# JM SUD INFORMATIQUE

*Solutions IT pour entreprises et collectivites*

# LIVRE BLANC TECHNIQUE B2B

## La bible des techniciens JMSI

*Mise en service - Exploitation - Depannage - Bonnes pratiques*

**Document interne - Diffusion restreinte aux collaborateurs JMSI**

Edition 2026 - version 1.0 - Reference : LBT-JMSI-2026-001

04 48 26 00 66 - contact@jmlab.eu - b2b.jmlab.eu

# Avertissement et confidentialite

Le present document constitue le referentiel technique interne de JM Sud Informatique (ci-apres << JMSI >>). Il est destine exclusivement aux collaborateurs techniques de JMSI : techniciens, ingenieurs systemes, ingenieurs reseau, chefs de projet, responsables infrastructure, ainsi que les apprentis et stagiaires sous couvert d'un encadrement permanent.

Toute diffusion a un tiers, qu'il soit client, partenaire, fournisseur ou editeur, est strictement interdite sans validation ecrite et nominative de la direction.

## Niveau de confidentialite : INTERNE - RESTREINT

- Lecture libre par tout collaborateur JMSI.
- Pas de transfert par e-mail externe non chiffre, pas d'impression hors locaux JMSI sans necessite.
- Si transmis sur cle USB ou disque externe, le support doit etre chiffre (BitLocker / VeraCrypt).
- La copie d'extrait a destination d'un client est possible mais doit etre anonymisee et validee par un responsable.

## Mise a jour du document

Ce livre blanc est un document vivant. Chaque procedure y est nominativement referencee (par exemple : SS 4.3.2 - Mise en service du NAS Synology DS923+) afin que tout retour d'experience puisse etre trace et integre dans la version suivante.

**Cycle de revision :**

- Revue mensuelle des fiches incident (a partir des tickets Dolibarr / GLPI) : ajustement des modes operatoires.
- Revue trimestrielle de la table des matieres : ajout/suppression de procedures, mise a jour des versions logicielles.
- Revue annuelle complete : refonte editoriale et publication d'une nouvelle edition (numerotee).

## Avertissement legal

Les marques, logos et noms de produits cites dans ce document sont la propriete exclusive de leurs detenteurs respectifs. Les modes operatoires y sont decrits a des fins pedagogiques internes : ils ne se substituent en aucun cas aux documentations officielles des editeurs. Le technicien JMSI doit toujours, en cas de doute, se referer aux documentations officielles, et solliciter le support N3 ou la direction technique avant toute action irreversible (formatage, ecrasement de configuration, reinitialisation usine, montee de version majeure).

# Sommaire

# Preface - La promesse JMSI

JMSI s'est construit sur une promesse simple : << Un seul interlocuteur pour toute l'informatique, des engagements chiffres, et un humain competent au bout du fil. >> Ce livre blanc en est la traduction technique. Il ne s'adresse pas a des clients ; il s'adresse a celles et ceux qui, sur le terrain ou a distance, transforment cette promesse en realite operationnelle - les techniciens JMSI.

La fidelisation d'un client se joue a 80 % sur la qualite technique de la mise en service, et a 20 % sur la rapidite de resolution lors des incidents. Une installation propre, documentee et securisee evite la quasi-totalite des incidents evitables. Un dossier de base bien tenu fait gagner des heures de diagnostic. Un test de restauration trimestriel reellement effectue nous protege contre les ransomwares - et nous protege aussi du litige avec le client.

Ce document rassemble en un seul corpus les modes operatoires, les configurations de reference, les commandes utiles, les pieges classiques et les bonnes pratiques pour chacun des produits et services commercialises par JMSI. Il ne remplace pas les documentations officielles des editeurs, ni la formation continue : il les organise pour le terrain.

## Qui doit lire ce livre blanc ?

- Les techniciens itinerants et techniciens d'astreinte.
- Les ingenieurs systemes et reseau intervenant chez nos clients.
- Les chefs de projet pilotant des deploiements multi-sites.
- Les apprentis et stagiaires (sous couvert de tutorat).
- Les commerciaux qui souhaitent comprendre techniquement ce qu'ils vendent.

## Ce que ce livre blanc n'est pas

- Ce n'est pas un argumentaire commercial : pour cela, voir le << Guide Commercial JMSI >>.
- Ce n'est pas un referentiel client : pour cela, voir les plaquettes officielles.
- Ce n'est pas un substitut a la documentation officielle des editeurs (Microsoft, Synology, Veeam, Bitdefender, etc.).
- Ce n'est pas fige : tout retour terrain valide par la direction technique a vocation a y etre integre.

# Comment lire ce livre blanc

Le livre blanc est organise en 7 parties, alignees avec les 12 offres commerciales JMSI et completees par un socle methodologique transversal et un volume d'annexes techniques. Chaque chapitre suit la meme structure standardisee :

| Section type | Contenu |
|---|---|
| **1. Perimetre et public** | Quelles offres JMSI sont concernees, quels intervenants sont impliques. |
| **2. References commerciales** | Codes Dolibarr (B2B_xxx), tarifs publics, contrats associes. |
| **3. Architecture cible** | Schema fonctionnel, composants materiels et logiciels, dimensionnement. |
| **4. Preparation et pre-requis** | Audit, recueil d'information, materiel a apporter, droits requis. |
| **5. Mise en service detaillee** | Procedure pas-a-pas avec commandes CLI, captures et configurations. |
| **6. Recette et validation** | Tests d'acceptation, livrables au client, signature PV. |
| **7. Exploitation courante** | Supervision, maintenance preventive, mises a jour, telesupport. |
| **8. Depannage** | Pannes typiques, arbres de decision, erreurs frequentes. |
| **9. Securite et conformite** | Bonnes pratiques cybersecurite, conformite RGPD/NIS2/CNIL. |
| **10. Desengagement / migration** | Procedure de sortie du contrat, restitution des donnees. |

Cette structure n'est pas dogmatique : certains chapitres l'adaptent a leur sujet (par exemple, le chapitre Videosurveillance accorde plus de place a la conformite CNIL ; le chapitre Telephonie consacre une section specifique a la portabilite). Mais en regle generale, le technicien sait ou chercher l'information dont il a besoin.

## Trois parcours de lecture conseilles

### *Parcours 1 - Nouveau technicien (4 semaines)*

Lire d'abord la Partie I (Chapitre 1) en entier : c'est le socle. Lire ensuite, dans l'ordre, les chapitres correspondant aux offres que vous allez reellement deployer en premiere mission (en general : Maintenance, Sauvegarde, Securite). Reporter Telephonie, Wi-Fi public, Videosurveillance et Salle de reunion a la phase 2.

### *Parcours 2 - Technicien experimente a la prise de poste JMSI (1 semaine)*

Lecture rapide de la Partie I (methodologie JMSI, dossier de base, ticketing, GTR). Survol des chapitres pour reperer les specificites JMSI par rapport aux pratiques habituelles : tarifs publics, codes Dolibarr, partenaires retenus, modeles de materiel.

### *Parcours 3 - Technicien en intervention ponctuelle*

Utiliser l'Index thematique (Annexe F) comme entree principale. Aller directement a la procedure recherchee. Verifier en marge la version logicielle de reference : si elle differe de votre contexte, demander confirmation a la direction technique avant action.

# Conventions et symboles

Le document utilise des conventions visuelles uniformes pour faciliter la lecture en intervention.

## Encadres

**INFO** Bloc INFO - Contexte, rappel theorique, ou precision utile mais non bloquante.

**ATTENTION** Bloc ATTENTION - Etape a risque, a executer avec controle. Une erreur ici peut occasionner une indisponibilite.

**CRITIQUE** Bloc CRITIQUE - Action irreversible ou impactant la securite/donnees. Validation N2/N3 requise.

**BONNE PRATIQUE** Bloc BONNE PRATIQUE - Recommandation issue du retour d'experience JMSI ou d'un standard reconnu.

**ASTUCE TERRAIN** Bloc ASTUCE TERRAIN - Truc et astuce concret, raccourci, methode rapide.

## Code et commandes

Les blocs suivants representent des commandes ou des fichiers de configuration. La police monospace, le filet bleu et le fond gris-clair les distinguent du texte courant.

```
# Linux - Affichage de la table de routage
ip route show

# Windows - Affichage de la table de routage
route print

# PowerShell - Equivalent moderne
Get-NetRoute | Format-Table
```

## Tableaux

Les tableaux recapitulatifs sont a fond bleu en en-tete, bandes alternees en gris-tres-clair pour la lisibilite.

| Champ | Convention |
|---|---|
| **Tarifs HT** | Tous les tarifs cites sont publies, hors taxes. |
| **Codes produits** | Format Dolibarr B2B_XXX_NN (categorie + numero). |
| **Versions logicielles** | Version de reference pour l'annee 2026, a valider avant deploiement. |
| **Niveaux d'intervention** | N1 (technicien), N2 (technicien senior), N3 (ingenieur), Direction technique. |

## Niveau de difficulte des procedures

| Symbole | Niveau | Profil minimum requis |
|---|---|---|

| | | |
|---|---|---|
| **[1]** | Standard | Tout technicien JMSI forme. |
| **[2]** | Avancee | Technicien senior ou ingenieur N2. |
| **[3]** | Expert | Ingenieur N3 ou Direction technique. Preparation et validation prealable obligatoires. |

## Termes JMSI a connaitre

| Terme | Signification |
|---|---|
| **Dossier de base** | Referentiel client unique : materiel, acces, contacts, contrats, plan de sauvegarde, plan PRA. |
| **GTR** | Garantie de Temps de Retablissement contractuel JMSI : 8 heures ouvrees. |
| **GTI** | Garantie de Temps d'Intervention : prise en compte sous 4 heures ouvrees. |
| **PV de mise en service** | Proces-verbal signe client a la livraison, attestant la conformite de la prestation. |
| **Audit initial** | Pre-vente technique gratuite, conduisant a un rapport et un devis. |
| **Astreinte** | Permanence technique hors heures ouvrees (option payante par contrat). |
| **RAS** | Rapport d'activite systeme, mensuel pour les contrats > 5 postes. |

# PARTIE I

# Methodologie et socle commun du technicien JMSI

# Chapitre 1 - Fondations : dossier de base, processus, outils, GTR

## 1.1 Perimetre et public

Ce chapitre est le pre-requis a tous les autres. Il decrit la maniere dont JMSI travaille au quotidien, independamment de l'offre commerciale concernee : structure du dossier client, outils internes, processus d'intervention, niveaux de support, GTR/GTI, traitement d'incident, qualite des livrables. Tout technicien JMSI - itinerant ou sedentaire - est tenu d'en appliquer integralement les regles.

> **BONNE PRATIQUE** Avant la premiere mission terrain : lire ce chapitre en entier (1 a 2 heures), puis le relire en revue mensuelle pendant les 3 premiers mois. C'est la base de la promesse JMSI.

## 1.2 Le dossier de base : pierre angulaire de la fidelisation

Chaque client JMSI dispose d'un << dossier de base >> unique, centralise, vivant, tenu a jour apres chaque intervention. Sans dossier de base : pas de delegation possible entre techniciens, pas de GTR tenable, pas de continuite de service. Avec un dossier de base bien tenu, n'importe quel technicien JMSI peut intervenir sur n'importe quel client en 5 minutes.

### 1.2.1 Localisation et arborescence

Le dossier de base est stocke sur le NAS interne JMSI dans l'arborescence suivante. Il est egalement indexe dans Dolibarr (fiche tiers) et dans GLPI (entite client). Aucune copie locale n'est autorisee : seul le NAS fait foi.

```
/clients/
  <CODE_CLIENT>_<NOM_COMMERCIAL>/
    00_administratif/       # contrats, devis signes, RIB, KBis, RGPD
    01_dossier_de_base/     # FICHE PRINCIPALE (ce chapitre)
    02_inventaire_parc/     # tableurs / exports GLPI
    03_schemas_reseau/      # Visio/draw.io + exports PDF
    04_acces_credentials/   # CHIFFRE - secrets via Bitwarden, jamais en clair ici
    05_sauvegardes_pra/     # plan, journaux, rapports de tests
    06_securite/            # politique, EDR, journaux audit
    07_telephonie/          # plan numerotation, exports PBX
    08_videosurveillance/   # plan d'implantation, registre RGPD
    09_wifi/                # site survey, configurations Omada/UniFi
    10_interventions/       # PV, comptes-rendus, photos avant/apres
    11_facturation/         # consommation contractuelle
    99_archives/            # > 3 ans, lecture seule
```

### 1.2.2 Contenu de la fiche principale (01_dossier_de_base)

La fiche principale est un document Word standardise, mis a jour a chaque visite. Elle compte 10 sections obligatoires.

| Section | Contenu obligatoire | Source |
|---|---|---|
| **1. Identite** | Raison sociale, SIRET, code APE, | Dolibarr |

| | | |
|---|---|---|
| | contact principal, contact technique, contact comptable, horaires, adresse(s) | |
| **2. Contrats** | Liste des contrats actifs (Maintenance, Hebergement, Sauvegarde, Securite, etc.) avec dates de debut/fin et numero | Dolibarr |
| **3. Architecture** | Schema reseau a jour (1 page A3 max), repartition VLAN, plan IP, fournisseur d'acces Internet, IP fixe(s) | Visio |
| **4. Inventaire** | Postes, serveurs, NAS, switches, routeurs, imprimantes : numero de serie, adresse MAC, IP, OS, version | GLPI |
| **5. Acces** | URL administration (firewall, switch, NAS, PBX, hyperviseur, AD) + reference au coffre Bitwarden | Bitwarden |
| **6. Sauvegarde** | Plan 3-2-1 du client : sources, destinations, retentions, planning, dernier test reussi | Plan PRA |
| **7. Securite** | EDR deploye, NGFW, MFA, politique mot de passe, cartographie des acces externes, registre RGPD | Audit |
| **8. Telephonie** | PBX/operateur, plan de numerotation, SDA, postes IP, mobile | Fiche telephonie |
| **9. PRA** | Procedure formelle de reprise d'activite : RTO, RPO, etapes, contacts, validation derniere | Plan PRA |
| **10. Notes** | Histoire technique, pieges connus, preferences client, derniere intervention | Tickets |

**ATTENTION** Le dossier de base ne contient JAMAIS de mots de passe en clair, sur aucun support. Tous les secrets sont stockes dans Bitwarden (collection nominative client) et le dossier de base ne porte que la reference de l'identifiant Bitwarden (par exemple : bw://JMSI/CLIENT_ABCD/firewall_admin).

### 1.2.3 Cycle de mise a jour

Le dossier de base est mis a jour systematiquement apres chacun des evenements suivants. La mise a jour fait partie integrante de la mission ; elle n'est pas optionnelle.

- Mise en service initiale : le technicien remet un dossier de base complet et un PV.
- Toute intervention modifiant la configuration : reseau, securite, sauvegarde, AD, telephonie.

- Tout changement materiel : ajout/suppression de poste, serveur, peripherique reseau.
- Tout changement de personnel cote client (contact technique, dirigeant).
- Une fois par an minimum : revue annuelle qualite (au moment de l'audit annuel inclus dans le contrat de maintenance).

**BONNE PRATIQUE** Reflexe technicien : a la fin de chaque intervention, on consacre 10 minutes a metre a jour le dossier de base. Un dossier de base obsolete coute 10 fois ce temps a la prochaine intervention.

## 1.3 Outils internes JMSI

JMSI s'appuie sur un parc d'outils internes que tout technicien doit maitriser. Cette section presente leur perimetre fonctionnel ; chaque chapitre concerne (Maintenance, Sauvegarde, etc.) detaille leur usage operationnel. Les acces sont fournis lors de l'integration du technicien.

| Outil | Role | URL interne | Reference dans le livre blanc |
|---|---|---|---|
| **Dolibarr** | ERP/CRM JMSI : tiers, devis, contrats, factures, tickets | erp.jmlab.eu | Chap. 13 (deploiement client) |
| **GLPI** | Inventaire parc client + helpdesk niveau 1 | glpi.jmlab.eu | Chap. 1 sect. 1.4 |
| **Bitwarden** | Coffre-fort de mots de passe organisation + clients | vault.bitwarden.com | Chap. 5 sect. 5.7 |
| **RustDesk Server** | Telesupport et acces poste client (alternative AnyDesk/TeamViewer) | rd.jmlab.eu | Chap. 2 sect. 2.6 |
| **TacticalRMM** | Supervision/RMM postes et serveurs : alertes, scripts, patch | rmm.jmlab.eu | Chap. 2 sect. 2.5 |
| **Nextcloud JMSI** | Espace documentaire client (GED) et echange de fichiers chiffre | cloud.jmlab.eu | Chap. 3 sect. 3.5 |
| **Mailcow** | Mail JMSI + hebergement mail client | mail.jmlab.eu | Chap. 3 sect. 3.4 |
| **Veeam B&R** | Sauvegarde infrastructure JMSI + clients infogeres | veeam.local | Chap. 4 sect. 4.5 |
| **Wasabi / S3** | Stockage objets immuable, hors-site (3-2-1) | wasabi.com | Chap. 4 sect. 4.4 |
| **Stack Wiki interne** | Procedures vivantes + retours terrain (BookStack) | wiki.jmlab.eu | Annexe E |
| **Mattermost JMSI** | Messagerie equipe et | chat.jmlab.eu | Chap. 1 sect. 1.7 |

| | coordination astreinte | | |
|---|---|---|---|
| **Plan d'astreinte** | Calendrier roulant des techniciens d'astreinte | PDF mensuel | Chap. 1 sect. 1.7 |

**INFO** Ces outils ne sont pas exposes en Internet sans VPN : les URL externes sont accessibles uniquement via le VPN d'entreprise WireGuard JMSI (procedure Chap. 5 sect. 5.5).

# 1.4 GLPI : inventaire et helpdesk niveau 1

GLPI (Gestionnaire Libre de Parc Informatique, version 10.x LTS) est l'outil central de gestion de parc et de helpdesk JMSI. Il assure trois fonctions majeures : inventaire automatique des machines clients via l'agent FusionInventory, gestion des tickets clients (formulaire externe + creation manuelle), et reporting de l'activite technique (temps passe, SLA respecte ou non).

## 1.4.1 Architecture

```
# Architecture GLPI JMSI (resume)
glpi.jmlab.eu       ->  Frontend Apache + PHP-FPM (Debian 12, MariaDB 10.11)
agent.jmlab.eu      ->  Endpoint d'inventaire (push agent FusionInventory)
glpi-bdd.local      ->  Base MariaDB (replication binlog vers serveur de secours)
glpi-files.local    ->  Stockage des PJ (files/) sur volume separe (sauvegarde dediee)
```

## 1.4.2 Conventions de nommage des entites GLPI

GLPI organise les clients en arborescence d'entites. La convention JMSI est stricte :

```
Entite racine : 'JMSI'
  +-- Sous-entite : 'JMSI - INTERNE'              # parc JMSI lui-meme
  +-- Sous-entite : 'B2B'
  |     +-- 'B2B - <CODE_CLIENT> - <NOM_COMMERCIAL>'
  +-- Sous-entite : 'B2C'
  |     +-- 'B2C - <CODE_CLIENT> - <NOM_COMMERCIAL>'
  +-- Sous-entite : 'COLLECTIVITES'
        +-- 'COLL - <CODE_CLIENT> - <NOM_COMMERCIAL>'
```

## 1.4.3 Categories de tickets standard JMSI

| Code | Categorie | Exemple | SLA defaut (contrat Maintenance) |
|---|---|---|---|
| **INC-MAT** | Incident materiel | PC ne demarre pas, ecran HS | GTI 4h ouvrees / GTR 8h ouvrees |
| **INC-LOG** | Incident logiciel | Plantage Outlook, lenteur ERP | GTI 4h / GTR 8h |
| **INC-RES** | Incident reseau | Internet HS, switch deconnecte | GTI 2h / GTR 4h (P1) |
| **INC-SEC** | Incident securite | Phishing recu, alerte EDR, suspicion ransomware | GTI immediate / GTR 2h (P1) |
| **INC-SAU** | Incident sauvegarde | Job en echec >24h, alerte | GTI 4h / GTR 24h |

| | | | |
|---|---|---|---|
| | | espace disque | |
| **INC-TEL** | Incident telephonie | Pas de tonalite, SDA non joignable | GTI 2h / GTR 4h |
| **DEM-EVO** | Demande d'evolution | Ajout d'utilisateur, nouvelle imprimante | Planifie 5j ouvres |
| **DEM-INF** | Demande d'information | Question, conseil, point d'avancement | Reponse 1j ouvre |
| **PRO-MAJ** | Projet - Mise a jour | Migration version, montee de release | Date convenue |
| **PRO-MEP** | Projet - Mise en service | Deploiement initial d'une offre | Date convenue |

**ATTENTION** Tout ticket P1 (priorite 1 : INC-RES, INC-SEC critique, ransomware) doit etre escalade immediatement vers le superviseur ou la direction technique, en parallele du traitement. Reflexe : Mattermost canal #astreinte + appel telephonique.

### 1.4.4 Workflow du ticket

Tout ticket suit le workflow standard suivant. Aucun raccourci n'est tolere : la tracabilite est la garantie de la facturation et du SLA.

1. Creation : par le formulaire client, par mail, par appel (cree par le technicien sous 15 min).
2. Qualification : categorisation, urgence/impact, assignation N1/N2, contact client si manque d'information.
3. Diagnostic : prise en main RustDesk si poste utilisateur, lecture journaux si serveur, isolation du perimetre.
4. Action : intervention a distance ou planification du deplacement.
5. Resolution : retablissement constate ; demander confirmation utilisateur.
6. Cloture : compte-rendu (3 sections : SYMPTOME / DIAGNOSTIC / ACTION) + temps passe + facturable O/N.
7. Mise a jour du dossier de base si la configuration a change.

**BONNE PRATIQUE** Compte-rendu de ticket : << SYMPTOME : ce que le client decrit / ce qu'on observe. DIAGNOSTIC : ce qui se passe vraiment et pourquoi. ACTION : ce qui a ete fait, dans quel ordre, pour quel resultat. >> Cette structure rend le ticket reutilisable pour le prochain technicien et pour le client.

## 1.5 GTR / GTI : engagements contractuels JMSI

JMSI s'engage par ecrit sur des delais de prise en compte et de retablissement. Ces engagements sont notre principal differenciateur ; ils doivent etre tenus systematiquement. Une violation de SLA non documentee est une cause directe de non-renouvellement de contrat.

### 1.5.1 Definitions

| Sigle | Nom complet | Definition |
|---|---|---|

| | | |
|---|---|---|
| **GTI** | Garantie de Temps d'Intervention | Delai entre la creation du ticket et la prise en compte par un technicien JMSI (premier message au client : << bonjour, je traite votre demande >>). |
| **GTR** | Garantie de Temps de Retablissement | Delai entre la creation du ticket et le retablissement du service. Pour les pannes materielles necessitant une piece, le GTR s'applique apres reception de la piece (clause precisee au contrat). |
| **GTI/GTR ouvre** | Heures ouvrees | JMSI travaille du lundi au vendredi de 8h a 20h. Les heures hors plage ne sont pas comptabilisees, sauf astreinte payante. |

### 1.5.2 Matrice des SLA contractuels

| Contrat | GTI | GTR | Astreinte | Penalites en cas de non-respect |
|---|---|---|---|---|
| **Maintenance B2B** | 4h ouvrees | 8h ouvrees | Optionnelle (devis specifique) | 1 jour offert par tranche de 4h depassees, plafond 1 mois |
| **Hebergement** | 1h H24 | 4h H24 | Inclus | 1 mois offert si SLA 99,9 % non tenu sur le mois |
| **Sauvegarde / PRA** | 2h ouvrees | Variable selon volume | Inclus restauration P1 | Test annuel obligatoire JMSI sans surcout |
| **Securite (Pack Pro)** | Immediate (auto) | 2h H24 incident P1 | Inclus | Audit gratuit + 1 mois offert |
| **Telephonie VoIP** | 2h ouvrees | 4h ouvrees | Optionnelle | 1 mois offert |
| **Videosurveillance** | 8h ouvrees | 48h ouvrees (piece) | Optionnelle | Aucune si piece sous garantie en attente |

### 1.5.3 Mesure et reporting

GLPI calcule automatiquement les SLA sur chaque ticket. Le rapport mensuel d'activite (RAS) remis aux clients > 5 postes inclut systematiquement le tableau de respect des SLA. Tout depassement est commente : cause, mesure corrective, prevention.

```
# Exemple d'extraction GLPI (script Python interne)
# Genere le RAS mensuel au format PDF
python3 /opt/jmsi/scripts/ras_mensuel.py \
      --entity 'B2B - ABCD - SARL Exemple' \
      --month 2026-04 \
      --output /clients/ABCD_SARL_Exemple/11_facturation/RAS_2026-04.pdf
```

## 1.6 Niveaux de support et escalade

JMSI fonctionne sur 3 niveaux de support, plus une direction technique. Chaque ticket est ouvert au niveau le plus bas qualifie ; l'escalade est explicite, documentee, sans honte.

| Niveau | Profil | Perimetre | Quand escalader |
|---|---|---|---|
| **N1** | Technicien helpdesk JMSI | Tickets standard : reset MDP, deblocage Outlook, ajout imprimante, depannage poste de travail simple, restauration de fichier sur sauvegarde. | Apres 30 min sans diagnostic, ou si le perimetre depasse le poste utilisateur. |
| **N2** | Technicien itinerant senior | Diagnostic reseau, configuration serveur AD/RDS, deploiement EDR, parametrage NGFW, sauvegardes serveur. | Apres 90 min sans solution, ou si action irreversible (formatage, reset usine, ecrasement de configuration). |
| **N3** | Ingenieur systeme / reseau | Architecture, cluster Hyper-V, AD multi-DC, deploiement Veeam, integration SD-WAN, audit securite, peering BGP. | Apres 4h sans solution, ou si action a impact infrastructure (ipfailover, modification VLAN, edition DNS critique). |
| **Direction technique** | Direction JMSI | Decision strategique : engagement contractuel, derogation SLA, autorisation d'achat exceptionnelle, communication crise. | Crise (ransomware, datacenter down), conflit client, depassement de budget. |

**BONNE PRATIQUE** L'escalade n'est pas un aveu d'echec : c'est un signe de maturite. Le N1 qui escalade au bon moment fait gagner du temps au client et au N2. Le N1 qui s'acharne sans escalader fait perdre une demi-journee a tout le monde.

## 1.7 Astreinte JMSI

L'astreinte est assuree en roulement par les techniciens N2 et N3, 7j/7, 20h-8h en semaine et weekends complets. Le planning est publie le 25 du mois precedent. Les clients en astreinte incluse (Hebergement,

Securite Pack Pro) declenchent par appel sur le standard ; les autres via le formulaire d'urgence en ligne (paiement a l'acte selon grille tarifaire).

### 1.7.1 Equipement du technicien d'astreinte

- Telephone d'astreinte fourni par JMSI (mobile + numero unique).
- Ordinateur portable JMSI charge a 100 %, avec VPN configure et Bitwarden synchronise.
- Acces a tous les outils internes JMSI (RustDesk, GLPI, Veeam, dashboard NGFW).
- Documentation hors-ligne : ce livre blanc, en version PDF, sur cle USB chiffree.
- Plan d'escalade : N3 reference + Direction technique, avec numeros directs.

### 1.7.2 Procedure d'intervention en astreinte

8. Reception de l'appel : noter heure, client, motif. Repondre dans les 5 minutes.
9. Qualification rapide : criticite (P1/P2/P3), perimetre, urgence client.
10. Telediagnostic via VPN, RustDesk, ou shell.
11. Intervention : a distance si possible, deplacement uniquement si P1 et impossible a distance.
12. Communication : message au client toutes les 30 min sur l'avancement (P1).
13. Cloture : ticket GLPI cree (meme a posteriori) avec compte-rendu detaille.
14. Si non-resolution sous 1h : escalade N3 obligatoire. La Direction technique est informee a 2h pour les P1.

> **ATTENTION** Toute intervention en astreinte est facturee selon la grille publique : forfait declenchement + taux horaire majore. Le technicien d'astreinte n'a pas le pouvoir de remiser ce tarif - seule la Direction commerciale peut le faire.

## 1.8 Outillage du technicien itinerant

Tout technicien JMSI itinerant transporte une trousse standard. La liste qui suit est le minimum vital : sa completude est verifiee une fois par trimestre par le responsable d'equipe.

### 1.8.1 Trousse de base

- Ordinateur portable JMSI 14 ou 15 pouces, double batterie ou chargeur secteur + USB-C.
- Cle USB bootable Ventoy avec : Windows 11 IoT LTSC, Debian 12 netinst, GParted Live, Hiren's BootCD, Memtest86, Clonezilla, Macrium Reflect Free.
- Cle USB-C avec adaptateurs HDMI / DisplayPort / VGA.
- Multimetre numerique (testeur de continuite, voltmetre).
- Testeur de cable RJ45 et tonalite cable.
- Pince a sertir RJ45 + 50 connecteurs Cat6A + 30 manchons.
- Tournevis cruciforme et plat, jeu Torx, jeu hexagonal, pince long bec.
- Sangle antistatique (ESD).
- Lampe frontale ou torche LED.
- Cable Ethernet RJ45 Cat6A 5 m + adaptateur USB-Ethernet.
- Cable serie USB->RJ45 (cisco style) pour console switch.
- Cle 4G/5G pour acces internet de secours sur intervention.
- Lingettes microfibre + mousse ecran + air sec en bombe (depoussierage).
- Disque externe USB-C 2 To dedie aux secours/restaurations (chiffre BitLocker).

- Onduleur USB portable (depannage rapide en cas de coupure).

### 1.8.2 Documents du technicien itinerant

- Carte professionnelle JMSI (badge employeur, decret signe).
- Mandat client signe par le decideur (acces locaux, traitement de donnees).
- Bon d'intervention vierge (5 exemplaires).
- Fiche d'inventaire (complement GLPI quand le reseau ne permet pas l'agent).
- Ce livre blanc, version PDF a jour, sur le portable.
- Numero d'astreinte JMSI et numero d'escalade N3 sur la coque du telephone.

## 1.9 Processus d'intervention en 7 etapes

Toute intervention JMSI - de la simple installation de cable au deploiement multi-sites - suit le meme processus en 7 etapes. La maitrise de ce processus est aussi importante que la maitrise technique.

### 1.9.1 Etape 1 : Preparation (J-1)

- Lire le ticket et le dossier de base. Resumer en 3 lignes ce qui va etre fait.
- Identifier les acces requis : cles, badges, codes alarme. Demander si manquants.
- Verifier le materiel a apporter (commande Dolibarr validee, livraison constatee).
- Imprimer le bon d'intervention pre-rempli.
- Verifier que le technicien sur site cote client est disponible (telephone, mail).
- Bloquer la marge horaire : prevoir 30 min de plus que l'estime.

### 1.9.2 Etape 2 : Arrivee sur site

- Se presenter, montrer la carte professionnelle, signer le registre d'entree si demande.
- Confirmer le perimetre de l'intervention avec le contact client (ce qui est inclus / exclus).
- Localiser physiquement les equipements, le local technique, l'arrivee internet, le tableau electrique.
- Identifier les issues de secours et les regles de securite du site.

### 1.9.3 Etape 3 : Etat des lieux

- Photographier l'existant avant toute modification (5-10 photos minimum). Stockees dans 10_interventions/<DATE>/avant/.
- Tester l'existant : Internet, partage de fichier, mail, applications metier. Reporter sur le bon d'intervention.
- Demander au client le perimetre de la modification autorisee : si la mission deborde, NE RIEN FAIRE de plus sans validation ecrite.

### 1.9.4 Etape 4 : Realisation

- Suivre le mode operatoire publie dans ce livre blanc (chapitre concerne).
- Documenter les valeurs reelles : adresses IP retenues, ports ouverts, comptes crees.
- Tester chaque sous-etape avant de passer a la suivante.
- En cas d'imprevu : ne pas improviser de scenarios non documentes. Escalader au N2/N3.

### 1.9.5 Etape 5 : Recette technique

- Verifier que tout ce qui marchait avant marche encore (regression).
- Verifier que ce qui devait etre installe / modifie fonctionne (acceptation).
- Faire valider par le contact client (test fonctionnel cote utilisateur).

### 1.9.6 Etape 6 : Documentation et signature

- Photographier l'apres : 10_interventions/<DATE>/apres/.
- Mettre a jour le dossier de base sur le NAS JMSI (si pas possible sur place : a J+1 maximum).
- Cloturer le ticket GLPI : compte-rendu structure SYMPTOME/DIAGNOSTIC/ACTION + temps + facturable.
- Faire signer le bon d'intervention par le client.
- Remettre le PV de mise en service si projet (Chap. 2 sect. 2.4 pour la maintenance, etc.).

### 1.9.7 Etape 7 : Suivi a J+7 et J+30

- Appel client a J+7 : tout va bien ? Verification de la stabilite.
- Pour les projets : verification a J+30 que la solution est appropriee, propositions d'optimisation.

## 1.10 Bonnes pratiques transversales

### 1.10.1 Hygiene de la console

- Ne jamais laisser une session admin ouverte sans surveillance.
- Toujours travailler avec un compte dedie au technicien (jamais avec << admin / admin >>).
- Apres une elevation de privilege : revenir a un compte standard des que possible.
- Acceder aux interfaces critiques (firewall, NGFW, AD) uniquement depuis le portable JMSI sur VPN.

### 1.10.2 Hygiene des modifications

- Une modification a la fois. Test entre chaque.
- Sauvegarde de la configuration AVANT toute modification (export firewall, export AD, snapshot VM).
- Documenter la modification dans GLPI : avant, apres, raison.
- Plan de rollback ecrit avant toute action critique.

### 1.10.3 Hygiene des donnees client

- Pas de copie de donnees client sur le portable JMSI sans necessite. Si necessaire : chiffre + supprime apres usage.
- Pas de cle USB personnelle inseree dans un poste client (ni l'inverse).
- Pas de capture d'ecran client envoyee sur Slack/WhatsApp personnel.
- Toute donnee transitant par JMSI fait l'objet du registre RGPD JMSI.

### 1.10.4 Communication avec le client

- Vouvoyer par defaut ; tutoiement uniquement si le client le propose.
- Reformuler la demande client avant d'agir : << Si je comprends bien, vous souhaitez... >>
- Pas de jargon technique : traduire pour l'utilisateur final.

- Annoncer chaque coupure : << Je vais redemarrer le serveur, le mail va etre indisponible 5 minutes >>.
- Ne jamais critiquer l'existant devant le client (un autre prestataire a peut-etre fait ce qu'il pouvait avec ce qu'il avait).

## 1.11 Securite, RGPD, NIS2 - obligations du technicien

JMSI est responsable de la conformite des prestations realisees chez le client. Le technicien applique strictement les regles ci-dessous, sans exception.

### 1.11.1 RGPD

- JMSI agit en tant que sous-traitant au sens RGPD (article 28). Toute prestation est encadree par le contrat ou par un avenant DPA (Data Processing Agreement).
- Les donnees personnelles client ne quittent jamais le territoire UE sans autorisation explicite (registre).
- Aucune donnee personnelle n'est conservee par JMSI plus longtemps que necessaire (purge apres mission).
- Toute violation suspectee (vol de portable, fuite de mot de passe) doit etre remontee a la Direction technique sous 1 heure (notification CNIL sous 72h).

### 1.11.2 NIS2

La directive NIS2 (transposition 2024-2025) impose aux entites essentielles et importantes des obligations de cybersecurite. JMSI accompagne ses clients concernes (sante, energie, transports, banque, fournisseurs de TIC). Le technicien doit :

- Identifier si le client est NIS2 (registre dans le dossier de base, section 7).
- Tracer toute action sur les systemes critiques (logs immuables 12 mois minimum).
- Reporter tout incident de securite a la Direction technique pour declaration ANSSI sous 24h.

### 1.11.3 Confidentialite des secrets

- Aucun mot de passe en clair dans un mail, un SMS, un ticket, un compte-rendu.
- Tout secret transite par Bitwarden (collection client) ou par echange chiffre Nextcloud.
- Mots de passe d'acces aux equipements infrastructure : rotation tous les 12 mois minimum.
- Comptes d'urgence (break-glass) : stockage chiffre, derniere utilisation a J+0 toleree, sinon investiguer.

## 1.12 Cloture et facturation

La derniere etape de toute mission est la transformation du temps passe en facture. Une intervention non facturee est une intervention non remontee a la production : c'est un risque pour la peenisation de la societe et pour la continuite des contrats.

- Cloture du ticket GLPI : compte-rendu, temps passe, facturable O/N (selon le contrat).
- Si hors contrat : creation devis Dolibarr, signature client, facture des le ticket clos.
- Si dans le contrat : decompte mensuel envoye automatiquement (RAS).

- Contrats au forfait : aucun facturable supplementaire ne doit echapper au client (sinon le contrat est intenable).
- Hors contrat ponctuel : facturation a l'acte selon grille tarifaire publique JMSI.

# PARTIE II

# Maintenance et infogerance

# Chapitre 2 - Contrats de maintenance B2B

## 2.1 Perimetre

Le contrat de maintenance JMSI est l'offre socle B2B. Il couvre la supervision, la telemaintenance, la maintenance preventive et corrective d'un parc informatique TPE/PME (1 a 50 postes). Les references commerciales sont :

| Code Dolibarr | Designation | Tarif HT mensuel | Engagement |
|---|---|---|---|
| **B2B_MAI_01** | Contrat Maintenance 1 poste | 21,90 EUR | 12 mois reconductible |
| **B2B_MAI_02** | Contrat Maintenance 5 postes | 89,00 EUR | 12 mois reconductible |
| **B2B_MAI_03** | Contrat Maintenance 10 postes | 159,00 EUR | 12 mois reconductible |
| **B2B_MAI_04** | Intervention hors contrat (taux horaire) | 95,00 EUR / heure | Aucun |

Au-dela de 10 postes, un contrat sur mesure est etabli (multiples de 5 postes ou tarification lineaire). Pour les structures > 30 postes, un Pack Performance peut etre plus pertinent (cf. chapitre 10).

> **INFO** Le contrat de maintenance N'INCLUT PAS la sauvegarde, ni la cybersecurite, ni l'hebergement. Ce sont des contrats distincts (chapitres 4, 5, 3 respectivement).

## 2.2 Architecture cible et pre-requis

JMSI s'appuie sur trois piliers techniques pour delivrer un contrat de maintenance : un agent de supervision sur chaque poste/serveur (RMM), un canal de telemaintenance, et un registre central (GLPI + dossier de base). Sans ces trois elements, le contrat ne peut pas etre tenu.

