux chiffrés (activez option), HTTPS pour internet; backups non chiffrés au stockage (ajoutez chiffrement externe). Intégrez à GLPI via inventaire (plugins comme FusionInventory détectent UrBackup) pour tickets DRP.

Cette solution gère les backups incrémentiels/images sur Windows/Linux/macOS via interface web (port 55414).

### 7.1 La sauvegarde incrémentielle

Comme rien ne vaut un simple schéma, le voici:



Rep

présentation d'une sauvegarde incrémentielle sur une semaine

Sur cet exemple je suis partie d'une sauvegarde sur une semaine.

Pour commencer, il va falloir réaliser en premier lieu une sauvegarde complète ici le lundi.

Ensuite, l'incrémentielle du mardi va se baser sur la précédente qui sera cette fois la complète en sauvegardant uniquement les nouveaux fichiers créés ou modifiés entre-temps.

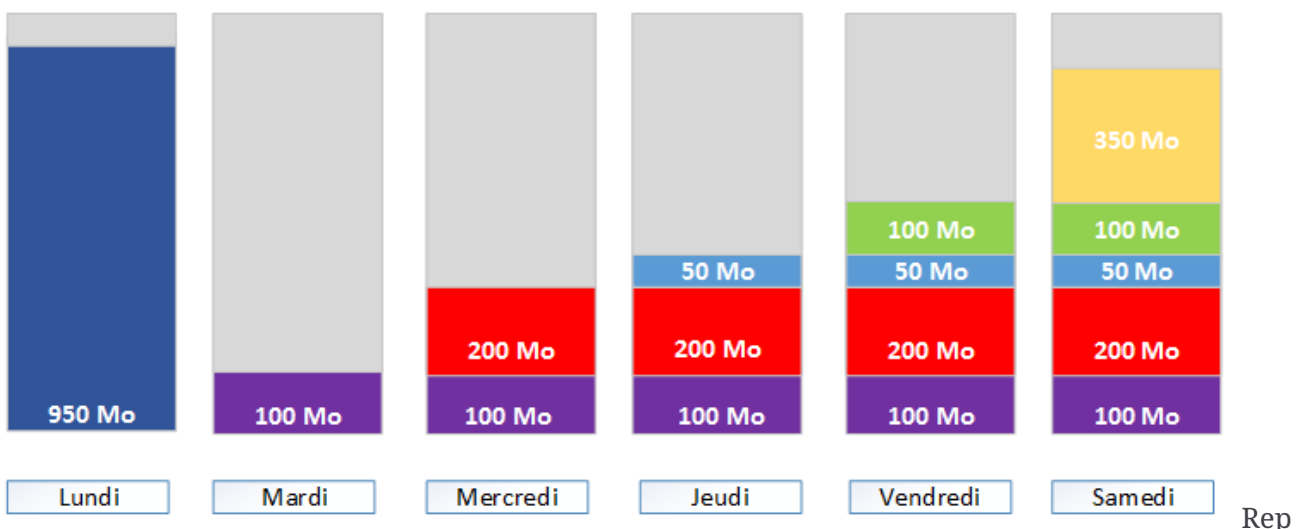
Mercredi, l'incrémentielle va se baser sur la précédente qui sera cette fois le mardi en sauvegardant uniquement les nouveaux fichiers créés ou modifiés entre-temps.

Et ainsi de suite jusqu'à la prochaine sauvegarde complète.

Si on souhaite récupérer l'ensemble de la sauvegarde de la semaine, il faudra restaurer tous les éléments du lundi au samedi ce qui prendra un certain temps, mais cela reste la méthode qui consomme le moins d'espace avec un total de 1750 Mo.

## 7.2. La sauvegarde différentielle

Exemple d'un schéma de sauvegarde différentielle :



Rep

présentation d'une sauvegarde différentielle sur une semaine

Le lundi, on démarre avec une sauvegarde complète. Et c'est à partir de cette sauvegarde que les différentielles se baseront chaque jour.

Mardi la différentielle va sauvegarder uniquement les nouveaux fichiers créés ou modifiés entre-temps d'après la complète.

|

Mercredi la différentielle va sauvegarder uniquement les nouveaux fichiers créés ou modifiés entre-temps d'après la complète.

Et ainsi de suite jusqu'à la prochaine sauvegarde complète.