### 2.2.1 Pile logicielle de reference

| Composant | Outil retenu | Role | Alternative tactique |
|---|---|---|---|
| **RMM (Remote Monitoring & Management)** | TacticalRMM (open source, auto-hebergement JMSI) | Inventaire continu, monitoring, scripts, patch management, alertes | N-able N-Central, NinjaOne (commerciaux) |
| **Telemaintenance assistee** | RustDesk Server (auto-hebergement JMSI) | Prise en main poste avec consentement utilisateur (clic) | AnyDesk, TeamViewer, ScreenConnect |
| **Helpdesk/ticketing** | GLPI 10.x (auto-hebergement JMSI) | Ticket, SLA, RAS, base de connaissances client | OTRS, Zammad, Freshservice |
| **Inventaire automatique** | FusionInventory Agent (integre TacticalRMM ou | Materiel, logiciel, MAJ, BIOS, antivirus | GLPI Agent natif |

| | | | |
|---|---|---|---|
| | autonome) | | |
| **Patch management** | TacticalRMM + WSUS (Windows Server) | Politique de mise a jour standardisee | ManageEngine Patch Manager |
| **Antivirus / EDR** | Bitdefender GravityZone Business (cloud) | Endpoint EDR, supervision menaces | Sophos Intercept X, ESET Inspect |

### 2.2.2 Pre-requis chez le client

- Connexion Internet symetrique 10/10 Mbps minimum (ideal : fibre 100/100 ou plus).
- Adresse IP fixe ou DNS dynamique (pour les remontees firewall).
- Acces administrateur sur les postes Windows/Mac (pour deploiement de l'agent RMM).
- Compte AD service jmsi-rmm (utilisateur de service avec elevation contextuelle).
- Ouverture firewall sortante : ports 443 (HTTPS) et 21115-21119 (RustDesk).
- Reseau local segmente VLAN si > 10 postes (cf. Annexe C).
- Accord ecrit du client sur l'installation des agents (annexe DPA RGPD).

## 2.3 Mise en service initiale d'un contrat de maintenance

La mise en service est sequencee en 6 phases sur 5 jours ouvres maximum. Le projet est pilote par un chef de mission JMSI (souvent N2). Un PV de mise en service est signe a J+5.

### 2.3.1 Phase 1 : audit de parc (J0, sur site, 0,5 a 2 jours)

L'audit de parc est offert (cf. plaquette Maintenance JMSI). Il est realise avant la signature du contrat OU dans la premiere semaine du contrat selon le cas.

#### *Materiel a apporter*

- Trousse standard (cf. chapitre 1.8).
- Cle USB Ventoy avec FusionInventory portable et Glasswire ou nmap.
- Bon d'audit JMSI vierge.

#### *Procedure*

15. Demander au contact client une cartographie sommaire (qui fait quoi, applications metier critiques, horaires).
16. Inventorier physiquement chaque equipement du parc.
17. Sur chaque poste, lancer FusionInventory portable pour collecte materiel + logiciel.
18. Cartographier le reseau : nmap depuis le portable JMSI sur le LAN client.

```
# Inventaire reseau rapide
# 1) Lister les hotes vivants sur le subnet
sudo nmap -sn 192.168.1.0/24 -oG /tmp/audit_hosts.txt

# 2) Detection OS et services pour chaque hote actif
sudo nmap -sV -O --open -oN /tmp/audit_services.txt 192.168.1.0/24

# 3) Verifier la presence de partages SMB ouverts (signal de risque)
sudo nmap --script smb-enum-shares -p 445 192.168.1.0/24 -oN /tmp/audit_shares.txt
```

```
# 4) Sauvegarder dans le dossier client
cp /tmp/audit_*.txt /clients/<CODE>/02_inventaire_parc/
```

19. Verifier l'arrivee internet : speedtest CLI, traceroute, ping vers 8.8.8.8 et 1.1.1.1.

```
# Test debit internet en CLI (Linux/Mac)
speedtest-cli --simple

# Verification routage et latence
mtr -rwc 100 8.8.8.8       # 100 paquets, rapport stable
mtr -rwc 100 1.1.1.1

# Verification DNS
dig @8.8.8.8 google.fr
dig @<DNS_CLIENT> google.fr   # comparer

# Verification IP publique et reverse DNS
curl ifconfig.me
dig -x <IP_PUBLIQUE>
```

20. Verifier les sauvegardes existantes : type, frequence, dernier test reussi. Photographier les ecrans de console.
21. Verifier la cybersecurite : antivirus actif, MFA actif sur les comptes, mots de passe par defaut residuels, ouvertures NAT externes.
22. Restituer un rapport d'audit (modele JMSI) sous 5 jours ouvres : etat des lieux + 5 recommandations chiffrees + estimation contrat.

**ATTENTION** L'audit n'est pas une intervention : ne PAS modifier la configuration client, meme si vous reperez un parametre << aberrant >>. La modification suit la signature du contrat.

### 2.3.2 Phase 2 : creation des entites internes (J+1)

23. Dolibarr : creer le tiers, charger le contrat signe, programmer l'echeancier de facturation.
24. GLPI : creer la sous-entite (cf. chapitre 1.4.2), creer les utilisateurs avec leur perimetre.
25. Bitwarden : creer la collection client, inviter les techniciens autorises.
26. NAS interne : creer l'arborescence /clients/<CODE>/.
27. Wiki interne : creer la page de synthese client (lien vers tous les outils).
28. Lister les contacts client (decideur, technique, comptabilite) dans GLPI et Dolibarr.

### 2.3.3 Phase 3 : deploiement des agents (J+1 a J+2)

#### *Agent TacticalRMM (Windows)*

L'agent est deploye via un installateur MSI signe, avec une cle de deploiement specifique au client.

```
REM Deploiement TacticalRMM Windows en silencieux
REM Telecharger l'agent depuis https://rmm.jmlab.eu/install/<CODE_CLIENT>

REM Sur le poste cible (en admin)
tacticalagent-v<VERSION>-windows-amd64.exe -m install \
   --api https://api.rmm.jmlab.eu \
   --client-id <ID_CLIENT> \
   --site-id <ID_SITE> \
   --auth <TOKEN_DEPLOIEMENT> \
   --silent

REM Verifier l'installation
```

```
sc query tacticalrmm
sc query tacticalrpc
```

### *Agent TacticalRMM (Linux/Mac)*

```
# Linux Debian/Ubuntu (en root)
wget -q https://rmm.jmlab.eu/install/<CODE>/linux -O /tmp/tactical.sh
chmod +x /tmp/tactical.sh
/tmp/tactical.sh

# Verifier le service
systemctl status tacticalagent

# macOS (en sudo)
sudo /Applications/Tactical\ Agent.app/Contents/MacOS/Tactical\ Agent \
    -m install --api https://api.rmm.jmlab.eu \
    --client-id <ID> --site-id <ID> --auth <TOKEN> --silent
```

### *Agent RustDesk (Windows)*

```
REM RustDesk Custom Client - les binaires sont prepackages JMSI
REM (build interne avec rendezvous = rd.jmlab.eu, key = <PRESHARED>)

REM Installation silencieuse
rustdesk-host=rd.jmlab.eu,key=<PUBLIC_KEY>.exe --silent-install

REM Verifier l'enregistrement
"%ProgramFiles%\RustDesk\rustdesk.exe" --get-id

REM Configurer mot de passe permanent et acces non interactif
"%ProgramFiles%\RustDesk\rustdesk.exe" --password <MDP_PERMANENT>
```

**ATTENTION** Le mot de passe RustDesk permanent est genere par poste, stocke dans Bitwarden, jamais identique a un autre client. La rotation est annuelle.

### *Agent EDR Bitdefender GravityZone*

```
REM Telecharger le package depuis la console GravityZone
REM (Configuration > Network > Installation Packages > <Package_JMSI_<CODE>>)

REM Installation Windows
setup.exe /silent

REM Verifier la presence du service
sc query EPSecurityService
sc query EPProtectedService
```

## 2.3.4 Phase 4 : configuration des standards JMSI (J+2)

Sur chaque poste/serveur, le technicien applique le << kit JMSI Standard >>. Il s'agit d'un ensemble de scripts et politiques internes garantissant l'homogeneite du parc.

### *Kit JMSI Standard - Windows*

```
# PowerShell - kit_jmsi_standard.ps1 (extrait)
# Lance par TacticalRMM (script global), idempotent

# 1) Activer Windows Defender Tamper Protection si absence d'EDR Bitdefender
Set-MpPreference -DisableRealtimeMonitoring 0
```

```
# 2) Definir le fuseau horaire et la langue
Set-TimeZone -Id 'Romance Standard Time'

# 3) Synchronisation horaire (NTP francais)
w32tm /config /manualpeerlist:'fr.pool.ntp.org,0x1' /syncfromflags:manual /update
Restart-Service w32time

# 4) Politique d'extinction ecran et veille (postes fixes : pas de veille systeme)
powercfg /change standby-timeout-ac 0
powercfg /change monitor-timeout-ac 30
powercfg /change hibernate-timeout-ac 0

# 5) Forcer SMBv1 desactive
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart

# 6) Bloquer execution scripts non signes (postes utilisateurs)
Set-ExecutionPolicy -Scope LocalMachine RemoteSigned -Force

# 7) Inventaire BitLocker (lever une alerte si OS non chiffre alors qu'il devrait l'etre)
manage-bde -status C:
```

### *Kit JMSI Standard - Linux serveur*

```
# bash - kit_jmsi_linux.sh
set -euo pipefail

# 1) Mise a jour systeme
apt-get update -y && apt-get upgrade -y
apt-get install -y unattended-upgrades fail2ban auditd ufw

# 2) Pare-feu de base (sortie autorisee, entree fermee sauf SSH IP JMSI)
ufw default deny incoming
ufw default allow outgoing
ufw allow from <IP_JMSI_VPN> to any port 22 proto tcp
ufw enable

# 3) Synchronisation horaire
timedatectl set-timezone Europe/Paris
systemctl enable systemd-timesyncd

# 4) Auditd avec regles de base
cat <<'EOR' > /etc/audit/rules.d/jmsi-standard.rules
-w /etc/passwd -p wa -k passwd_changes
-w /etc/shadow -p wa -k shadow_changes
-w /etc/sudoers -p wa -k sudoers_changes
-w /var/log -p wa -k log_changes
EOR
systemctl restart auditd

# 5) Mises a jour securite automatiques
echo 'APT::Periodic::Update-Package-Lists "1";' > /etc/apt/apt.conf.d/20auto-upgrades
echo 'APT::Periodic::Unattended-Upgrade "1";' >> /etc/apt/apt.conf.d/20auto-upgrades
```

## 2.3.5 Phase 5 : recette technique et formation rapide (J+3)

- Verifier la presence des agents dans la console TacticalRMM (toutes les machines remontent).
- Verifier la prise en main RustDesk (1 poste de chaque type).
- Verifier la remontee EDR (toutes machines vertes en console GravityZone).

- Tester l'ouverture d'un ticket par le client : par formulaire, par mail, par appel.
- Former l'utilisateur principal cote client (30 minutes : ouvrir un ticket, accepter une session RustDesk).
- Distribuer la fiche << Comment contacter JMSI >> (PDF officiel JMSI).

### 2.3.6 Phase 6 : PV de mise en service et bascule en exploitation (J+5)

- Imprimer le PV de mise en service maintenance (modele JMSI).
- Sections : perimetre, equipements integres, agents installes, services actives, personnes formees.
- Signature du chef d'etablissement client + chef de mission JMSI + Direction technique JMSI (electronique).
- Premiere supervision : verifier qu'un cycle de patch a tourne, qu'une sauvegarde a ete prise, qu'aucune alerte critique n'est presente.
- Bascule en exploitation : assignation au technicien titulaire du compte.
- Email de bienvenue au client (signature << contact@jmlab.eu / 04 48 26 00 66 >>).

## 2.4 Recette et livrables

### 2.4.1 PV de mise en service - modele JMSI

Le PV doit comporter au minimum les rubriques suivantes :

| Rubrique | Contenu attendu |
|---|---|
| **Identification client et contrat** | Raison sociale, contrat n, signataires |
| **Perimetre supervise** | Liste des postes et serveurs (numero de serie + IP) |
| **Outils JMSI deployes** | Versions de TacticalRMM, RustDesk, Bitdefender |
| **Standards appliques** | Reference au kit JMSI Standard, version en vigueur |
| **Tests realises** | Liste des tests (ouverture ticket, prise main RustDesk, reception alerte) |
| **Personnes formees** | Nom + signature de chaque utilisateur forme cote client |
| **Reserves** | Eventuelles reserves a lever (ex. : poste comptable a remplacer en J+30) |
| **Reserves levees** | Annexe a signer apres correction des reserves |
| **Plan de la prochaine intervention** | Date du premier RAS, date de l'audit annuel inclus |
| **Donnees personnelles** | Liste des donnees auxquelles JMSI accede (annexe DPA RGPD) |

### 2.4.2 Livrables remis au client

- PV de mise en service signe (PDF + papier).
- Fiche << Comment contacter JMSI >> (PDF officiel).
- Synthese du dossier de base (sections non sensibles uniquement, sans secrets).

- Calendrier prevu : RAS mensuel J+30, audit annuel J+335.
- RIB JMSI et echeancier de facturation.

## 2.5 Exploitation courante du contrat de maintenance

### 2.5.1 Tableau de bord TacticalRMM

Toute equipe technique JMSI consulte le tableau de bord RMM en debut de journee. Les alertes y sont triees par client et par criticite. Le N1 d'astreinte de la journee est responsable du tri des alertes.

| Type d'alerte | Action attendue | Delai de traitement |
|---|---|---|
| **Disque < 10 % libre** | Ouverture ticket DEM-INF, communication client | Jour ouvre |
| **Disque < 5 % libre** | Ouverture ticket INC-LOG, intervention preventive | GTI 4h |
| **Sauvegarde failed > 24h** | Ouverture ticket INC-SAU, contact client | GTI 4h |
| **EDR : malware detecte** | Ouverture ticket INC-SEC, isolation poste | GTI immediate (P1) |
| **EDR : agent offline > 24h** | Ouverture DEM-INF, verifier connectivite | Jour ouvre |
| **Service Windows en echec** | Ticket INC-LOG, redemarrage service ou poste | GTI 4h |
| **Patch en echec > 7 jours** | Investigation ticket DEM-EVO, planification | 5 jours ouvres |
| **Carte SMART pre-fail** | Ticket INC-MAT, devis remplacement disque | GTI 4h - GTR 8h piece dispo |
| **Onduleur batterie defaillante** | Ticket INC-MAT, devis remplacement batterie | 5 jours ouvres |

### 2.5.2 Politique de patch management

La politique de patch JMSI vise a equilibrer securite et stabilite : on patche vite ce qui est critique, on patche differe ce qui ne l'est pas.

| Type de mise a jour | Delai d'application sur le parc client | Mode |
|---|---|---|
| **Patch securite Microsoft (Patch Tuesday)** | J+7 a J+10 (apres test interne JMSI sur lab) | Automatique via TacticalRMM (post-validation lab) |
| **Mise a jour drivers / firmware** | J+30 (apres validation de la stabilite) | Manuel via TacticalRMM script |
| **Mise a jour applicatif metier** | Selon planning client (jamais en | Manuel, demande client + plan de |

| | | |
|---|---|---|
| | aveugle) | retour arriere |
| **CVE en exploitation active** | J+0 a J+1 (urgence) | Automatique apres validation Direction technique |

**BONNE PRATIQUE** Avant tout patch deploye en production : test sur le lab JMSI (poste image identique au client cible). Le retour d'experience lab evite 90 % des regressions client.

### 2.5.3 Maintenance preventive

Au-dela des automatismes RMM, certaines taches restent humaines. Elles sont planifiees dans GLPI (taches recurrentes).

| Frequence | Tache | Profil |
|---|---|---|
| **Hebdomadaire** | Revue tableau de bord RMM, fermeture des alertes traitees, contact client si tendance. | N1 |
| **Mensuelle** | Generation et envoi du RAS, revue des SLA, point client telephonique 15 min si tickets > 5. | N2 |
| **Trimestrielle** | Test de restauration de fichier (sauvegarde), test EDR (fichier EICAR), revue des comptes admin actifs. | N2 |
| **Semestrielle** | Audit BitLocker / chiffrement disque, audit MFA et droits utilisateurs, mise a jour kit JMSI Standard. | N2 |
| **Annuelle** | Audit complet sur site (4h sur place inclus dans le contrat) + revue contrat + plan d'evolution. | N2 + Commercial |

### 2.5.4 RAS mensuel - structure type

- Page 1 - synthese : nombre de tickets ouverts, % SLA respecte, alertes critiques.
- Page 2 - tickets : liste anonymisee, categories, temps moyen de resolution.
- Page 3 - parc : evolution du nombre de postes, sante materielle (SMART, batterie).
- Page 4 - securite : EDR (detections), patch management (% conformite), MFA.
- Page 5 - sauvegarde : succes/echec, dernier test de restauration.
- Page 6 - recommandations : 3 a 5 actions recommandees pour le mois suivant.
- Page 7 - facturation : decompte du forfait, eventuels hors forfait.

# 2.6 Telemaintenance avec RustDesk

## 2.6.1 Principes JMSI

- Toute prise en main est sollicitee : le client donne son consentement explicite (clic 'Accepter').
- Toute prise en main est tracee dans GLPI (date, technicien, motif, duree).
- Les sessions non interactives (utilisateur absent) sont possibles uniquement avec mention au contrat et autorisation hierarchique cote client.
- Aucun fichier transfere depuis le poste client n'est conserve sur le poste technicien plus longtemps que necessaire.

## 2.6.2 Procedure standard de prise en main

29. Le client appelle ou envoie un mail decrivant le probleme.
30. Creation du ticket GLPI (categorie, urgence, description).
31. Le technicien rappelle le client, demande un << ID RustDesk >> ou utilise l'ID enregistre dans le dossier de base.
32. Connexion : le client clique << Accepter >> a l'invite.
33. Diagnostic et resolution. Communication audio recommandee (par appel parallele).
34. Fin de session : remplir le compte-rendu GLPI, prevenir le client.

## 2.6.3 Configuration avancee RustDesk pour les serveurs

Pour les serveurs Windows, on configure un acces non interactif securise.

```
REM Sur le serveur Windows (en admin)
"%ProgramFiles%\RustDesk\rustdesk.exe" --config

REM Reglages a verifier dans la GUI :
REM - Service automatique : OUI
REM - Demarrage avec Windows : OUI
REM - Mode connexion : Permis directement et via relais
REM - Acces : avec mot de passe permanent (genere)
REM - Notifier l'utilisateur lors de la connexion : OUI (preferable)

REM Pour les serveurs sans utilisateur : configurer en mode console privilege
"%ProgramFiles%\RustDesk\rustdesk.exe" --service
"%ProgramFiles%\RustDesk\rustdesk.exe" --port-forward 1

REM Stocker l'ID + mot de passe dans Bitwarden (collection client, item server-rustdesk)
```

# 2.7 Depannage

## 2.7.1 Arbre de decision : poste qui rame

35. Verifier l'utilisation CPU/RAM/disque (Gestionnaire des taches ou TacticalRMM).
36. Si CPU > 90 % : identifier le processus dominant. Service Windows en boucle ? Antivirus en scan ? Office en panne ?
37. Si RAM > 90 % : identifier le processus. Memory leak (Chrome, Outlook plus de 500 onglets/mails) ? RAM insuffisante (< 8 Go en 2026 = sous-dimensionne).
38. Si disque a 100 % : SMART en pre-fail ? Disque sature ?

39. Si reseau lent : DNS, latence, debit. Tester avec speedtest CLI sur le poste.
40. Si tout est normal : profil utilisateur corrompu (creer un nouveau profil pour valider).

### 2.7.2 Arbre de decision : pas d'internet

41. Verifier la diode du switch / box. Si eteinte : couper / rebrancher l'alimentation, attendre 2 min.
42. Verifier IP du poste : ipconfig /all (Windows) ou ip a (Linux). DHCP fonctionnel ?
43. Si IP en 169.254.x.x : pas de DHCP. Probleme box / DHCP serveur.
44. Test ping : ping 192.168.1.1 (passerelle) puis 8.8.8.8 (Google) puis google.fr.
45. Si ping IP OK mais pas le nom : probleme DNS. Forcer 8.8.8.8 et 1.1.1.1 temporairement.
46. Si ping passerelle KO : cable, switch, port port. Tester autre cable / autre port.
47. Si echec generalise du site : appel operateur (FAI). Documenter le ticket avec n incident operateur.

### 2.7.3 Erreurs et codes typiques

| Symptome | Cause probable | Action |
|---|---|---|
| **BSOD 0x7B (boot)** | Disque non detecte / pilote SATA absent | Boot recovery, reparer demarrage, reinstaller pilote chipset |
| **Ecran bleu CRITICAL_PROCESS_DIED** | Mise a jour Windows en echec / pilote | DISM + SFC, restauration systeme, point de restauration |
| **Lenteur Outlook 2019 / 365** | Fichier OST > 50 Go, complement bug, profil corrompu | Compactage OST, scanpst.exe, recreation profil |
| **Imprimante hors ligne intermittente** | Pilote, IP en DHCP variable, Bonjour | Fixer IP, pilote constructeur, port TCP/IP standard |
| **Telephonie : pas de tonalite** | QoS, NAT, codec, DNS SRV | Verifier port 5060/5070 sortant, voir chap. 6.7 |
| **Sauvegarde Veeam : Backup Job End Time exceeded** | Volume trop volumineux, fenetre courte | Allonger fenetre, reduire perimetre, backup synth full |
| **VPN deconnexion frequente** | MTU, NAT, connexion instable | MTU 1380, replier sur fallback TCP/443 |
| **MFA Microsoft 365 echec** | Horloge desynchronisee, mauvais teleph. | Resync NTP, reinit MFA cote admin |

## 2.8 Securite et conformite du contrat de maintenance

- Tout acces administrateur JMSI sur le parc client est trace dans le journal RustDesk + GLPI.
- Les comptes de service jmsi-rmm sont rotates annuellement (Bitwarden + AD).
- Les agents RMM communiquent via canal chiffre TLS 1.2+ (verifier certificat racine valide).
- Aucune donnee client n'est sortie du systeme sans accord ecrit du DPO client.
- La sortie de contrat impose la suppression des agents et des donnees stockees JMSI (cf. sect. 2.9).

# 2.9 Desengagement et migration

Le client peut a tout moment resilier (preavis 3 mois). JMSI s'engage a faciliter la transition vers le prestataire suivant. Aucun verrouillage technologique.

## 2.9.1 Procedure de sortie

48. Lettre de resiliation recue (mail ou courrier).
49. Reponse JMSI : accuse de reception + planning de sortie. Premier RDV de coordination.
50. Inventaire complet : remettre l'inventaire actualise, schemas, mots de passe (transfert chiffre Bitwarden export).
51. Phase de tuilage avec le nouveau prestataire (jusqu'a 2 reunions techniques de 1h incluses).
52. Desinstallation des agents JMSI : TacticalRMM, RustDesk, Bitdefender (si licence non transferee).
53. Suppression du compte de service jmsi-rmm dans l'AD client.
54. Archivage cote JMSI : le dossier de base passe en /99_archives/ (lecture seule, retention 5 ans pour comptabilite).
55. Confirmation ecrite au client : << Vos donnees ont ete supprimees de nos systemes operationnels. >>

## 2.9.2 Scripts de desinstallation

```
REM TacticalRMM Windows - desinstallation propre
"%ProgramFiles%\TacticalAgent\tacticalrmm.exe" -m uninstall
REM Verifier services
sc query tacticalrmm 2>NUL || echo 'Service supprime'

REM RustDesk Windows
"%ProgramFiles%\RustDesk\Uninstall.exe" /S

REM Bitdefender Endpoint Security Tools
"%ProgramFiles(x86)%\Bitdefender\Endpoint Security\product.console.exe" /uninstall:full

REM Verification post-desinstallation
wmic product where 'name like "%%RMM%%"' get name,version
wmic product where 'name like "%%RustDesk%%"' get name,version
wmic product where 'name like "%%Bitdefender%%"' get name,version
```

# Chapitre 3 - Hebergement et services en ligne

## 3.1 Perimetre

L'offre Hebergement JMSI couvre l'ensemble des services en ligne hebergeables : domaines, boites mail, sites web (vitrine, e-commerce), GED Nextcloud, ERP/CRM Dolibarr (cf. chap. 13), applications metier (Simply Food, etc.), et services anti-spam/anti-phishing.

| Code Dolibarr | Designation | Tarif HT mensuel |
|---|---|---|
| **B2B_HEB_01** | Hebergement Essentiel (parking domaine) | 2,90 EUR / domaine |
| **B2B_HEB_02** | Hebergement Mail (1 boite + alias) | 4,90 EUR / boite |
| **B2B_HEB_03** | Hebergement Web (1 site mutualise + 1 BDD) | 9,90 EUR / mois |
| **B2B_HEB_04** | WordPress infogere (mutualise + maj + sauv.) | 69,00 EUR / site |
| **B2B_HEB_05** | Gestion Documentaire (Nextcloud) | 69,00 EUR / instance |
| **B2B_HEB_06** | CRM en ligne (Dolibarr ou autre) | 19,00 EUR / utilisateur |
| **B2B_HEB_07** | Mailinblack (anti-spam/phishing) | 2,90 EUR / boite |
| **B2B_HEB_08** | Migration hebergement | OFFERTE |
| **B2B_HEB_09** | Dolibarr infogere Essentiel | 9,00 EUR / utilisateur |
| **B2B_HEB_10** | Dolibarr infogere Pro | 19,00 EUR / utilisateur |
| **B2B_HEB_11** | Mise en service Dolibarr (one-shot) | 690,00 EUR |

## 3.2 Architecture cible JMSI

JMSI exploite une infrastructure souveraine en France (datacenter Tier III). L'architecture est resilante, redondee, supervisee 24/7. Les techniciens n'agissent jamais sur l'infrastructure de production sans validation N3 - cette section explicite l'architecture pour comprehension, mais l'exploitation est de niveau N3.

| Couche | Technologie | Role |
|---|---|---|
| **Bare-metal** | Hyperviseurs Proxmox VE 8.x (cluster 3 nodes minimum) | Heberge tous les services en VM/CT |
| **Stockage** | Ceph cluster (3 nodes, replication 3x) | Stockage VM, snapshots, replication |
| **Reseau** | VLAN frontend / backend / | Segmentation, isolation des |

| | | |
|---|---|---|
| | management, switches L3 redondes | locataires |
| **Reverse proxy** | HAProxy + Let's Encrypt (Caddy en option) | TLS, repartition de charge, WAF basique |
| **Web** | LiteSpeed / Nginx + PHP-FPM + MariaDB / PostgreSQL | Mutualise (jail Linux) ou VM dediee |
| **Mail** | Mailcow (Postfix + Dovecot + Rspamd + SOGo) | SMTP, IMAP/POP, webmail, calendar |
| **Anti-spam/phishing** | Mailinblack (SaaS partenaire) ou Rspamd interne | Protection mail entrante |
| **Nextcloud** | Nextcloud Hub (cluster Redis + Object Storage) | GED, partage, calendrier, talk |
| **DNS authoritatif** | PowerDNS (master/slave) | Zones clientes, dnssec optionnel |
| **Sauvegarde** | Borg / Restic vers stockage objet (Wasabi) | Sauvegardes immuables hors site |

## 3.3 Migration et mise en service d'un domaine

Cette procedure couvre la prise en charge d'un nom de domaine existant chez un autre registrar.

### 3.3.1 Pre-requis

- Acceder au panneau du registrar actuel (login fourni par le client) ou demander le code de transfert (auth code).
- Lister les enregistrements DNS actifs (export zone fichier ou capture ecran).
- Identifier les services en ligne (mail, site, autre) qui dependent du domaine.
- Identifier le DNSSEC eventuel (a desactiver avant transfert).

### 3.3.2 Procedure de transfert vers JMSI

56. Inventorier la zone DNS source (commande dig recommandee).

```
# Inventaire complet de la zone
dig <domaine> ANY +noall +answer
dig <domaine> A AAAA MX TXT NS CNAME +noall +answer
dig _dmarc.<domaine> TXT +short
dig <selector>._domainkey.<domaine> TXT +short  # DKIM

# Capture vers fichier de reference (a stocker dans 03_schemas_reseau)
for type in A AAAA MX TXT NS CNAME SOA SRV CAA; do
  echo "--- $type ---"; dig <domaine> $type +short
done > /clients/<CODE>/03_schemas_reseau/dns_avant_transfert.txt
```

57. Reconstruire la zone DNS cote JMSI (PowerDNS) AVANT le transfert : meme contenu, TTL court (300s).
58. Reduire le TTL des enregistrements actifs cote registrar source 24h avant le D-Day.

59. D-Day : recuperer le code de transfert, deverrouiller le domaine, lancer le transfert depuis le panneau JMSI.
60. Confirmer reception cote registrar source (mail).
61. Une fois le transfert acheve (1 a 5 jours selon TLD), basculer les NS vers ceux de JMSI : ns1.jmlab.eu, ns2.jmlab.eu.
62. Verifier la propagation : whois et dig depuis plusieurs resolveurs publics (8.8.8.8, 1.1.1.1, 9.9.9.9).

**ATTENTION** La bascule des NS prend jusqu'a 48h pour se propager mondialement. Pendant cette periode, services hybrides (certains visiteurs sur ancien NS, d'autres sur nouveau) : la zone DOIT etre identique des deux cotes.

# 3.4 Mail : domaine, boites, SPF/DKIM/DMARC

## 3.4.1 Architecture mail JMSI (Mailcow)

L'environnement mail JMSI repose sur la suite Mailcow Dockerized, en haute disponibilite. Une instance par client (ou mutualisee selon volume).

```
# Mailcow - structure docker-compose (resume technicien)
# Conteneurs principaux
# - postfix-mailcow      (SMTP)
# - dovecot-mailcow      (IMAP/POP/Sieve)
# - rspamd-mailcow       (anti-spam)
# - sogo-mailcow         (webmail + calendar/contacts)
# - nginx-mailcow        (reverse proxy + auto-cert Let's Encrypt)
# - mysql-mailcow        (mariadb backend)
# - clamd-mailcow        (antivirus)
# - acme-mailcow         (gestion certificats)
```

## 3.4.2 Procedure : ajout d'un domaine + boite mail

63. Creer le domaine dans la console Mailcow JMSI (https://mail.jmlab.eu/admin) : Domain > Add domain.
64. Definir le nombre maximum de boites, l'espace par boite, le DKIM (selector dkim).
65. Recuperer la cle publique DKIM generee : Configuration > ARC/DKIM keys > <domaine>.
66. Sur la zone DNS du client (PowerDNS JMSI), publier les 3 enregistrements de protection :

```
; SPF - declare les emetteurs autorises pour ce domaine
<domaine>.          300 IN  TXT  "v=spf1 mx a:mail.jmlab.eu ~all"

; DKIM - signe les mails sortants (selector visible en console Mailcow)
dkim._domainkey.<domaine>. 300 IN TXT "v=DKIM1; k=rsa; p=<clef_publique_RSA>"

; DMARC - politique applicable aux mails non-conformes
_dmarc.<domaine>.     300 IN  TXT  "v=DMARC1; p=quarantine;
rua=mailto:dmarc@<domaine>; ruf=mailto:dmarc@<domaine>; sp=quarantine; aspf=s;
adkim=s"

; MX - serveur de messagerie
<domaine>.          3600 IN MX 10 mail.jmlab.eu.

; AutoConfig (Thunderbird)
autoconfig.<domaine>. 3600 IN CNAME mail.jmlab.eu.

; AutoDiscover (Outlook)
```

```
autodiscover.<domaine>. 3600 IN CNAME mail.jmlab.eu.
_autodiscover._tcp.<domaine>. 3600 IN SRV 0 0 443 mail.jmlab.eu.
```

67. Creer la boite mail : Mailbox > Add mailbox. Note du mot de passe initial dans Bitwarden (collection client).
68. Le client recoit un mail d'activation (modele JMSI) : URL webmail, parametres IMAP/SMTP, capture du parametrage Outlook/Thunderbird.
69. Verifier le scoring SPF/DKIM/DMARC du domaine : envoyer un mail vers check-auth@verifier.port25.com et lire la reponse.

**ATTENTION** Si le client passe d'un autre prestataire, prevoir une fenetre de test : creer la boite cote JMSI, faire pointer le MX progressivement (TTL court), surveiller les retours pendant 24h avant suppression chez l'ancien prestataire.

### 3.4.3 Politique anti-spam Rspamd

Rspamd est configure avec les politiques JMSI : seuil 6 (greylist), seuil 12 (rejet). Ajustement par client si faux positifs frequents.

```
# Settings Rspamd JMSI (extraits)
actions {
  reject = 12;
  add_header = 6;
  greylist = 4;
}

# Whitelist client : IP, domaine, expediteur
# /etc/rspamd/local.d/whitelist.local.conf
local_addrs = [ "127.0.0.1", "::1", "<IP_CLIENT_RELAIS>" ];
```

### 3.4.4 Mailinblack : protection avancee anti-phishing

Mailinblack est une protection mail SaaS partenaire. Activation pour les clients sensibles (NIS2, professions reglementees, finance). Tarif : 2,90 EUR HT/boite/mois (B2B_HEB_07).

70. Cote console Mailinblack JMSI : creer le compte client, ajouter le domaine.
71. Recuperer les MX et les hostnames Mailinblack (in-eu.mailinblack.com) a publier sur la zone DNS client.
72. Publier en zone DNS : MX 10 in-eu.mailinblack.com (et MX 20 in-eu2.mailinblack.com).
73. Mettre en place le rerouting cote Mailinblack : envoi vers mail.jmlab.eu apres analyse.
74. Cote Mailcow : whitelister les IPs Mailinblack (sortant Mailinblack vers Mailcow).
75. Tester avec un mail externe : verifier les en-tetes (X-MailScanner-* ou equivalent).

## 3.5 Hebergement Web - WordPress infogere

### 3.5.1 Architecture

Pour les sites WordPress, JMSI propose deux options :

- Option mutualisee (B2B_HEB_03 + WordPress libre, 9,90 EUR) : LiteSpeed Web Server, jails Linux par site, < 50 sites par node, sauvegarde quotidienne.

- Option WordPress infogere (B2B_HEB_04, 69 EUR) : meme infrastructure + MAJ noyau et plugins, sauvegarde toutes les heures, supervision uptime, durcissement Wordfence ou Solid Security, audit annuel.

### 3.5.2 Migration d'un site WordPress vers JMSI

76. Creer l'instance vide cote JMSI : choix de la version PHP (8.2 ou 8.3 selon compatibilite plugins).
77. Acceder au site source : SFTP ou cPanel ou Plesk.
78. Sauvegarder la base : depuis phpMyAdmin source, export SQL complet (avec DROP TABLE).
79. Sauvegarder les fichiers : tar.gz du dossier wp-content (themes, plugins, uploads) + wp-config.php pour reference.

```
# En SSH cote source (si possible)
cd /chemin/du/site/wordpress
tar czvf /tmp/wp_files.tgz wp-content
mysqldump --single-transaction --routines --triggers \
        -u <USER> -p <DB> > /tmp/wp_db.sql
# Telechargement vers le poste technicien (scp ou sftp)
scp /tmp/wp_files.tgz technicien@<IP>:/tmp/
scp /tmp/wp_db.sql   technicien@<IP>:/tmp/
```

80. Cote JMSI : decompresser wp_files.tgz dans /var/www/<domaine>/.
81. Importer la base : mysql -u <USER> -p <NEW_DB> < wp_db.sql.
82. Editer wp-config.php : nouvelles credentials BDD, nouvelle URL si differente.
83. Mettre a jour les URL dans la base (search-replace WP-CLI) :

```
# WP-CLI - obligatoire pour les URL serialisees
cd /var/www/<domaine>
wp search-replace 'http://ancien-domaine.fr' 'https://nouveau-domaine.fr' \
    --skip-columns=guid --all-tables

# Verifier l'integrite
wp core verify-checksums
wp plugin verify-checksums --all

# Reinitialiser les permaliens
wp rewrite flush --hard

# Verifier la sante du site
wp doctor check --all

# Mises a jour
wp core update
wp plugin update --all
wp theme update --all
```

84. Configurer le certificat TLS Let's Encrypt (HAProxy + acme.sh JMSI).
85. Tester en preprod via le fichier hosts (avant bascule DNS).
86. Bascule DNS (TTL court) + monitoring uptime 24h.
87. Une fois la bascule stable : suppression du site source.

### 3.5.3 Durcissement WordPress

- MAJ noyau, themes et plugins automatiques (option WordPress infogere).
- Plugin securite : Wordfence ou Solid Security Pro (Bitdefender Cybersecurity for Cloud Workloads en option).

- Limiter les tentatives de connexion : Limit Login Attempts ou natif Wordfence.
- Desactiver l'editeur de fichier admin (DISALLOW_FILE_EDIT = true).
- Forcer SSL administration (FORCE_SSL_ADMIN = true).
- Desactiver XML-RPC si non utilise.
- Sauvegarde toutes les heures (incremental) + 1 quotidienne (full + immuable Wasabi).
- Scan malware hebdomadaire (Wordfence ou ClamAV serveur).
- Audit fichiers .php non standard tous les mois.

# 3.6 Nextcloud (GED B2B_HEB_05)

## 3.6.1 Architecture

Nextcloud est deploye en VM dediee par client (capacite > 50 utilisateurs ou > 500 Go) ou mutualise.

| Composant | Logiciel | Role |
|---|---|---|
| **Application** | Nextcloud Hub 28+ | Front PHP, partage, calendar, contacts, talk |
| **Base de donnees** | PostgreSQL 15 | Metadonnees, sessions |
| **Cache** | Redis | Sessions, fichiers locks |
| **Stockage primaire** | POSIX local (volume Ceph) | Fichiers utilisateurs |
| **Stockage secondaire** | S3 Wasabi | Archivage cold + sauvegarde immuable |
| **Antivirus** | ClamAV | Scan a l'upload |

## 3.6.2 Procedure d'ouverture d'un acces Nextcloud

88. Cote console JMSI Nextcloud : creer le groupe client (si n'existe pas).
89. Creer l'utilisateur, l'affecter au groupe, definir le quota.
90. Activer la double authentification (TOTP par defaut) - obligatoire pour les clients NIS2.
91. Generer un mot de passe initial robuste (15 chars min) et le placer dans Bitwarden.
92. Envoyer le mail d'activation (modele JMSI) : URL https://cloud.<sous-domaine>.fr, login, mot de passe, lien vers le client desktop.
93. Si demande : creer un partage de groupe initial avec les dossiers metiers (RH, Ventes, etc.).

## 3.6.3 Configuration client de bureau

```
# Le client desktop Nextcloud est telechargeable depuis :
# https://nextcloud.com/install/#install-clients

# Configuration en CLI Linux
nextcloudcmd --user <login> --password <mdp> \
          --silent /home/<user>/Nextcloud https://cloud.jmlab.eu

# Recommandations JMSI :
# - Choisir 'Synchroniser uniquement ce que je demande' (Virtual Files) si > 100 Go
# - Activer le chiffrement bout en bout sur les dossiers sensibles
# - Configurer les notifications (mention, partage, conflit)
```

# 3.7 Deploiement CRM en ligne (B2B_HEB_06)

Le CRM en ligne JMSI est generalement Dolibarr (cf. chapitre 13) ou un CRM dedie partenaire (SuiteCRM, EspoCRM). Cette section traite du cas generique : creation d'un environnement, import des donnees, integration aux outils en place.

## 3.7.1 Procedure type de creation d'instance

94. Provisionner la VM (template JMSI : Debian 12, 4 vCPU, 8 Go RAM, 80 Go disque).
95. Installer le stack LAMP/LEMP : Apache/Nginx, PHP-FPM, MariaDB/PostgreSQL.
96. Deployer le CRM choisi (cf. chapitre dedie).
97. Creer les utilisateurs initiaux. MFA obligatoire.
98. Importer les donnees client (CSV, ODS) en utilisant les outils natifs ou un script Python sur mesure.
99. Configurer la sauvegarde (backup-job dedie : dump SQL + tar des fichiers, vers Wasabi).
100. Tester par un utilisateur reel avant la formation.

# 3.8 Mise en service Simply Food (et applications metier hebergees)

Simply Food (logiciel pour la restauration collective) est un exemple representatif des applications metier que JMSI heberge en mode SaaS pour ses clients. Le mode operatoire est transposable a la plupart des applications PHP/MySQL ou .NET hebergees.

## 3.8.1 Pre-requis editeur

- Recuperer la documentation editeur (Simply Food : version, dependances, ports, droits).
- Verifier la licence (cle, periode, nombre d'utilisateurs).
- Identifier le sens de l'integration : standalone, ERP back-end, EDI fournisseur.

## 3.8.2 Procedure de mise en service generique

101. Provisionner la VM selon les specifications editeur (souvent : Debian 12, 8 Go RAM mini, 100 Go disque).
102. Installer les pre-requis logiciels : nginx, PHP-FPM 8.x, MySQL 8 ou MariaDB 10.11, ImageMagick selon module.
103. Installer l'application via le package fourni par l'editeur.
104. Configurer le pool PHP-FPM dedie (limites memory, max_children).
105. Configurer le reverse proxy HAProxy (cote DMZ JMSI) avec TLS Let's Encrypt.
106. Configurer la sauvegarde dediee (planification interne JMSI).
107. Tester en condition reelle (utilisateur metier client).
108. Documenter dans le dossier de base : URL, version, contact editeur, plan de MAJ.

# 3.9 Supervision et exploitation hebergement

L'infrastructure hebergement JMSI est supervisee 24/7 par un duo Zabbix + UptimeRobot.

| Composant supervise | Outil | Frequence | Seuil d'alerte |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **Disponibilite externe (HTTP/HTTPS)** | UptimeRobot | 60s | 2 echecs consecutifs |
| **Latence et certificat TLS** | Zabbix | 5 min | Latence > 1500 ms / certif < 30 jours |
| **CPU/RAM/Disk hyperviseurs** | Zabbix | 1 min | > 85 % pendant 10 min |
| **Espace disque VM clientes** | Zabbix agent | 5 min | > 85 % |
| **Etat sauvegardes** | Borgmatic + alerte mail | Apres chaque job | Echec ou warning |
| **File mail (queue Postfix)** | Zabbix script | 1 min | > 100 mails en queue |
| **Detection rebond mail (bounce)** | Zabbix log | Temps reel | Bond > 5 % en 1h |
| **Mise a jour securite** | Wazuh / OSSEC | Quotidien | Nouvelle CVE > 7 / 10 |

### 3.9.1 Procedures recurrentes

- Quotidien : verifier les sauvegardes (Borgmatic + Veeam pour les VM strategiques).
- Quotidien : revue des alertes Zabbix nuit -> 8h.
- Hebdomadaire : revue des accumulations de mails en quarantaine, blacklist Postfix.
- Mensuel : RAS hebergement aux clients > 2 services.
- Trimestriel : test de restauration sur un site WordPress (cyclique).
- Semestriel : test de bascule HAProxy (failover noeud).
- Annuel : montee de version Mailcow / Nextcloud / Dolibarr (planifiees, communiquees).

## 3.10 Depannage hebergement

### 3.10.1 Site web 502 Bad Gateway

109. Verifier l'etat du backend (PHP-FPM ou app cible) : systemctl status php8.2-fpm.
110. Examiner les logs : tail -f /var/log/php8.2-fpm.log et /var/log/nginx/error.log.
111. Si crash PHP : augmenter memory_limit (mais investiguer la cause).
112. Si timeout : verifier max_execution_time, fastcgi_read_timeout HAProxy.
113. Si surcharge : verifier les processus, eventuellement throttling Wordfence.

### 3.10.2 Mail rejete par destinataires (free.fr, orange.fr)

114. Verifier reverse DNS : dig -x <IP_SORTIE_MAILCOW> doit pointer vers mail.jmlab.eu.
115. Verifier blacklists : check-auth, mxtoolbox, spamhaus.
116. Verifier SPF/DKIM/DMARC sur le domaine emetteur.
117. Si rate-limit operateur : reduire le debit mail (transport_maps), ouvrir un dossier deliverability.

### 3.10.3 Nextcloud lent

118. Verifier Redis : redis-cli ping.

119. Activer mode preview generator pour reduire le calcul a la volee.
120. Verifier les commandes occ : occ files:scan --all et occ db:add-missing-indices.

## 3.11 Securite et conformite

- TLS 1.2/1.3 obligatoire ; ssl_protocols nginx restrictif.
- HSTS active (preload pour les domaines critiques apres validation client).
- CSP (Content Security Policy) sur les apps modernes.
- Authentification a 2 facteurs obligatoire pour tous les acces administration.
- Audit semestriel : revue des CVE applicables aux applications hebergees.
- Conformite RGPD : registre des traitements JMSI (interne) + clauses DPA dans le contrat.
- Conformite eIDAS pour les signatures electroniques (DocuSign / Yousign integres).

## 3.12 Migration sortante / desengagement

Comme pour la maintenance, le client peut a tout moment demander la migration sortante. JMSI s'engage a fournir l'export complet de son patrimoine numerique.

- Mail : export IMAP complet via imapsync (boites + dossiers + flags).
- Site web : archive ZIP du document root + dump SQL.
- Nextcloud : export OCC + tar des fichiers /data utilisateur.
- Dolibarr/CRM : dump SQL + dossier documents/.
- Domaine : code de transfert + delegation NS au choix du client.
- Apres migration : retention des donnees 30 jours puis purge securisee.

# PARTIE III

# Securite et resilience

# Chapitre 4 - Sauvegarde et Plan de Reprise d'Activite (3-2-1)

## 4.1 Perimetre

La sauvegarde est l'offre la plus strategique de JMSI : elle protege la continuite d'activite du client. Une sauvegarde mal configuree, jamais testee, ou trop lente est pire qu'une absence de sauvegarde : elle cree une fausse securite. Ce chapitre est de niveau pratique avancee et impose la regle 3-2-1 a tout client JMSI sans exception.

| Code Dolibarr | Designation | Tarif HT mensuel |
|---|---|---|
| **B2B_SAU_01** | Backup Poste de travail (par poste) | 4,90 EUR |
| **B2B_SAU_02** | Backup Serveur 500 Go | 29,00 EUR |
| **B2B_SAU_03** | Backup Serveur 2 To | 79,00 EUR |
| **B2B_SAU_04** | PRA Complet (sauvegarde + plan + tests) | 149,00 EUR / mois |
| **B2B_SAU_05** | Audit Donnees Critiques | OFFERT |

## 4.2 La regle 3-2-1 appliquee

La regle 3-2-1 est le standard de fait des sauvegardes professionnelles. JMSI l'applique sans exception sur tous les contrats Sauvegarde et PRA. Les variantes 3-2-1-1 et 3-2-1-1-0 sont introduites pour les clients NIS2 et les structures > 50 postes.

| Regle | Signification | Implementation JMSI standard |
|---|---|---|
| **3** | 3 copies des donnees | Production + sauvegarde locale + sauvegarde hors site |
| **2** | 2 supports differents | Disque interne + NAS local + stockage objet (Wasabi/B2) |
| **1** | 1 copie hors site | Wasabi (Hambourg/Amsterdam) ou serveur sauvegarde JMSI |
| **+1 (variante)** | 1 copie immuable / offline | Wasabi compliance (S3 Object Lock) ou disque externe rotatif |
| **+0 (variante)** | 0 erreur a la verification | Test de restauration trimestriel obligatoire |

**ATTENTION** Une sauvegarde non testee n'est pas une sauvegarde. Le test de restauration trimestriel est inclus de droit dans le contrat PRA Complet (B2B_SAU_04).

# 4.3 NAS Synology - mise en service standard JMSI

Le NAS Synology est la cible de sauvegarde locale privilegiee chez nos clients PME. Modeles standards JMSI :

| Modele | Cible | Disques recommandes | Volume utile |
|---|---|---|---|
| **DS224+** | TPE 1-5 postes | 2 x WD Red Plus 4 To | 4 To en RAID 1 |
| **DS423+** | PME 5-15 postes | 4 x Synology HAT3300 8 To | 16 To en SHR-1 |
| **DS923+** | PME 15-30 postes | 4 x HAT5300 12 To | 32 To en SHR-1 |
| **RS1221+** | PME 30+ postes / serveurs critiques | 8 x HAT5300 16 To + 2 SSD M.2 cache | 84 To en RAID 6 |

## 4.3.1 Pre-deploiement - hardening et configuration de base

121. Reception du NAS : controle visuel, photo serie, photo des disques.
122. Insertion des disques (poste antistatique).
123. Premier branchement reseau : utiliser le LAN JMSI bench (pas directement chez le client).
124. Decouverte sur LAN : Synology Assistant ou find.synology.com.
125. Installation DSM 7.2.x ou superieur (DSM 7.3 si disponible).
126. Application immediate des reglages JMSI suivants (avant toute donnee).

```
# Hardening JMSI initial - DSM Web UI puis CLI SSH (admin temp)

# 1) Renommer le NAS, fuseau horaire, pool NTP
#    Panneau de configuration > Regional Options : Europe/Paris, fr_FR
#    Panneau de configuration > Time : NTP fr.pool.ntp.org

# 2) Compte admin : desactiver, creer un compte JMSI dedie
#    Panneau de configuration > Utilisateur > admin > Desactiver
#    Creer 'jmsi-admin' avec MFA TOTP obligatoire (mot de passe fort en Bitwarden)

# 3) Reseau
#    IP fixe selon plan client (cf. dossier de base)
#    Activer LACP si 2 ports (NAS / switch)
#    Activer SSH UNIQUEMENT si necessaire, sur port non-standard, IP source restreinte

# 4) Firewall DSM
#    Activer le pare-feu, autoriser uniquement 5000/5001 depuis LAN
#    Bloquer Internet sortant sauf NTP, MAJ DSM, Active Backup destination

# 5) Auto-block et 2FA
#    Panneau > Securite > Compte : Auto-block active 5 echecs / 10 min, ban 30 min
#    2FA OBLIGATOIRE pour admin

# 6) Securite avancee
#    Activer DoS protection, Security Advisor en mode Maximum
#    Activer 'Auto rotate logs', conservation 12 mois minimum

# 7) Reseau cible : forcer SMB v2/v3, desactiver SMB1, AFP off
#    File Services > SMB > Avance : SMB Min v2, Max v3
#    Activer le chiffrement SMB encryption (CIFS encryption)
```

### 4.3.2 Creation des dossiers et permissions

127. Creer le pool de stockage SHR-1 (ou SHR-2 si > 5 disques).
128. Creer un volume (1 a 3 selon usage).
129. Creer les dossiers partages : 'sauvegardes' (cible Active Backup) + 'shares' si partage de fichiers actif.
130. Pour le dossier sauvegardes : ACL stricte (uniquement compte de service backup) + SnapShot Replication.
131. Activer Snapshots planifies : toutes les heures, retention 24 snapshots ; quotidiens 14 jours ; hebdo 4 semaines ; mensuels 6 mois.
132. Verifier que les snapshots sont immuables (read-only system snapshots).

### 4.3.3 Active Backup for Business

ABB est l'outil natif Synology pour sauvegarder les postes Windows, serveurs Windows, Hyper-V, VMware, Microsoft 365, Google Workspace.

- Sauvegarde Windows : agent ABB Windows installe sur chaque poste/serveur, image incremental forever.
- Sauvegarde Hyper-V/VMware : sans agent, snapshot CBT-aware, fenetre nuit.
- Sauvegarde Microsoft 365 : token OAuth, snapshot quotidien des boites + OneDrive + SharePoint + Teams.
- Politique JMSI : retention 30 jours quotidiens + 12 mois hebdo + 7 ans mensuels (conformite comptable FR).

### 4.3.4 Hyper Backup vers Wasabi (3-2-1)

Hyper Backup envoie les donnees du NAS vers un stockage objet hors site (Wasabi).

```
# Cote NAS Synology - Hyper Backup
# Source : dossiers 'sauvegardes' + applications selectionnees
# Destination : 'S3 storage' compatible -> Wasabi region eu-central-1
# Compte JMSI Wasabi : un bucket par client, naming jmsi-<CODE>-backup

# Compression et chiffrement OBLIGATOIRES
# - Compression : oui
# - Cle de chiffrement : AES-256, cle generee, stockee en Bitwarden
# - Lifecycle : non (Wasabi inclut deja 90 jours minimum)
# - Plan : 'Smart Recycle' (jour, semaine, mois)

# Politique JMSI : 30/12/7 (30 jours, 12 hebdo, 7 mensuels)
# Object Lock cote Wasabi : Compliance mode pour les clients NIS2
```

### 4.3.5 Synology et ransomware - hardening avance

- Compte de service avec MFA et droits limites au dossier de sauvegarde uniquement.
- SMB chiffre (encryption SMB3).
- Snapshots immuables (DSM ne permet pas de supprimer un snapshot system avant fin de retention).
- Active Backup : repertoire de destination accessible uniquement par compte de service backup.
- Retention WORM (write once read many) cote Wasabi avec Object Lock en mode Compliance.
- Alerte SMS au technicien JMSI en cas de suppression de snapshot ou volume (Synology Notification + script).

# 4.4 Sauvegarde Cloud immuable - Wasabi / S3

## 4.4.1 Choix de la solution objet

| Fournisseur | Region UE | Tarif indicatif | Object Lock | Notes |
|---|---|---|---|---|
| **Wasabi** | eu-central-1 (Amsterdam) | 5,99 USD/To/mois - egress gratuit | Oui (Compliance) | Choix par defaut JMSI |
| **Backblaze B2** | eu-central-003 | 6 USD/To/mois - egress 1 % gratuit | Oui | Alternative tactique |
| **Scaleway Object Storage** | fr-par-1 | 0,01 EUR/Go/mois | Oui | Souverainete FR |
| **AWS S3 Glacier Deep Archive** | eu-west-3 (Paris) | 0,002 USD/Go/mois | Oui | Archivage long terme uniquement (delai restitution > 12h) |

## 4.4.2 Configuration cote Wasabi (par client)

133. Creer le bucket : jmsi-<CODE_CLIENT>-backup (region eu-central-1).
134. Activer Object Lock en mode Compliance, retention 30 jours minimum.
135. Creer une politique IAM : accees write-only au bucket pour le compte client (pas de delete avant expiration).
136. Generer access_key + secret_key, stockees Bitwarden (collection client).
137. Publier les credentials dans le tool de sauvegarde (Hyper Backup, Veeam, Borg, etc.).

# 4.5 Veeam Backup & Replication (architecture serveur)

## 4.5.1 Cas d'usage

Veeam B&R est deploye sur tous les sites avec :

- Plus de 2 serveurs (physiques ou VM).
- Hyperviseur Hyper-V ou VMware.
- Volume sauvegarde > 1 To.
- RPO requis < 4h.

## 4.5.2 Architecture standard

| Composant | Localisation | Role |
|---|---|---|
| **Veeam Backup Server** | VM Windows Server 2022 | Console, scheduler, WAN accelerator si multi-site |
| **Veeam Repository (primaire)** | NAS Synology (iSCSI ou SMB) ou serveur dedie | Repository disque local |
| **Veeam Repository (secondaire)** | Wasabi via Capacity Tier | Tier objet, immutability Object Lock |

| | | |
|---|---|---|
| **Veeam Proxy** | VM dans cluster Hyper-V | Lecture des snapshots, deduplication, compression |
| **Veeam Agent Windows** | Sur les serveurs physiques bare-metal | Sauvegarde des serveurs hors hyperviseur |

### 4.5.3 Procedure de mise en service Veeam

138. Provisionner la VM : Windows Server 2022 Standard, 8 vCPU, 16 Go RAM, 100 Go OS + 200 Go BD.
139. Installer Veeam B&R 12.x (cle JMSI MSP).
140. Ajouter les hyperviseurs (Hyper-V, vCenter, ESXi standalone).
141. Ajouter les repositories : repo primaire (Synology iSCSI), capacity tier (Wasabi).
142. Creer Scale-Out Backup Repository (SOBR) : performance tier + capacity tier + offload immediate (immutable).
143. Creer les Backup Jobs :

- Job 'Critical' : RPO 1h, retention 30 restore points + GFS 12 hebdo + 7 mensuels.
- Job 'Production' : RPO 4h, retention 14 restore points + GFS 4 hebdo + 12 mensuels.
- Job 'File Server' : RPO 12h, retention 7 restore points.
- Job 'Microsoft 365' : agent Veeam Backup for Microsoft 365 (separe).

144. Configurer SureBackup : verification automatique de restaurabilite (boot et test ping VM cloned).
145. Configurer la replication vers le site secondaire (datacenter JMSI) si client critique.
146. Documenter dans le dossier de base : RTO/RPO atteignables reellement.

### 4.5.4 Veeam SureBackup et tests automatises

```
# Veeam PowerShell - Test automatise mensuel
Add-PSSnapin VeeamPSSnapin

$jobs = Get-VBRJob | Where-Object { $_.JobType -eq 'Backup' }
foreach ($job in $jobs) {
    Start-VBRSureBackupJob -Job (Get-VBRSureBackupJob -Name "SB-$($job.Name)") -RunAsync
}

# Le rapport est genere automatiquement et envoye en mail
# JMSI : copie du rapport dans
/clients/<CODE>/05_sauvegardes_pra/<DATE>_surebackup.html
```

## 4.6 Kopia (alternative open source)

Kopia est une alternative legere a Veeam pour les structures plus petites (1-3 serveurs). Elle est utilisee par JMSI pour les clients TPE qui souhaitent une solution open-source auditable, ou en complement comme troisieme copie.

### 4.6.1 Installation Kopia

```
# Linux server (Debian 12)
curl -s https://kopia.io/signing-key | sudo apt-key add -
echo 'deb http://packages.kopia.io/apt/ stable main' | \
    sudo tee /etc/apt/sources.list.d/kopia.list
```

```
sudo apt update && sudo apt install -y kopia

# Windows server
# Telecharger l'installeur MSI depuis kopia.io
# Installer en mode silencieux
msiexec /i KopiaUI-<version>-x64.msi /quiet /norestart

# Initialiser un repository S3 / Wasabi
kopia repository create s3 \
  --bucket=jmsi-<CODE>-kopia \
  --endpoint=s3.eu-central-1.wasabisys.com \
  --access-key=<AK> --secret-access-key=<SK>

# Creer une source et un snapshot
kopia snapshot create /var/data

# Definir une politique
kopia policy set /var/data \
  --keep-hourly 24 --keep-daily 30 --keep-weekly 12 --keep-monthly 12 --keep-annual 7

# Planifier - via systemd timer ou scheduler natif Kopia
systemctl enable --now kopia.service
```

## 4.7 Sauvegarde HDD externe (sites isoles, complementaires)

Le HDD externe rotatif reste pertinent : connexion ponctuelle au NAS, sortie hors site, retour. Methode 'air-gap' simple et efficace contre le ransomware. JMSI utilise cette methode en complement et non en remplacement.

### 4.7.1 Procedure JMSI standard

- 3 disques externes 2,5" USB-C (typiquement Seagate IronWolf Pro 6 To).
- Etiquetage clair : << Sauvegarde JMSI - Semaine A / B / C - <CLIENT> >>.
- Roulement hebdomadaire : disque A en local, disque B au coffre, disque C chez l'expert-comptable / dirigeant.
- Connexion : SHA-only (mode lecture seule en l'absence de sauvegarde active).
- Chiffrement BitLocker (Windows) ou LUKS (Linux). Cles dans Bitwarden.
- Verification mensuelle : checksum des fichiers, lecture aleatoire de 100 fichiers.

**ATTENTION** Le HDD externe ne suffit jamais seul. C'est un complement, pas une sauvegarde primaire. Les durees de vie reelles d'un HDD externe sont de 2 a 4 ans en usage rotatif.

## 4.8 PRA - Plan de Reprise d'Activite

Le PRA est le document maitre de la reprise d'activite client. Il decrit qui fait quoi, dans quel ordre, avec quels moyens, en cas de sinistre majeur (ransomware total, incendie, destruction du site, vol). Ce document doit tenir sur 5 a 8 pages, etre clair pour un non-IT, et etre TESTE chaque trimestre. Sans test, aucune confiance possible.

### 4.8.1 Structure type d'un PRA

| Section | Contenu |
|---|---|

| | |
|---|---|
| **1. Identification** | Client, sites concernes, criticite metier |
| **2. RTO / RPO** | Engagements chiffres : RTO 8h, RPO 1h pour les services critiques |
| **3. Sinistres couverts** | Ransomware, defaillance materiel critique, incendie, vol, inondation, force majeure |
| **4. Sinistres exclus** | Cyberattaque etat-nation, sinistre datacenter Wasabi (couvert par leur SLA) |
| **5. Inventaire critique** | Serveurs, applications, donnees - matrice criticite |
| **6. Acteurs et roles** | Decideur cote client, contact JMSI, contact assurance, contact metier |
| **7. Procedure de declenchement** | Quand on declenche, qui, comment (decision arbre) |
| **8. Procedure de reconstruction** | Sequence de restauration : socle reseau, AD, FS, applis |
| **9. Procedure de bascule** | Bascule sur site de secours / ressources cloud temporaires |
| **10. Test trimestriel** | Date du dernier test, scenario, resultat, anomalies, ameliorations |
| **11. Communication crise** | Messages types pour clients, salaries, partenaires, presse |

### 4.8.2 RTO et RPO de reference JMSI

| Service | RTO atteignable (avec PRA) | RPO atteignable (avec PRA) |
|---|---|---|
| **Active Directory** | 2 h | 1 h |
| **File Server (donnees)** | 4 h | 1 h |
| **Mail (Mailcow JMSI)** | 1 h | 5 min |
| **ERP/CRM (Dolibarr)** | 4 h | 1 h |
| **Application metier hebergee** | 8 h | 4 h |
| **Postes de travail (image)** | 2 h par poste | Aucun (master + profil itinerant) |
| **Telephonie VoIP** | 30 min | Aucun (cloud) |

### 4.8.3 Procedure de declenchement et premiere heure

147. [T+0] Detection : alerte EDR ransomware, appel utilisateur << tout est crypte >>.
148. [T+5 min] Isolation : couper le LAN du site (firewall en mode NO-INTERNET-INBOUND), couper VLAN clients sur le switch, debrancher les serveurs.
149. [T+15 min] Notification : Direction cote client + Direction technique JMSI + assurance cyber si presente.
150. [T+30 min] Constat : prise de notes (ce qui marche, ce qui ne marche pas), photos.
151. [T+45 min] Decision : invocation officielle du PRA - signature du decideur client.

152. [T+1h] Communication interne : equipe technique mobilisee, salaries informes, plan de continuite metier degrade enclenche.

### 4.8.4 Procedure de reconstruction (J+0 a J+1)

153. Verifier l'integrite du repository immuable Wasabi (le ransomware n'a pas pu y supprimer les sauvegardes).
154. Provisionner l'environnement de restauration : VM neuves dans datacenter JMSI ou sur site (si materiel sain).
155. Restaurer dans l'ordre : Active Directory > Reseau (DNS, DHCP) > File Servers > Applications metier.
156. Pour chaque service restaure : valider l'integrite (checksum, premier lancement controle, test fonctionnel).
157. Reseau : appliquer une politique restrictive (deny all, autoriser progressivement).
158. Postes utilisateurs : reset complet, reformatage, redeploiement par image master + restauration des donnees personnelles.
159. Bascule progressive utilisateur par utilisateur, par service.

### 4.8.5 Test PRA trimestriel - scenarios standard

| Trimestre | Scenario | Cible |
|---|---|---|
| **T1 (mars)** | Restauration d'un serveur AD a partir des sauvegardes | Verifier l'integrite des Veeam restore points |
| **T2 (juin)** | Restauration partielle d'une boite mail (10 messages) | Workflow de restauration utilisateur final |
| **T3 (septembre)** | Restauration complete d'une VM critique en environnement isole | Mesurer le RTO reel |
| **T4 (decembre)** | Test de declenchement complet (table-top exercise) | Coordination cote client + JMSI |

## 4.9 Procedures de restauration

### 4.9.1 Restauration de fichier (utilisateur final)

160. Demande utilisateur : ouvrir un ticket DEM-INF avec chemin du fichier perdu.
161. Identifier la sauvegarde la plus recente : Veeam Self-Service File Restore ou Synology File Station Snapshot.
162. Restaurer dans un repertoire temporaire (jamais directement sur l'emplacement original).
163. Demander a l'utilisateur de valider, puis copier au bon endroit.
164. Cloturer le ticket avec compte-rendu.

### 4.9.2 Restauration de boite mail

Selon l'outil :

```
# Mailcow - restaurer une boite via dump SQL + import
# Les sauvegardes Mailcow sont gerees par helper.sh
cd /opt/mailcow-dockerized
./helper-scripts/backup_and_restore.sh restore /backup/mailcow_<DATE>.tar.gz

# Veeam Backup for Microsoft 365 - PowerShell
# Restauration de boite individuelle
$session = Get-VBORestoreSession
$mailbox = Get-VBOMailbox -RestoreSession $session -Name 'user@domaine.fr'
Save-VBOEmailItem -Mailbox $mailbox -Path 'C:\Restore' -All
```

### 4.9.3 Restauration complete d'un serveur (bare-metal recovery)

165. Booter sur la cle Veeam Recovery Media (USB).
166. Choisir 'Bare Metal Recovery'.
167. Pointer vers le repository Veeam (LAN ou Wasabi).
168. Selectionner le restore point cible.
169. Mapper les disques (verifier la taille).
170. Lancer la restauration (compter 1 a 4h pour 500 Go).
171. Au reboot : configuration reseau, verification AD, controleur de domaine.

## 4.10 Audit donnees critiques (B2B_SAU_05) - methode JMSI

L'audit donnees critiques est offert (cf. plaquette). Il debouche sur le contrat PRA Complet. Methode JMSI : interview metier + cartographie technique + chiffrage du cout d'arret.

### 4.10.1 Trame d'interview metier

- Qu'est-ce que l'entreprise ne peut pas se permettre de perdre ?
- Combien de temps pouvez-vous supporter sans <X> avant un impact significatif ? (X = mail, ERP, fichiers, telephonie, applications metier)
- Quelle est l'ancienne te des donnees indispensables : 1 jour, 1 semaine, 1 an ?
- Combien coute une heure d'arret en chiffre d'affaires perdu ? (Tirer une fourchette : 200 - 800 EUR pour la PME francaise, ANSSI 2024).
- Avez-vous une assurance cyber ? Quelles exclusions ?
- Quels collaborateurs ont des droits administrateurs ? Sont-ils tous formes ?
- Avez-vous deja perdu des donnees ? Comment avez-vous reagi ?

### 4.10.2 Cartographie technique de l'audit

- Volumetrie precise par source de donnee (avec des-doublonage : repartition incremental vs full).
- Croissance moyenne mensuelle.
- Acceleration sur les annees recentes.
- Localisation des donnees : on-prem, NAS, cloud public, cloud prive.
- Test de la qualite des sauvegardes en place.
- Recensement des single points of failure (un seul tech, un seul switch, un seul serveur).

### 4.10.3 Livrable audit

- Page 1 - executive summary (a destination du dirigeant).

- Pages 2-3 - cartographie des donnees critiques.
- Pages 4-5 - etat actuel des sauvegardes (forces / faiblesses).
- Pages 6-7 - propositions JMSI (3 options : Essentiel, Confort, Premium).
- Page 8 - chiffrage et calendrier.

# Chapitre 5 - Cybersecurite : EDR, NGFW, VPN, MFA, gestion des secrets

## 5.1 Perimetre

L'offre Cybersecurite JMSI met en oeuvre une defense en profondeur : protection endpoint (EDR), perimetre reseau (NGFW), connexions distantes (VPN), gestion des identites (MFA), gestion des secrets (Bitwarden), audit et pentest. La logique est strictement defensive : nous ne livrons pas d'outil offensif au client, et nous ne touchons pas aux installations du client sans autorisation ecrite explicite.

| Code Dolibarr | Designation | Tarif HT mensuel |
|---|---|---|
| **B2B_SEC_01** | Pack Securite Essentiel | 4,90 EUR / poste |
| **B2B_SEC_02** | Pack Securite Pro | 9,90 EUR / poste |
| **B2B_SEC_03** | Bitwarden Entreprise | 4,00 EUR / utilisateur |
| **B2B_SEC_04** | Audit de securite / Pentest | 890,00 EUR (one-shot) |
| **B2B_SEC_05** | Audit initial securite | OFFERT |
| **B2B_SEC_06** | Pare-feu nouvelle generation VPN | 690,00 EUR (materiel) + 49,00 EUR/mois (infogerance) |

## 5.2 Pack Securite Essentiel vs Pro - matrice

| Composant | Essentiel | Pro |
|---|---|---|
| **EDR Bitdefender GravityZone Business Security** | Inclus | Inclus |
| **Anti-spam (Rspamd)** | Inclus mail JMSI | Inclus mail JMSI |
| **Mailinblack anti-phishing** | - | Inclus |
| **Protection ransomware avancee (Bitdefender ATP)** | - | Inclus |
| **Bitwarden Teams** | Inclus 1 utilisateur | Inclus 5 utilisateurs |
| **MFA gere** | TOTP standard | Hardware key (Yubikey) en option |
| **VPN entreprise (WireGuard)** | Sur demande | Inclus |
| **Audit semestriel** | - | Inclus |
| **Pentest (B2B_SEC_04)** | En option | 1 par an inclus pour > 20 postes |
| **Sensibilisation collaborateurs** | Email mensuel | Email + simulation phishing trimestrielle |
| **Conformite NIS2 (rapport annuel)** | - | Inclus |

| | | |
|---|---|---|

# 5.3 Mise en service EDR Bitdefender GravityZone

## 5.3.1 Architecture

JMSI exploite une console GravityZone Business Security multi-tenant (cloud Bitdefender). Chaque client est une 'company' au sens GravityZone. Les techniciens disposent d'un acces delegue.

## 5.3.2 Pre-requis sur les postes

- Windows 10 22H2 / 11 (toutes editions Pro/Enterprise/Education).
- RAM minimum 4 Go (8 Go recommande).
- Espace disque 2 Go libres.
- Pas d'autre antivirus (desinstaller Norton, McAfee, Avast - voir scripts ci-dessous).
- Pour macOS : 12 Ventura ou superieur.
- Pour Linux : Debian/Ubuntu LTS, RHEL/Rocky 8/9.

## 5.3.3 Procedure de deploiement

172. Cote console GravityZone : Companies > Add Company > <CODE_CLIENT>.
173. Network > Installation Packages > Create Package : choisir modules (Antimalware, Firewall, Content Control, Patch Management, ATP, EDR).
174. Telecharger le package MSI (Windows) ou DMG/RPM/DEB.
175. Deploiement : par TacticalRMM (script global), par GPO (msiexec), ou manuel.

```
REM Desinstallation des AV concurrents (script JMSI standard)
REM nettoyage_av_concurrents.bat - executer en admin

REM Norton
"%ProgramFiles(x86)%\NortonInstaller\InstallStub.exe" /Uninstall /SkipSurvey

REM McAfee
"%ProgramFiles%\McAfee\Endpoint\<v>\Uninstall.exe" /silent

REM Avast
"%ProgramFiles%\AVAST Software\Avast\setup\Instup.exe" /uninstall /silent

REM AVG
"%ProgramFiles%\AVG\setup\AVG_TuneUp\Instup.exe" /uninstall /silent

REM Reboot
shutdown /r /t 30 /c 'Reboot apres nettoyage AV - JMSI'

REM Installation Bitdefender silencieuse
REM Le package est obtenu depuis la console GravityZone (URL temporaire ou packageshare)

REM Installer en silencieux
epskit_x64.exe /silent /no-reboot

REM Verifier le service
sc query 'EPSecurityService'
```

```
sc query 'EPProtectedService'

REM Forcer la mise a jour signatures
"%ProgramFiles%\Bitdefender\Endpoint Security\product.console.exe" /update

REM Verifier la remontee dans la console
REM (le poste apparait sous 5 min)
```

### 5.3.4 Politique de securite JMSI standard

La politique JMSI (Endpoint > Policies > JMSI Standard) applique :

- Antimalware : scan en arriere-plan, scan complet hebdomadaire dimanche 22h.
- Web/HTTPS scan : actif, exclusion domaines metier autorises.
- Firewall : profil bureautique strict, autorisation des protocoles courants seulement.
- Content Control : blocage URL malveillantes, regles JMSI prefered.
- Device Control : blocage USB inconnus, ouverture badge USB autorisee.
- Patch Management : auto patch securite Windows + apps Microsoft.
- ATP (Pro uniquement) : behavioural detection, anti-exploit, ransomware protection.
- EDR (Pro uniquement) : telemetrie complete, retention 30 jours minimum.

### 5.3.5 Reponse a incident EDR

176. Alerte recue dans la console GravityZone (et par mail interne JMSI).
177. Triage : faux positif probable (heuristique sur app metier) ou vrai positif ?
178. Si vrai positif : isoler le poste (action 'Isolate from network' depuis la console).
179. Investiguer : timeline des processus, fichiers crees, connexions reseau.
180. Si ransomware : declencher PRA (cf. chapitre 4.8).
181. Si phishing/credential theft : reinitialiser les mots de passe, revoquer les sessions, MFA reset.
182. Si malware non destructif : nettoyage, scan complet, surveillance 7 jours.
183. Compte-rendu detaille au client (modele JMSI) sous 48h.

## 5.4 Pare-feu nouvelle generation (NGFW)

### 5.4.1 Choix d'equipement JMSI

| Modele | Cible | Debit FW (claire) | Debit avec IPS+SSL inspection |
|---|---|---|---|
| **OPNsense (PC industriel JMSI)** | PME 5-30 utilisateurs, budget serre | 1+ Gbps | 300-500 Mbps |
| **Stormshield SN-S 320** | PME 30-80 utilisateurs, conformite FR | 5 Gbps | 800 Mbps |
| **Stormshield SN-M 720** | PME 80-300 utilisateurs | 10 Gbps | 2 Gbps |
| **Fortinet FortiGate 60F** | PME 30-100, multi-site SD-WAN | 10 Gbps | 1.4 Gbps |
| **Fortinet FortiGate 100F** | PME 100-300, multi-VLAN avancees | 20 Gbps | 3 Gbps |

### 5.4.2 Mise en service OPNsense (cas standard PME)

184. Reception du materiel : PC industriel quad NIC (e.g. Protectli VP4670 ou equivalent JMSI).
185. Installer OPNsense 24.x sur le SSD interne (USB bootable).
186. Premier boot : assigner les interfaces (WAN, LAN, OPT1=DMZ, OPT2=GUEST).
187. Connexion via le LAN : https://192.168.1.1, login root.
188. Importer le template de configuration JMSI (XML).
189. Adapter au plan IP client (cf. dossier de base section 3).

#### *Reglages JMSI standard OPNsense*

```
# OPNsense - reglages JMSI a appliquer sur tout deploiement

# 1) Interfaces et VLANs
#   LAN         - 10.<ID_CLIENT>.10.0/24
#   GUEST (Wi-Fi)- 10.<ID_CLIENT>.50.0/24 (NAT, pas d'acces LAN)
#   DMZ         - 10.<ID_CLIENT>.100.0/24 (acces selectif)
#   MGMT        - 10.<ID_CLIENT>.99.0/24 (interfaces admin equipements)

# 2) DNS
#   Resolveur Unbound active
#   Forwarders : 9.9.9.9 (Quad9, blocage malware), 1.1.1.2 (Cloudflare safe)
#   DNS-over-TLS active

# 3) Suricata IDS/IPS
#   Regles ET Open + ETPro Telemetry (gratuites)
#   Mode IPS sur WAN, alerte uniquement sur LAN
#   Auto-update tous les jours 02:00

# 4) ClamAV en proxy + SquidGuard
#   Filtrage URL listes JMSI (categories : malware, phishing, drogue, adulte)
#   Whitelist par client (sites metier autorises)

# 5) WireGuard VPN site-to-site et road-warrior
#   Tunnel JMSI <-> client : MTU 1380, persistent keepalive 25s
#   Roadwarrior : peer par utilisateur, MFA Bitwarden + cle TOTP

# 6) Backups configuration
#   Auto-backup vers cloud JMSI (XML chiffre AES) toutes les nuits
#   Retention 90 jours

# 7) Monitoring
#   SNMP v3 lecture seule pour Zabbix JMSI
#   Syslog vers SIEM JMSI (rsyslog TCP 514)
```

### 5.4.3 Stormshield (cas conformite FR)

Stormshield est un editeur francais qualifie ANSSI (DR/CSPN). Choix prive pour les clients publics, sante, banque, et NIS2. Mise en service via Stormshield Network Management Center (SMC) qui permet la gestion centralisee.

- Provisionnement par template JMSI sur SMC.
- Bootstrapping ZTP (Zero Touch Provisioning) : usine -> auto-config a la premiere connexion.
- Politique JMSI : plage DMZ, IDS/IPS, ASQ (Active Security Qualification) en mode IPS.

- Reseau VPN IPsec ou SSL : MFA OBLIGATOIRE.
- Monitoring centralise dans SMC + SIEM JMSI.