### Statut de ton déploiement

Serveur : 10.16.140.11 (Debian/Ubuntu, dossiers /srv/urbackup).  
 Problèmes résolus : Client "En attente" → Pare-feu Windows ouvert (TCP 55413, UDP 35621-23), serveur internet vide dans config client.  
 Statuts attendus : "En ligne" (vert) → Indexation → Backup auto.

### Actions rapides:

- Vérifie interface : <http://10.16.140.11:55414> → Onglet **État**.
- Client Windows : Icône barre tâches verte ("Connecté").
- Test : Backup manuel → Restauration fichier pour PPE.

## 7.1.1 Installation

### Installation Serveur (Ubuntu/Debian)

Installez le serveur UrBackup via le PPA officiel pour une mise à jour automatique.

- Ajoutez le dépôt : `sudo add-apt-repository ppa:uroni/urbackup`
- Mettez à jour : `sudo apt update`
- Installez : `sudo apt install urbackup-server`

### Configuration Initiale Serveur

Protégez l'accès et paramétrez les bases.

- Créez un compte admin dans **Réglages > Utilisateurs** (nom et mot de passe fort).
- Définissez le type de sauvegarde (fichiers, images ou les deux) dans **Réglages > Général**.
- Configurez la fréquence (ex. incrémentielles quotidiennes), rétention et notifications SMTP.
- Excluez le dossier temporaire (urbackup\_tmp\_files) des scans antivirus.

### Installation Client Linux

Déployez le client sur les machines à sauvegarder.

- Exécutez : `TF=$(mktemp) && wget "http://IP_SERVEUR:55414/x?a=download_client&os=linux" -O $TF && sudo sh $TF; rm $TF`
- Éditez /etc/default/urbackupclient : mettez `INTERNET_ONLY=false` pour réseau local, et `RESTORE="server-confirms"` pour autoriser les restaurations.
- Redémarrez : `sudo systemctl restart urbackupclientbackend`

Ouvrez les ports 35621-35623 (UDP/TCP) vers le serveur (ex. via UFW : `ufw allow from IP_SERVEUR to any port 35621:35623/proto udp`).

### Ajout Client et Sauvegarde

Intégrez les clients via l'interface web.

- Cliquez **Ajouter un nouveau client**, entrez IP/hostname du client.

- Le client apparaît ; configurez dossiers (ex. /home, /etc), intervalles et filtres.
- Lancez une sauvegarde manuelle ; les suivantes sont incrémentielles.

### Restauration Données

Restaurez fichiers ou images simplement.

- Fichiers : Via web (**Sauvegardes > Client > Explorer > Restaurer**), ou client local.
- Image système : Téléchargez l'ISO UrBackup Restore, bootez dessus, sélectionnez client/image/disque cible.

Testez régulièrement les restaurations pour valider. Pour Windows client/serveur, téléchargez les MSI depuis [urbackup.org](http://urbackup.org).

## 7.3 Stockage sur le réseau interne

## 7.4 Test de restauration

# 8. GLPI

GLPI (Gestionnaire Libre de Parc Informatique) est une solution open-source gratuite d'aide à la gestion des services informatiques (ITSM), développée depuis 2003 par l'équipe Teclib'.

Cette solution open-source centralise l'inventaire automatique du parc (matériel/logiciel), le helpdesk/ticketing, la gestion des contrats/licences et le suivi des interventions.

### Gestion d'Inventaire:

GLPI excelle dans l'inventaire automatique ou manuel du parc IT, couvrant ordinateurs, serveurs, périphériques réseau, imprimantes, câblage, baies de données et même clusters. Vous pouvez référencer tous les éléments avec des détails précis (modèle, numéro de série, état, historique des interventions) via des plugins comme FusionInventory ou OCS pour une remontée automatique des données système. Cela offre une vue en temps réel des actifs, essentielle pour la haute disponibilité et les audits RGPD dans un contexte d'apprentissage comme le vôtre.

### Helpdesk et Tickets

Le module tickets distingue incidents et demandes via un catalogue de services, avec workflows personnalisables, assignations automatiques et priorisation (urgence, impact). Les utilisateurs finaux accèdent à une interface simplifiée gratuite pour créer des tickets, suivis d'un historique complet, validations et notifications par email paramétrables.

### Contrats et Fournisseurs:

GLPI gère contrats, garanties, licences et fournisseurs, avec rappels automatisés pour renouvellements et association aux actifs (tickets, parc). Définissez périodes de facturation, heures d'intervention et liens avec budgets, évitant les

expirations imprévues lors d'audits.  
 Utile pour tracer les partenaires et consommables (stockage, responsable technique), en lien avec vos pratiques de gestion d'infrastructure.

### Rapports et Tableaux de Bord:

Créez des dashboards personnalisés pour visualiser tickets en attente, statistiques (temps moyen de traitement, satisfaction), évolutions et top demandeurs. Les statistiques couvrent tickets, actifs, enquêtes de satisfaction et composants hardware, exportables en rapports. Cela facilite l'analyse pour des présentations en CFA ou rapports d'apprentissage, avec GANTT/Kanban pour projets.

### Administration et Sécurité:

Profils multiples (8 par défaut), groupes, entités et permissions fines via LDAP/SSO/Active Directory pour un contrôle d'accès granulaire. Moteur de règles pour automatisations (tickets, inventaire), dictionnaires pour fusionner données et actions planifiées (fréquence, notifications). Supporte bases de données, domaines, applicatifs, cartes SIM et documents uploadés, avec API REST pour intégrations (Zabbix, etc.).

#### Extensibilité

Architecture modulaire avec plugins pour supervision, flotte mobile ou automatisation, compatible Linux/Windows Server comme vos environnements. Gestion de projets, notes/rappels, domaines et énergie dans les baies pour une vue complète du data center.

Open-source et gratuit (sauf options cloud), parfait pour un étudiant en IT à Paris testant en labo personnel.

-----

## **8.1. Fonctionnalités Clés**

- *Inventaire : Scan auto via agents FusionInventory/OCS (PC, serveurs, imprimantes).*
- *Helpdesk : Tickets utilisateurs (incidents/demandes), suivi SLA ITIL.*
- *Admin : Utilisateurs LDAP/AD, multi-entités, rapports financiers.*
- *Plugins : Monitoring (Zabbix), réservation matériel, projet planning.*

## **8.2. Architecture Technique**

*Application web PHP/MySQL (MariaDB 11.4+ recommandé) sur Apache/Nginx. Interface responsive multi-langues (45 dont français), API REST pour intégrations. Parfait complément UrBackup pour PPE BTS SIO SISR : inventaire + sauvegardes.*

*Installation GLPI :*

*Version : Debian 13*

*Utilisation : SRV Lamp (GLPI)*

|

## Ressources allouées :

	Summary	Add	Remove	Edit	Disk Action	Revert
> Console	Memory					
Hardware	Processors	2 (1 sockets, 2 cores) [x86-64-v2-AES]				
Cloud-Init	BIOS	Default (SeaBIOS)				
Options	Display	Default				
Task History	Machine	Default (i440fx)				
Monitor	SCSI Controller	VirtIO SCSI single				
Backup	CD/DVD Drive (ide2)	local:iso/debian-13.1.0-amd64-netinst.iso,media=cdrom,size=783M				
Replication	Hard Disk (scsi0)	local-lvm:vm-105-disk-0,iosthread=1,size=32G				
Snapshots	Network Device (net0)	virtio=BC:24:11:50:38:3C,bridge=vibr0,firewall=1				
Firewall						
Permissions						

## Installation sur une VM

## Création d'un utilisateur :

User : glpi

Mdp : glpi

Root : MDPadmin44

## Préparation du serveur GLPI

Hostname : LSRV—GLPI

≡
Annuaire LDAP - Active Directory - AMMNS - ID 1

- Annuaire LDAP
- Tester
- Utilisateurs
- Groupes
- Informations avancées
- Réplicats
- Historique 4
- Tous

### Test LDAP Serveur : Active Directory - AMMNS

- 1
**Flux TCP**  
 Connexion à 10.16.140.10 sur le port 389 réussie
- 2
**Base DN**  
 Base DN "OU=ADM1,OU=Utilisateurs,DC=AMMNS,DC=local" configurée
- 3
**LDAP URI**  
 Vérification de l'URI LDAP réussie
- 4
**Connexion Bind**  
 Authentification réussie
- 5
**Chercher (50 premiers résultats)**  
 Recherche réussie (5 entrées trouvées)