### 5.4.4 Filtrage web et categories

La politique JMSI standard bloque par defaut les categories suivantes :

- Malware, phishing, command-and-control, anonymizers (Tor, VPN tiers non autorises).
- Adulte, jeux d'argent, drogue.
- Reseaux sociaux : autorise par defaut, sauf demande explicite client (productivite).
- Partage de fichiers personnel (WeTransfer, MegaUpload) : bloque, sauf exception.
- Streaming video : autorise mais throttle si > 50 % du debit (QoS).

## 5.5 VPN d'entreprise - WireGuard

### 5.5.1 Architecture

JMSI deploie WireGuard pour ses clients (rapidite, simplicite, securite). IPsec et OpenVPN sont conserves pour interconnexion site-to-site avec equipements legacy.

### 5.5.2 Configuration cote serveur (NGFW JMSI ou OPNsense)

```
# WireGuard cote serveur (OPNsense - editor du fichier ou via UI)
# /usr/local/etc/wireguard/wg0.conf

[Interface]
PrivateKey = <SERVER_PRIVATE_KEY>
Address = 10.99.99.1/24
ListenPort = 51820

# Peer roadwarrior - utilisateur client.example
[Peer]
PublicKey = <PEER_PUBLIC_KEY>
AllowedIPs = 10.99.99.10/32
PersistentKeepalive = 25

# Peer site-to-site - succursale Lyon
[Peer]
PublicKey = <PEER_PUBLIC_KEY_LYON>
AllowedIPs = 10.10.20.0/24
Endpoint = lyon.exemple.fr:51820
PersistentKeepalive = 25
```

### 5.5.3 Configuration cote client (Windows)

190. Telecharger l'application WireGuard pour Windows.
191. Importer le tunnel : cle .conf fournie par JMSI (signe DocuSign cote utilisateur, transmise via Bitwarden Send).
192. Configurer split-tunnel ou full-tunnel selon politique client.
193. Activer 'Block untunneled traffic' (kill-switch) : aucune fuite hors VPN.
194. Tester : ping vers IP interne client + verification IP publique.

### 5.5.4 RDP via VPN - cas frequent

Beaucoup de clients utilisent RDP (Bureau a distance Windows). JMSI N'AUTORISE JAMAIS RDP directement expose en Internet. RDP doit imperativement passer par VPN ou par RD Gateway MFA.

- Ouvrir le VPN WireGuard cote utilisateur.
- RDP vers le serveur cible : login = compte AD utilisateur.
- MFA : exiger une authentification forte (Duo, Azure MFA, ou hardware key) avant la session RDP.
- Politique GPO : verrouillage automatique apres 10 min, deconnexion apres 30 min d'inactivite.
- Audit : journaliser toutes les sessions RDP (event log + SIEM).

> **ATTENTION** RDP brute-force est l'un des vecteurs d'attaque les plus exploites. Tout RDP expose en clair sur Internet est une faute professionnelle.

## 5.6 Double authentification (MFA)

### 5.6.1 Politiques JMSI

- MFA obligatoire pour tout acces administrateur (poste, serveur, console JMSI).
- MFA obligatoire pour tout acces VPN, mail webmail, Microsoft 365, Google Workspace.
- MFA obligatoire pour Bitwarden, Nextcloud, Dolibarr (cote admin).
- MFA recommande pour les utilisateurs finaux (formation client).
- Methodes acceptees : TOTP (Google Authenticator, Aegis, Bitwarden Authenticator), Yubikey FIDO2.
- SMS interdit comme seul facteur (susceptible au SIM swap).

### 5.6.2 Deploiement MFA Microsoft 365

195. Acces console : entra.microsoft.com (Microsoft Entra ID).
196. Politique d'acces conditionnel JMSI standard : ALL USERS + MFA obligatoire + Block legacy authentication.
197. Sensibilisation utilisateurs : email + reunion 30 min + flyer.
198. Prevoir un compte break-glass (sans MFA, mot de passe long, supervision active).

## 5.7 Gestion des secrets - Bitwarden

### 5.7.1 Organisation Bitwarden JMSI

JMSI exploite une organisation Bitwarden Teams. Chaque client a une collection dediee. Les techniciens sont membres de groupes correspondant a leur perimetre.

- Organisation : 'JMSI'.
- Collections : 'INTERNE-JMSI', 'CLIENT-<CODE>' (une par client).
- Groupes : 'JMSI-N1', 'JMSI-N2', 'JMSI-N3', 'JMSI-DIRECTION'.
- Acces des techniciens : 'JMSI-N2' a toutes les collections clients en lecture/ecriture, 'JMSI-N1' en lecture seule sauf clients assignes.
- Audit log : toute lecture/modification est tracee, revue mensuelle JMSI.

### 5.7.2 Conventions de nommage Bitwarden

```
# Nom d'item Bitwarden : <CONTEXTE>:<CIBLE>:<COMPTE>
# Exemples

# Equipement reseau
NET:firewall.exemple.fr:admin
NET:switch-coeur.exemple.fr:admin

# Serveur
SRV:dc01.exemple.local:Administrator
SRV:dc01.exemple.local:jmsi-rmm   <-- compte de service JMSI

# Application
APP:dolibarr.exemple.fr:admin
APP:nextcloud.exemple.fr:admin

# Boite mail
MAIL:contact@exemple.fr:imap

# Bitwarden Send pour transmettre des secrets temporaires
# Toujours TTL 24h max, 1 seul acces, password protege
```

### 5.7.3 Bitwarden Entreprise pour le client (B2B_SEC_03)

- Creation d'organisation cliente dediee (separee de l'organisation JMSI).
- MFA obligatoire pour les utilisateurs.
- Politique de mots de passe : 14 chars min, complexite haute, rotation 12 mois.
- Formation utilisateurs : 1 webinaire JMSI + cheat sheet.
- Integration SSO en option (Microsoft Entra, Google Workspace).

## 5.8 Audit de securite et pentest (B2B_SEC_04)

### 5.8.1 Methode JMSI (audit interne 1 a 3 jours)

199. Audit organisationnel : politique mots de passe, MFA, sensibilisation, gestion incidents, gouvernance.
200. Audit technique externe : scan exposition Internet (Shodan-like), open ports, certificats expires, headers HTTP.
201. Audit reseau interne : scan nmap LAN, detection SMB/RDP/RPC mal configures.
202. Audit Active Directory : Bloodhound (path d'attaque), PingCastle, ADRecon.
203. Audit endpoint : configuration Bitdefender, BitLocker, MFA, comptes locaux.
204. Audit applicatif : test de l'application metier critique (entree user, acces concurrents).
205. Restitution : rapport executive (5 pages) + rapport technique (20-50 pages) + plan d'action chiffre.

### 5.8.2 Outils JMSI typiques

| Outil | Usage | Type |
|---|---|---|
| **Nmap** | Scan ports et services | Open source |
| **PingCastle** | Audit Active Directory | Gratuit/Pro |

| | | |
|---|---|---|
| **Bloodhound + SharpHound** | Cartographie chemins d'attaque AD | Open source |
| **Nessus Essentials** | Scan vulnerabilites | Gratuit jusqu'a 16 IPs |
| **OpenVAS / Greenbone** | Scan vulnerabilites complet | Open source |
| **Mitre ATT&CK Navigator** | Cadrage menace | Open source |
| **Have I Been Pwned API** | Verification mots de passe compromis | API gratuite |

### 5.8.3 Pentest - delegation a partenaire JMSI

Pour les pentests intrusifs (boite noire ou grise), JMSI delegue a un partenaire qualifie PASSI (Bercom, Synacktiv, Pradeo, Lexsi). JMSI cadre le perimetre, recoit le rapport, et accompagne la remediation.

## 5.9 Conformite NIS2 - rapport annuel (Pack Pro)

La directive NIS2 (UE 2022/2555, transposition FR 2024-2025) impose aux entites essentielles et importantes des obligations de gouvernance, de gestion des risques, de notification d'incident et de chaine d'approvisionnement. JMSI accompagne ses clients concernes.

### 5.9.1 Identification du client NIS2

- Secteurs essentiels : energie, transports, banque, infrastructures financieres, sante, eau, infrastructures numeriques, administration publique, espace.
- Secteurs importants : services postaux, gestion dechets, agroalimentaire, fabrication chimique, fournisseurs numeriques.
- Seuils : moyenne entreprise (> 50 salaries OU > 10 M EUR CA) en general.

### 5.9.2 Mesures techniques minimales attendues (Annexe A directive)

- Politique securite SI redigee.
- Gestion des incidents documentee.
- Continuite d'activite (PRA teste).
- Securite chaine d'approvisionnement.
- Securite acquisition et maintenance des SI.
- Politiques cryptographie.
- Politiques RH (sensibilisation, droit d'acces).
- Hygiene cyber et formation.
- Authentification multifacteur.
- Communications securisees.

### 5.9.3 Notification d'incident (24h - 72h - 1 mois)

- [24h] Pre-notification a l'autorite competente (ANSSI / cyberveille.gouv.fr).
- [72h] Notification de mise a jour avec evaluation initiale.
- [1 mois] Rapport final detaille.

- JMSI accompagne le client a chaque etape (preparation des contenus, transmission, suivi).

# 5.10 Sensibilisation collaborateurs

## 5.10.1 Programme JMSI annuel

- Janvier : email mensuel + flyer phishing.
- Fevrier : webinaire 30 min 'Mot de passe et MFA'.
- Mars : campagne phishing test (Pack Pro uniquement).
- Avril : email mensuel + flyer rancongiciel.
- Mai : webinaire 'RGPD et donnees personnelles'.
- Juin : email + cheatsheet 'Reagir face a un mail suspect'.
- Juillet/Aout : conseils vacances (telephone perdu, Wi-Fi public).
- Septembre : campagne phishing test (Pack Pro).
- Octobre : Mois europeen de la cybersecurite : 4 emails hebdo.
- Novembre : webinaire 'Securiser son smartphone et son cloud personnel'.
- Decembre : bilan annuel + 5 bonnes resolutions cyber.

# 5.11 Reponse a incident grave - playbook

## 5.11.1 Playbook ransomware

206. [T+0] Detection (alerte EDR, appel utilisateur).
207. [T+5 min] Isoler les machines infectees du reseau.
208. [T+10 min] Notifier la Direction technique JMSI + Decideur client.
209. [T+15 min] Couper le LAN site (firewall en deny-all).
210. [T+30 min] Constat photo + journaux. NE PAS payer la rancon.
211. [T+1h] Verifier l'integrite des sauvegardes immuables Wasabi (le ransomware n'y a pas acces).
212. [T+2h] Ouverture du dossier sinistre cyber-assurance, plainte commissariat.
213. [T+4h] Analyse forensique : souche du ransomware (NoMoreRansom.org), vecteur d'entree.
214. [T+6h] Decision officielle : reconstruire (PRA) - signe par le decideur.
215. [Jour 1-3] Restauration controlee - nouvelles VM, sauvegarde anterieure compromise verifiee.
216. [Jour 5-7] Bascule progressive utilisateurs.
217. [Jour 30] Retex complet ; mise a jour du PRA et durcissement post-incident.

## 5.11.2 Playbook compromission de comptes

218. Reset des mots de passe concernes (compte + delegations).
219. Revocation des sessions (Microsoft 365 : revoke-mguser ; Google Workspace : signOutAll).
220. Revocation des consentements OAuth.
221. Verification des regles de transfert mail (les attaquants creent des regles d'exfiltration).
222. Revue des derniers acces (audit log).
223. Activation MFA si manquant.
224. Communication metier (le compte a-t-il fait des actions douteuses ?).
225. Suivi 30 jours.

# PARTIE IV

# Communications

# Chapitre 6 - Telephonie IP et standard cloud

## 6.1 Perimetre

JMSI commercialise une telephonie IP cloud sous marque blanche, basee sur 3CX et un trunk SIP partenaire (Sewan, OVH Telecom ou Centile selon la zone). L'offre inclut postes IP, softphone mobile, SVI, portabilite, statistiques d'appel, integration CRM.

| Code Dolibarr | Designation | Tarif HT mensuel |
|---|---|---|
| **B2B_TEL_01** | Telephonie Starter (1 ligne) | 9,95 EUR |
| **B2B_TEL_02** | Telephonie Business (illimite fixe + 5 lignes) | 19,95 EUR |
| **B2B_TEL_03** | Telephonie Business Mobile (illimite + mobile) | 29,95 EUR |
| **B2B_TEL_04** | Numero ligne supplementaire | 4,90 EUR |
| **B2B_TEL_05** | Standard Vocal Interactif (SVI) | 9,90 EUR |
| **B2B_TEL_06** | Telephone IP (poste) | 59,00 EUR (achat unitaire) |
| **B2B_TEL_07** | Portabilite numero | OFFERTE |

## 6.2 Architecture cible

L'architecture standard JMSI repose sur un PBX 3CX heberge en Europe, des trunks SIP redondes vers operateurs partenaires, et un site client equipe de postes IP Yealink ou Fanvil + un firewall configure pour la VoIP.

| Composant | Modele de reference JMSI | Notes |
|---|---|---|
| **PBX** | 3CX v20 PRO ou Enterprise | Heberge dans cloud JMSI ou en VM client |
| **Trunk SIP** | Sewan / Centile / OVH / Bouygues Telecom Pro | Choix selon zone et tarif |
| **Postes IP entree de gamme** | Yealink T31G ou Fanvil X3SP-V2 | PoE, 2 lignes, ecran LCD |
| **Postes IP cadre** | Yealink T54W ou Fanvil X5U | Ecran couleur, BLF, Bluetooth, Wi-Fi |
| **Postes IP DECT (sans-fil)** | Yealink W76P (base + combine) | Etablissements multi-pieces |
| **Casque** | Jabra Engage 50 II / Yealink WH63 | USB ou DECT, suppresseur de bruit |
| **Softphone mobile** | 3CX Mobile App (iOS/Android) | QR code provisioning |
| **SBC/Firewall VoIP** | OPNsense + module siproxd ou | Si NAT problematique |

| | | |
|---|---|---|
| | NGFW | |

## 6.3 Pre-requis reseau

- Connexion Internet symetrique 5 Mbps + 100 kbps par appel concurrent (codec G.711) ou 35 kbps (G.729 / Opus).
- Latence < 150 ms vers le PBX. Jitter < 30 ms.
- VLAN VOICE dedie (recommande), tagging cote switch, priorisation QoS.
- Switches PoE+ (norme 802.3at) pour alimenter les postes IP en PoE.
- Ports UDP ouverts sortant : 5060 (SIP), 10000-20000 (RTP), 443 (TLS provisioning).
- DNS SRV pour decouverte du PBX (si configuration manuelle).

## 6.4 Mise en service d'un client telephonie

### 6.4.1 Phase 1 : recueil et plan de numerotation

226. Recueillir les numeros existants : SDA, GTR, SVA. Document d'audit Dolibarr 'Recueil info copieur' adapte VoIP.
227. Recueillir l'effectif et les besoins : qui prend les appels, qui appelle, en mobilite.
228. Etablir le plan de numerotation interne :

```
# Plan de numerotation type JMSI (adaptable)
# Postes : 1xx (1 a 99 postes)
#   100-199 : postes principaux
#   200-299 : postes salles, fax virtuel, conferences
# Standard : 9 (touche 0 redirige vers standard / SVI)
# International : 00 + indicatif + numero
# Local : numero direct sans prefixe
# SVI : 8xxx (en interne uniquement)

# Groupes de sonnerie
# 800 : Standard general (les 5 postes accueil)
# 801 : SAV (file d'attente)
# 802 : Compta
# 803 : Direction (decroche secretariat)
```

229. Definir les heures d'ouverture, les messages d'accueil, les renvois.

### 6.4.2 Phase 2 : creation cote 3CX

230. Console 3CX JMSI : Tenants > Add tenant > <CODE_CLIENT>.
231. Definir les regles entrante / sortante : trunk, prefixe, identification appelant.
232. Creer les extensions : nom, prenom, email (provisioning), groupe.
233. Creer les groupes de sonnerie / files d'attente.
234. Configurer le SVI (IVR) : enregistrer les messages (fichiers .wav 8 kHz mono, 16 bits si PCMU).
235. Configurer la taxation, l'enregistrement legal des appels (si client demande - DPA RGPD obligatoire).

### 6.4.3 Phase 3 : provisioning des postes IP

Le provisioning automatique evite la configuration manuelle de chaque poste.

```
# 3CX cote PBX
# Settings > Provisioning > add device
# - MAC adresse poste -> 00:0B:82:xx:xx:xx (Fanvil) ou 80:5E:0C (Yealink)
# - Modele detecte
# - Extension assignee
# - URL de provisioning generee

# Cote poste Yealink (factory reset)
# 1) Branchement PoE - le poste boote
# 2) Recupere DHCP option 66 (URL provisioning) ou pointer manuellement
# 3) Telecharge la config XML signee, applique et reboot

# Verification cote 3CX : l'extension passe en 'Registered'
```

### 6.4.4 Phase 4 : portabilite (B2B_TEL_07)

La portabilite consiste a porter le numero historique du client de son operateur actuel vers JMSI sans changer de numero.

236. Demande de portabilite signee par le titulaire (mandat de portabilite).
237. RIO (Releve d'Identite Operateur) du numero a porter (le client compose 3179 sur la ligne fixe).
238. Soumission a l'operateur partenaire (Sewan/Centile) - delai 6 a 10 jours ouvres.
239. Date de bascule confirmee : preparation cote 3CX (numero pret a recevoir).
240. Jour J : fenetre 6h-10h, bascule operateur, test entrant/sortant immediat.
241. Resiliation automatique de l'ancien contrat operateur a J+1.

**ATTENTION** Pendant la fenetre de portabilite (typ. 1h), les appels entrants peuvent etre rejetes. Prevenir le client. Faire un test depuis un mobile externe a J = bascule effective.

### 6.4.5 Phase 5 : softphone mobile

242. Cote 3CX : reextension > QR code provisioning, valable 60 min.
243. Cote utilisateur : telecharger 3CX Mobile, scanner le QR.
244. Tester en 4G/5G : appels entrant et sortant, push notification.
245. Recommander le mode Push, le codec Opus pour mobile (qualite + economie).

## 6.5 Configuration du firewall pour la VoIP

### 6.5.1 Regles VoIP minimales (OPNsense / Stormshield)

```
# Regles sortantes depuis VLAN VOICE
# UDP 5060 (SIP) vers PBX
# UDP 5061 (SIP TLS) vers PBX
# UDP 10000-20000 (RTP) vers PBX
# UDP 53 (DNS) vers DNS LAN
# TCP 443 (HTTPS) vers PBX (provisioning + acces management)
# UDP 123 (NTP) vers serveurs NTP autorises

# Pour les softphones (LAN ou WAN)
# Memes ports - autoriser depuis groupe utilisateur softphone
```

```
# IMPORTANT : SIP ALG DOIT ETRE DESACTIVE
# (sur OPNsense : Firewall > Settings > Advanced - decocher SIP ALG)
# (sur box operateur : desactiver SIP ALG via interface admin)
```

**ATTENTION** Le SIP ALG des box grand public (Livebox, Freebox, BBox) modifie les paquets SIP et casse les enregistrements. Il doit etre IMPERATIVEMENT desactive ou contourne (mode bridge IP fixe).

### 6.5.2 QoS pour la voix

```
# OPNsense - Traffic Shaper
# Cible : DSCP EF (46) pour la voix, AF31 (26) pour la signalisation

# Pipe 1 - VOICE-RTP
# Bandwidth : reservee 100 kbps par appel x N
# Match : DSCP=EF OR (UDP src/dst port 10000-20000)

# Pipe 2 - VOICE-SIG
# Bandwidth : 64 kbps total
# Match : DSCP=AF31 OR (UDP src/dst port 5060,5061)

# Cote switch (Cisco/Aruba/UniFi)
# Trust DSCP en provenance des postes VoIP (port-based ou mac-based)
# Mapper queue 4 (ou 5) a EF sur trunk uplink
```

## 6.6 SVI (Standard Vocal Interactif)

Le SVI est l'arbre d'accueil telephonique du client. JMSI accompagne sa redaction.

### 6.6.1 Bonnes pratiques de scenario SVI

- Pas plus de 3 niveaux de profondeur (frustration utilisateur).
- Pas plus de 5 options par niveau.
- Touche 0 = standard humain ou SAV principal en heure ouvre.
- Message principal < 30 secondes.
- Voix professionnelle (off : http://nuageVoice.fr ou prestataire local).
- Mention obligatoire si enregistrement actif : <<Cet appel peut etre enregistre pour des fins de qualite. Vous pouvez vous opposer en appuyant sur la touche etoile.>>

### 6.6.2 Arbre type

```
# Exemple SVI client commerce
# Niveau 1 (accueil)
#   1 - Service commercial (-> file 801 - 8h-19h)
#   2 - SAV (-> file 802 - 9h-17h)
#   3 - Comptabilite (-> file 803 - 9h-12h, 14h-17h)
#   9 ou 0 - Standard humain (poste 100)
#   * - Repeter
#
# Hors heures (apres 19h)
#   Message : 'Nos bureaux sont fermes...' + redirection messagerie generale
```

# 6.7 Depannage telephonie

## 6.7.1 Pas de tonalite sur le poste

246. Verifier l'alimentation : LED PoE allumee sur le switch ?
247. Verifier l'enregistrement : sur le poste, menu Status > SIP - 'Registered' ?
248. Si 'Unregistered' : reseau ? URL PBX correcte ? credentials ?
249. Verifier cote PBX : Extensions > <ext> - quel etat ?
250. Si poste vu comme 'Active mais NOT registered' : firewall, NAT, SIP ALG.
251. Tester avec un cable ethernet direct switch-poste (eviter switch intermediaire).

## 6.7.2 Voix unidirectionnelle (un seul cote entend l'autre)

252. Symptome typique de NAT mal traverse / RTP bloque.
253. Verifier : SIP ALG desactive sur tous les routeurs ?
254. Verifier : ports UDP 10000-20000 sortants autorises ?
255. Verifier : External IP correctement detecte cote 3CX (Settings > Network > Public IP).
256. Si NAT symetrique cote operateur : forcer codec Opus + media bypass.

## 6.7.3 Echo / Decalage

257. Verifier le casque (interferences, USB defectueux).
258. Reduire le volume du combine.
259. Verifier la latence reseau : ping vers PBX < 50 ms ideal.
260. Tester avec un autre codec (Opus au lieu de G.711).

## 6.7.4 Codes d'erreur SIP

| Code | Signification | Action |
|---|---|---|
| **401 / 407** | Authentification requise | Verifier credentials, attention aux caracteres speciaux |
| **403** | Forbidden | Compte bloque cote operateur, plafond credit |
| **404 / 484** | Not Found / Address Incomplete | Numero compose incorrect, verifier prefixe |
| **486** | Busy Here | Destinataire occupe ou file pleine |
| **488** | Not Acceptable Here | Codec non supporte |
| **503** | Service Unavailable | PBX surcharge / down |
| **603 / 487** | Decline / Request Terminated | Refuse manuellement, appel raccroche |
| **Timeout** | Pas de reponse SIP | Routeur, firewall, ALG actif, PBX inaccessible |

## 6.8 Statistiques d'appels et reporting

3CX inclut des rapports natifs : taux de decroche, duree moyenne, abandons, repartition. JMSI les configure pour envoi automatique au manager client (mensuel).

- Rapport mensuel : appels entrants (decrocher / manque / abandonne), duree, repartition.
- Rapport SVI : taux d'utilisation des choix, abandons en SVI.
- File d'attente : SLA (decroche < 30s), agents les plus actifs, peak hours.
- Integration CRM (Dolibarr) : popup CTI, journal d'appels lie au tiers.

## 6.9 Securite VoIP

- Trunk SIP authentifie par IP whitelist + credentials forts (16 chars min).
- TLS sur SIP (5061) et SRTP sur RTP - obligatoire pour les clients sensibles.
- Detection de toll fraud : alertes si > 10 appels internationaux dans une heure.
- Plafond depenses operateur (alerte cote operateur a 100 EUR/jour).
- Mots de passe extensions : bloque par 3CX < 12 chars + complexite.
- Mise a jour firmware postes IP : annuelle obligatoire (vulnerabilites Yealink/Fanvil regulieres).

## 6.10 Migration sortante

- Export des contacts (CSV) et des messages messagerie (zip).
- Conservation du numero : portabilite vers nouvel operateur (le client compose 3179, transmet RIO).
- Suppression des extensions cote 3CX a J+15 (delai pour eventuelle relance ).
- Restitution des postes IP physiques au client (proprietaire si achete).

# Chapitre 7 - Wi-Fi public, professionnel et portail captif

## 7.1 Perimetre

Le Wi-Fi public JMSI est conforme au cadre legal francais : retention des logs de connexion 1 an (article L34-1 CPCE) sous peine d'amende jusqu'a 75 000 EUR. JMSI deploie egalement le Wi-Fi professionnel (sans portail captif) pour les besoins internes.

| Code Dolibarr | Designation | Tarif HT mensuel |
|---|---|---|
| **B2B_WIF_01** | Borne Wi-Fi interieure (achat materiel) | 149,00 EUR |
| **B2B_WIF_02** | Borne Wi-Fi exterieure (achat materiel) | 289,00 EUR |
| **B2B_WIF_03** | Portail captif + supervision | 29,00 EUR / mois |
| **B2B_WIF_04** | Module paiement / monetisation | 19,00 EUR / mois |
| **B2B_WIF_05** | Installation et parametrage Wi-Fi | Sur devis |
| **B2B_WIF_06** | Etude couverture Wi-Fi | OFFERTE |

## 7.2 Architecture cible et choix de marque

JMSI utilise principalement deux ecosystemes Wi-Fi : TP-Link Omada (rapport qualite/prix, client TPE/PME) et Ubiquiti UniFi (PME et environnements plus complexes, multi-site, campagnes WPA3-Enterprise).

| Modele | Type | Cible | Vitesse |
|---|---|---|---|
| **TP-Link EAP650** | Interieur Wi-Fi 6 (AX3000) | Bureau 50-150 m2 | 574 + 2402 Mbps |
| **TP-Link EAP683 LR** | Interieur longue portee Wi-Fi 6 | Bureau 150-300 m2 | 574 + 2402 Mbps |
| **TP-Link EAP610-Outdoor** | Exterieur Wi-Fi 6 | Terrasse, parking | 574 + 1201 Mbps |
| **UniFi U6 Pro** | Interieur Wi-Fi 6 (AX5400) | Bureau dense | 574 + 4800 Mbps |
| **UniFi U6 Mesh** | Interieur Wi-Fi 6 maillee | Etablissement multi-pieces | 574 + 2400 Mbps |
| **UniFi Mesh Pro** | Exterieur Wi-Fi 5 (AC1750) | Camping, hotel exterieur | 300 + 1300 Mbps |

# 7.3 Etude de couverture (B2B_WIF_06)

L'etude est offerte (cf. plaquette Wi-Fi). Methode JMSI : visite de site avec un kit de site survey (Ekahau Sidekick ou TP-Link survey + smartphone WiFi Analyzer).

## 7.3.1 Methode

261. Releve du plan a l'echelle (DWG, PDF) ou cle photogrammetrie.
262. Identification des materiaux : cloisons placo (faible attenuation), beton (forte), verre (legere reflexion).
263. Mesure du signal existant (RSSI) en plusieurs points - releve avec smartphone WiFi Analyzer.
264. Identification des zones a couvrir prioritairement (postes de travail, salles de reunion, accueil).
265. Identification des contraintes (alimentation PoE, esthetique, accessibilite pour maintenance).
266. Predictif Ekahau : nombre et placement optimal des bornes.
267. Restitution : plan annote + recommandations + devis.

# 7.4 Mise en service Omada (TP-Link)

## 7.4.1 Architecture controleur

- Cloud Based Controller (CBC) JMSI : multi-tenant, deja heberge.
- OC200 / OC300 (controleur hardware) : pour les clients qui souhaitent rester on-premise.
- Software controller (Linux/Windows) : alternative open de l'OC200.

## 7.4.2 Procedure de deploiement

268. Cote console JMSI Omada : ajouter un nouveau site, choisir 'Adopter en attente'.
269. Sur site : installer les bornes (PoE), connecter au switch.
270. Les bornes apparaissent en 'Pending' apres 30-60 secondes.
271. Adopter chaque borne dans la console.
272. Configurer SSIDs : Pro (WPA3 ou WPA2-PSK), Guest (portail captif), IoT (segmente).
273. Configurer VLANs : SSID Pro -> VLAN 10, Guest -> VLAN 50, IoT -> VLAN 60.
274. Calibration : laisser tourner 24h en auto-tx-power, puis figer les canaux.

## 7.4.3 Configuration WPA3-Enterprise (cas avance)

```
# Sur le controleur Omada
# Settings > Wireless > Wireless Settings > <Site>
# Add SSID:
#   Name: jmsi-corp
#   Type: Standard SSID
#   Mode: WPA3-Enterprise
#   Encryption: AES (CCMP)
#   PMF (Protected Management Frames): required
#   Authentication Server: <RADIUS_IP> port 1812 secret <SECRET>
#   Accounting Server: <RADIUS_IP> port 1813 secret <SECRET>

# Cote serveur RADIUS (FreeRADIUS, NPS Microsoft, ou daloRADIUS)
# Authentication via Active Directory ou base local
# - PEAP-MSCHAPv2 (compatible Windows + AD)
# - EAP-TLS (cert utilisateur, plus securise mais deploiement complexe)
```

# 7.5 Wi-Fi public conforme

## 7.5.1 Cadre legal

L'article L34-1 du Code des Postes et des Communications Electroniques impose aux exploitants de Wi-Fi public la conservation des donnees techniques permettant l'identification de l'utilisateur (date, heure, IP attribuee, MAC, login eventuel) pendant 1 an. La directive ePrivacy et le RGPD encadrent par ailleurs l'usage commercial des donnees collectees (consentement explicite, opt-in).

| Donnee | Conservation | Base legale |
|---|---|---|
| **Adresse IP attribuee** | 1 an | L34-1 CPCE |
| **Adresse MAC** | 1 an | L34-1 CPCE |
| **Date / heure debut + duree session** | 1 an | L34-1 CPCE |
| **Identifiant utilisateur (login + email/mobile si demande)** | 1 an apres derniere session | L34-1 CPCE + RGPD |
| **Email pour campagnes marketing** | Tant que opt-in actif | RGPD - consentement explicite |
| **Logs d'acces aux sites externes** | Interdit (vie privee) sauf decision de justice | RGPD |

## 7.5.2 Architecture portail captif JMSI

JMSI utilise une plateforme partenaire (UCOPIA, ZAP-Hotspot, ou portail Omada interne) ou une solution custom Coova-Chilli + RADIUS pour les besoins specifiques. Architecture type :

- Borne Wi-Fi avec SSID Guest dans VLAN dedie.
- VLAN Guest isole du LAN (firewall : deny LAN, allow Internet).
- Trafic Guest redirige vers le portail captif (HTTP/HTTPS hijack).
- Apres authentification (email/mobile/code), l'utilisateur est libere vers Internet.
- Logs centralises sur le portail (CSV exportable).
- Sauvegarde quotidienne des logs sur Wasabi (immuable, retention 13 mois).

## 7.5.3 Configuration portail captif Omada

275. Settings > Authentication > Portal > Add Portal.
276. Portal Type : Local Web Authentication.
277. Authentication Type : email / SMS / voucher / sponsor.
278. Background image : logo client (charte JMSI ou client).
279. Conditions generales d'utilisation : version texte JMSI standard + adaptation client.
280. Politique : duree session 4h, debit max 5 Mbps (ajustable), nb peripherique max 3.
281. Logs : export quotidien automatique vers serveur SFTP JMSI.

# 7.6 Module paiement / monetisation (B2B_WIF_04)

Pour les hotels, campings, espaces premium : integration paiement via Stripe ou prestataire partenaire.

- Plan : 1h gratuit puis 1 EUR/24h, ou packs 10 EUR/semaine.
- Reversement au client : commission JMSI 20 %, 80 % au client.
- Reception du paiement Stripe : association compte, reglages anti-fraud.
- Mise en place : cf. doc partenaire (UCOPIA / ZAP).

## 7.7 Wi-Fi multi-site et roaming

- WPA3-Enterprise + RADIUS centralise : roaming transparent entre sites.
- 802.11k/v/r active sur les bornes : negociation handover < 50 ms.
- VLAN coherent a travers les sites (tunneling L2VPN ou EVPN-VXLAN).
- Test du roaming : marche d'une borne a l'autre avec un appel VoIP softphone, mesurer la coupure.

## 7.8 Depannage Wi-Fi

### 7.8.1 Pas de connexion

282. Verifier le SSID visible (smartphone, scanner Wi-Fi).
283. Verifier le canal et l'intensite signal au point de panne.
284. Verifier le statut de la borne dans la console (Online / Offline / Adopting).
285. Test : se connecter avec MAC autorisee de reference (smartphone JMSI bench).
286. Si echec auth : cote RADIUS - verifier qu'on recoit bien la requete (debug live).

### 7.8.2 Lenteur Wi-Fi

287. Verifier la charge cellule (nb clients par borne, occupation canal).
288. Recalibrer canaux et puissance (Auto Tune Omada / RF UniFi).
289. Detection interference : scan spectre (Sidekick).
290. Verifier le backhaul (uplink switch saturated ?).
291. Si reseau congestionne : ajouter une borne, segmenter en plus de SSID.

### 7.8.3 Roaming sticky (clients qui s'accrochent a une borne lointaine)

292. Activer Band Steering (5GHz prefere).
293. Activer Min RSSI (deconnecter les clients en dessous de -75 dBm).
294. Activer 802.11k/v.
295. Verifier la puissance des bornes (eviter les overlap excessifs).

## 7.9 Conformite et obligations administratives

- Affichage en clair : << Reseau Wi-Fi proprietaire de <client>. Connexion soumise a CGU. Conservation des logs : 1 an. >>
- Mention CNIL si collecte d'email/mobile : finalite, droits d'acces et de suppression.
- DPA signe entre JMSI et le client : qui est responsable des donnees, qui est sous-traitant.
- Registre des traitements cote client (responsabilite client, JMSI accompagne).

## 7.10 Migration sortante

- Export des bornes (sauvegarde de configuration).
- Export des logs (CSV) et purge securisee dans Wasabi.
- Si bornes propriete client : libelle, code de provisioning fourni.
- Bascule du portail captif vers le nouveau prestataire (migration des CGU).

# PARTIE V

# Securite physique

# Chapitre 8 - Videosurveillance, controle d'acces et alarme

## 8.1 Perimetre

Ce chapitre couvre les solutions de securite physique commercialisees par JMSI : videosurveillance IP (cameras, NVR, supervision), controle d'acces electronique, alarme intrusion, telesurveillance 24/7. Le perimetre est strictement professionnel : JMSI n'intervient pas chez le particulier sur ces solutions (sauf cas exceptionnels valides Direction).

| Code Dolibarr | Designation | Tarif HT |
|---|---|---|
| **B2B_VID_01** | Camera IP HD interieure | 129,00 EUR (achat) |
| **B2B_VID_02** | Camera IP 4K exterieure | 249,00 EUR (achat) |
| **B2B_VID_03** | NVR 4 voies 2 To | 449,00 EUR (achat) |
| **B2B_VID_04** | NVR 8 voies 4 To | 789,00 EUR (achat) |
| **B2B_VID_05** | Installation cablage par camera | 149,00 EUR / camera |
| **B2B_VID_06** | Supervision et maintenance video | 29,00 EUR / mois |
| **B2B_VID_07** | Etude de site video | OFFERTE |
| **B2B_ACC_01** | Kit controle d'acces 1 porte | 890,00 EUR (achat) |
| **B2B_ACC_02** | Centrale alarme intrusion 6 zones | 590,00 EUR (achat) |
| **B2B_ACC_03** | Detecteur alarme supplementaire | 49,00 EUR (achat) |
| **B2B_ACC_04** | Badge ou telecommande supplementaire | 9,00 EUR (achat) |
| **B2B_ACC_05** | Installation controle acces et alarme | 290,00 EUR / installation |
| **B2B_ACC_06** | Telesurveillance 24/7 | 29,00 EUR / mois |
| **B2B_ACC_07** | Etude securite acces intrusion | OFFERTE |

## 8.2 Architecture cible

JMSI s'appuie sur deux ecosystemes principaux : Hikvision/Dahua pour la video classique, et UniFi Protect / Synology Surveillance Station pour les architectures IT-friendly.

### 8.2.1 Architecture Hikvision (cas standard)

| Composant | Modele de reference JMSI | Notes |
|---|---|---|
| **NVR 4 voies** | Hikvision DS-7604NI-K1/4P | PoE integre, disque 2 To |

| | | |
|---|---|---|
| | | Surveillance |
| **NVR 8 voies** | Hikvision DS-7608NI-K2/8P | PoE integre, 2 baies 4 To, RAID 1 option |
| **NVR 16 voies** | Hikvision DS-7716NI-I4/16P | RAID, 4 baies, 4K Acusense |
| **Camera bullet HD** | DS-2CD2046G2-I | 4 MP, IR 30m, IP67 |
| **Camera dome 4K** | DS-2CD2386G2-IU | 8 MP, IR 30m, audio integre, AcuSense |
| **Camera PTZ** | DS-2DE4A425IW-DE | 4 MP, zoom optique x25, IR 100m, AcuSense |
| **Switch PoE+ dedie** | Hikvision DS-3E0510P-E ou TP-Link TL-SG1008P | 8 ports PoE 60W |

### 8.2.2 Architecture UniFi Protect (alternative IT-friendly)

Pour les clients deja UniFi (cf. chapitre 7), Protect s'integre nativement, partage le controleur, et offre une UX moderne.

- UniFi Network Application + Protect Application sur la meme Cloud Key Gen2 Plus ou UDM Pro.
- Cameras UniFi G4 / G5 : Bullet, Dome, PTZ.
- Stockage local + option backup vers UniFi Talk / cloud.

## 8.3 Cadre legal et CNIL

La videosurveillance est tres encadree en France. JMSI applique systematiquement les regles suivantes ; tout ecart engage la responsabilite penale du dirigeant client (et la responsabilite contractuelle JMSI).

### 8.3.1 Affichage et information

- Panneau visible a chaque entree : pictogramme camera + mention 'Etablissement sous videoprotection. Responsable : <NOM>. Vous pouvez exercer votre droit d'acces : <CONTACT>'.
- Information ecrite des salaries (note interne, registre RGPD).
- Consultation prealable du CSE si > 11 salaries.

### 8.3.2 Champ de prise de vue

- INTERDIT : filmer la voie publique (sauf abords immediats, < 1 m de la facade).
- INTERDIT : filmer les postes de travail individuels en plan rapproche (vie privee).
- INTERDIT : filmer les zones de pause, vestiaires, sanitaires.
- AUTORISE : entrees, caisses, zones de vol potentiel, parkings prives, peripheries internes.

### 8.3.3 Conservation

- Duree maximum : 30 jours (sauf rares cas justifies a 1 mois et motives).
- Suppression automatique au-dela : verifier que le NVR est configure en cycle ferme.
- Acces aux images : restreint, journalise (qui a regarde quoi, quand).

### 8.3.4 Declarations administratives

- Si lieu non ouvert au public : registre des traitements RGPD interne (pas de demande prealable).
- Si lieu ouvert au public : autorisation prefectorale OBLIGATOIRE avant installation (dossier CERFA 13806*04).
- Le dossier d'autorisation est de la responsabilite client. JMSI fournit la matrice technique.

## 8.4 Etude de site (B2B_VID_07)

L'etude est offerte. Sa qualite determine 80 % du succes du projet.

### 8.4.1 Methode

296. Visite site avec le client. Recenser les zones a couvrir et leur priorite.
297. Identifier les contraintes : eclairage variable, jour/nuit, exterieur intemperies, exposition vandalisme.
298. Choisir le type de camera par zone : bullet (long shot), dome (interieur fixe), PTZ (parking grand angle), turret (compromis).
299. Definir l'arrivee electrique (PoE depuis NVR ou injecteur PoE / midspan).
300. Definir le passage de cables (faux-plafonds, gaines, nappes).
301. Localiser le NVR (local technique, baie informatique).
302. Schema d'implantation (plan + cones de vue + label cameras CAM01...CAMn).
303. Devis : materiel + cablage (B2B_VID_05 a 149 EUR/camera) + parametrage.

### 8.4.2 Calcul de stockage

```
# Calcul stockage NVR
# Hypotheses :
#   8 cameras 4 MP @ 15 fps en H.265+
#   Bitrate moyen apres compression : 4 Mbps par camera
#   Enregistrement permanent (24/7)
#   Retention voulue : 30 jours
#
# Calcul :
#   8 cam x 4 Mbps = 32 Mbps
#   32 Mbps = 4 Mo/s
#   86400 s/jour x 4 Mo/s = ~345 Go/jour
#   30 jours = ~10,4 To
#
# Optimisations :
#   Enregistrement sur evenement seul (-60 % vs permanent typiquement)
#   H.265+ smart codec (-30 % vs H.265)
#   AcuSense filtres faux positifs (humain/vehicule uniquement)
#
# Disques recommandes : Seagate SkyHawk ou WD Purple, calibres surveillance 24/7
```

## 8.5 Mise en service Hikvision (cas standard)

### 8.5.1 Preparation - lab JMSI

304. Mise a jour firmware NVR + cameras a la derniere version stable (apres validation lab JMSI).

305. Pre-configuration en LAN bench : changement mot de passe par defaut, IP fixe par camera, NVR en client cloud Hikvision desactive.
306. Documentation : noter MAC, serie, IP cible, login admin (Bitwarden).

### 8.5.2 Sur site - installation physique

307. Installer les cameras selon le plan d'implantation (orientation testee in situ).
308. Cabler en RJ45 Cat6A (resistant exterieur si pose extl).
309. Brancher les cameras au NVR (PoE 802.3af pour bullets, 802.3at pour PTZ).
310. Verifier la presence sur le NVR (Auto Add / Plug-and-Play).
311. Configurer chaque camera : nom, zones de detection, planning d'enregistrement.
312. Configurer le NVR : disques en mode 'Surveillance', recyclage cyclique, formattage.

### 8.5.3 Configurations standard JMSI

```
# Hikvision NVR/IPC - parametres JMSI standards

# 1) Securite
#    - Activer SADP IP filter (filtrer decouverte non-LAN)
#    - Desactiver UPnP, Hik-Connect cloud, ISAPI external
#    - Activer 'Force admin password change at first login'
#    - HTTPS uniquement (port 443) pour acces web
#    - SSH desactive (sauf depannage)

# 2) Acces a distance
#    - JAMAIS expose en Internet directement
#    - Acces via VPN WireGuard JMSI ou client uniquement
#    - Compte 'admin' fort (16 chars) + compte 'operator' pour client

# 3) Detection
#    - AcuSense active (humain/vehicule uniquement)
#    - Sensibilite : ajuster apres 48h de retours faux positifs
#    - Masque privacy sur zones non legales

# 4) Notifications
#    - Email + SMTP JMSI (alertes vers technicien)
#    - FTP / NAS pour upload images sur evenement

# 5) Stockage
#    - HDD WD Purple Pro 8 To minimum, calibre surveillance
#    - SMART monitoring active, alerte sur pre-fail
#    - Recyclage cyclique 30 jours

# 6) Heure
#    - NTP fr.pool.ntp.org
#    - Fuseau Europe/Paris
#    - L'incrustation horloge sur l'image est OBLIGATOIRE pour valeur juridique
```

### 8.5.4 Provisioning d'une camera Hikvision en CLI

```
# Outil SADPTool (Hikvision)
# - Decouverte camera sur LAN
# - Activation initiale (mot de passe)
# - Reset du mot de passe via image .xml signee constructeur

# CLI - configuration via API ISAPI
```

```
curl -k --digest -u admin:<PWD> \
 -X PUT \
 -H 'Content-Type: application/xml' \
 --data-binary @network.xml \
 https://<IP>/ISAPI/System/Network/interfaces/1

# Exemple network.xml
# <NetworkInterface>
#   <id>1</id>
#   <IPAddress><ipVersion>v4</ipVersion>
#     <addressingType>static</addressingType>
#     <ipAddress>10.10.20.30</ipAddress>
#     <subnetMask>255.255.255.0</subnetMask>
#     <DefaultGateway><ipAddress>10.10.20.1</ipAddress></DefaultGateway>
#   </IPAddress>
# </NetworkInterface>
```

### 8.5.5 Acces utilisateur final

- Cote PC client : navigateur HTTPS NVR (LAN ou via VPN).
- Cote mobile : appli iVMS-4500 ou Hik-Connect (mode P2P) - JMSI prefere VPN si possible.
- Restriction : compte 'operator' avec droits de lecture seule + replay limite, pas de modification de configuration.
- Audit : toutes les consultations sont journalisees cote NVR (Logs).

## 8.6 Controle d'acces (B2B_ACC_01)

### 8.6.1 Architecture standard

Kit controle d'acces 1 porte JMSI - composants :

- Centrale 1 porte (Hikvision DS-K2601T ou Suprema BioStation 2).
- Lecteur badge (RFID Mifare 13.56 MHz) ou biometrie (empreinte / face).
- Gache electrique a securiser (rupture en cas de coupure ou maintien selon cas).
- Bouton de sortie cote interieur (poussoir mecanique).
- Detecteur de porte (contact magnetique).
- Alimentation secourue (batterie 12V 7Ah).

### 8.6.2 Procedure d'installation

313. Decoupage / pose de la gache cote chambranle (menuisier si porte massive).
314. Pose du lecteur cote exterieur a hauteur conventionnelle (1,15 m du sol).
315. Pose de la centrale en local technique (proximite).
316. Cablage : alimentation 12V centrale + bus RS-485 + cable lecteur (4 fils + alim).
317. Test alimentation et puissance gache (sous tension reelle).
318. Provisioning des badges utilisateur dans le logiciel.
319. Test ouverture / fermeture / refus en bas de la chaine.

### 8.6.3 Configuration logicielle

```
# Hikvision iVMS-4200 ou Suprema BioStar
# Workflow standard
```

```
# 1) Creer les zones (zones d'acces)
# 2) Creer les utilisateurs (nom, prenom, photo, email)
# 3) Enroller le badge ou les empreintes (USB enrolment)
# 4) Creer les plages horaires (semaine type)
# 5) Lier user x zones x plages
# 6) Tester acces et refus (jour ouvre / weekend)
# 7) Backup de configuration toutes les 24h vers serveur JMSI
```

# 8.7 Alarme intrusion (B2B_ACC_02)

## 8.7.1 Architecture standard

Centrale alarme 6 zones JMSI - typique :

- Centrale Hikvision AX Pro (DS-PWA64-Kit) ou Risco LightSYS+ ou Ajax Hub2 Plus.
- Detecteurs PIR (passifs infrarouges) volumetriques.
- Detecteurs ouverture porte/fenetre.
- Sirene exterieure (visible) + sirene interieure.
- Telecommande activation / desactivation.
- Module GSM/GPRS pour transmission alarme.
- Communication centrale > telesurveillance via IP + GPRS de secours.

## 8.7.2 Programmation des zones

| Zone type | Configuration | Cas d'usage |
|---|---|---|
| **Instantanee** | Declenchement immediat | Fenetres, portes secondaires |
| **Temporisation entree** | Delai 30s pour entrer le code | Porte principale |
| **Temporisation sortie** | Delai 60s pour sortir apres armement | Porte principale |
| **Suiveuse** | Active uniquement si une autre zone se declenche d'abord | Couloirs interieurs |
| **24h** | Active meme alarme desarmee | Bris de glace, panique |
| **Incendie** | Active 24/7, alarme distincte | Detecteur fumee |

# 8.8 Telesurveillance 24/7 (B2B_ACC_06)

JMSI s'appuie sur un PC SOC (centre operations securite) partenaire, agree APSAD P5 (Sensae, Securitas, Acoma). En cas d'alarme : levee de doute par video / audio si possible, puis intervention agent / police selon protocole.

- Programmation des contacts d'urgence (3 maxi, dans l'ordre).
- Protocole d'intervention : verification, intervention, restitution rapport.
- Tarif partenaire repercute : 29 EUR HT/mois.
- Tests trimestriels obligatoires (mise en alarme test, validation reception PC SOC).

# 8.9 Supervision et maintenance video (B2B_VID_06)

## 8.9.1 Verifications periodiques

| Frequence | Tache | Profil |
|---|---|---|
| **Hebdo** | Verification distante : NVR online, toutes cameras 'live', stockage > 10 % libre | N1 |
| **Mensuel** | Test enregistrement aleatoire, verification SMART HDD, alerte si sat | N1 |
| **Trimestriel** | Visite sur site : nettoyage objectifs, verification etancheite exterieur | N2 |
| **Annuel** | MAJ firmware (apres validation lab), audit complet (orientation, declarations CNIL a jour) | N2 |
| **Sur incident** | Extraction d'image / video pour le client (sous formel mandate cote client) | N1/N2 |

## 8.9.2 Extraction de sequence (procedure formelle)

320. Demande ecrite client (mail) avec date/heure/zone.
321. Le client verifie qu'il a la base legale (procedure interne, constat avocat, requisition).
322. Sur le NVR : Search > Date / Time / Channel / Event.
323. Export en MP4 ou format constructeur signe (preuve).
324. Transmission au client via Bitwarden Send (chiffrement, expiration 24h).
325. Trace dans GLPI (qui, quand, pour qui).

# 8.10 Depannage video

## 8.10.1 Camera offline

326. Verifier la diode du switch PoE pour la camera concernee.
327. Verifier le port (cable, ou autre cable de test).
328. Tester l'alimentation injecteur (multimetre) si pas de PoE switch.
329. Si LAN OK et camera HS : firmware corrompu, factory reset (bouton ou outil constructeur).

## 8.10.2 Image floue / mauvaise nuit

330. Nettoyer l'objectif (chiffon micro-fibres + eau distillee).
331. Verifier que l'IR illumine la zone (camera face a vitre = reflet IR).
332. Verifier les parametres : Day/Night auto, IR cut-filter swap.
333. Mauvaise focale : verifier que l'objectif n'a pas bouge (vis de blocage).

## 8.11 Securite et bonnes pratiques

- AUCUN NVR/camera ne doit etre expose en Internet directement (port forwarding interdit).
- Mots de passe constructeur par defaut imperativement changes (Mirai botnet exploitable encore en 2026 sur Hikvision/Dahua mal configures).
- Comptes 'operator' separes des comptes 'admin' (privileges differencies).
- Mises a jour firmware annuelles minimum.
- VLAN dedie cameras (segmentation : cameras n'ont pas besoin d'acces Internet).
- Audit annuel des acces (qui peut consulter les images, journal des consultations).

# PARTIE VI

# Infrastructure materielle

# Chapitre 9 - Materiel : postes, serveurs, reseau, baies

## 9.1 Perimetre

Ce chapitre couvre tout le materiel commercialise par JMSI et toutes les operations techniques associees : preparation poste de travail, deploiement serveur (avec ou sans hyperviseur), montage/brassage/etiquetage de baie, cablage VDI, deploiement d'imprimantes. C'est le chapitre le plus volumineux car le plus operationnel.

| Categorie | Codes Dolibarr |
|---|---|
| **Postes de travail** | B2B_MAT_01 a B2B_MAT_06 |
| **Stockage** | B2B_MAT_07 (NAS), B2B_NET_05 (SAN) |
| **Baies** | B2B_MAT_08, B2B_VDI_02, B2B_VDI_03 |
| **Reseau** | B2B_NET_01 a B2B_NET_04 |
| **Serveurs** | B2B_SRV_01 a B2B_SRV_04 |
| **Cablage VDI** | B2B_VDI_01, B2B_VDI_04, B2B_VDI_05 |
| **Salle de reunion** | Cf. chapitre 11 |

## 9.2 Postes de travail

### 9.2.1 Modeles de reference JMSI

| Code | Designation | Configuration cible |
|---|---|---|
| **B2B_MAT_01** | PC bureau i3 neuf - 599 EUR | i3-12100, 16 Go DDR4, SSD NVMe 512 Go, Win 11 Pro |
| **B2B_MAT_02** | PC bureau i3 reconditionne - 349 EUR | Lenovo M715/M720, Ryzen 5 PRO 2400, 16 Go, SSD 256 Go, Win 11 Pro |
| **B2B_MAT_03** | PC portable i5 neuf - 899 EUR | ThinkPad E15 / Latitude 3540, i5 13e gen, 16 Go, SSD 512 Go |
| **B2B_MAT_04** | PC portable i5 reconditionne - 549 EUR | Latitude 7400/7420 reconditionne, i5/i7 8e/10e gen, 16 Go, SSD 256 Go |
| **B2B_MAT_05** | Ecran 24'' Full HD - 159 EUR | Dell P2422H ou equivalent, IPS, hauteur reglable |
| **B2B_MAT_06** | Onduleur 1000 VA - 169 EUR | APC Back-UPS Pro BR1000MS |

### 9.2.2 Procedure de preparation d'un poste de travail

334. Reception et controle visuel (carton intact, n de serie correspondant a la commande Dolibarr).
335. Demarrage hors ligne. Acceptation du CLUF. Compte local 'JMSI-Tech' (a supprimer en fin de prep).
336. Branchement reseau LAN bench JMSI (VLAN 'Bench' isole).
337. Mise a jour Windows complete : Settings > Update.
338. Mise a jour des pilotes : depuis l'utilitaire constructeur (Lenovo Vantage, Dell SupportAssist, HP Image Assistant).
339. Suppression des bloatwares (HP : Smart Friend, Dell : SupportAssist Inventory, Lenovo : preinstalls McAfee).
340. Application du kit JMSI Standard (cf. chapitre 2.3.4).
341. Installation des logiciels client (selon liste contractuelle) : Office 365, navigateur prefere, Outlook profile, applications metier.
342. Activation BitLocker : chiffrement integral, recuperation enregistree dans AD ou Bitwarden si autonome.
343. Joining domain (si AD) ou Microsoft Entra ID join (si Microsoft 365).
344. Test fonctionnel : reseau, internet, imprimante, application metier, mail, sauvegarde.
345. Documentation : photo poste + sticker JMSI inventaire (n GLPI, date prep, technicien).
346. Suppression compte local 'JMSI-Tech', verification absence de mots de passe locaux.
347. Emballage pour livraison : housse antistatique + carton d'origine + accessoires.

### 9.2.3 BitLocker - procedure detaillee

```
REM PowerShell - activation BitLocker avec TPM + recovery key dans AD

REM Verifier le TPM
Get-Tpm
Get-BitLockerVolume

REM Activer BitLocker XTS-AES 256 sur C:
Enable-BitLocker -MountPoint 'C:' -EncryptionMethod XtsAes256 \
  -UsedSpaceOnly -TpmProtector -SkipHardwareTest

REM Ajouter le mot de passe de secours et exporter la cle de recuperation
$Recovery = Add-BitLockerKeyProtector -MountPoint 'C:' -RecoveryPasswordProtector
$Recovery.KeyProtector | Where { $_.KeyProtectorType -eq 'RecoveryPassword' } | \
  Format-List KeyProtectorId, RecoveryPassword

REM Sauvegarder la cle de recuperation dans Active Directory
Backup-BitLockerKeyProtector -MountPoint 'C:' -KeyProtectorId $Recovery.KeyProtectorId

REM Verification
manage-bde -status C:
manage-bde -protectors -get C:
```

**ATTENTION** Conserver TOUJOURS la cle de recuperation BitLocker dans le coffre Bitwarden (collection client) ET dans l'AD si client domaine. Sans cle de recuperation : le poste devient inutilisable apres tout incident TPM.

### 9.2.4 Postes reconditionnes - controle qualite

JMSI propose des postes reconditionnes (-40 % vs neuf, garantie 1 an). Procedure rigoureuse de controle avant remise au client.

- Controle visuel : chassis, charnieres, clavier (touches manquantes), ecran (pixels morts).
- Test batterie (laptops) : capacite restante > 70 % obligatoire ; sinon remplacement.
- Test memoire : memtest86 - 4 cycles minimum.
- Test stockage : SMART, surface complete (badblocks ou Crystal Disk Info).
- Effacement securise du disque : DBAN ou diskpart > clean all > nouvelle install Windows clean.
- Reinstallation Windows 11 IoT LTSC ou 11 Pro Education (selon cible).
- Etiquette : 'Reconditionne JMSI - Garantie 12 mois - <DATE>'.
- Engagement contractuel : remplacement gratuit en cas de defaut majeur dans les 12 mois.

## 9.3 Onduleurs

L'onduleur (UPS - Uninterruptible Power Supply) protege contre les microcoupures et permet la fermeture propre des serveurs en cas de coupure prolongee.

### 9.3.1 Dimensionnement

```
# Calcul de puissance UPS necessaire
# Methode :
#   1) Sommer la consommation de tous les equipements (Watts)
#   2) Marge de securite +20 %
#   3) Convertir en VA : VA = W / facteur de puissance (~0,7)

# Exemple : poste + ecran + tel IP = 80W + 30W + 5W = 115W
#   115 W * 1,2 = 138 W de besoin
#   138 / 0,7 = 197 VA -> UPS 500 VA convient (autonomie 5-10 min)

# Petit serveur : 250W + switch 30W = 280W -> 350W -> 500VA -> APC SMT750
# Baie complete (ex: 1 serveur + switch + NAS) -> APC SRT2200 ou Smart-UPS X 3000

# Verifier la batterie 1 fois/an (autonomie reelle vs annoncee)
```

### 9.3.2 Configuration NUT (Network UPS Tools) sur Linux

```
# Installation NUT - serveur de reference
apt install nut nut-client nut-server

# /etc/nut/ups.conf
[apc-srt]
  driver = usbhid-ups
  port = auto
  desc = 'APC Smart-UPS SRT 2200'

# /etc/nut/upsd.conf
LISTEN 127.0.0.1
LISTEN 10.<NET>.<HOST>

# /etc/nut/upsd.users
[upsmon]
  password = <SECRET>
  upsmon master
```

```
# /etc/nut/upsmon.conf
MONITOR apc-srt@localhost 1 upsmon <SECRET> master
SHUTDOWNCMD '/sbin/shutdown -h +0'
NOTIFYCMD /etc/nut/notify.sh

# /etc/nut/nut.conf
MODE=netserver

# Demarrage et test
systemctl enable --now nut-server nut-monitor
upsc apc-srt@localhost

# Test : couper l'alimentation manuelle pour valider la sequence shutdown
```

## 9.4 NAS Synology - hors sauvegarde (cf. chap 4)

Le NAS Synology est aussi utilise comme : serveur de fichiers, hote de partage, VPN, Hyper Backup pour des sauvegardes croisees, hebergement de petites apps via Container Manager, stockage iSCSI pour Veeam ou pour serveurs.

- Serveur de fichiers SMB : creation de partages avec ACL Active Directory si AD present.
- Active Directory Domain Services package : pour les TPE sans Windows Server, le NAS peut faire AD.
- Synology Drive : alternative legere a Nextcloud pour synchronisation client desktop.
- VPN Server package : OpenVPN / SSTP / WireGuard light.
- Container Manager (Docker) : heberger Bitwarden self-host, Vaultwarden, Pi-hole, etc.

## 9.5 Serveurs - choix et dimensionnement

### 9.5.1 Modeles JMSI

| Code | Designation | Cible |
|---|---|---|
| **B2B_SRV_01** | Serveur tour PME entree - 1290 EUR | Hyper-V 1 host, 1 a 5 VM legeres |
| **B2B_SRV_02** | Serveur tour PME pro - 2490 EUR | Hyper-V 1 host, 5 a 10 VM |
| **B2B_SRV_03** | Serveur rack 1U - 3490 EUR | Pour clients ayant baie informatique |
| **B2B_SRV_04** | Serveur rack 2U haute disponibilite - 5990 EUR | Cluster Hyper-V 2 nodes ou Proxmox 3 nodes |

### 9.5.2 Configurations standards

| Modele JMSI | CPU | RAM | Stockage | Notes |
|---|---|---|---|---|
| **Tour PME entree** | Xeon E-2334 4c/8t | 32 Go DDR4 ECC | 2x SSD 480Go RAID1 + 2x HDD 4To RAID1 | Lenovo ST50 V2 / Dell T350 |
| **Tour PME pro** | Xeon Silver 4310 12c/24t | 64 Go DDR4 ECC | 2x SSD NVMe 1To RAID1 + 4x HDD 8To | Lenovo ST650 V2 / |

| | | | | |
|---|---|---|---|---|
| | | | RAID10 | Dell T550 |
| **Rack 1U** | Xeon Silver 4314 16c/32t | 128 Go DDR4 ECC | 2x SSD NVMe 1.92To RAID1 + 4x SAS 1.92To RAID10 | Lenovo SR630 V2 / Dell R650 |
| **Rack 2U HA (par node)** | Xeon Gold 6326 16c/32t | 256 Go DDR4 ECC | 2x SSD NVMe 1.92To RAID1 + 8x NVMe 3.84To Ceph/SDS | Lenovo SR650 V3 / Dell R750 |

**BONNE PRATIQUE** Toujours choisir des disques calibres serveur (Enterprise, ECC RAM). Les disques desktop ne sont JAMAIS valides en serveur, meme en environnement TPE. Le cout en cas de panne depasse largement l'economie initiale.

# 9.6 Hyperviseur - Hyper-V (Windows Server)

## 9.6.1 Cas d'usage

JMSI deploie Hyper-V comme hyperviseur principal sur les architectures Windows-centric : domaine AD, RDS, applicatifs Windows. Choix par defaut pour les clients ayant deja l'experience Windows et un partenaire MSFT.

## 9.6.2 Pre-requis

- Windows Server 2022 Datacenter (couvre nb illimite de VM Windows licenciees) ou Standard (2 VM par licence).
- VT-x/AMD-V active dans le BIOS, SLAT compatible.
- RAM ECC obligatoire, minimum 32 Go pour 1 hote 5 VM.
- Stockage rapide : NVMe RAID1 pour OS + RAID10 pour VM data.
- Reseau : 2 cartes physiques + LACP (Switch Independent Mode SET).

## 9.6.3 Procedure de mise en service Hyper-V

348. Installer Windows Server 2022 (Datacenter, Desktop Experience).
349. Renommer la machine, IP fixe, joindre le domaine.
350. Mises a jour completes (Windows Update).
351. Activer le role Hyper-V via PowerShell :

```
# Installation du role Hyper-V
Install-WindowsFeature -Name Hyper-V -IncludeManagementTools -Restart

# Configuration du switch virtuel SET (Switch Embedded Teaming)
# (preferre depuis Server 2016 - LACP non supporte directement, on utilise SET)

New-VMSwitch -Name 'vSwitch-Prod' \
  -NetAdapterName 'NIC1','NIC2' \
  -EnableEmbeddedTeaming $true \
  -AllowManagementOS $true

# Renommer la VLAN management (sans tag) si necessaire
Set-VMNetworkAdapterVlan -ManagementOS -Untagged
```

```
# Si VLAN tagging cote switch : creer un Network Adapter par VLAN
Add-VMNetworkAdapter -ManagementOS -SwitchName 'vSwitch-Prod' -Name 'MGMT'
Set-VMNetworkAdapterVlan -ManagementOS -VMNetworkAdapterName 'MGMT' -Access
-VlanId 99

# Stockage VM : creer le LCD
New-Item -Path 'D:\VMs' -ItemType Directory

# Default storage path
Set-VMHost -VirtualMachinePath 'D:\VMs' -VirtualHardDiskPath 'D:\VMs\VHD'

# Activer enhanced session (cas multi-domain) et live migration si cluster
Enable-VMMigration
Set-VMHost -VirtualMachineMigrationAuthenticationType Kerberos
```

### 9.6.4 Creation d'une VM standard

```
# Exemple : VM Windows Server 2022 standard (DC, RDS, ou applicatif)

$VM_NAME = 'srv-app01'
$VM_PATH = 'D:\VMs'

New-VM -Name $VM_NAME `
      -MemoryStartupBytes 8GB `
      -Generation 2 `
      -Path $VM_PATH `
      -NewVHDPath "$VM_PATH\$VM_NAME\$VM_NAME-OS.vhdx" `
      -NewVHDSizeBytes 100GB `
      -SwitchName 'vSwitch-Prod'

# Configuration RAM dynamique
Set-VMMemory -VMName $VM_NAME -DynamicMemoryEnabled $true `
  -MinimumBytes 4GB -MaximumBytes 16GB -StartupBytes 8GB

# Ajouter un disque data
New-VHD -Path "$VM_PATH\$VM_NAME\$VM_NAME-DATA.vhdx" -SizeBytes 200GB -Dynamic
Add-VMHardDiskDrive -VMName $VM_NAME -Path "$VM_PATH\$VM_NAME\$VM_NAME-
DATA.vhdx"

# Activer Secure Boot (Generation 2)
Set-VMFirmware -VMName $VM_NAME -EnableSecureBoot On

# Monter ISO Windows Server
Set-VMDvdDrive -VMName $VM_NAME -Path 'C:\ISOs\WS2022.iso'

# Demarrer
Start-VM -Name $VM_NAME
```

## 9.7 Hyperviseur - Proxmox VE

### 9.7.1 Cas d'usage

Proxmox VE (Debian + KVM + LXC) est l'hyperviseur Linux open source de reference JMSI. Choix prefere pour : multi-OS (Linux, BSD, Windows), cluster 3+ nodes, Ceph distribue, clients sensibles au cout de licence.

### 9.7.2 Procedure d'installation Proxmox standalone

352. Boot sur ISO Proxmox VE 8.x (Ventoy ou USB direct).
353. Choix du disque cible : ZFS RAID1 sur 2 SSD NVMe.
354. Reglages locale, fuseau, mot de passe root, IP fixe management.
355. Premier acces : https://<IP>:8006.
356. Reglages immediats post-install :

```
# Sur le node Proxmox apres install (SSH root)

# 1) Sources non-souscription (depots gratuits)
sed -i 's/^deb/#deb/' /etc/apt/sources.list.d/pve-enterprise.list
sed -i 's/^deb/#deb/' /etc/apt/sources.list.d/ceph.list || true
echo 'deb http://download.proxmox.com/debian/pve bookworm pve-no-subscription' \
  > /etc/apt/sources.list.d/pve-no-subscription.list

# 2) Mise a jour
apt update && apt -y dist-upgrade

# 3) Pas de message d'avertissement souscription dans la GUI
sed -i "s/data.status !== 'Active'/false/g" \
  /usr/share/javascript/proxmox-widget-toolkit/proxmoxlib.js
systemctl restart pveproxy

# 4) Outils complementaires JMSI
apt install -y htop iftop iotop sysstat tmux molly-guard apparmor-profiles

# 5) Sauvegarde - creer un Backup Storage
#    GUI > Datacenter > Storage > Add > NFS / SMB / PBS
#    Cible : NAS Synology client + Wasabi pour offsite (PBS)

# 6) NTP
timedatectl set-timezone Europe/Paris
timedatectl set-ntp on

# 7) Securisation acces : root SSH par cle, MFA console GUI
#    Datacenter > Permissions > Two Factor : TOTP active pour root@pam et tech
```

### 9.7.3 Cluster Proxmox 3 nodes

Pour la haute disponibilite : 3 nodes minimum, Ceph distribue, fencing automatique.

```
# Sur le 1er node (cluster init)
pvecm create jmsi-cluster

# Sur les autres nodes (rejoindre)
pvecm add 10.0.0.10 -use_ssh

# Verifier l'etat
pvecm status
pvecm nodes

# Stockage Ceph : prerequis 3 nodes minimum, 4 OSD minimum
# GUI > Datacenter > Ceph > Init
# Suivre l'assistant : public network, cluster network (replication)

# OSD par node : ajouter chaque disque dedie data
pveceph createosd /dev/nvme1n1
```

```
pveceph createosd /dev/nvme2n1

# Pool RBD pour les VM
# GUI > Ceph > Pools > Create
#   Name: vm-pool, Size: 3, Min size: 2

# HA cluster
# GUI > Datacenter > HA > Group : creer un groupe HA
# GUI > Datacenter > HA > Resources : ajouter les VM critiques au groupe
```

# 9.8 Active Directory (Windows Server)

## 9.8.1 Promotion d'un controleur de domaine

```
# Pre-requis : VM Windows Server 2022, IP fixe, NTP synchro, joinable au domaine cible si extension

# Installation des roles ADDS + DNS
Install-WindowsFeature -Name AD-Domain-Services,DNS \
  -IncludeManagementTools

# Creation d'une nouvelle foret (cas standalone PME)
$DomainName = 'exemple.local'
$NetbiosName = 'EXEMPLE'
$SafeMode    = ConvertTo-SecureString -String '<MOT_PASSE_DSRM>' -AsPlainText -Force

Install-ADDSForest -DomainName $DomainName \
  -DomainNetbiosName $NetbiosName \
  -DomainMode 'WinThreshold' \
  -ForestMode 'WinThreshold' \
  -SafeModeAdministratorPassword $SafeMode \
  -InstallDns -NoRebootOnCompletion -Force

Restart-Computer -Force

# Verifications post-promo
Get-ADForest
Get-ADDomain
dcdiag /v
repadmin /replsummary
```

## 9.8.2 Bonnes pratiques AD

- Toujours 2 controleurs de domaine minimum (pas de SPOF).
- Schema AD : groupes par fonction (RH, Compta, IT, etc.) plutot que groupes nominatifs.
- OU structurees : Servers, Workstations, Users, Groups, Service Accounts.
- Tier 0 / Tier 1 / Tier 2 : separation des comptes admin par criticite (PAM).
- Audit policy GPO : journaliser logon/logoff, modifications privilegiees.
- Pingcastle annuel : score < 30 cible.
- KRBTGT password rotation : tous les 6 mois (Microsoft New-KrbtgtKeys).

## 9.8.3 GPO de base JMSI

| Nom GPO | Cible | Effet |
|---|---|---|

| | | |
|---|---|---|
| **JMSI_SEC_PolicyMDP** | Domaine entier | 12 chars min, complexite, historique 24, expiration 90 jours |
| **JMSI_SEC_AccountLockout** | Domaine entier | 5 echecs / 30 min lockout |
| **JMSI_SEC_AuditPol** | DCs | Audit logon, audit privilege use, audit policy change |
| **JMSI_DEPLOY_Imprimantes** | Workstations | Connexion imprimantes par site (script ou ItemLevel) |
| **JMSI_DEPLOY_NetworkDrives** | Users | Lecteurs reseau X: Y: par groupe |
| **JMSI_SEC_Firewall** | Workstations | Profil domaine / public stricts |
| **JMSI_SEC_USB** | Workstations | Bloquer USB stockage en exterieur de IT |
| **JMSI_DEPLOY_Wallpaper** | Users | Fond d'ecran corporate (information legale) |

# 9.9 Serveur RDS (Remote Desktop Services)

## 9.9.1 Architecture

Pour les clients qui veulent un acces distant a une session de bureau partagee : RDS via RD Gateway + RD Web Access. CAL utilisateur ou device requise.

- RD Connection Broker : repartit les sessions.
- RD Session Host : 1 a N hotes selon charge utilisateur.
- RD Gateway : passerelle Internet (port TCP 443 expose).
- RD Web Access : portail HTTPS RDP.
- Licensing Server : gestion des CAL.
- MFA OBLIGATOIRE sur la passerelle RD (Duo, Azure MFA, etc.).

## 9.9.2 Procedure de deploiement RDS

```
# Pre-requis : Active Directory + 1 a 3 VM (Broker, SH, Gateway)
# Tout fonctionne en VM Windows Server 2022 Standard

# 1) Sur les VM, joindre le domaine
Add-Computer -DomainName 'exemple.local' -Restart

# 2) Sur le serveur Broker - installer le role RDS
Install-WindowsFeature -Name RDS-Connection-Broker -IncludeManagementTools

# 3) Sur le SH - installer le role RD Session Host
Install-WindowsFeature -Name RDS-RD-Server -IncludeManagementTools

# 4) Sur la Gateway - installer le role RD Gateway
Install-WindowsFeature -Name RDS-Gateway -IncludeManagementTools

# 5) Deployer la session collection (depuis Broker)
New-RDSessionDeployment -ConnectionBroker 'rdcb.exemple.local' \
```

```
 -SessionHost 'rdsh.exemple.local','rdsh2.exemple.local'

New-RDSessionCollection -CollectionName 'COL01' \
 -SessionHost 'rdsh.exemple.local','rdsh2.exemple.local' \
 -ConnectionBroker 'rdcb.exemple.local'

# 6) Configurer les profils utilisateurs (FSLogix)
#    FSLogix gere les profils en VHD/VHDX, evite la corruption des profiles roaming

# 7) Certificat TLS pour la Gateway
#    Let's Encrypt via win-acme (wacs.exe), liaison au RD Gateway

# 8) MFA cote Gateway via NPS + extension Azure MFA ou Duo
#    Configuration RADIUS proxy
```

## 9.10 Serveur de fichiers (FS)

Le file server est l'epine dorsale du partage interne. Architecture standard JMSI :

- VM Windows Server 2022 Standard, 16 Go RAM minimum, disque data dedie (RAID 6 ou Storage Spaces).
- Roles : File Server + File Server Resource Manager (FSRM) + DFS Namespaces (multi-site).
- Quotas et screening (FSRM) : par OU, blocage extensions ransomware connues.
- Auditing : Object Access activite logged.
- Sauvegarde : Veeam VM-level + Veeam File Backup pour granularite.

### 9.10.1 Configuration FSRM avec ransomware screening

```
# Activer FSRM
Install-WindowsFeature -Name FS-Resource-Manager,FS-DFS-Namespace,FS-DFS-Replication

# Liste des extensions ransomware connues - groupe a creer
$blocked = @(
 '*.locked', '*.encrypted', '*.crypt', '*.crypted',
 '*.cryptolocker', '*.cerber', '*.zepto', '*.locky',
 '*.zzz', '*.aaa', '*.xyz', '*.ccc', '*.exx', '*.ezz',
 '*.[*].ad*', '!_HELP_INSTRUCTIONS.txt', 'HOW_TO_DECRYPT*'
)

New-FsrmFileGroup -Name 'JMSI Ransomware Extensions' -IncludePattern $blocked

# Creer un screen template
New-FsrmFileScreenTemplate -Name 'Block Ransomware (JMSI)' -Active `
 -IncludeGroup 'JMSI Ransomware Extensions' `
 -Notification @(
   New-FsrmAction Email -MailTo 'soc@jmlab.eu' -Subject 'RANSOMWARE DETECTED on file
server' \
      -Body 'File <{0}> matched ransomware pattern' -RunLimitInterval 1
 )

# Appliquer sur les volumes data
New-FsrmFileScreen -Path 'D:\Shares' -Template 'Block Ransomware (JMSI)' -Active
```

# 9.11 Imprimantes / copieurs

## 9.11.1 Recueil d'information avant deploiement

JMSI dispose d'un formulaire dedie 'Recueil info copieur' (cf. dossier Communication). Donnees a collecter :

- Marque, modele, n de serie.
- Adresse IP fixe + plage du subnet.
- Codes admin imprimante (interface web).
- Comptes utilisateurs (codes badges si copieur a badge).
- Carnet d'adresses scan-to-email (modele : SMTP IP/port, chiffrement).
- Volume mensuel (couleur, NB).
- Contrat existant (pages forfait, surplus, telemaintenance editeur).

## 9.11.2 Procedure de mise en service

357. Recevoir et deballer (controle visuel).
358. Branchement reseau LAN.
359. Configuration IP fixe (en mode menu local ou via script constructeur).
360. Definition du gateway, DNS, proxy si necessaire.
361. Configuration scan-to-email : SMTP, expediteur, authentification (Microsoft 365 OAuth dans les versions modernes).
362. Configuration scan-to-folder : SMB serveur de fichier client, compte de service dedie.
363. Activation Print to / AirPrint si demande.
364. Mise en place de la file d'impression cote Print Server (Windows Server) ou installation locale par utilisateur.
365. Test impression / scan / copie.
366. Documentation : ip, codes, n serie, deploye dans GLPI.