**Annuaire LDAP**

- Tester
- Utilisateurs
- Groupes
- Informations avancées
- Réplicats
- Historique 4
- Tous

Nom:

Serveur par défaut:  Activé:

Serveur:  Port (par défaut 389):

Commentaires:

Filtre de connexion:

BaseDN:

Utiliser bind:

DN du compte (pour les connexions non anonymes):

Mot de passe du compte (pour les connexions non anonymes):   Effacer

Champ de l'identifiant:  Champ de synchronisation:

### 8.3. Base utilisateurs

Actions						
IDENTIFIANT	NOM DE FAMILLE	E-MAILS	TÉLÉPHONE	LIEU	ACTIVÉ	
<input type="checkbox"/>	glpi				Oui	
<input type="checkbox"/>	post-only				Oui	
<input type="checkbox"/>	tech				Oui	
<input type="checkbox"/>	normal				Oui	
<input type="checkbox"/>	glpi-system	Support			Oui	
<input checked="" type="checkbox"/>	adm.s.simon	SIMON			Oui	
<input checked="" type="checkbox"/>	adm.n.bellanger	BELLANGER			Oui	
<input checked="" type="checkbox"/>	adm.m.maisonneuve	MAISONNEUVE			Oui	
<input checked="" type="checkbox"/>	adm.m.lucette	LUCETTE			Oui	
<input checked="" type="checkbox"/>	adm.a.roux	ROUX			Oui	

20 lignes / pages De 1 à 10 sur 10 lignes

### 8.4 Tests

## 9. Zabbix

Zabbix est une plateforme open-source d'observabilité d'entreprise pour superviser les réseaux, serveurs, applications et cloud.

Collecte de Données:

Zabbix supporte push/pull pour tout : SNMP réseaux, agents OS (Linux/Windows), logs, DB, API/cloud (AWS/Azure), IoT, web/HTTP, GPUs NVIDIA, JSON/XML/CSV. Fréquences flexibles (1s min), deltas/JS preprocessing, bloc pour bande passante, throttling anti-duplicatas.

Agents auto-déploiement, proxies pour sites distants comme vos SSH remotes.

Détection et Alertes:

Seuils intelligents : anomalies ML, prédictions tendances, causes/symptômes, anti-flap, tags pour corrélation.

Gravités multiples, résolution auto, export realtime (Elastic/Splunk), suppression manuelle. Alertes multi-canaux (email/SMS/scripts).

Visualisation et Cartes:

Dashboards/maps interactives : realtime data, drag-drop, liens/scripts, nested/sub-maps, contextuel. Graphs, screencasts, problèmes hiérarchiques avec ACK/suppression.

### 7.3.1. Ajout hôtes

### 7.3.2 Supervision services

## 10. FORTINET (FortiWifi 60D)

Fortinet est spécialisé dans les pare-feux de nouvelle génération (NGFW) via FortiGate, avec une Security Fabric unifiée pour menaces avancées.

FortiGate combine hardware ASIC accéléré et FortiOS pour performances élevées (jusqu'à Tbps).

Le FortiWifi 60D est un appareil compact fanless (desktop) de la série FortiGate 60D (2013), intégrant firewall UTM et WiFi intégré pour les PME ayant un maximum de 50 utilisateurs.

Spécifications Techniques:

- **Interfaces** : 10 GE RJ45 (dont 8 switch internes), 2 WAN GE, WiFi AP intégré (SSID multiple WPA2-Enterprise).
- **Performances** : Firewall 1.5 Gbps (1518B), 800 Mbps (512B), 4µs latency, 2.2 Mpps, 500k sessions TCP, 3.2k new/sec, 5k policies.
- **VPN** : IPSec 500 Mbps (512B), 200 tunnels G2G, SSL-VPN 400 Mbps (200 users).
- **UTM** : IPS 600 Mbps, AV 400 Mbps, Threat Prot 300 Mbps, 1U rackmount option.
- **Hardware** : Dual-core 1.0GHz, 2GB RAM, 32GB flash, PoE out port5.

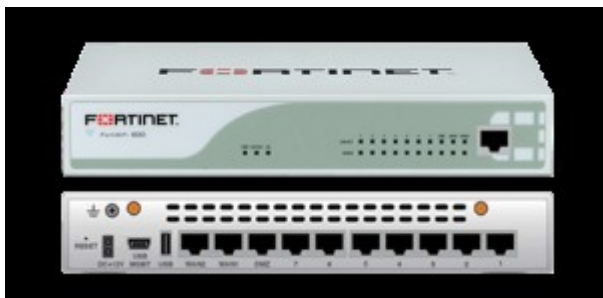
Fonctionnalités NGFW FortiGate:

Inspection approfondie paquets (DPI) contenu entier, IPS signatures mises à jour, anti-malware ATP, filtrage web/URL, antivirus réseau. SD-WAN intelligent (choix liens auto SLA), ZTNA/SASE pour accès zero-trust, VPN SSL/IPsec, inspection SSL/TLS (JA3 fingerprinting sans décryptage complet). UTM complet : DNS security (anti-tunneling), WAAP (WAF/API/bots), NDR/IDS IA corrélation.

Gestion et Orchestration:

FortiManager centralise configs/policies multi-sites, FortiAnalyzer logs/SIEM, VDOMs pour multi-tenants, HA clustering, templates Zero-Touch Provisioning. Interface web/CLI intuitive, GUI moderne pour VLAN/SD-WAN/WiFi (FortiAP/Switch).

## 10.1 Installation



## 10.2 Configuration interface

Etat	Nom	Membres	IP/Masque	Type d'Intrusion	Accès	Ref.
Physique (4)						
dmz			10.10.10.1 255.255.255.0	Physical Interface	PING HTTPS HTTP FMG-Access CAPWAP	1
wan1			10.16.27.8 255.255.255.0	Physical Interface	PING FMG-Access	1
wan2			0.0.0.0 0.0.0.0	Physical Interface	PING FMG-Access	0
Switch Logiciel (4)						
lan	internal, wifi ( SSID: AMMNS_DSI)		172.16.0.1 255.255.255.0	Software Switch (2)	PING HTTPS SSH HTTP FMG-Access CAPWAP	9

### Routes statiques

Destination	Passerelle	Interface	Commentaire
10.16.140.0/24	172.16.0.2	lan	SRV
10.16.141.0/24	172.16.0.2	lan	
10.16.142.0/24	172.16.0.2	lan	
10.16.143.0/24	172.16.0.2	lan	

## 10.3 VPN

## 10.4 Filtrage trafics

# 11. Nextcloud

Nextcloud est une plateforme open-source de collaboration et stockage cloud auto-hébergée, idéale pour vos partages sécurisés.

Elle centralise fichiers, calendrier, mail, chat et édition collaborative en temps réel, sans céder données à tiers.

### Stockage et Synchronisation:

Gestion fichiers intuitive : upload, recherche avancée, favoris offline, restauration versions/supprimés, partage liens protégés mot de passe/expiration. Clients desktop/mobile sync bi-directionnelle (photos/vidéos auto, exclusions), multi-comptes,

chiffrement

E2EE

client-side.

**Collaboration et Groupware:**

Édition docs temps réel (Text/Collabora/Code), Talk vidéo/chat E2EE (appels cryptés), Deck Kanban, Mail, Contacts/Calendrier DAV sync. File Drop pour uploads anonymes vers dossiers E2EE, boîtes partagées, modèles docs. VDR : recherche, versions, sécurité multicouche militaire.

**Sécurité et Admin:**

Chiffrement E2EE dossiers illimités (clé hardware/token), 2FA, audit logs, bruteforce protection, S3/Object storage backend. LDAP/AD/OIDC/SSO intégrés, groupes/users avancés. Conforme RGPD, historique versions, suppression distante.

**Installation Ubuntu/Debian**

Prérequis : Apache/Nginx, PHP 8.3+, MariaDB/PostgreSQL, Redis, apt install apache2 mariadb-server php libapache2-mod-php php-gd php-mysql php-curl php-xml php-zip php-mbstring php-intl redis-server.

Téléchargez tarball wget <https://download.nextcloud.com/server/releases/latest.tar.bz2>, extrait /var/www/html/nextcloud, chown www-data, config DB via occ. Web setup : admin/password, trusted\_domains ('localhost','IP','domaine'), HTTPS Let's Encrypt, occ maintenance:install.