## 9.11.3 Print Server centralise (cas multi-imprimantes)

```
# Sur Windows Server 2022 - role Print and Document Services
Install-WindowsFeature -Name Print-Services -IncludeManagementTools

# Ajouter une imprimante via PowerShell
Add-PrinterPort -Name 'IP_192.168.1.50' -PrinterHostAddress '192.168.1.50'
Add-PrinterDriver -Name 'KONICA MINOLTA bizhub C360i PCL' -InfPath 'C:
\Drivers\bizhub\PCL\KOAXJSP_.inf'
Add-Printer -Name 'IMP-Compta-RDC' \
  -DriverName 'KONICA MINOLTA bizhub C360i PCL' \
  -PortName 'IP_192.168.1.50' \
  -Shared -ShareName 'IMP-Compta-RDC' -Published

# GPO pour deploiement automatique aux utilisateurs
# (User Configuration > Preferences > Control Panel Settings > Printers)
```

# 9.12 Reseau - switches, routeurs, baies

## 9.12.1 Switches PoE JMSI standard

| Code | Modele | Specification |
|---|---|---|
| **B2B_NET_01** | Switch PoE 8 ports Gigabit | TP-Link TL-SG2008P (PoE+ 802.3at, 62W total) ou UniFi USW-Lite-8-PoE |
| **B2B_NET_02** | Switch PoE 24 ports Gigabit | UniFi USW-24-PoE (250W, 16 ports PoE+) ou TP-Link TL-SG2428P |
| **B2B_NET_03** | Switch PoE 48 ports Gigabit | UniFi USW-48-PoE (380W, 32 ports PoE+) ou Aruba 1830-48G-PoE+ |

## 9.12.2 Configuration switch UniFi standard

```
# Cote console UniFi
# Switch > Settings > Networks (VLANs)

# Creer 4 reseaux JMSI standard :
# 1 Management   - VLAN 1   - 10.X.0.0/24
# 10 Production  - VLAN 10  - 10.X.10.0/24
# 20 Voice       - VLAN 20  - 10.X.20.0/24 (DHCP option 66 vers PBX provisioning)
# 50 Guest       - VLAN 50  - 10.X.50.0/24 (isole de tout le reste)
# 60 IoT         - VLAN 60  - 10.X.60.0/24 (isole + access list specifique)
# 99 Surveillance- VLAN 99  - 10.X.99.0/24 (isole, pas d'Internet sortant)

# Profils de port :
# 'JMSI-Trunk-AP' (uplinks AP UniFi) : All VLANs tagged, Native VLAN 1
# 'JMSI-Acces-Bureau' : Native VLAN 10, Voice VLAN 20
# 'JMSI-Acces-Visioconf' : Native VLAN 10
# 'JMSI-Camera' : Native VLAN 99
# 'JMSI-Imprimante' : Native VLAN 10
# 'JMSI-Trunk-Switch' : tagged toutes les VLAN clients

# 802.1X / MAC Auth : optionnel pour les clients NIS2
# Storm Control : actif par defaut sur VLAN 50/60
# DHCP Snooping : actif sur VLAN 10
# IGMP Snooping : actif (multicast)
```

## 9.12.3 Routeur SD-WAN PME (B2B_NET_04)

Pour les clients multi-site ou ayant deux liaisons WAN (fibre + 4G/5G secours), JMSI deploie un routeur SD-WAN type Peplink Balance, Cisco Meraki MX64, ou OPNsense + multi-WAN.

- Bonding des liens (load balancing par session ou par paquet).
- Failover automatique : detection coupure + bascule en < 5 secondes.
- Tunnel IPSec ou WireGuard vers les autres sites.
- QoS - priorisation voix et visioconference.
- Statistiques : utilisation par lien, top apps, top hosts.

### 9.12.4 Baie de stockage SAN (B2B_NET_05)

Pour les clients > 50 utilisateurs ou avec besoin de hautes performances stockage : SAN dedie.

- Synology UC3400 / SA3600 (iSCSI + NFS, redondance controleurs).
- Dell PowerVault ME5024 (FC + iSCSI, dual ctrl).
- Dimensionnement par devis (volumetrie, IOPS, debit, RPO local).

## 9.13 Baies informatiques

### 9.13.1 Modeles JMSI

| Code | Designation | Cas d'usage |
|---|---|---|
| **B2B_VDI_02** | Baie brassage 12U fournie - 690 EUR | TPE 1-15 utilisateurs |
| **B2B_VDI_03** | Baie brassage 24U fournie - 1290 EUR | PME 15-80 utilisateurs |
| **B2B_MAT_08** | Baie informatique - sur devis | Datacenter / serveurs |

### 9.13.2 Montage et brassage - methode JMSI

Une baie bien montee se reconnait au premier coup d'oeil : rangees ordonnees, etiquetage clair, cables de longueur exacte, code couleur respecte. Une baie mal montee genere des heures de diagnostic.

#### *Code couleur cables JMSI*

| Couleur | Usage |
|---|---|
| **Bleu** | LAN bureautique |
| **Jaune** | Telephonie VoIP / Voice |
| **Vert** | Wi-Fi (uplink AP) / DMZ |
| **Rouge** | Liens management / hyperviseurs / SAN |
| **Violet** | Camera surveillance |
| **Orange** | WAN / Internet |
| **Noir** | Power / shielded special |

#### *Etiquetage*

- Format JMSI : <SITE>-<EMPLACEMENT>-<TYPE>-<NUMERO>. Exemple : 'SIE-RDC-LAN-01'.
- Etiquettes thermiques (Brother PT-D210 ou equivalent) - jamais manuscrites.
- Etiquette aux deux extremites du cable.
- Etiquette plastifiee sur la facade de baie : plan de brassage (PDF imprime A3 -> A4 plastifie).

### *Bandes velcro vs colliers serre-cables*

- VELCRO uniquement dans la baie (reutilisable, pas de coupure).
- COLLIERS plastiques tolerés en arriere de chemins de cables fixes uniquement.
- Jamais de scotch, jamais de fil de fer.

### *Sequence de montage de baie*

367. Plancher : passage cables remontes du faux-plancher / dalle.
368. Bas de baie : onduleur (poids).
369. Servers (poids decroissant en remontant).
370. Switch core (typiquement vers le milieu).
371. NVR / NAS.
372. Patch panel(s).
373. Switches d'acces.
374. Cable management horizontal entre patch panel et switches (rangees velcro).
375. Espace haut : cable management vertical lateraux.

## 9.14 Cablage VDI - pre-cablage RJ45 Cat 6A

### 9.14.1 Pre-cablage par prise (B2B_VDI_01 - 89 EUR/prise)

- Cable Cat 6A 23 AWG U/FTP ou F/UTP (selon perturbations).
- Goulotte ou faux-plafond vers patch panel.
- Sertissage sur patch panel : keystone Cat 6A T568B (standard JMSI).
- Test au testeur certifie (Fluke / Trend) - obligatoire si demande de certification.
- Certification Cat 6A (B2B_VDI_04 - 29 EUR/prise) : test exhaustif (NEXT, ACR-F, return loss, propagation delay).

### 9.14.2 Liaison fibre optique inter-batiments (B2B_VDI_05)

- Etude prealable : distance, traversees (chemin de cables, fourreau, aerien).
- Choix du cable : OM4 multimode (jusqu'a 400m a 10G) ou OS2 monomode (km).
- Connectique : LC/UPC standard, MTP/MPO pour densite haute.
- Soudure (fusionneuse Fujikura ou equivalent loue) si raboutage.
- Test photometrique (perte d'insertion, perte de retour, longueur).
- Documentation : schema, photos, certificat de mesure.

## 9.15 Maintenance preventive du materiel

| Composant | Frequence | Tache |
|---|---|---|
| **Postes** | Semestrielle | Depoussierage + verification SMART + batterie laptop |
| **Onduleurs** | Annuelle | Test autonomie reelle - remplacement batterie tous les 3-4 ans |
| **Serveurs** | Trimestrielle | Verification SMART, RAID battery, |

| | | |
|---|---|---|
| | | BBU controller, retour temperature |
| **Switches** | Semestrielle | Verification log d'erreurs port, mises a jour firmware annuelles |
| **Imprimantes** | Trimestrielle | Verification niveaux, nettoyage, capteurs |
| **Baies** | Trimestrielle | Verification ventilation, temperature, filtre poussiere |
| **Climatisation salle serveurs** | Trimestrielle | Maintenance par specialiste, verification redondance |
| **Cameras** | Trimestrielle | Nettoyage objectifs, verification etancheite (exterieur) |

# PARTIE VII

# Solutions integrees

# Chapitre 10 - Pack Pro (Serenite, Performance, A composer)

## 10.1 Perimetre

Le Pack Pro JMSI est une offre integree : materiel + maintenance + sauvegarde, en une seule facture, avec un seul interlocuteur. Trois variantes existent.

| Code Dolibarr | Designation | Tarif HT |
|---|---|---|
| **B2B_PAK_01** | Pack Serenite | 937,00 EUR (hardware) + 21,90 EUR/poste/mois (services) |
| **B2B_PAK_02** | Pack Performance | 6 760,00 EUR (hardware base) + services |
| **B2B_PAK_03** | Pack a composer | Sur devis |

## 10.2 Pack Serenite - composition standard

### 10.2.1 Hardware inclus (1 poste)

- PC bureau i3 neuf (B2B_MAT_01) ou portable i5 neuf (B2B_MAT_03).
- Ecran 24'' Full HD (B2B_MAT_05).
- Onduleur 1000 VA (B2B_MAT_06).
- NAS 2 baies 8 To (B2B_MAT_07) - mutualise pour les Packs Serenite multi-postes.
- Livraison et installation incluse (B2B_MAT_09).

### 10.2.2 Services inclus (mensuel)

- Maintenance 1 poste (B2B_MAI_01).
- Sauvegarde poste (B2B_SAU_01).
- Securite essentiel (B2B_SEC_01).

### 10.2.3 Procedure de mise en service Pack Serenite (1 jour)

376. Reception du materiel chez JMSI bench (J-2).
377. Preparation poste (J-1) : application du chap. 9.2.2.
378. Preparation NAS (J-1 si premier deploiement client) : chap. 4.3.
379. Installation BitLocker, EDR Bitdefender, RustDesk, TacticalRMM.
380. Configuration sauvegarde Active Backup pour Business vers NAS.
381. Sur site (J0) : raccordement reseau, branchement onduleur, formation utilisateur 30 min.
382. Test : ouverture session, internet, application metier, sauvegarde planifiee.
383. PV de mise en service signe.

# 10.3 Pack Performance - composition standard

## 10.3.1 Hardware inclus (5 postes)

- 5 PC bureau (mix i3/i5 selon besoin metier).
- 5 ecrans 24'' Full HD.
- 5 onduleurs ou 1 onduleur baie.
- Serveur tour PME pro (B2B_SRV_02) avec Hyper-V + VM AD + VM File Server.
- Switch PoE 8 ports (B2B_NET_01).
- NAS 4 baies 16 To en SHR-1 (DS423+ avec 4x HAT3300 8 To).
- Pre-cablage 5 prises Cat 6A.
- Baie brassage 12U (B2B_VDI_02).

## 10.3.2 Services inclus (mensuel)

- Maintenance 5 postes (B2B_MAI_02).
- Sauvegarde serveur 500 Go (B2B_SAU_02).
- Securite Pro (B2B_SEC_02) sur tous les postes et le serveur.

## 10.3.3 Procedure de mise en service Pack Performance (5 jours)

384. J0 - Reception et controle materiel.
385. J1 - Pre-cablage Cat 6A et installation baie 12U sur site (chap. 9.13-9.14).
386. J1 - Montage du serveur dans la baie + brassage initial.
387. J2 - Installation Windows Server + Hyper-V (chap. 9.6).
388. J2 - Promotion AD + creation OUs + GPO de base (chap. 9.8).
389. J3 - Creation VM File Server, configuration partages, FSRM.
390. J3 - Mise en service NAS Synology + Active Backup for Business (chap. 4.3).
391. J4 - Preparation des 5 postes (image master ou install one-by-one).
392. J4 - Joining domain, deploiement EDR, deploiement TacticalRMM.
393. J5 - Recette : test login utilisateur, partages, mail, sauvegarde, EDR remontee.
394. J5 - Formation utilisateurs (1h) + remise PV de mise en service.

# 10.4 Pack a composer (B2B_PAK_03)

Pour les besoins specifiques : combinaison libre des codes Dolibarr. Methodologie de chiffrage :

395. Audit gratuit (chap. 2.3.1 ou 4.10).
396. Recommandation chiffree avec 3 options (Essentiel, Confort, Premium).
397. Validation client.
398. Chefferie de projet : un N2 designe coordinateur, planning par lot, livrable / lot.
399. Mise en service par phases (cf. chapitres concernes).
400. Recette globale + PV multi-services.

# 10.5 Migration entre packs (Serenite vers Performance)

- Audit pre-migration : inventaire utilisateur reel vs Pack Serenite couvert.

- Apport materiel complementaire (serveur, switch, NAS upgrade).
- Bascule progressive (par groupe d'utilisateurs).
- Ajustement du contrat de services (passage maintenance 5 -> 10 postes par exemple).
- PV de transition.

# Chapitre 11 - Salle de reunion et affichage dynamique

## 11.1 Perimetre

| Code Dolibarr | Designation | Tarif HT |
|---|---|---|
| **B2B_REU_01** | Ecran interactif 65 pouces | 2 490,00 EUR |
| **B2B_REU_02** | Ecran interactif 75 pouces | 3 290,00 EUR |
| **B2B_REU_03** | Barre video Teams Zoom | 1 290,00 EUR |
| **B2B_REU_04** | Systeme visio salle moyenne | 2 890,00 EUR |
| **B2B_REU_05** | Affichage dynamique | 890,00 EUR (HW) + 19,00 EUR/mois (B2B_REU_09) |
| **B2B_REU_06** | Installation cablage formation | Sur devis |
| **B2B_REU_07** | Ecran professionnel 50 pouces | 590,00 EUR |
| **B2B_REU_08** | Ecran professionnel 55 pouces | 690,00 EUR |
| **B2B_REU_09** | Module diffusion video salle d'attente | 19,00 EUR / mois |

## 11.2 Choix d'equipement par taille de salle

| Taille salle | Capacite | Equipement recommande |
|---|---|---|
| **Petite (4-6 pers.)** | Bureau d'angle, salle reunion 1-2 visios/sem. | Ecran pro 55'' + Logitech MeetUp ou Yealink VC210 |
| **Moyenne (8-12 pers.)** | Salle hebdo, hybride frequent | Ecran interactif 65'' + barre video Logitech Rally Bar Mini |
| **Grande (12-20 pers.)** | Salle direction, conseil | Ecran interactif 75'' + camera PTZ Logitech Rally + microphones plafond |
| **Conference (>20 pers.)** | Auditorium, formation | Vidéoprojecteur laser + ecran motorise + multi-cameras + table de mixage |

## 11.3 Mise en service - barre video Teams/Zoom (B2B_REU_03)

Cas d'usage le plus frequent : barre video Logitech / Yealink + ecran TV pro + tablette de pilotage.

### 11.3.1 Equipement type

- Barre video : Logitech Rally Bar / Rally Bar Mini OU Yealink MeetingBoard 65 OU Cisco Room Bar.
- Ecran : ecran TV pro 55'' ou 65'' (Samsung BE / LG UR / NEC E series).
- Tablette controle : Logitech Tap / Yealink CTP18.
- Mode : Microsoft Teams Rooms (MTR) ou Zoom Rooms ou BYOD (USB).

### 11.3.2 Procedure d'installation

401. Etude positionnement : ecran face a la table, barre video dessous (1,1m du sol pour le cadrage).
402. Cablage : prise reseau Cat 6A (PoE+) au niveau barre, prise HDMI vers ecran, prise secteur.
403. Goulottes ou passages murs - pas de cables apparents.
404. Provisioning Microsoft Teams Rooms : compte de salle dedie (room@exemple.fr) avec licence MTR.
405. Configuration sur la console Teams Admin : politique salle (calendrier, sonnerie, ecran de veille).
406. Configuration de la barre : decouverte sur LAN, jumelage tablette, signing in compte de salle.
407. Test reunion : creation reunion Teams + appel depuis poste utilisateur + verification audio/video bidirectionnel.
408. Formation utilisateurs : 30 minutes (demarrer reunion, partager ecran, inviter participants).

### 11.3.3 Configuration Microsoft Teams Rooms

```
# Cote tenant Microsoft 365 (PowerShell Exchange Online)
# Compte de salle dedie

$Room = 'salle-direction@exemple.fr'

# Creer une room mailbox
New-Mailbox -Name 'Salle Direction' -Alias 'salle-direction' -Room \
  -EnableRoomMailboxAccount $true -RoomMailboxPassword (ConvertTo-SecureString -String
'<MDP>' -AsPlainText -Force)

# Reglages calendrier
Set-CalendarProcessing -Identity $Room -AutomateProcessing AutoAccept \
  -AddOrganizerToSubject $false -DeleteComments $false \
  -DeleteSubject $false -RemovePrivateProperty $false

# Affecter la licence MTR (Teams Rooms Pro = ~ 50 USD/mois/salle)
# A faire dans la console admin Microsoft

# Cote console Teams Admin
# Devices > Teams Rooms > Configuration policies
# Creer une policy 'JMSI Standard' :
#   - Auto join meetings : Yes
#   - Hide private meeting names : No (ajustable client)
#   - Allow ad-hoc meetings : Yes
#   - Login session timeout : 8h
```

## 11.4 Ecran interactif (B2B_REU_01 / B2B_REU_02)

Les ecrans interactifs (BenQ, Newline, ViewSonic, Promethean) integrent un OS Android + un PC Windows OPS optionnel.

### 11.4.1 Mise en service

- Fixation murale ou pied roulant.
- Cablage : RJ45 + secteur + HDMI/USB-C ports utilisateurs accessibles (carrelage de prise).
- Premier boot : configuration locale, mise a jour firmware.
- Joindre le Wi-Fi corporate (ou cable preferable - QoS et stabilite).
- Inscription dans la console fabricant (BenQ X-sign, Newline Care).
- Telecharger les apps voulues (Whiteboard, Zoom, Teams, navigateur).
- Si OPS PC integré : configuration Windows comme un poste de salle.

## 11.5 Affichage dynamique (B2B_REU_05) - Porteus + scenarios

JMSI utilise une distribution Linux legere (Porteus Kiosk ou Yodeck cloud) pour transformer un ecran TV en panneau d'affichage dynamique. Cas d'usage : accueil entreprise, salle d'attente, hall industriel, ecole, retail.

### 11.5.1 Configuration Porteus Kiosk

```
# Image Porteus Kiosk personnalisee JMSI
# Telechargement : porteus-kiosk.org
# Pre-config JMSI : URL d'affichage + reglages reseau/clavier

# Boot sur USB (mini PC HP / Intel NUC)
# Reglages Porteus essentiels :
#   * URL : https://signage.jmlab.eu/<CODE_CLIENT>/play
#   * Mode kiosque, ecran plein, Esc desactive
#   * Reboot automatique : tous les jours 02:00
#   * Cache offline : oui (resilience coupure Internet)
#   * Mise a jour Porteus : auto monthly

# Cote serveur signage.jmlab.eu (Yodeck hebergé ou Xibo open source)
# - Layouts : zones video / texte / horloge / logo
# - Playlists : sequences contenu
# - Schedules : par jour / heure / ecran
# - Tags : par site, par salle

# Module diffusion video salle d'attente (B2B_REU_09)
# - Boucle de 30 min : message d'accueil + actu metier client + horloge
# - Mute par defaut, sons activables sur certains plages
```

## 11.6 Audio amplifie (cas grandes salles)

- Microphones plafond (Sennheiser TeamConnect Ceiling, Shure MXA920) : couverture homogene.
- Cablage Dante (audio sur IP) ou propriétaire selon ecosysteme.
- DSP (Biamp Tesira) ou solution integree (Logitech Rally + extension microphones).
- Calibration acoustique : reverberation < 0,6s ideale, mesurer au sonometre apres pose.

## 11.7 Recette et formation

- Test reunion reelle avec 3 participants distants (pas seulement console).
- Test partage ecran : laptop USB-C, laptop HDMI dongle, smartphone iOS/Android.

- Test ecran interactif : prise de notes, inscription, sauvegarde session.
- Formation 30-60 min utilisateur : guide pas-a-pas + cheat sheet plastifiee dans la salle.

## 11.8 Depannage frequent

### 11.8.1 Pas de son cote distant

409. Verifier mute du microphone barre video.
410. Verifier le mute cote logiciel (Teams / Zoom).
411. Verifier la source audio (utiliser le micro de la barre, pas le micro du laptop).

### 11.8.2 Image saccadee

412. Verifier le debit Internet (10 Mbps mini par salle).
413. Verifier QoS - prioriser les ports UDP video.
414. Reduire la qualite video (Teams : Low data mode).

# Chapitre 12 - Particulier Tranquillite (B2C)

## 12.1 Perimetre

L'Offre Tranquillite est l'unique offre B2C de JMSI. Elle s'adresse aux particuliers, seniors, teletravailleurs, familles avec plusieurs ordinateurs.

| Code | Designation | Tarif HT mensuel |
|---|---|---|
| **B2C_PAR_01** | Offre Tranquillite | 13,90 EUR / mois |
| **B2C_PAR_02** | Appareil supplementaire | 6,90 EUR / mois |
| **B2C_PAR_03** | Intervention a domicile | 49,00 EUR / intervention |
| **B2C_PAR_04** | Passage atelier supplementaire | 29,00 EUR |
| **B2C_PAR_05** | Sauvegarde cloud etendue 500 Go | 4,90 EUR / mois |
| **B2C_PAR_06** | Installation/migration nouveau PC | 59,00 EUR / poste |
| **B2C_PAR_07** | Recuperation de donnees | Sur devis |

## 12.2 Architecture B2C - simplifiee

- Pas de RMM TacticalRMM (trop intrusif pour le particulier - usage RustDesk a la demande seulement).
- Antivirus premium : Bitdefender Total Security (licence partenaire JMSI).
- Sauvegarde cloud : Backblaze Personal Backup ou Synology C2 Backup (5 Go inclus, +500 Go option B2C_PAR_05).
- Hotline 8h-20h, francophone, JMSI (numero direct).
- Pas de SLA contractuel (best-effort), mais qualite de service prioritaire.

## 12.3 Mise en service B2C

415. Inscription en ligne ou par telephone.
416. Prelevement SEPA ou CB.
417. Envoi du kit de bienvenue (mail) : numero de hotline, lien telechargement antivirus + sauvegarde + RustDesk.
418. Premiere session telephonique guide d'installation (gratuite, ~30 min).
419. Verification que l'antivirus tourne, que la premiere sauvegarde demarre.
420. Bilan a J+30 : appel client, ajustements.

## 12.4 Interventions

### 12.4.1 Hotline a distance (incluse)

- Le client appelle, donne son ID RustDesk.
- Diagnostic + resolution (typique : Outlook, imprimante, virus, lenteur, mot de passe).
- Conseil au client (vulgarisation).
- Cloture de la session, jamais de prise de main non sollicitee.

### 12.4.2 Intervention atelier (1 inclus / mois)

- Le client apporte sa machine au local JMSI.
- Diagnostic complet : SMART, memoire, virus, sauvegarde.
- Reparation simple incluse.
- Devis pour reparation lourde (changement disque, ecran, etc.).
- Restitution sous 5 jours ouvres maximum.

### 12.4.3 Intervention a domicile (B2C_PAR_03)

- Forfait 49 EUR pour deplacement + 1h sur place.
- Geographie : limite a 30 km du local JMSI.
- Cas typique : configuration Internet, installation imprimante reseau, recuperation poste apres deces.

## 12.5 Recuperation de donnees (B2C_PAR_07)

Sur devis. JMSI sous-traite a un prestataire specialise (Recoveo, Datacent) si manipulation salle blanche necessaire (defaillance physique disque).

- Tentative niveau 1 (logique) : tester avec PhotoRec, TestDisk - gratuit jusqu'au diagnostic.
- Niveau 2 (physique) : envoi specialise, devis prealable, retour en 2-4 semaines.
- Tarifs typiques specialise : 250 a 1500 EUR selon complexite.

## 12.6 Sensibilisation B2C

- Newsletter mensuelle simple : 1 conseil pratique + 1 alerte arnaque en cours.
- Lors de chaque appel : verifier MFA mail, MFA banque, sauvegarde active.
- Conseil specifique seniors : appeler en cas de doute (faux service technique, fausse banque, faux Microsoft).

# Chapitre 13 - Dolibarr ERP/CRM infogere

## 13.1 Perimetre

Dolibarr ERP/CRM est le logiciel de gestion open-source francais de reference. JMSI le deploie en mode infogere pour ses clients TPE/PME : ERP + CRM + facturation + stock + RH dans une seule interface.

| Code | Designation | Tarif HT |
|---|---|---|
| **B2B_HEB_09** | Dolibarr infogere Essentiel | 9,00 EUR / utilisateur / mois |
| **B2B_HEB_10** | Dolibarr infogere Pro | 19,00 EUR / utilisateur / mois |
| **B2B_HEB_11** | Mise en service Dolibarr | 690,00 EUR (one-shot) |

## 13.2 Differences Essentiel vs Pro

| Critere | Essentiel | Pro |
|---|---|---|
| **Modules actives** | Tiers, devis, factures, paiements, produits | Tous + projets, stocks, RH, expedition, comptabilite avancee |
| **Personnalisations** | Theme JMSI standard | Modules custom, hooks, templates personnalises |
| **Sauvegarde** | Quotidienne | Toutes les heures + dump SQL |
| **Migration de donnees** | Import CSV | Mapping sur mesure (PHP / SQL) |
| **Support** | Mail < 24h ouvres | Mail < 4h ouvres, prise main sous 1h ouvre |
| **Formation incluse** | 1h | 4h + cheat sheet |
| **Mises a jour** | Une par an | Continue (LTS) |
| **Conformite TVA loi anti-fraude** | Oui (certification editeur) | Oui + audit annuel JMSI |

## 13.3 Architecture cible

- VM dediee par client (Debian 12, 4 vCPU, 8 Go RAM, 80 Go SSD).
- Stack : Nginx 1.24 + PHP-FPM 8.2 + MariaDB 10.11.
- Reverse proxy HAProxy + Let's Encrypt.
- Sauvegarde Borg quotidienne + Wasabi.
- Acces : https://erp.<sous-domaine-client>.fr (HTTPS only, HSTS).
- MFA active sur les comptes admin (TOTP Bitwarden).

# 13.4 Procedure de mise en service

## 13.4.1 Provisioning de l'instance

```
# Sur l'hote KVM/Proxmox JMSI - provisionner la VM
# Template Debian 12 deja prepare

# Apres premier boot - script JMSI dolibarr_provision.sh
#!/bin/bash
set -euo pipefail

CLIENT=$1
DOMAINE=$2

# Mise a jour
apt update && apt upgrade -y
apt install -y nginx mariadb-server php8.2-fpm php8.2-mysql php8.2-curl \
  php8.2-gd php8.2-mbstring php8.2-xml php8.2-zip php8.2-imap php8.2-soap \
  composer git unzip ufw fail2ban

# Securisation MariaDB
mysql_secure_installation

# Creation BDD et user
DB_PASSWORD=$(openssl rand -base64 24)
mysql <<EOF
CREATE DATABASE dolibarr CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'dolibarr'@'localhost' IDENTIFIED BY '$DB_PASSWORD';
GRANT ALL ON dolibarr.* TO 'dolibarr'@'localhost';
FLUSH PRIVILEGES;
EOF

# Telechargement Dolibarr 20 (LTS)
cd /var/www
wget https://www.dolibarr.org/files/stable/dolibarr-<VERSION>.tgz
tar xzf dolibarr-<VERSION>.tgz && mv dolibarr-<VERSION> $CLIENT
chown -R www-data:www-data $CLIENT
chmod -R 750 $CLIENT

# Configuration Nginx vhost
cat > /etc/nginx/sites-available/$CLIENT <<NG
server {
    listen 80;
    server_name erp.$DOMAINE;
    root /var/www/$CLIENT/htdocs;
    index index.php index.html;
    client_max_body_size 64M;

    location / {
        try_files \$uri \$uri/ /index.php?\$args;
    }
    location ~ \\.php\$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.2-fpm.sock;
    }
    location ~ /\\.ht { deny all; }
}
NG
```

```
ln -s /etc/nginx/sites-available/$CLIENT /etc/nginx/sites-enabled/
nginx -t && systemctl reload nginx

# Certificat Let's Encrypt
apt install -y certbot python3-certbot-nginx
certbot --nginx -d erp.$DOMAINE --non-interactive --agree-tos -m contact@jmlab.eu

# Premier acces : https://erp.<DOMAINE>/install/index.php
# Suivre l'assistant en utilisant les credentials BDD generes
```

### 13.4.2 Configuration initiale (assistant Dolibarr)

421. Acceder a https://erp.<domaine>/install/index.php.
422. Renseigner les credentials BDD.
423. Creer le premier admin (login admin, mot de passe fort).
424. Choisir le pays (France) et la devise (EUR).
425. Activer les modules necessaires : Tiers, Produits/Services, Devis, Commandes, Factures, Paiements (Essentiel) ; ajouter Stocks, Projets, RH, Expedition, Comptabilite (Pro).
426. Configurer la societe : RIB, n SIREN, TVA intracom, logo.
427. Modeles de documents : choisir le modele JMSI (charte adaptable).
428. Numerotation : DV<YEAR>-<NUM> pour devis, FA<YEAR>-<NUM> pour factures.
429. Importer les donnees : tiers (CSV), produits (CSV), comptes comptables (CSV).
430. Creer les utilisateurs : 1 par collaborateur + role.
431. Configurer MFA (module 'TOTP / Authentification a 2 facteurs').

## 13.5 Conformite TVA loi anti-fraude (LFR 2018-2022)

Depuis le 1er janvier 2018, les logiciels de caisse et de facturation doivent etre conformes a la loi anti-fraude TVA. Dolibarr est certifie depuis la version 7+ et inclut le module obligatoire.

- Verifier l'activation du module 'BlockedLog'.
- Verifier que les factures sont signees electroniquement (chainage SHA-256).
- Aucune modification possible apres validation : seul un avoir / regularisation possible.
- Audit annuel JMSI (Pack Pro) : verification de la chaine d'integrite.

## 13.6 Migration de donnees - methode JMSI

### 13.6.1 Format source courant

| Outil source | Format export | Methode JMSI |
|---|---|---|
| **Excel maison** | XLSX / CSV | Conversion CSV UTF-8 + import Dolibarr (assistant) |
| **Sage 100** | Export texte propriétaire | Script PHP JMSI / outil Manager Dolibarr |
| **EBP** | Export ASCII delimite | Mapping CSV puis import |
| **Quickbooks** | Export QBO / IIF | Conversion CSV via outil tiers |
| **CRM legacy (Tigerpaw, Vtiger)** | Dump SQL | Script SQL JMSI |

### 13.6.2 Procedure type de migration

432. Recuperer les exports source.
433. Mapper les champs source -> Dolibarr (tableur Excel intermediaire).
434. Nettoyage : doublons, valeurs aberrantes, formats date / decimaux.
435. Import par module : tiers d'abord, puis produits, puis pieces (devis/factures historiques).
436. Verification : compter les lignes, recalculer les totaux.
437. Validation client : echantillon de 20 fiches verifie ligne a ligne.
438. Bascule en production : freeze de l'ancien, ouverture du nouveau.

## 13.7 Modules custom (Pro uniquement)

JMSI developpe des modules sur mesure si besoin client. Quelques exemples deja realises :

- Module connecteur Mailcow (sync contacts).
- Module integration 3CX (popup CTI sur appel entrant).
- Module export comptable specifique experts-comptables locaux.
- Module connecteur banque (CFONB, OFX) pour rapprochement automatique.
- Module facturation electronique format Factur-X (futur obligatoire).

## 13.8 Mises a jour Dolibarr

- Cycle JMSI : 1 mise a jour majeure par an (entre versions LTS), apres test sur lab.
- Communication client J-30 : email + planning.
- Sauvegarde complete avant MAJ (full SQL + tar documents).
- MAJ en heures creuses (typiquement weekend).
- Test post-MAJ : login admin + parcours metier critiques (devis, facture, paiement).
- Rollback procedure documentee.

## 13.9 Sauvegarde et restauration Dolibarr

```
# Sauvegarde quotidienne (cron)
#!/bin/bash
DATE=$(date +%Y%m%d-%H%M)
BDD=/backup/dolibarr/db-$DATE.sql.gz
FILES=/backup/dolibarr/documents-$DATE.tgz

mysqldump --single-transaction --routines --triggers \
  -u dolibarr -p<MDP> dolibarr | gzip > $BDD

tar czf $FILES /var/www/<CLIENT>/documents

# Envoi vers Wasabi (rclone)
rclone copy $BDD wasabi:jmsi-<CLIENT>-backup/dolibarr/
rclone copy $FILES wasabi:jmsi-<CLIENT>-backup/dolibarr/

# Retention locale 7 jours
find /backup/dolibarr -mtime +7 -delete
```

```
# Restauration
# 1) Reinstaller le code Dolibarr (meme version)
# 2) Restaurer documents
tar xzf documents-<DATE>.tgz -C /var/www/<CLIENT>/
# 3) Restaurer la BDD
gunzip < db-<DATE>.sql.gz | mysql -u dolibarr -p<MDP> dolibarr
# 4) Verifier conf.php (chemins, BDD)
```

# Chapitre 14 - Reprise et recyclage materiel securise

## 14.1 Perimetre

| Code | Designation | Tarif HT |
|---|---|---|
| **B2B_REC_01** | Reprise materiel obsolete | OFFERTE (deduction sur la facture du nouveau) |
| **B2B_REC_02** | Destruction securisee disque dur | 29,00 EUR / disque |
| **B2B_REC_03** | Destruction securisee serveur et NAS | 89,00 EUR / appareil |
| **B2B_REC_04** | Effacement logiciel certifie | 19,00 EUR / disque |

## 14.2 Cadre legal et reglementaire

- Decret n 2022-1495 (DEEE D3E professionnels) : obligation de tracabilite.
- RGPD article 5 : effacement securise des donnees personnelles.
- Norme NIST SP 800-88 : effacement (Clear, Purge, Destroy).
- Norme DoD 5220.22-M : 3 passes (depasse, mais souvent demandee en marche public).

## 14.3 Effacement logiciel (B2B_REC_04)

### 14.3.1 Methodes JMSI

| Outil | Niveau NIST | Cible | Notes |
|---|---|---|---|
| **DBAN (Darik's Boot and Nuke)** | Clear | HDD magnetique | Open source, 1 a 3 passes (3 passes = DoD) |
| **ATA Secure Erase (hdparm)** | Purge | SSD SATA, HDD SATA | Commande native ATA, rapide, fiable |
| **nvme-cli format** | Purge | SSD NVMe | Commande native, instant si crypto-erase |
| **Blancco Drive Eraser** | Purge | Tout type (certif marche) | Payant, certifie ISO 9001 / Common Criteria |
| **PartedMagic Erase Disk** | Purge | Tout SSD/HDD | Bootable USB, gratuit avant 2017, payant depuis |

### 14.3.2 Procedure JMSI standard - effacement SSD NVMe

```
# Boot sur Linux Live (Debian Live, Ubuntu Live, ou Parted Magic)

# 1) Identifier le SSD
lsblk
nvme list

# 2) Verifier le support de Crypto-Erase ou Format
nvme id-ctrl -H /dev/nvme0n1 | grep -i 'crypto\|format\|sanitize'

# 3) Format avec destruction des cles (crypto erase)
# Mode 1 = User Data Erase, Mode 2 = Cryptographic Erase
sudo nvme format /dev/nvme0n1 -s 1 -f       # secure erase user data
sudo nvme format /dev/nvme0n1 -s 2 -f       # cryptographic erase (preferable si dispo)

# 4) Verifier (lecture brute des premiers blocs)
sudo dd if=/dev/nvme0n1 bs=1M count=10 | hexdump -C | head

# 5) Generer le certificat
echo 'Effacement NVMe Crypto Erase reussi' > /tmp/cert_$(date +%Y%m%d_%H%M%S).txt
echo "Disque : $(nvme id-ctrl /dev/nvme0n1 | grep -E 'sn|mn')" >> /tmp/cert_*.txt
```

### 14.3.3 Procedure JMSI standard - effacement HDD SATA

```
# 1) Identifier
lsblk
sudo hdparm -I /dev/sda | head -30

# 2) Verifier support Secure Erase
sudo hdparm -I /dev/sda | grep -i 'security\|frozen'
# Le disque doit etre 'not frozen'

# 3) Si frozen, suspendre/reveiller le PC pour le degeler
# (commande depend du modele : sleep then resume, ou hot-plug)

# 4) Definir mot de passe utilisateur (technique)
sudo hdparm --user-master u --security-set-pass jmsi /dev/sda

# 5) Lancer Enhanced Secure Erase si possible (plus complet)
sudo hdparm --user-master u --security-erase-enhanced jmsi /dev/sda
# OU Secure Erase classique
sudo hdparm --user-master u --security-erase jmsi /dev/sda

# Compter le temps : un disque 4 To = ~ 6h en Secure Erase

# 6) Verification
sudo dd if=/dev/sda bs=1M count=10 | hexdump -C | head
```

### 14.3.4 Certificat JMSI (modele)

A chaque effacement, JMSI emet un certificat numerique signe (PDF) :

- Date / heure de l'operation.
- Identification du disque : marque, modele, numero de serie, capacite.
- Methode utilisee : NIST Clear / Purge, Crypto Erase, etc.
- Outil utilise : version logiciel.
- Resultat : succes / echec.

- Technicien JMSI executant : nom + signature electronique.
- Reference client + dossier de base.

## 14.4 Destruction physique (B2B_REC_02 / B2B_REC_03)

La destruction physique est exigee dans plusieurs cas : marche public, defense, sante, donnees ultra-sensibles, ou disque defaillant ne pouvant pas etre efface logiciellement.

- Methode 1 : perforation hydraulique (broyeur a disques) - JMSI partenariat avec Lemonpitch.
- Methode 2 : degaussage (HDD magnetiques uniquement, inefficace SSD).
- Methode 3 : broyage (shredder DEEE) - certificat de destruction.
- Tracabilite : photos avant/apres + bordereau remis au client.

## 14.5 Reprise materiel obsolete (B2B_REC_01)

JMSI reprend gratuitement le materiel obsolete dans le cadre d'un nouveau projet. Le materiel reconditionnable alimente le stock B2B_MAT_02 / B2B_MAT_04. Les composants DEEE non reutilisables sont remis a un eco-organisme agree (Ecologic, Ecosystem).

- Bordereau de reprise : liste detaillee du materiel.
- Photos avant transport.
- Effacement logiciel SYSTEMATIQUE meme pour materiel reconditionne.
- Si materiel destine a destruction : certificat DEEE remis sous 7 jours.

# PARTIE VIII

# Annexes techniques

# Annexe A - Modeles de fiches d'intervention

## A.1 Bon d'intervention JMSI standard

Le bon d'intervention est rempli sur place et signe par le client. Format A4, papier carbone (3 exemplaires : client / JMSI / archives). Disponible aussi en version electronique (Yousign ou tablette JMSI).

| Champ | Description |
|---|---|
| **Reference** | BI-<YEAR>-<NUM> (genere automatiquement par GLPI) |
| **Date / heure debut** | Marque par le technicien |
| **Date / heure fin** | Marque a la cloture |
| **Client** | Raison sociale + adresse |
| **Contact sur site** | Nom, qualite, signature |
| **Technicien JMSI** | Nom, qualite, signature |
| **Motif initial** | Resume de la demande / ticket |
| **Travaux realises** | Description detaillee (3 sections : SYMPTOME / DIAGNOSTIC / ACTION) |
| **Materiel utilise** | Liste : pieces installees, consommables, accessoires |
| **Temps passe** | Heures sur place + deplacement |
| **Hors contrat ?** | Case a cocher + reference devis si oui |
| **Reserves client** | Eventuels points en attente |
| **Validation** | Signature client : << Travaux conformes a la demande >> |
| **Annexes** | Photos jointes, schema, captures d'ecran |

## A.2 PV de mise en service

Document plus formel que le bon d'intervention, signe lors d'un projet (mise en service initiale, deploiement Pack Pro, etc.). Cf. chapitre 2.4.1 pour la trame Maintenance ; trames similaires pour les autres offres.