**Intégrations Stack IT**

**GLPI** : stockez tickets/docs, inventoriez instances via plugins.  
**Zabbix** : template monitoring users/quota/lastlogin, alertes Talk.  
**UrBackup** : backup DB/fichiers Nextcloud (/var/www/html/data), templates Zabbix pour monitorer.

## 12. Vaultwarden

Vaultwarden est un serveur de gestionnaire de mots de passe open-source ultra-léger, compatible à 100% avec les clients Bitwarden officiels (apps mobiles, extensions navigateur, desktop). Écrit en Rust, c'est l'idéal pour self-hosting sur un Raspberry Pi, NAS ou VPS low-cost dans ton stack open-source BTS SIO (Nextcloud, GLPI, UrBackup).

**Avantages Clés:**

Vaultwarden consomme 10x moins de ressources que Bitwarden officiel (1 container Docker vs 10+, SQLite par défaut vs SQL Server), parfait pour labo perso ou PME. Chiffrement zero-knowledge client-side (AES-256), TOTP 2FA, partage sécurisé, audit logs, sans tracking/metadata vers Bitwarden Inc. Fonctionnalités "premium" gratuites (TOTP import, attachments illimités, emergency access).

## 13. High Availability (H.A) via FORTINET

La **haute disponibilité** ou **high availability (HA)** est un terme souvent utilisé en informatique, à propos d'architecture de système ou d'un service pour désigner le fait que cette architecture ou ce service a un taux de disponibilité convenable.

La disponibilité est aujourd'hui un enjeu important des infrastructures informatiques. Ces coûts se chiffrent en milliards d'euros à l'échelle d'un pays. L'indisponibilité des services informatiques est particulièrement critique dans le domaine de l'industrie, notamment en cas d'arrêt d'une chaîne de production.

Deux moyens complémentaires sont utilisés pour améliorer la disponibilité :

- la mise en place d'une infrastructure matérielle spécialisée, généralement en se basant sur de la redondance matérielle. Est alors créé un **cluster** de haute-disponibilité (par opposition à un cluster de calcul) : une grappe d'ordinateurs dont le but est d'assurer un service en évitant au maximum les indisponibilités ;
- la mise en place de processus adaptés permettant de réduire les erreurs, et d'accélérer la reprise en cas d'erreur. **ITIL** contient de nombreux processus de ce type.

La haute disponibilité (HA) Fortinet sur FortiGate/FortiWifi (comme 60D/60F) crée un cluster synchronisé pour failover transparent (sessions/VPN/policies), modes A-P (active-passive, recommandé PME) ou A-A (load-balance).

Requiert 2 unités identiques (switch direct ou VLAN isolé).

## 14. Sauvegarde et plan de reprise d'activité (PRA)

### 14.1. Analyse des services critiques

### 14.2. Stratégie de sauvegarde

### 14.3. Stockage des backups

### 14.4. Automatisation

### 14.5. Test PRA :

- Simulation panne AD
- Restauration VM depuis Urbackup
- Validation de l'intégrité

## 15. Tests & validations

### 15.1. Tableau test complet (DoD = Definition of Done)

| Service | Test | Résultat | OK/NOK |

### 15.2. Tests sécurité

## **16. Gestion de projet (obligatoire si vous êtes plusieurs)**

### **16.1. Organisation de l'équipe**

### **16.2. Rôles et responsabilités**

### **16.3. Planning Gantt**

### **16.4. Difficultés rencontrées / Solutions apportées**

### **16.5. Limites identifiées**

### **16.5. Rétrospective**

## **17. Annexes**

## Annexe 1 : logos + logiciels utilisés



**PROXMOX**



**UrBackup**



## Annexe 2 : Sources

Pour mener à bien notre projet, nous avons utilisé différentes sources.