## A.3 Rapport d'audit (modele)

| Section | Contenu cible |
|---|---|

| | |
|---|---|
| **Executive summary** | 1 page, lecture dirigeant client |
| **Contexte** | Activite client, taille, criticite IT |
| **Inventaire materiel** | Tableau detaille du parc |
| **Cartographie reseau** | Schema avec IP, VLAN, fournisseurs |
| **Cartographie services** | Mail, web, applications metier |
| **Constats forts/faibles** | Tableau a 3 colonnes : etat, risque, recommandation |
| **Plan d'action chiffre** | 3 options : Essentiel, Confort, Premium |
| **Calendrier** | Phasage propose |
| **Annexes** | Captures, scripts, references |

## A.4 RAS mensuel - structure type

Cf. chapitre 2.5.4 pour la structure detaillee. Le modele Word est dans /jmsi/templates/RAS_mensuel.docx.

## A.5 Trame compte-rendu de ticket

Tout ticket cloture porte un compte-rendu structure SYMPTOME / DIAGNOSTIC / ACTION :

```
# Exemple compte-rendu type

## SYMPTOME (ce que le client / la console decrit)
L'utilisateur Mme Dupont signale que le poste 'COMPTA-PC02' demarre avec
un ecran bleu BSOD intermittent (3 fois sur 10).

## DIAGNOSTIC (ce qui se passe vraiment)
Analyse du minidump : driver storport.sys ; SMART du disque montre
des secteurs realloues (pre-fail). RAID en degraded sur
le serveur File Server connecte (verifie a posteriori).

## ACTION (ce qui a ete fait)
1) Lancement d'un test SMART complet : disque OK
2) Mise a jour du driver storage Intel Rapid Storage
3) Reboot, observation 30 min : pas de BSOD
4) Communication client : surveillance 7 jours, devis disque
   en parallele en cas de recurrence

Temps : 1h25 (45 min telediag + 40 min telesupport)
Facturable : oui (hors contrat) / non (contrat Maintenance) - selon
Suite : ticket en attente cloture ; reverif J+7
```

# Annexe B - Scripts d'automatisation prets a l'emploi

## B.1 Inventaire d'un poste Windows (PowerShell)

```
# inventaire_poste.ps1
# Genere un rapport JSON de l'etat d'un poste

$Report = @{}
$Report.Date = (Get-Date).ToString('o')
$Report.Hostname = $env:COMPUTERNAME
$Report.Domain = (Get-WmiObject Win32_ComputerSystem).Domain
$Report.OS = (Get-WmiObject Win32_OperatingSystem | \
  Select Caption,Version,OSArchitecture,InstallDate,LastBootUpTime)
$Report.CPU = (Get-WmiObject Win32_Processor | Select Name,NumberOfCores)
$Report.RAM = [math]::Round((Get-CimInstance Win32_PhysicalMemory | \
  Measure-Object -Property Capacity -Sum).Sum / 1GB, 2)
$Report.Disks = Get-PhysicalDisk | Select FriendlyName,MediaType,HealthStatus,Size
$Report.Volumes = Get-Volume | Where DriveLetter | \
  Select DriveLetter,FileSystem,SizeRemaining,Size
$Report.Network = Get-NetIPAddress -AddressFamily IPv4 | \
  Where { $_.PrefixOrigin -ne 'WellKnown' } | Select InterfaceAlias,IPAddress
$Report.BitLocker = Get-BitLockerVolume | Select
MountPoint,VolumeStatus,EncryptionMethod
$Report.AV = Get-MpComputerStatus | Select
AntivirusEnabled,AntispywareEnabled,RealTimeProtectionEnabled
$Report.LastUpdate = Get-HotFix | Sort-Object InstalledOn -Descending | Select -First 5

$Report | ConvertTo-Json -Depth 5 | Out-File \
  "C:\Temp\inventaire_$($env:COMPUTERNAME)_$(Get-Date -Format 'yyyyMMdd').json"
```

## B.2 Audit Active Directory (PowerShell)

```
# audit_ad.ps1
# Inventaire AD : utilisateurs inactifs, comptes admin, GPO

Import-Module ActiveDirectory

# Comptes inactifs > 90 jours
$inactifs = Search-ADAccount -AccountInactive -TimeSpan (New-TimeSpan -Days 90) \
  -UsersOnly | Select Name,SamAccountName,LastLogonDate,Enabled
$inactifs | Export-Csv -NoTypeInformation 'C:\Temp\AD_inactifs.csv' -Encoding UTF8

# Membres groupes prive eleves
$grp = 'Domain Admins','Enterprise Admins','Schema Admins','Account Operators'
foreach ($g in $grp) {
    $m = Get-ADGroupMember $g | Select Name,SamAccountName,objectClass
    $m | Export-Csv -NoTypeInformation "C:\Temp\AD_groupe_$g.csv" -Encoding UTF8
}

# Mots de passe non expirables (alerte)
$nopwexp = Get-ADUser -Filter { PasswordNeverExpires -eq $true -and Enabled -eq $true } \
  | Select Name,SamAccountName
```

```
$nopwexp | Export-Csv -NoTypeInformation 'C:\Temp\AD_pwd_no_expire.csv' -Encoding UTF8

# Liste GPOs
Get-GPO -All | Select DisplayName,GpoStatus,CreationTime,ModificationTime | \
  Export-Csv -NoTypeInformation 'C:\Temp\AD_gpo_list.csv' -Encoding UTF8

# OU structure (premier niveau)
Get-ADOrganizationalUnit -Filter * | Select Name,DistinguishedName,Description | \
  Export-Csv -NoTypeInformation 'C:\Temp\AD_ou.csv' -Encoding UTF8
```

## B.3 Health-check serveur Linux (bash)

```
#!/bin/bash
# health_check.sh - Verifications de base
OUT=/tmp/health_$(hostname)_$(date +%Y%m%d_%H%M).txt

echo '== UPTIME ==' >> $OUT
uptime >> $OUT

echo '== DISK USAGE ==' >> $OUT
df -h | grep -vE 'tmpfs|udev' >> $OUT

echo '== MEMORY ==' >> $OUT
free -h >> $OUT

echo '== TOP 10 RAM ==' >> $OUT
ps aux --sort=-%mem | head -11 >> $OUT

echo '== TOP 10 CPU ==' >> $OUT
ps aux --sort=-%cpu | head -11 >> $OUT

echo '== FAILED SERVICES ==' >> $OUT
systemctl --failed --no-pager >> $OUT

echo '== LAST 30 LIGNES JOURNAL ==' >> $OUT
journalctl -p 3 -xb --no-pager | tail -30 >> $OUT

echo '== LISTENING PORTS ==' >> $OUT
ss -lntp >> $OUT

echo '== CONNEXIONS ETABLIES TOP 10 ==' >> $OUT
ss -tn | awk 'NR>1 {print $5}' | sed 's/:[^:]*$//' | sort | uniq -c | sort -rn | head

echo '== DISK SMART ==' >> $OUT
for d in /dev/sd? /dev/nvme?n1; do
  [ -e $d ] && smartctl -H $d | grep -i 'overall\|result' >> $OUT
done

echo '== UPDATES ATTENTE ==' >> $OUT
apt list --upgradable 2>/dev/null | wc -l | xargs -I{} echo '{} packages a mettre a jour' >> $OUT

# Envoi mail au technicien si anomalies
grep -E 'failed|FAIL|error' $OUT && \
  mail -s "Health check ALERT $(hostname)" support@jmlab.eu < $OUT
```

## B.4 Reset profil utilisateur Windows (PowerShell)

```
# reset_profil.ps1 - Migrer un profil utilisateur corrompu
param(
  [Parameter(Mandatory)][string]$User
)

$ProfilePath = "C:\Users\$User"
$BackupPath  = "C:\Users\${User}_backup_$(Get-Date -Format yyyyMMdd_HHmm)"

# Confirmer
Write-Host "Sauvegarde : $ProfilePath -> $BackupPath"
$go = Read-Host 'Confirmer (O/N) ?'
if ($go -ne 'O') { exit }

# Sauvegarder Documents, Desktop, Downloads, Pictures, Videos
Copy-Item "$ProfilePath\Documents" -Destination "$BackupPath\Documents" -Recurse
Copy-Item "$ProfilePath\Desktop" -Destination "$BackupPath\Desktop" -Recurse
Copy-Item "$ProfilePath\Downloads" -Destination "$BackupPath\Downloads" -Recurse
-ErrorAction SilentlyContinue

# Suppression du profil
# Ouvrir gpedit pour effacer la cle SID utilisateur
# (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\<SID>)

# Approche moderne : Remove-WmiObject win32_userprofile
Get-WmiObject Win32_UserProfile | Where { $_.LocalPath -eq "C:\Users\$User" } | \
  Remove-WmiObject

# Au prochain login, le profil sera recree. Restaurer les donnees apres login.
```

## B.5 Bash - rotation logs et alertes

```
#!/bin/bash
# clean_logs.sh - rotation manuelle si logrotate fait defaut

LOGS=( /var/log/syslog /var/log/auth.log /var/log/nginx/access.log /var/log/mail.log )
MAX=104857600   # 100 Mo

for L in "${LOGS[@]}"; do
  [ -f $L ] || continue
  SIZE=$(stat -c%s $L)
  if [ $SIZE -gt $MAX ]; then
    cp $L $L.$(date +%Y%m%d)
    > $L
    gzip $L.$(date +%Y%m%d)
    echo "Rotated $L" | logger -t jmsi
  fi
done

# Purge anciennes archives > 30 jours
find /var/log -name '*.gz' -mtime +30 -delete
```

# Annexe C - Plan d'adressage IP, plan VLAN et conventions de nommage

## C.1 Plan IP standard JMSI (par client)

JMSI applique un plan IP coherent par client : 10.X.Y.0/24 ou X est l'identifiant client (1 a 254) et Y est l'usage. Ce plan permet de standardiser l'integration multi-site et d'eviter les conflits VPN.

| Plage | Usage | Notes |
|---|---|---|
| **10.X.0.0/24** | Management equipements | Switch, AP, NAS, NVR, hyperviseurs |
| **10.X.10.0/24** | Production utilisateurs | Postes de travail, imprimantes |
| **10.X.20.0/24** | Voix (VoIP) | Postes IP, softphones |
| **10.X.30.0/24** | Servers internes | AD, FS, RDS, applicatifs |
| **10.X.50.0/24** | Wi-Fi invite | Isole de tout le LAN |
| **10.X.60.0/24** | IoT | Camera, capteurs, etc. (isole) |
| **10.X.70.0/24** | DMZ | Reverse proxy, services exposes |
| **10.X.99.0/24** | Surveillance | Cameras IP, NVR |

## C.2 Plan VLAN aligne

Memes ID de VLAN que le 3e octet de la plage IP (lisibilite).

- VLAN 1 : Management (10.X.0.0/24).
- VLAN 10 : Production (10.X.10.0/24).
- VLAN 20 : Voix (10.X.20.0/24).
- VLAN 30 : Servers (10.X.30.0/24).
- VLAN 50 : Guest (10.X.50.0/24).
- VLAN 60 : IoT (10.X.60.0/24).
- VLAN 70 : DMZ (10.X.70.0/24).
- VLAN 99 : Surveillance (10.X.99.0/24).

## C.3 Conventions de nommage

### C.3.1 Hostnames

```
# Format : <ROLE>-<INSTANCE>-<SITE>
# ROLE 3 lettres : DC, FS, RDS, APP, WEB, MAIL, NAS, NVR, FW, SW, AP
# INSTANCE 2 chiffres : 01, 02 (multi-site / multi-instance)
# SITE 3-4 lettres : SIE (siege), AGN (agence), DEP (depot)

# Exemples
```

```
DC-01-SIE.exemple.local
DC-02-SIE.exemple.local
FS-01-SIE.exemple.local
RDS-01-SIE.exemple.local
NAS-01-SIE
NVR-01-SIE
FW-01-SIE
SW-CORE-01-SIE
SW-ACC-01-SIE
AP-RDC-01-SIE
```

### C.3.2 Comptes AD

- Utilisateurs : <prenom>.<nom> (Jean.Dupont).
- Comptes de service : svc-<role>-<application> (svc-rmm-tactical).
- Comptes admin Tier 0 : adm0-<initiales> (adm0-jd).
- Comptes admin Tier 1 : adm1-<initiales> (adm1-jd).
- Comptes break-glass : bg-emergency-<NUMERO> (bg-emergency-01).

### C.3.3 Groupes de securite

- Format : SEC_<DEPARTEMENT>_<DROIT> (SEC_RH_LECTURE, SEC_DIRECTION_ECRITURE).
- Groupes d'application : APP_<NomApp>_<Role> (APP_DOLIBARR_USER, APP_DOLIBARR_ADMIN).
- Groupes globaux : GG_<usage>. Groupes de domaine local : DL_<usage>.

### C.3.4 Partages de fichiers

- Format : \\FS-01-SIE\<dept>$ (CIFS hidden share).
- Exemples : \\FS-01\COMPTA$, \\FS-01\COMMERCIAL$, \\FS-01\COMMUN$.
- Lecteurs reseau cote utilisateur via GPO :

```
# Lecteurs JMSI standard
# H: -> dossier perso utilisateur (\\FS-01\HOMES$\%username%)
# P: -> dossier publique commun a tous (\\FS-01\COMMUN$)
# Q: -> dossier departement (mappe par filtrage groupe)
# Z: -> archives / projets (lecture seule)
```

# Annexe D - Referentiel fournisseurs et contacts editeurs

## D.1 Distributeurs partenaires JMSI

| Categorie | Distributeur | Contact JMSI | Notes |
|---|---|---|---|
| **Materiel grand public et bureau** | TD Synnex (ex Tech Data) | Compte JMSI | Le plus large, livraison J+1 |
| **Materiel professionnel** | Ingram Micro | Compte JMSI | Bonnes conditions Lenovo, Dell, HP |
| **Reseau** | Wifirst (UniFi/Ubiquiti) | Compte JMSI | Direct constructeur |
| **Reconditionne pro** | Recommerce, Backmarket Pro | Compte JMSI | Garantie 12 mois |
| **Pieces detachees laptops** | Lapstore, eSupport.fr | Web | Batteries, claviers, ecrans |
| **Cables et VDI** | Conrad, RS Components | Compte JMSI | Cat 6A, fibre, accessoires baie |

## D.2 Editeurs strategiques

| Editeur | Produit | URL support | Modalite acces |
|---|---|---|---|
| **Microsoft** | Windows / Office / Azure | support.microsoft.com | Compte partenaire CSP via TD Synnex |
| **Bitdefender** | GravityZone / EDR | businessinsights.bitdefender.com | MSP partenaire JMSI |
| **Synology** | DSM / NAS / ABB | kb.synology.com | Compte revendeur |
| **Veeam** | Backup & Replication | veeam.com/services | VCSP MSP |
| **Stormshield** | NGFW / SMC | stormshield.com/support | Partenaire qualifie |
| **3CX** | PBX VoIP | 3cx.com/partner-portal | Partenaire Silver |
| **Yealink** | Postes IP / casques | support.yealink.com | Compte revendeur |
| **TP-Link Omada** | Wi-Fi / switch | community.tp-link.com | Compte JMSI |
| **Wasabi** | Stockage objet | wasabi.com/support | Compte direct + MSP rebadge |
| **Hikvision** | Videosurveillance | hikvision.com/europe/support | Partenaire installateur |
| **APC / Schneider** | Onduleurs | schneider-electric.com | Compte partenaire |

| | | | |
|---|---|---|---|
| **Bitwarden** | Gestion secrets | bitwarden.com/help | MSP |

## D.3 Sous-traitants speciaux

| Type | Partenaire JMSI | Cas d'usage |
|---|---|---|
| **Cablage VDI lourd** | Plombiers du reseau (sous-traitant) | Pre-cablage > 50 prises, fibre inter-batiment |
| **PC SOC telesurveillance** | Sensae / Securitas | Telesurveillance video et alarme 24/7 |
| **Recuperation de donnees** | Recoveo, Datacent | Disques defaillants salle blanche |
| **Pentest qualifie** | Synacktiv, Lexsi, Pradeo | Audits PASSI |
| **Destruction DEEE** | Ecologic, Ecosystem | Reprise DEEE professionnel |

# Annexe E - Glossaire technique

| Terme | Definition |
|---|---|
| **ACL** | Access Control List - regles d'acces granulaires. |
| **AD** | Active Directory - service d'annuaire Microsoft. |
| **AD DS** | Active Directory Domain Services - role serveur. |
| **AES-256** | Advanced Encryption Standard 256 bits - chiffrement symetrique. |
| **ANSSI** | Agence Nationale de la Securite des Systemes d'Information. |
| **APSAD** | Assemblee pleniere des societes d'assurances dommages - referentiels securite. |
| **ATP** | Advanced Threat Protection (Bitdefender) - analyse comportementale. |
| **Audit** | Verification documentee de la conformite a un referentiel. |
| **BCP** | Business Continuity Plan - plan de continuite d'activite. |
| **Bitlocker** | Chiffrement integral du disque sous Windows. |
| **BMR** | Bare Metal Recovery - restauration complete d'un OS. |
| **BLF** | Busy Lamp Field - voyant occupation telephone IP. |
| **BSOD** | Blue Screen Of Death - ecran bleu Windows. |
| **Borg / Borgmatic** | Outils de sauvegarde dedupliques. |
| **CBT** | Changed Block Tracking - sauvegarde incremental rapide hyperviseurs. |
| **Ceph** | Stockage distribue open source utilise par Proxmox. |
| **CDP** | Continuous Data Protection - sauvegarde continue. |
| **CGU** | Conditions Generales d'Utilisation. |
| **CNIL** | Commission Nationale Informatique et Libertes. |
| **CSP** | Cloud Solution Provider - revendeur Microsoft. |
| **CVE** | Common Vulnerabilities and Exposures - identifiant vulnerabilite. |
| **DC** | Domain Controller - controleur de domaine AD. |
| **DEEE / D3E** | Dechets d'Equipements Electriques et Electroniques. |
| **DFS** | Distributed File System - partages multi-serveurs. |
| **DKIM** | DomainKeys Identified Mail - signature mail. |
| **DMARC** | Domain-based Message Authentication, Reporting & |

| | |
|---|---|
| | Conformance. |
| **DPA** | Data Processing Agreement - article 28 RGPD. |
| **DSM** | DiskStation Manager - OS Synology. |
| **EDR** | Endpoint Detection and Response - antivirus avance. |
| **ESXi** | Hyperviseur VMware. |
| **FSRM** | File Server Resource Manager - quotas et screening Windows. |
| **GDPR / RGPD** | Reglement General sur la Protection des Donnees. |
| **GLPI** | Gestionnaire Libre de Parc Informatique - logiciel JMSI. |
| **GPO** | Group Policy Object - politique de groupe AD. |
| **GTI** | Garantie de Temps d'Intervention - JMSI 4h ouvres. |
| **GTR** | Garantie de Temps de Retablissement - JMSI 8h ouvres. |
| **HSTS** | HTTP Strict Transport Security - force HTTPS. |
| **Hyper-V** | Hyperviseur Microsoft (role Windows Server). |
| **HMAC** | Hash-based Message Authentication Code. |
| **IDS / IPS** | Intrusion Detection / Prevention System. |
| **Immuable** | Sauvegarde non modifiable, anti-ransomware. |
| **IRP** | Incident Response Plan. |
| **KVM** | Kernel-based Virtual Machine - hyperviseur Linux. |
| **LACP** | Link Aggregation Control Protocol - bonding 802.3ad. |
| **LDAP** | Lightweight Directory Access Protocol. |
| **LXC** | Linux Containers - containerisation systeme. |
| **MDM** | Mobile Device Management. |
| **MFA** | Multi-Factor Authentication. |
| **MTR** | Microsoft Teams Rooms. |
| **NAS** | Network Attached Storage. |
| **NGFW** | Next Generation Firewall. |
| **NIS2** | Network and Information Security 2 - directive UE 2022/2555. |
| **NPS** | Network Policy Server - serveur RADIUS Microsoft. |
| **NVR** | Network Video Recorder - enregistreur video reseau. |
| **OAuth** | Open Authorization - protocole delegation. |
| **OPNsense** | Pare-feu open source FreeBSD. |
| **OU** | Organizational Unit - conteneur AD. |

| | |
|---|---|
| **PAM** | Privileged Access Management. |
| **PCA** | Plan de Continuite d'Activite. |
| **PoE / PoE+** | Power over Ethernet (802.3af 15W / 802.3at 30W) / 802.3bt 60-90W. |
| **PRA** | Plan de Reprise d'Activite. |
| **Proxmox VE** | Hyperviseur open source Debian + KVM + LXC. |
| **RADIUS** | Remote Authentication Dial-In User Service. |
| **RAID** | Redundant Array of Independent Disks. |
| **RAS** | Rapport d'Activite Systeme - mensuel JMSI. |
| **RDP** | Remote Desktop Protocol. |
| **RDS** | Remote Desktop Services. |
| **RMM** | Remote Monitoring and Management - TacticalRMM. |
| **RPO** | Recovery Point Objective - perte de donnee maximale acceptable. |
| **RTO** | Recovery Time Objective - temps de reprise maximal acceptable. |
| **SAN** | Storage Area Network. |
| **SBC** | Session Border Controller (VoIP). |
| **SD-WAN** | Software-Defined WAN. |
| **SHR** | Synology Hybrid RAID. |
| **SIEM** | Security Information and Event Management. |
| **SLA** | Service Level Agreement. |
| **SMART** | Self-Monitoring, Analysis and Reporting Technology - sante disque. |
| **SOAR** | Security Orchestration, Automation and Response. |
| **SPF** | Sender Policy Framework - declaration mail. |
| **SVI / IVR** | Standard Vocal Interactif / Interactive Voice Response. |
| **TLS** | Transport Layer Security. |
| **TPM** | Trusted Platform Module. |
| **TOTP** | Time-based One-Time Password. |
| **UPS / Onduleur** | Uninterruptible Power Supply. |
| **VLAN** | Virtual LAN - segmentation reseau 802.1Q. |
| **VoIP** | Voice over IP. |
| **VPN** | Virtual Private Network. |
| **WAF** | Web Application Firewall. |

| | |
|---|---|
| **WAL** | Write-Ahead Logging - integrite BDD. |
| **Wasabi** | Fournisseur stockage objet S3-compatible. |
| **Windows Hello** | Authentification biometrique Windows. |
| **WireGuard** | VPN moderne base sur cryptographie elliptique. |
| **WORM** | Write Once Read Many - immutabilite. |
| **WPA3** | Wi-Fi Protected Access 3 - chiffrement Wi-Fi moderne. |
| **WSUS** | Windows Server Update Services. |
| **XDR** | Extended Detection and Response. |
| **ZTP** | Zero Touch Provisioning. |

# Annexe F - Index thematique

Index par mots-cles avec renvoi aux sections principales :

| Mot-cle | Reference |
|---|---|
| **3-2-1 (regle de sauvegarde)** | Chap. 4 sect. 4.2 |
| **Active Directory - promotion DC** | Chap. 9 sect. 9.8 |
| **Active Directory - GPO de base** | Chap. 9 sect. 9.8.3 |
| **Active Backup for Business (Synology)** | Chap. 4 sect. 4.3.3 |
| **Astreinte JMSI** | Chap. 1 sect. 1.7 |
| **Audit donnees critiques** | Chap. 4 sect. 4.10 |
| **Audit de parc (mise en service maintenance)** | Chap. 2 sect. 2.3.1 |
| **Audit de securite et pentest** | Chap. 5 sect. 5.8 |
| **Bare Metal Recovery (Veeam)** | Chap. 4 sect. 4.9.3 |
| **Bitdefender GravityZone** | Chap. 5 sect. 5.3 |
| **BitLocker - activation** | Chap. 9 sect. 9.2.3 |
| **Bitwarden - organisation JMSI** | Chap. 5 sect. 5.7 |
| **Bornes Wi-Fi Omada** | Chap. 7 sect. 7.4 |
| **Cablage Cat 6A** | Chap. 9 sect. 9.14 |
| **Cameras Hikvision - mise en service** | Chap. 8 sect. 8.5 |
| **Cle de recuperation BitLocker** | Chap. 9 sect. 9.2.3 |
| **CNIL et videosurveillance** | Chap. 8 sect. 8.3 |
| **Compte-rendu de ticket** | Chap. 1 sect. 1.4.4 + Annexe A.5 |
| **Conformite NIS2** | Chap. 5 sect. 5.9 |
| **Configuration NUT (onduleur Linux)** | Chap. 9 sect. 9.3.2 |
| **DKIM / SPF / DMARC** | Chap. 3 sect. 3.4.2 |
| **Dolibarr - mise en service** | Chap. 13 |
| **Dossier de base** | Chap. 1 sect. 1.2 |
| **Effacement securise SSD NVMe** | Chap. 14 sect. 14.3.2 |
| **Effacement securise HDD SATA** | Chap. 14 sect. 14.3.3 |
| **Filtrage web (NGFW)** | Chap. 5 sect. 5.4.4 |
| **FSRM - blocage ransomware** | Chap. 9 sect. 9.10.1 |
| **GLPI - workflow ticket** | Chap. 1 sect. 1.4.4 |
| **GTR / GTI** | Chap. 1 sect. 1.5 |

# PARTIE IX

# Complements techniques approfondis

# Complement 1 - Procedures de mise en service serveur (zoom)

## X1.1 Active Directory - structure JMSI standard 'Tier model'

JMSI applique le modele Tiering Microsoft adapte aux PME : separation des comptes administrateurs en 3 niveaux selon la criticite de l'asset administre. Cela protege contre le pass-the-hash et le credential theft.

| Tier | Asset administre | Comptes admin | Postes admin |
|---|---|---|---|
| **Tier 0** | Controleurs de domaine, Veeam server, Bitwarden, NGFW, hyperviseurs | adm0-<initiales> | PAW (Privileged Access Workstation) Tier 0 dedie - jamais Internet |
| **Tier 1** | Serveurs applicatifs, file servers, RDS, Exchange/Mailcow | adm1-<initiales> | PAW Tier 1 ou jump server |
| **Tier 2** | Postes utilisateurs, imprimantes, telephones IP | adm2-<initiales> | Poste IT classique |
| **Tier U** | Utilisateurs finaux | <prenom>.<nom> | Poste standard |

**ATTENTION** Un compte adm0 ne doit JAMAIS se connecter sur un poste Tier 1 ou 2. Sinon le hash NTLM ou le ticket Kerberos peut etre vole, et l'AD entier compromis.

### X1.1.1 OUs JMSI standard

```
# Structure d'OUs deployee par script JMSI sur tout AD greenfield

DC=exemple,DC=local
 +-- OU=Tier-0
 |    +-- OU=Admin-Accounts (comptes adm0)
 |    +-- OU=Service-Accounts (svc-* tier 0)
 |    +-- OU=Privileged-Workstations (PAW)
 |    +-- OU=Domain-Controllers (default GPO)
 |
 +-- OU=Tier-1
 |    +-- OU=Admin-Accounts (comptes adm1)
 |    +-- OU=Service-Accounts
 |    +-- OU=Servers
 |         +-- OU=Servers-FS
 |         +-- OU=Servers-APP
 |         +-- OU=Servers-RDS
 |
 +-- OU=Tier-2
 |    +-- OU=Admin-Accounts (comptes adm2)
 |    +-- OU=Workstations
 |    +-- OU=Printers
```

```
|    +-- OU=Mobile-Devices
|
+-- OU=Tier-U
|    +-- OU=Users
|        +-- OU=Direction
|        +-- OU=Compta
|        +-- OU=Commercial
|        +-- OU=Production
|    +-- OU=Groups
|        +-- OU=Security-Groups
|        +-- OU=Distribution-Lists
|
+-- OU=Disabled (objets desactives, retention 1 an avant suppression)
+-- OU=Quarantine (comptes compromis ou suspects)
```

### X1.1.2 Politique de mot de passe Fine-Grained (PSO)

```
# 3 PSO JMSI (PowerShell)

# PSO Tier 0 (admins) - 25 chars min, complexite max, expiration 60 jours
New-ADFineGrainedPasswordPolicy -Name 'PSO-Tier-0' \
   -Precedence 10 -ComplexityEnabled $true \
   -MinPasswordLength 25 -PasswordHistoryCount 24 \
   -MaxPasswordAge (New-TimeSpan -Days 60) \
   -MinPasswordAge (New-TimeSpan -Days 1) \
   -LockoutThreshold 3 -LockoutObservationWindow (New-TimeSpan -Minutes 30) \
   -LockoutDuration (New-TimeSpan -Hours 1) \
   -ReversibleEncryptionEnabled $false

Add-ADFineGrainedPasswordPolicySubject -Identity 'PSO-Tier-0' \
   -Subjects 'Domain Admins','Enterprise Admins','Schema Admins'

# PSO Tier 1 - 18 chars min, expiration 90 jours
New-ADFineGrainedPasswordPolicy -Name 'PSO-Tier-1' \
   -Precedence 20 -ComplexityEnabled $true \
   -MinPasswordLength 18 -PasswordHistoryCount 12 \
   -MaxPasswordAge (New-TimeSpan -Days 90) \
   -LockoutThreshold 5

# PSO Utilisateurs standard - 12 chars, 365 jours (NIST recent)
New-ADFineGrainedPasswordPolicy -Name 'PSO-Users' \
   -Precedence 100 -ComplexityEnabled $true \
   -MinPasswordLength 12 -PasswordHistoryCount 6 \
   -MaxPasswordAge (New-TimeSpan -Days 365) \
   -LockoutThreshold 10
```

## X1.2 Mise en service complete d'un serveur RDS (5 jours)

Procedure complete cas typique : 1 broker + 2 session hosts + 1 gateway, environ 30 utilisateurs concurrents sur applications metier. RDS CAL utilisateurs (preferable a CAL device pour les TPE/PME multi-poste).

### X1.2.1 Topologie cible

```
# 4 VM Windows Server 2022 Standard

VM 1 : RDCB-01 (Connection Broker)
```

```
      2 vCPU, 4 Go RAM, 80 Go SSD
      Roles : RDS-Connection-Broker + RDS-Licensing

VM 2 : RDSH-01 (Session Host)
      8 vCPU, 32 Go RAM, 200 Go SSD
      Role : RDS-RD-Server

VM 3 : RDSH-02 (Session Host - copy of RDSH-01)
      8 vCPU, 32 Go RAM, 200 Go SSD

VM 4 : RDGW-01 (Gateway + Web Access, expose Internet via firewall)
      4 vCPU, 8 Go RAM, 80 Go SSD
      Roles : RDS-Gateway + RDS-Web-Access

+ FSLogix profile container : VHDX prive utilisateur sur File Server
+ Office 365 Apps avec mode Shared Computer Activation
+ Stockage profils : \\FS-01-SIE\FSLogix$\%username%\
+ Sauvegarde des VHDX FSLogix : Veeam File Backup hourly
```

### X1.2.2 Sequence detaillee de deploiement

439. J0 - Provisionner les 4 VM (template Windows Server 2022 + sysprep) - 2h.
440. J0 - Joindre au domaine, redemarrer, mettre a jour Windows - 2h.
441. J1 matin - Installer les roles via PowerShell (cf. ci-dessous).
442. J1 apres-midi - Configurer le deploiement RDS, lier au Broker.
443. J2 - Installer les applications metier sur RDSH-01, sysprep, image, deployer sur RDSH-02.
444. J3 - Configurer FSLogix, tester profils.
445. J3 - Configurer la Gateway : certificat TLS Let's Encrypt, RAP/CAP.
446. J4 matin - Configurer MFA cote Gateway via NPS + Duo (ou Azure MFA NPS Extension).
447. J4 apres-midi - Tests de bout en bout : login Internet, lancement applications, deconnexion propre.
448. J5 - Formation utilisateurs : 1h en groupe + cheat sheet.
449. J5 - PV de mise en service.

### X1.2.3 Script PowerShell : installation roles RDS

```
# A executer sur RDCB-01 en admin du domaine (compte adm1-jmsi)

$broker = 'RDCB-01.exemple.local'
$shost1 = 'RDSH-01.exemple.local'
$shost2 = 'RDSH-02.exemple.local'
$gateway = 'RDGW-01.exemple.local'

# 1) Installer les roles sur les hosts cibles
Invoke-Command -ComputerName $broker  -ScriptBlock { Install-WindowsFeature RDS-
Connection-Broker,RDS-Licensing -IncludeManagementTools }
Invoke-Command -ComputerName $shost1  -ScriptBlock { Install-WindowsFeature RDS-RD-
Server -IncludeManagementTools }
Invoke-Command -ComputerName $shost2  -ScriptBlock { Install-WindowsFeature RDS-RD-
Server -IncludeManagementTools }
Invoke-Command -ComputerName $gateway -ScriptBlock { Install-WindowsFeature RDS-
Gateway,RDS-Web-Access,Web-Server -IncludeManagementTools }

# 2) Creer le deploiement RDS
New-RDSessionDeployment -ConnectionBroker $broker `
   -SessionHost $shost1,$shost2 `
```

```
    -WebAccessServer $gateway

# 3) Ajouter Licensing et Gateway au deploiement
Add-RDServer -Server $broker -Role 'RDS-LICENSING' -ConnectionBroker $broker
Set-RDLicenseConfiguration -LicenseServer $broker -Mode PerUser -ConnectionBroker $broker
-Force

Add-RDServer -Server $gateway -Role 'RDS-GATEWAY' -ConnectionBroker $broker `
    -GatewayExternalFqdn 'rds.exemple.fr'

# 4) Creer la collection (1 collection partagee Office)
New-RDSessionCollection -CollectionName 'COL-Office' `
    -SessionHost $shost1,$shost2 `
    -CollectionDescription 'Bureautique partagee Office 365' `
    -ConnectionBroker $broker

# 5) Publier RemoteApp ou Full Desktop
# Pour Full Desktop : pas d'action specifique, deja accessible
# Pour RemoteApp : ajouter chaque app
New-RDRemoteApp -Alias 'Outlook' -DisplayName 'Outlook' `
    -FilePath 'C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE' `
    -CollectionName 'COL-Office' -ConnectionBroker $broker

# 6) Ajustement parametres collection - charge moyenne
Set-RDSessionCollectionConfiguration -CollectionName 'COL-Office' `
    -DisconnectedSessionLimitMin 60 -IdleSessionLimitMin 30 `
    -ActiveSessionLimitMin 720 `
    -ConnectionBroker $broker

# 7) Activer FSLogix
# (telecharger MSI Microsoft FSLogix Apps)
# Installer sur les Session Hosts
# GPO Computer > Admin Templates > FSLogix > Profile Containers :
# - Enabled = 1
# - VHD Locations = \\FS-01-SIE\FSLogix$\%username%
# - Volume Type = VHDX
# - Size in MBs = 30000
# - Delete Local Profile When VHD Should Apply = 1
```

## X1.3 Hyper-V replication entre 2 sites

Pour les clients multi-site avec besoin de PCA (sans cluster complet) : Hyper-V Replica asynchrone entre 2 hyperviseurs. RPO atteignable 30 secondes a 15 minutes selon configuration. C'est une solution PRA legere mais efficace.

```
# Cote source (HYPERV-SIE) et destination (HYPERV-AGN) - admin tier 0

# 1) Activer Hyper-V Replica Broker (cluster) ou direct (standalone)
# - Sur destination : autoriser la replication entrante
Set-VMReplicationServer -ReplicationEnabled $true `
    -AllowedAuthenticationType Kerberos `
    -ReplicationAllowedFromAnyServer $false

# Autoriser server source
New-VMReplicationAuthorizationEntry `
    -AllowedPrimaryServer 'HYPERV-SIE.exemple.local' `
    -ReplicaStorageLocation 'D:\Replicas' `
    -TrustGroup 'JMSI-Replica'
```

```
# 2) Cote source : enable replication d'une VM critique
Enable-VMReplication -VMName 'srv-app01' `
   -ReplicaServerName 'HYPERV-AGN.exemple.local' `
   -ReplicaServerPort 80 `
   -AuthenticationType Kerberos `
   -CompressionEnabled $true `
   -ReplicationFrequencySec 30        # 30s ou 300s ou 900s

# 3) Initial replication (peut prendre des heures pour grandes VM)
Start-VMInitialReplication -VMName 'srv-app01'

# 4) Verification
Get-VMReplication -VMName 'srv-app01'
Measure-VMReplication -VMName 'srv-app01'

# 5) Test failover (sur destination)
# Cree une VM test deconnectee a partir du replica - non destructif
Start-VMFailover -VMName 'srv-app01' -AsTest

# 6) Failover reel (sinistre site source)
Stop-VMFailoverTest -VMName 'srv-app01'
Start-VMFailover -VMName 'srv-app01' -Confirm:$false
# La VM repart sur le site secondaire - changer DNS / firewall pour rediriger trafic

# 7) Reverse replication apres reconstruction site source
Set-VMReplication -VMName 'srv-app01' -Reverse
```

# Complement 2 - Reseau avance et SD-WAN multi-site

## X2.1 OPNsense - configuration multi-WAN avec failover

Configuration type pour client avec une fibre principale + une 4G/5G de secours.

```
# OPNsense - menu Interfaces > Assignments
# WAN1 = igc0 (fibre principale)
# WAN2 = igc1 (4G/5G via routeur Teltonika RUT240 ou similaire)

# 1) Configurer chaque interface WAN avec sa passerelle
# Interfaces > [WAN1] > IPv4 Configuration Type : DHCP ou Static
# Interfaces > [WAN2] > IPv4 Configuration Type : DHCP

# 2) Creer les Gateway Monitors
# System > Gateways > Single
# WAN1_GW : monitor IP 1.1.1.1, latency low 100ms / high 200ms
# WAN2_GW : monitor IP 8.8.8.8, latency low 200ms / high 500ms

# 3) Creer un Gateway Group avec failover
# System > Gateways > Group
# Name : WAN_FAILOVER
# Gateways : WAN1_GW (Tier 1), WAN2_GW (Tier 2)
# Trigger Level : Member Down (basculer si WAN1 perdu)

# 4) Regler les regles firewall sortantes WAN
# Firewall > Rules > LAN
# Default rule : Source = LAN net, Gateway = WAN_FAILOVER (au lieu de default)

# 5) NAT outbound
# Firewall > NAT > Outbound : 'Hybrid' mode
# Auto rules : present / Custom rules :
#   src LAN net -> WAN1 (priorite)
#   src LAN net -> WAN2 (failover)

# 6) DNS hijack pour eviter cache obsoletes pendant failover
# Services > Unbound DNS : forwarder mode, cache TTL min reduit
# OU configurer chaque LAN client avec 1.1.1.1 + 9.9.9.9

# 7) Tests :
# - Debrancher fibre principale
# - Verifier qu'un ping continu vers 1.1.1.1 redemarre apres ~5s
# - Verifier que WAN_FAILOVER passe a WAN2 dans Dashboard
```