Ces sources sont:

- Le site internet de [www.it-connect.fr](http://www.it-connect.fr) pour la configuration de GLPI, URBACKUP.
- Le site internet de [www.zabbix.fr](http://www.zabbix.fr) pour l'installation et la configuration.
- Le site internet de [www.fortinet.com](http://www.fortinet.com) pour la configuration du routeur.
- 
- 

## Annexe 3 :

### 2.2. Dimensionnement

## Annexe 4 : Capture d'écran / configuration du Switch

(Cisco IOS 2960 X- Series )

### 4.1 Création des VLANs

```
enable
configure terminal

vlan 10
name ADMIN-SI

vlan 20
name WIFI

vlan 30
name SRV

vlan 40
name PROD

Vlan 50
Name DMZ

exit
```

### 4.2 Configuration des ports

```
! --- GigabitEthernet1/0/1 --- ADMIN-SI (Access VLAN 10)
interface GigabitEthernet1/0/1
```

```
switchport mode access
switchport access vlan 10
no shutdown

! --- GigabitEthernet1/0/2 — WIFI (Access VLAN 20)
interface GigabitEthernet1/0/2
switchport mode access
switchport access vlan 20
no shutdown

! --- GigabitEthernet1/0/3-4 — Non assignés
interface range GigabitEthernet1/0/3 - 4
switchport mode access
no shutdown

! --- GigabitEthernet1/0/5 — Access VLAN 20
interface GigabitEthernet1/0/5
switchport mode access
switchport access vlan 20
no shutdown

! --- GigabitEthernet1/0/6 — Trunk vers le Fortinet
interface GigabitEthernet1/0/6
switchport mode trunk
switchport trunk allowed vlan 1,10,20,30,40
no shutdown

! --- GigabitEthernet1/0/7 à 1/0/12 — Trunk Proxmox / Windows Server
interface range GigabitEthernet1/0/7 - 12
switchport mode trunk
switchport trunk allowed vlan 10,30
no shutdown

! --- GigabitEthernet1/0/13 à 1/0/21 — PROD (Access VLAN 40)
interface range GigabitEthernet1/0/13 - 21
switchport mode access
switchport access vlan 40
```

```

no shutdown
! --- GigabitEthernet1/0/22 à 1/0/24 --- Trunk Proxmox / Windows Server
interface range GigabitEthernet1/0/22 - 24
switchport mode trunk
switchport trunk allowed vlan 10,30
no shutdown
end
write memory

```

## Annexe 5: Capture d'écrans GLPI

### Architecture Technique

Application web PHP/MySQL (MariaDB 11.4+ recommandé) sur Apache/Nginx. Interface responsive multi-langues (45 dont français), API REST pour intégrations. Parfait complément UrBackup pour PPE BTS SIO SISR : inventaire + sauvegardes.

Installation GLPI :

Version : Debian 13

Utilisation : SRV Lamp (GLPI)

Ressources allouées :

	Add	Remove	Edit	Disk Action	Revert
Summary					
>_ Console					
Hardware					
Cloud-Init					
Options					
Task History					
Monitor					
Backup					
Replication					
Snapshots					
Firewall					
Permissions					
Memory					
Processors					
BIOS					
Display					
Machine					
SCSI Controller					
CD/DVD Drive (ide2)					
Hard Disk (scsi0)					
Network Device (net0)					

Installation sur une machine virtuelle (VM):

Création d'un utilisateur :

User : glpi

Mdp : glpi

Root : MDPadmin44

Préparation du serveur GLPI

Hostname : LSRV—GLPI

Annuaire LDAP - Active Directory - AMMNS - ID 1

Annuaire LDAP

Tester

Utilisateurs

Groupes

Informations avancées

Réplicats

Historique 4

Tous

### Test LDAP Serveur : Active Directory - AMMNS

- Flux TCP**  
Connexion à 10.16.140.10 sur le port 389 réussie
- Base DN**  
Base DN "OU=ADM1,OU=Utilisateurs,DC=AMMNS,DC=local" configurée
- LDAP URI**  
Vérification de l'URI LDAP réussie
- Connexion Bind**  
Authentification réussie
- Chercher (50 premiers résultats)**  
Recherche réussie (5 entrées trouvées)

Annuaire LDAP

Tester

Utilisateurs

Groupes

Informations avancées

Réplicats

Historique 4

Tous

Nom: Active Directory - AMMNS

Serveur par défaut: Oui

Activé: Oui

Serveur: 10.16.140.10

Port (par défaut 389): 389

Commentaires:

Filtre de connexion: (&(objectClass=user)(objectCategory=person)((userAccountControl:1.2.840.113556.1.4.803:=2)))

BaseDN: OU=ADM1,OU=Utilisateurs,DC=AMMNS,DC=local

Utiliser bind: Oui

DN du compte (pour les connexions non anonymes): adm.s.simon@AMMNS.local

Mot de passe du compte (pour les connexions non anonymes):

Effacer

Champ de l'identifiant: samaccountname

Champ de synchronisation: objectguid

Supprimer définitivement

Sauvegarder

### 7.3.1 Base utilisateurs

Actions

IDENTIFIANT	NOM DE FAMILLE	E-MAILS	TÉLÉPHONE	LIEU	ACTIVÉ
<input type="checkbox"/> GL glpi					Oui
<input type="checkbox"/> PG post-only					Oui
<input type="checkbox"/> TE tech					Oui
<input type="checkbox"/> ND normal					Oui
<input type="checkbox"/> S glpi-system	Support				Oui
<input checked="" type="checkbox"/> AS adm.s.simon	SIMON				Oui
<input checked="" type="checkbox"/> AB adm.n.bellanger	BELLANGER				Oui
<input checked="" type="checkbox"/> AM adm.m.maisonneuve	MAISONNEUVE				Oui
<input checked="" type="checkbox"/> AL adm.m.lucette	LUCETTE				Oui
<input checked="" type="checkbox"/> AR adm.a.roux	ROUX				Oui

20 lignes / pages De 1 à 10 sur 10 lignes

- 102 (WSRV--Fichier)
- 103 (LSRV-ZABBIX)
- 104 (PC-CLIENT-TP)
- 105 (LSRV--GLPI)
- 111 (LSRV-URBACKUP)
- 112 (LSRV--Replication)
- localnetwork (pve)
- SA (pve)
- local (pve)
- local-lvm (pve)
- 109 (CT--NEXTCLOUD) ●●
    - 110 (CT-VAULTWARDEN) ●●●
    - 100 (WSRV1--AD)
    - 106 (Raccourcis)
    - 107 (LSRV--DOCKER) ●
    - 108 (WSRV-BACKUP)
    - localnetwork (pve2)
    - SA (pve2)
    - local (pve2)
    - local-lvm (pve2)

Phase	Tâches	M1	M2	M3	M4	M5	M6	M7	M8
<b>Cadrage &amp; Analyse</b>	Kick-off & recueil des besoins	■							
	Audit de l'existant	■							
	Analyse des risques	■	■						
<b>Conception</b>	Architecture réseau (LAN/WAN/WiFi)		■	■					
	Plan d'adressage IP & VLAN		■						
	Choix des équipements		■	■					
<b>Approvisionnement</b>	Commande matériel & licences			■	■				
	Réception & validation matériel				■				
<b>Configuration &amp; Préparation</b>	Configuration en lab			■	■				
	Rédaction documentation technique			■	■	■			
<b>Déploiement</b>	Installation physique					■			
	Configuration sur site					■	■		
	Migration progressive						■		
<b>Tests &amp; Recette</b>	Tests de performance						■		
	Tests de sécurité						■		
	Recette utilisateur							■	■
<b>Mise en production</b>	Go-live							■	
	Supervision renforcée							■	■
<b>Clôture projet</b>	Documentation finale								■
	Bilan & retour d'expérience								■

Phase	Tâches	M1	M2	M3	M4	M5	M6	M7	M8
<b>1. Audit &amp; Cadrage</b>	Analyse infra existante	■							
	Définition besoins & risques	■							
<b>2. Architecture &amp; Design</b>	Design cluster Proxmox		■						
	Plan réseau & VLAN		■	■					
	Plan PRA / Sauvegarde		■	■					
<b>3. Mise en place socle</b>	Configuration cluster			■					
	Stockage (local-lvm, réplication)			■	■				

Phase	Tâches	M1	M2	M3	M4	M5	M6	M7	M8
	Sécurisation accès			■	■				
<b>4. Déploiement Services Critiques</b>	AD (100)				■				
	Serveur fichiers (102)				■				
	UrBackup (108 + 111)				■	■			
	Docker (107)					■			
	Nextcloud (109)					■	■		
	Vaultwarden (110)					■			
	GLPI (105)					■			
	Zabbix (103)						■		
<b>5. Tests &amp; Validation</b>	Tests PRA / restauration						■		
	Tests charge & supervision						■		
<b>6. Mise en production globale</b>	Migration utilisateurs							■	
	Stabilisation & monitoring							■	■
<b>7. Documentation &amp; Clôture</b>	Documentation technique								■
	Bilan projet								■