## X2.2 Tunnel WireGuard inter-sites (3 sites)

```
# Topologie hub-and-spoke : Siege = hub, agences = spokes

# Cote SIEGE (10.10.0.0/16, OPNsense)
# /usr/local/etc/wireguard/wg-mesh.conf

[Interface]
```

```
PrivateKey = <SIEGE_PRIVATE>
Address    = 10.99.0.1/24
ListenPort = 51820
PostUp     = iptables -A FORWARD -i %i -j ACCEPT; iptables -t nat -A POSTROUTING -o igc0 -j
MASQUERADE

# Spoke 1 - AGN-LYON (10.20.0.0/16)
[Peer]
PublicKey  = <LYON_PUB>
AllowedIPs = 10.99.0.10/32, 10.20.0.0/16
PersistentKeepalive = 25

# Spoke 2 - AGN-BOR (10.30.0.0/16)
[Peer]
PublicKey  = <BOR_PUB>
AllowedIPs = 10.99.0.20/32, 10.30.0.0/16
PersistentKeepalive = 25

# Cote LYON (spoke)
[Interface]
PrivateKey = <LYON_PRIVATE>
Address    = 10.99.0.10/24

[Peer]
PublicKey  = <SIEGE_PUB>
Endpoint   = siege.exemple.fr:51820
AllowedIPs = 10.99.0.0/24, 10.10.0.0/16, 10.30.0.0/16
PersistentKeepalive = 25

# Test depuis LYON :
# ping 10.10.0.1   (siege gateway)
# ping 10.30.0.1   (BOR via siege)
```

## X2.3 QoS avancee - reservation voix et visioconference

```
# OPNsense - Traffic Shaper (pf shaper, IPFW pipes)

# Pipe 1 - Voix (priorite 1)
# Bandwidth : 30 % du WAN1 reserve
# Match : DSCP=EF OR DSCP=AF41 OR (UDP src/dst 10000-20000)

# Pipe 2 - Visioconf (priorite 2)
# Bandwidth : 30 % du WAN1 reserve
# Match : DSCP=AF41 OR (TCP/UDP dst 80,443 dst-host *.zoom.us,*.teams.microsoft.com)

# Pipe 3 - Bureautique standard (priorite 3)
# Bandwidth : 30 % minimum, jusqu'a 100 % si pipes 1+2 inactifs
# Match : tout autre

# Pipe 4 - Saturation potentielle (priorite 4)
# Bandwidth : 10 % maximum si pipes 1+2+3 sollicites
# Match : telechargement (Steam, OneDrive sync, Windows Update large)

# Activation
# Firewall > Shaper > Pipes : creer les 4 pipes ci-dessus
# Firewall > Shaper > Queues : creer 4 queues correspondantes
# Firewall > Shaper > Rules : matcher les flux selon DSCP/port/host
```

# Complement 3 - Securite operationnelle approfondie

## X3.1 PingCastle - audit AD trimestriel

PingCastle est l'outil de reference pour l'audit AD. Score < 30 cible JMSI.

```
# Telechargement PingCastle - https://www.pingcastle.com/download/
# Decompresser sur PAW Tier 0 (jamais sur poste utilisateur)

# Audit par le compte adm0 - mode standard
PingCastle.exe --healthcheck --server exemple.local --user adm0-jmsi

# Output : ad_hc_exemple.local.html (rapport HTML)

# Pour aller plus loin : module Carto (cartographie graphique des relations)
PingCastle.exe --carto

# Module ScanWeak - mots de passe faibles AD via attaque dictionnaire offline
PingCastle.exe --scanner password --scmode-file commonpasswords.txt

# Verification specifique : KRBTGT password rotation
PingCastle.exe --scanner krbtgt

# Stocker le rapport dans /clients/<CODE>/06_securite/<DATE>_pingcastle.html
```

## X3.2 Bloodhound - detection chemins d'attaque

```
# Bloodhound + SharpHound - JMSI utilise pour audit prospect ou demarrage contrat

# Sur poste audit (Tier 0 ou bench JMSI)
# 1) Telecharger SharpHound (collecteur)
#    https://github.com/BloodHoundAD/BloodHound/releases

# 2) Lancer la collecte (depuis un compte Domain User)
SharpHound.exe -c All --domain exemple.local --zipfilename collect.zip
# Methodes : Default, ACL, Group, Trusts, GPOLocalGroup, LoggedOn, Session, ObjectProps

# 3) Importer dans Bloodhound CE (Community Edition)
# Lancer le serveur Bloodhound (Docker)
docker run -d -p 8080:8080 specterops/bloodhound
# Acceder a localhost:8080, importer collect.zip

# 4) Queries d'interet :
# - 'Find Shortest Paths to Domain Admins'
# - 'Find Computers with Unconstrained Delegation'
# - 'Find Kerberoastable Users'
# - 'Find AS-REP Roastable Users'
# - 'Find DCSync Privileges'

# 5) Remediations typiques :
# - Retirer les comptes user des groupes admin
# - Definir 'sensitive and cannot be delegated' pour les comptes high-value
```

```
# - Forcer 'Smart card required' pour les comptes admin
# - Mettre 'Account is sensitive' sur les comptes Domain Admins
```

## X3.3 Politique de patching avancee

| Categorie patch | Test lab | Wave 1 (10 % parc) | Wave 2 (90 % parc) | Audit final |
|---|---|---|---|---|
| **Securite Microsoft Patch Tuesday** | J+0 a J+3 | J+4 a J+7 | J+8 a J+10 | J+11 |
| **CVE en exploitation active (CISA KEV)** | J+0 (max 2h) | J+0 (max 6h) | J+1 | J+2 |
| **Cumulative Updates Windows** | J+0 a J+5 | J+6 a J+10 | J+11 a J+15 | J+16 |
| **Drivers BIOS / firmware** | J+0 a J+15 | J+15 a J+25 | J+25 a J+35 | J+40 |
| **Applicatif metier (ERP, CRM)** | Selon planning client | Selon planning client | Selon planning client | Selon planning client |
| **Hyperviseur (Hyper-V/Proxmox/ ESXi)** | J+0 a J+30 | J+30 a J+45 | J+45 a J+60 | J+65 (test PRA) |
| **Pare-feu / NGFW** | J+0 a J+15 | J+15 a J+25 | J+25 a J+35 | J+40 |

## X3.4 Procedure CVE en exploitation active

Procedure d'urgence quand une CVE critique est ajoutee a la liste CISA KEV (Known Exploited Vulnerabilities).

450. [T+0] Detection : alerte mailing list ANSSI/CERT-FR/CISA KEV.
451. [T+0:30] Direction technique JMSI : revue de la CVE - applicabilite parc clients.
452. [T+1h] Identification des clients impactes (TacticalRMM : query par version logicielle).
453. [T+2h] Mise en place du patch sur lab JMSI - test stabilite.
454. [T+4h] Communication clients impactes (mail + telephone P1).
455. [T+6h] Patch automatise sur le parc client (TacticalRMM script global).
456. [T+12h] Verification post-patch sur l'ensemble du parc.
457. [T+24h] RAS exceptionnel envoye aux clients : description CVE + patch applique.

## X3.5 Yubikey FIDO2 - deploiement entreprise

Cas Pack Pro avec demande hardware key. Deploiement Yubikey 5 NFC.

- Achat : 50 EUR HT par Yubikey 5 NFC (Bouquetin / Fnac Pro).
- Deploiement Microsoft Entra ID : Activer FIDO2 dans les politiques d'authentification.
- Inscription utilisateur : aka.ms/mysecurityinfo > Add FIDO2 security key.
- Tester avec un service support FIDO2 : Microsoft 365, Google Workspace, GitHub, AWS.

- Procedure de perte : revocation immediate de la cle, reset MFA, expedition cle de remplacement sous 24h.
- Bonne pratique : 2 cles par utilisateur (1 portee, 1 stockee).

# X3.6 EDR - cas pratiques de reponse

## X3.6.1 Phishing detecte par Bitdefender

458. Alerte : 'Suspicious URL clicked' dans la console.
459. Verifier le poste : etat de l'utilisateur (a clique ?), processus enfants suspectes.
460. Si suspicion d'execution de macro malveillante : isoler le poste (action Console).
461. Reset des mots de passe utilisateur (mail, AD, applications metier).
462. Revue des derniers acces : Microsoft 365 sign-in logs, AD security logs.
463. Communication : utilisateur informe + bonne pratique pour le futur.
464. Suivi 14 jours.

## X3.6.2 Lateral movement detecte

465. Alerte EDR sur un poste + alerte sur un serveur quasi-simultanees.
466. DECLAREMENT INCIDENT P1 - alerte Direction technique.
467. Isoler les deux machines.
468. Capture forensique avant tout reformatage : disque + memoire (FTK Imager / Belkasoft).
469. Analyse - identifier le compte compromis (souvent admin local re-utilise).
470. Reset MASSIF des mots de passe : tier 0 d'abord, puis 1, puis 2, puis utilisateurs.
471. Revue complete des comptes admin actifs et derniers usages.
472. Reconstruction des machines isolees (formatage + reinstallation depuis master).
473. Audit AD complet (PingCastle, Bloodhound, comptes admin) post-incident.
474. Retex 7 jours apres : timeline, root cause, mesures correctives.

# Complement 4 - Microsoft 365 et Azure pour les clients JMSI

## X4.1 Tenant Microsoft 365 - configuration JMSI standard

JMSI est partenaire CSP Microsoft (via TD Synnex). Pour chaque client : creation tenant ou rattachement existant, configuration des baselines de securite recommandees.

### X4.1.1 Politiques d'acces conditionnel - baseline JMSI

| Politique | Cible | Conditions | Actions |
|---|---|---|---|
| **CA01 - MFA pour tous** | All users (sauf comptes break-glass) | Tous les apps | MFA obligatoire |
| **CA02 - Block legacy auth** | All users | Client apps : Exchange ActiveSync legacy, IMAP, POP, SMTP basic | Block |
| **CA03 - MFA admins** | Tous les roles administrateurs | Tous les apps | MFA + Sign-in frequency 4h |
| **CA04 - Geo restriction** | All users | Pays autres que FR / UE | Block ou MFA strong |
| **CA05 - Risk-based** | All users | Sign-in risk = Medium ou High | Block / require MFA |
| **CA06 - Compliant device** | Tous les apps sensibles (Microsoft 365 admin) | Device non-Intune compliant | Block |
| **CA07 - Break-glass** | Comptes bg-emergency-* | Tous les apps | EXCLUSION (acces direct sans MFA pour secours) |

### X4.1.2 PowerShell - configuration baseline

```
# Connexion Microsoft Graph PowerShell
Install-Module Microsoft.Graph -Scope CurrentUser
Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess','Application.ReadWrite.All'

# Verifier les politiques actives
Get-MgIdentityConditionalAccessPolicy | Select Id,DisplayName,State

# Creer une politique 'Block legacy auth'
$params = @{
   displayName = 'CA02 - Block legacy authentication'
   state = 'enabled'
   conditions = @{
      users = @{
         includeUsers = @('All')
         excludeGroups = @('<GUID groupe break-glass>')
      }
```

```
        applications = @{ includeApplications = @('All') }
        clientAppTypes = @('exchangeActiveSync','other')
    }
    grantControls = @{
        operator = 'OR'
        builtInControls = @('block')
    }
}
New-MgIdentityConditionalAccessPolicy -BodyParameter $params

# Activer Security Defaults SI politiques personnalisees pas pretes
Update-MgPolicyIdentitySecurityDefaultEnforcementPolicy -IsEnabled $true
```

# X4.2 Microsoft Intune - mobile management

Pour les clients Pack Pro avec parc mobile (smartphones professionnels), Intune permet le MDM/MAM.

- Microsoft Intune Plan 1 inclus dans Microsoft 365 Business Premium.
- Compliance Policy : code PIN 6 chiffres, chiffrement, anti-rooting.
- Configuration Profile : Wi-Fi entreprise, VPN auto, certificats.
- App Protection Policy : restreindre copy/paste hors apps gerees, effacement selectif a la sortie utilisateur.
- Compliant device requirement dans CA06 (politique d'acces conditionnel).

# X4.3 Sauvegarde Microsoft 365 - Veeam Backup for Microsoft 365

## X4.3.1 Architecture

- VM Veeam Backup for M365 (peut etre la meme que Veeam B&R).
- Acces consenti via OAuth (Azure App Registration).
- Repository : disque local OU object storage (Wasabi / Azure Blob immuable).
- Sauvegarde : Exchange Online (boites + dossiers public), SharePoint, OneDrive, Teams.

## X4.3.2 Procedure de mise en service

475. Installer Veeam Backup for M365 v8 (compatibilite Veeam B&R).
476. Cote Azure : creer une App Registration 'JMSI-Veeam-Backup' avec permissions Graph (full backup).
477. Generer un secret OAuth + accord administrateur tenant.
478. Cote Veeam Backup for M365 : Add Organization > Modern app authentication > coller App ID + secret.
479. Selectionner les utilisateurs / sites a sauvegarder (organisation entiere par defaut).
480. Creer le job de sauvegarde : quotidien 22h.
481. Configurer Object Lock cote stockage S3 immuable (anti-ransomware).
482. Test de restauration : 1 boite mail, 1 dossier OneDrive, 1 site SharePoint, 1 canal Teams.

# Complement 5 - Devops infra JMSI (gestion de configuration)

## X5.1 Ansible - automatisation des deploiements client

JMSI utilise Ansible pour automatiser les configurations recurrentes (Linux et reseau principalement). Inventaire dynamique generes depuis Dolibarr / GLPI.

### X5.1.1 Structure d'un repository JMSI

```
jmsi-ansible/
  ansible.cfg
  inventories/
    production/
      hosts.yml
      group_vars/
        all.yml
        clients/<CODE>.yml      # variables par client
  playbooks/
    bootstrap.yml             # premiere config Linux JMSI standard
    upgrade.yml               # mise a jour systeme
    backup_setup.yml            # deploiement Borg/Kopia/Veeam agent
    monitoring.yml             # installer agent Zabbix
    hardening.yml              # CIS-like hardening
  roles/
    common/
    nginx/
    nextcloud/
    dolibarr/
    mailcow/
  README.md
```

### X5.1.2 Exemple : deploiement standard Debian

```
---
# playbooks/bootstrap.yml
- hosts: linux
  become: true
  tasks:
    - name: Mise a jour des paquets
      apt:
        update_cache: true
        upgrade: dist
    - name: Installer paquets de base JMSI
      apt:
        name:
          - vim
          - htop
          - curl
          - unzip
          - tmux
          - ufw
          - fail2ban
```

```
        - auditd
        - rsyslog
        - chrony
        - unattended-upgrades
      state: present
  - name: Configurer le timezone
    timezone:
      name: Europe/Paris
  - name: Configurer le firewall UFW
    community.general.ufw:
      rule: allow
      port: '22'
      from_ip: '{{ jmsi_management_subnet }}'
  - name: Configurer fail2ban SSH
    copy:
      src: jail.local
      dest: /etc/fail2ban/jail.local
    notify: restart fail2ban
  - name: Activer mises a jour securite auto
    copy:
      content: |
        APT::Periodic::Update-Package-Lists "1";
        APT::Periodic::Unattended-Upgrade "1";
      dest: /etc/apt/apt.conf.d/20auto-upgrades
  - name: Deployer cle SSH JMSI tech
    authorized_key:
      user: root
      key: '{{ jmsi_pubkey }}'
      state: present
handlers:
  - name: restart fail2ban
    service:
      name: fail2ban
      state: restarted
```

## X5.2 Backup avec Borg + Borgmatic (Linux serveurs)

```
# /etc/borgmatic/config.yaml

location:
    source_directories:
        - /etc
        - /home
        - /var/www
        - /var/lib/mysql
        - /opt/<app>

    repositories:
        # Local repo (1ere copie)
        - path: /backup/borg
          label: local
        # Wasabi repo via SSH backend (2eme copie hors-site)
        - path: ssh://u<ID>@<HOST>/./repo
          label: wasabi

    exclude_patterns:
        - '*.tmp'
        - '/var/cache'
```

```
        - '/var/tmp'

storage:
    encryption_passphrase: '<PASSPHRASE_BITWARDEN>'
    compression: zstd,5
    archive_name_format: '{hostname}-{now:%Y%m%dT%H%M%S}'

retention:
    keep_hourly: 24
    keep_daily: 30
    keep_weekly: 12
    keep_monthly: 12
    keep_yearly: 7

consistency:
    checks:
        - name: archives
          frequency: 4 weeks

hooks:
    on_error:
        - echo 'Backup ERROR on {hostname}' | mail -s 'Borg ERROR' soc@jmlab.eu
    after_backup:
        - logger -t jmsi-borg 'Backup OK'

# Test
borgmatic --verbosity 1 list
borgmatic --verbosity 1 info

# Planification systemd timer
# /etc/systemd/system/borgmatic.service deja fourni
# /etc/systemd/system/borgmatic.timer : OnCalendar=*-*-* 02:00
systemctl enable --now borgmatic.timer
```

# Complement 6 - Tableaux de depannage detailles

## X6.1 Pannes Active Directory

| Symptome | Cause possible | Diagnostic | Resolution |
|---|---|---|---|
| **Replication AD en erreur** | Pare-feu, DNS, double NIC | repadmin /replsummary, /showrepl | Ouvrir RPC dyn, fixer reverse DNS |
| **Logon utilisateur lent (> 60s)** | Profil itinerant gros, GPO trop nombreuses | gpresult /h, RSoP | Migrer vers FSLogix, audit GPO |
| **FRS / DFS-R replication SYSVOL** | Service arrete, disque saturé | dfsrdiag pollAD, check repadmin | Reset NTFRS / DFS-R selon edition |
| **Mots de passe ne se synchronisent pas** | Tombstone expired, replication broken | ntdsutil 'metadata cleanup' | Force sync, supprimer DC obsolete |
| **Comptes verrouilles repetes** | App qui boucle avec ancien mdp | Event 4740, find source | Trouver l'app, mettre a jour cred |
| **Strange GPO behavior** | GPO bloquees par WMI filter | gpresult, gpupdate /force | Verifier filter, refuser inheritance |
| **DCDIAG erreur 'sysvol shared'** | Demarrage de service, droits | Event 13568 (NTFRS) | Force authoritative restore SYSVOL |

## X6.2 Pannes Hyper-V

| Symptome | Cause possible | Resolution |
|---|---|---|
| **VM ne demarre pas (BSOD)** | Snapshot de checkpoint corrompu, RAM | Supprimer checkpoints, allouer plus de RAM |
| **Migration en echec** | RDMA, Kerberos, SPN | setspn -A Microsoft Virtual System Migration Service ... |
| **VM lente apres clone** | Cache disque, paging | Configurer memory dynamic, disable paging |
| **Live Migration KO** | Pas de cluster, pas Kerberos | Configurer VMM > Authentication = Kerberos, joindre cluster |
| **VM Linux ne boot pas (Gen 2)** | Secure Boot template Microsoft pas active | Set-VMFirmware -SecureBootTemplate MicrosoftUEFICertificateAuthority |
| **Disque virtuel grossit indefiniment** | Pas de TRIM/UNMAP | Optimize-VHD, Defrag dans VM, Compact |

| | | |
|---|---|---|
| **Reseau VM lent** | VMQ, RSS mal configures | Disable-NetAdapterVmq, Set-VMNetworkAdapter -VrssEnabled $true |

## X6.3 Pannes Mailcow / Mail

| Symptome | Cause possible | Resolution |
|---|---|---|
| **Mail rejete par Gmail** | DKIM/SPF/DMARC, blacklist | Verifier dig, mxtoolbox, demande delisting |
| **Boite a 100 % quota** | Pas d'archivage | Augmenter quota, archivage, suppression |
| **Webmail lent** | DB MariaDB pleine, Redis HS | Optimize tables, redis ping, restart |
| **Mail entrant pas livre** | Greylist, fitre, espace disque | logs Postfix, verifier disque |
| **Client Outlook ne se connecte pas** | Autodiscover, MFA, mot de passe | Verifier autodiscover.* DNS, app password si MFA |
| **Spam volumineux dans Junk** | Rspamd policy stricte | Reduire seuil, whitelist IP/domaine |
| **Sortie mail bloquee chez l'operateur** | Port 25 bloque | Utiliser smarthost partenaire (587) |

## X6.4 Pannes Veeam

| Erreur Veeam | Signification | Resolution |
|---|---|---|
| **Failed to connect to host** | Hyperviseur deconnecte | Reconnecter dans Inventory, verifier credentials |
| **VSS writer failed** | Service VSS bloque | vssadmin list writers, redemarrer COM+ |
| **Backup file is corrupted** | Coupure pendant ecriture, repository | Repair file (Veeam validator), recreer chain |
| **Snapshot consolidation failed** | Stockage plein, snapshot orphelin | Etendre LUN, consolidate manuel |
| **CBT data is invalid** | Snapshot manuel pendant job | Reset CBT (Reset-VBRJobObject) |
| **Job timeout** | Network slow, fenetre courte | Augmenter timeout, transport mode 'Direct SAN' si possible |
| **Repository full** | Retention non purgee | Verifier GFS, lancer cleanup |

## X6.5 Pannes reseau profondes

| Symptome | Cause | Outils diagnostic | Resolution |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **Loop reseau (broadcast storm)** | Cable mal branche, STP off | Switch counters, console | Activer RSTP, port-security |
| **VLAN ne passe pas trunk** | Native VLAN mismatch, trunk allow | show interfaces trunk | Aligner native VLAN, allow VLAN |
| **DHCP ne fonctionne plus** | DHCP serveur HS, scope plein, helper-address | ipconfig /all, dhcp logs | Renew, etendre scope, ajouter relay |
| **MTU asymetrique (lents transferts)** | Path MTU > 1500 sur tunnel | ping -f -l 1472, tracepath | Reduire MTU TCP MSS clamp 1380 |
| **DNS lent** | Foward, DNS recursif sature | dig +stats, journalctl unbound | Forwarders multiples, cache pre-warm |
| **Multicast / mDNS HS** | IGMP snooping mauvais, querier | tcpdump, switch igmp-querier | Activer querier sur 1 switch |
| **Wifi lent client unique** | Channel co-canal, distance | WiFi Analyzer, signal | Replacer borne, changer canal |

# Complement 7 - Conformite et controles

## X7.1 Checklist conformite RGPD client

- Registre des traitements client a jour (responsabilite client, JMSI accompagne).
- DPA (article 28) signe entre JMSI et client.
- Sous-traitants ulterieurs JMSI (Wasabi, Microsoft, etc.) listes en annexe DPA.
- Politique de conservation : durees fixees par finalite, suppression automatique configuree.
- Procedure de droit d'acces / suppression / rectification documentee (RGPD article 15-22).
- Notification violation : process en place pour notification CNIL sous 72h (article 33).
- DPO ou referent designe cote client.
- Sensibilisation collaborateurs : 1 fois par an minimum.
- AIPD (analyse d'impact) realisee si traitement a haut risque (videosurveillance massive, suivi geolocalise, etc.).

## X7.2 Checklist NIS2 (entites essentielles et importantes)

- Identification du statut NIS2 (essentielle ou importante - cf. Annexe I/II directive).
- Politique de gouvernance cyber documentee, validee par la direction.
- Analyse de risque : cartographie des actifs, des menaces, des impacts.
- Mesures techniques minimales (Annexe A) : MFA, chiffrement, gestion des incidents, supervision, sauvegarde, PRA.
- Audit de maturite : annuel, par tiers qualifie ou auto-evaluation justifiee.
- Notification d'incident : 24h pre-notification, 72h evaluation, 1 mois rapport final.
- Designation d'un responsable cyber (interne ou prestataire).
- Securite chaine d'approvisionnement : evaluation des sous-traitants critiques.
- Tests de continuite : exercice annuel minimum.
- Formation des dirigeants : obligation de connaissance des risques cyber (cf. CNCA).

## X7.3 Audit annuel JMSI - check-list

| Domaine | Verification | Justificatif |
|---|---|---|
| **Inventaire** | Match GLPI vs realite physique | Capture GLPI + photos baie |
| **Sauvegardes** | Tests de restauration trimestriels effectues | Rapports SureBackup, fichiers tests |
| **Securite endpoint** | 100 % postes sous EDR, version a jour | Console GravityZone export |
| **Mises a jour** | Patch lag < 30 jours sur securite | Rapport patch management |
| **Comptes admin** | Revue trimestrielle, derniers usages | Audit AD + Bitwarden access logs |
| **Politique mots de passe** | FGPP active, conformite | Get-ADFineGrainedPasswordPolicy |
| **MFA** | 100 % comptes admin, > 80 % | Microsoft Entra report |

| | | |
|---|---|---|
| | utilisateurs | |
| **Pare-feu** | Configuration vs baseline JMSI | Backup config + diff |
| **PRA** | Test annuel realise | PV de test PRA |
| **Pentest** | Pentest annuel inclus Pack Pro | Rapport partenaire qualifie |
| **Sensibilisation** | Programme annuel execute | Statistique campagnes phishing |
| **Conformite RGPD** | Registre traitements a jour | Export registre |
| **Documentation** | Dossier de base actualise | Verification cote NAS JMSI |

# Complement 8 - Modeles de communication crise

## X8.1 Email - declaration incident P1 vers le client

> Objet : [URGENT] Incident de production - <CLIENT> - Plan d'action JMSI
>
> Bonjour M./Mme <NOM_CONTACT>,
>
> Un incident majeur affectant <SERVICE_TOUCHE> est en cours sur votre infrastructure.
>
> Ce que nous savons a <HEURE> :
> - Symptome : <DESCRIPTION_FACTUELLE>
> - Perimetre touche : <UTILISATEURS_AFFECTES>
> - Hypothese de cause : <CAUSE_PROBABLE>
>
> Ce que nous faisons :
> - Action 1 : <EN_COURS>
> - Action 2 : <PREVU>
>
> Prochain point a : <DELAI>
>
> Le ticket de reference est : <NUM_TICKET>.
> Le technicien dedie est : <NOM> - <TEL>.
>
> Direction technique JMSI - 04 48 26 00 66 - contact@jmlab.eu
> <NOM_DT>

## X8.2 Email - notification ransomware (a froid, redaction soignee)

> Objet : [INCIDENT MAJEUR] Suspicion de chiffrement - <CLIENT>
>
> Bonjour M./Mme <NOM_DECIDEUR>,
>
> Nous avons detecte ce <DATE> a <HEURE> des signes evocateurs d'une cyberattaque par chiffrement sur votre systeme d'information. Notre equipe technique est mobilisee.
>
> Mesures conservatoires deja prises :
> - Isolation du reseau Internet (effective a <HEURE>)
> - Coupure des serveurs identifies comme touches
> - Verification de l'integrite des sauvegardes hors site (en cours)
>
> Ce que nous vous demandons MAINTENANT :
> 1. Nous accuser reception de cet email.
> 2. Reunir un point de coordination crise sous 1h (telephone ou physique).
> 3. Ne PAS rallumer ni manipuler les machines tant qu'aucune autorisation n'est donnee.
> 4. Informer votre assurance cyber (si presente).
> 5. Ne pas communiquer avec d'eventuels attaquants - aucune transaction sans validation d'avocat et de la Direction technique JMSI.
>
> Notre engagement :

- Mobilisation 24/7 jusqu'a la reprise.
- Plan de reconstruction PRA active (cf. votre dossier de base section 9).
- Communication formelle toutes les 4 heures jusqu'a stabilisation.

Direction technique JMSI - 04 48 26 00 66 (24/7) - contact@jmlab.eu
<NOM_DT>

## X8.3 Communication interne aux salaries client (modele a adapter)

Objet : Incident technique en cours - mode degrade

Cher(e)s collegues,

Nous rencontrons actuellement un incident technique affectant <SERVICE>. Notre prestataire JMSI est mobilise pour resoudre la situation au plus vite.

Ce que cela change pour vous :
- <SERVICE> n'est temporairement pas accessible.
- Pour les urgences metier, merci de contacter <NOM_REFERENT> par telephone.
- Vous pouvez continuer a travailler localement (Word/Excel sur le poste).
- Ne supprimez aucun fichier, n'eteignez pas votre poste.

Nous vous tiendrons informes par email ou affichage des le retablissement.

Merci pour votre comprehension.
<NOM_DIRIGEANT>

# Complement 9 - Tarification et chiffrage des projets

## X9.1 Grille interne JMSI (taux horaires)

| Profil | Taux horaire HT | Cas d'usage |
|---|---|---|
| **N1 - Technicien helpdesk** | 75 EUR | Tickets standard, telesupport |
| **N2 - Technicien itinerant senior** | 95 EUR | Intervention site, configuration serveur |
| **N3 - Ingenieur systeme/reseau** | 120 EUR | Architecture, audit, integration complexe |
| **Direction technique** | 150 EUR | Pilotage projet, expertise, audit qualifie |
| **Astreinte (forfait)** | 150 EUR + 1,5x taux | Hors heures ouvres |
| **Deplacement (zone proche)** | Forfait 30 EUR | Inclus dans 30 km |
| **Deplacement (zone elargie)** | 0,55 EUR / km | Au-dela de 30 km |

## X9.2 Methode de chiffrage projet

483. Decomposer en lots techniques (un par chapitre du livre blanc).
484. Estimer chaque lot en jours-homme par profil (N1/N2/N3).
485. Ajouter buffer 15-25 % selon complexite et inconnu.
486. Materiel : marge JMSI 8-15 % sur prix de revient (hors gros volumes).
487. Prestation : taux horaire * heures.
488. Recurrent (services) : tarif catalogue ou tarif sur mesure (volume).
489. Garanties : inclure 1 mois de support post-mise en service comme standard.
490. Validation : 3 options (Essentiel, Confort, Premium).

## X9.3 Chiffrage type Pack Performance (5 postes)

| Element | Quantite | Prix unitaire HT | Total HT |
|---|---|---|---|
| **Serveur tour PME pro** | 1 | 2 490 EUR | 2 490 EUR |
| **Switch PoE 8 ports** | 1 | 199 EUR | 199 EUR |
| **NAS DS423+ + 4 disques 8 To** | 1 | 1 200 EUR | 1 200 EUR |
| **Onduleur 1500 VA** | 1 | 350 EUR | 350 EUR |
| **Baie brassage 12U** | 1 | 690 EUR | 690 EUR |

| | | | |
|---|---|---|---|
| **PC bureau i3 neuf + ecran 24''** | 5 | 758 EUR | 3 790 EUR |
| **Pre-cablage Cat 6A 5 prises** | 5 | 89 EUR | 445 EUR |
| **Mise en service complete (5 jours)** | 1 | 5 000 EUR | 5 000 EUR |
| **Sous-total materiel + mise en service** | | | 14 164 EUR |
| | | | |
| **RECURRENT MENSUEL** | | | |
| **Maintenance 5 postes** | 1 | 89 EUR/mois | 89 EUR/mois |
| **Sauvegarde serveur 500 Go** | 1 | 29 EUR/mois | 29 EUR/mois |
| **Securite Pro 5 postes** | 5 | 9,90 EUR/mois | 49,50 EUR/mois |
| **Total mensuel** | | | 167,50 EUR/mois |

# Complement 10 - Bonnes pratiques editorial JMSI

## X10.1 Charte de redaction des comptes-rendus

- Toujours en francais, vouvoiement.
- Pas d'argot ni de jargon non explique.
- Phrases courtes, paragraphes < 5 lignes.
- Structure SYMPTOME / DIAGNOSTIC / ACTION.
- Chiffres explicites : << en 47 minutes >> plutot que << rapidement >>.
- Eviter le << on >> impersonnel : preferer << JMSI >> ou << le technicien >>.
- Reformuler le besoin client avant la solution.
- Signature et identification systematiques.

## X10.2 Photos d'intervention - bonnes pratiques

- Toujours photographier l'avant et l'apres (au moins 5 + 5 photos).
- Photographier les serial numbers, etiquettes, configurations particulieres.
- Eviter de photographier des donnees personnelles client (ecrans avec mails, factures, photos).
- Stockage immediat dans /clients/<CODE>/10_interventions/<DATE>/.
- Format : photo telephone JMSI > sync auto vers Nextcloud > rangement par technicien.

## X10.3 Comportement client - les 10 commandements du technicien JMSI

491. Tu vouvoieras par defaut.
492. Tu reformuleras le besoin avant d'agir.
493. Tu annonceras chaque coupure de service.
494. Tu ne critiqueras jamais l'existant devant le client.
495. Tu refuseras poliment ce qui sort du contrat (et tu enverras un devis).
496. Tu sauvegarderas avant tout changement.
497. Tu testeras chaque etape avant la suivante.
498. Tu documenteras chaque modification (GLPI + dossier de base).
499. Tu escaladeras quand tu sors de ton perimetre.
500. Tu prendras conge en disant : << si vous avez le moindre doute, ouvrez un ticket. >>

# Complement 11 - Supervision avec Zabbix

## X11.1 Architecture Zabbix JMSI

Zabbix 6.x LTS est l'outil de supervision JMSI pour les clients ayant un parc significatif (> 5 serveurs) ou des contraintes de SLA fortes. Auto-hebergement JMSI sur VM dediee. Une instance JMSI multi-tenant pour les clients standards, une instance dediee pour les clients Pack Pro avec donnees particulierement sensibles.

### X11.1.1 Composants

| Composant | Role |
|---|---|
| **Zabbix Server** | Coeur : collecte, calcul, alertes, base de donnees PostgreSQL |
| **Zabbix Frontend** | Interface web (PHP-FPM + Nginx) |
| **Zabbix Proxy** | Relais de collecte par site client (active ou passive) |
| **Zabbix Agent 2** | Agent endpoint - serveurs et postes critiques |
| **SNMP** | Switches, NAS, NVR, onduleurs, NGFW |
| **HTTP / SSL Check** | Sites web, certificats TLS |
| **Custom scripts** | Audit specifique (queue mail Postfix, etc.) |

### X11.1.2 Templates JMSI standard

- Template OS Linux by Zabbix agent 2 : CPU, memory, disk, network, services.
- Template OS Windows by Zabbix agent 2 : memory, services, perfcounters.
- Template Net Synology by SNMP : disques, RAID, services DSM.
- Template App MariaDB / PostgreSQL : connexions, query rate, cache hit.
- Template App Mailcow : queue, deliveries, bounces.
- Template SSL Certificate : expiration, chain.
- Template Network Generic by SNMP : interface up/down, throughput, errors.
- Template UPS APC by SNMP : statut, batterie, charge.

### X11.1.3 Triggers et severites JMSI

| Severite | Couleur | Action JMSI |
|---|---|---|
| **Not classified** | Gris | Information, pas d'alerte |
| **Information** | Bleu | Email log, pas d'urgence |
| **Warning** | Jaune | Email + ticket DEM-INF |
| **Average** | Orange | Email + ticket INC-LOG, GTI 4h |
| **High** | Rouge clair | Email + SMS + ticket INC-x, GTI 2h |

| | | |
|---|---|---|
| **Disaster** | Rouge fonce | Email + SMS + appel automatique, P1, GTI immediate |

### X11.1.4 Installation Zabbix Agent 2 sur Linux

```
# Debian 12 - Zabbix Agent 2

# Repository officiel Zabbix
wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian12_all.deb
dpkg -i zabbix-release_6.4-1+debian12_all.deb
apt update
apt install -y zabbix-agent2 zabbix-agent2-plugin-*

# Configuration
cat > /etc/zabbix/zabbix_agent2.conf <<'EOF'
Server=zabbix.jmlab.eu,zabbix-proxy.<CODE>.local
ServerActive=zabbix-proxy.<CODE>.local
Hostname=$(hostname -f)
HostMetadata=jmsi,linux,production
Include=/etc/zabbix/zabbix_agent2.d/*.conf
PSKIdentity=jmsi-<HOST>
PSKFile=/etc/zabbix/agent.psk
TLSConnect=psk
TLSAccept=psk
EOF

# Generer une cle PSK
openssl rand -hex 32 > /etc/zabbix/agent.psk
chown zabbix:zabbix /etc/zabbix/agent.psk
chmod 600 /etc/zabbix/agent.psk

# Enrolement cote serveur Zabbix : Configuration > Hosts > Create host
#   Host name = match Hostname agent
#   Templates = Linux by Zabbix agent 2 + JMSI Standard
#   Encryption : PSK only (coller la PSK)

systemctl enable --now zabbix-agent2

# Verification
zabbix_agent2 -t 'agent.ping'
zabbix_agent2 -t 'system.cpu.load'

# Cote serveur, verifier dans Latest data que l'host repond
```

## X11.2 Templates personnalises - exemple : queue Postfix Mailcow

```
# /etc/zabbix/zabbix_agent2.d/postfix.conf

UserParameter=postfix.queue.size,/usr/sbin/postqueue -p | tail -n 1 | awk '{print $5}'
UserParameter=postfix.queue.deferred,find /var/spool/postfix/deferred -type f | wc -l
UserParameter=postfix.queue.active,find /var/spool/postfix/active -type f | wc -l

# Cote Zabbix - Items :
```

```
#   postfix.queue.size       (Numeric int) - taille totale en octets
#   postfix.queue.deferred   (Numeric int) - nb mails differes

# Triggers JMSI :
#   { Mailcow:postfix.queue.deferred.last() } > 100  -> Average
#   { Mailcow:postfix.queue.deferred.last() } > 500  -> High
#   { Mailcow:postfix.queue.size.last() } > 1G       -> High

# Action Zabbix associee : envoyer mail au technicien JMSI + creer ticket GLPI auto
```

# Complement 12 - SIEM Wazuh pour clients NIS2

## X12.1 Pourquoi un SIEM ?

Wazuh est un SIEM open source utilise pour la detection d'intrusion, la conformite (PCI-DSS, NIS2, HIPAA), et la centralisation des logs. JMSI le deploie pour les clients Pack Pro NIS2 ou demande explicite. Auto-hebergement, communication TLS chiffree, retention 12 mois minimum.

## X12.2 Architecture

| Composant | Role | Specifications minimales |
|---|---|---|
| **Wazuh Manager** | Coeur : reception, analyse, regles, alertes | 8 vCPU, 32 Go RAM, SSD 500 Go |
| **Wazuh Indexer (OpenSearch)** | Stockage et recherche des evenements | 8 vCPU, 32 Go RAM, SSD 1 To+ |
| **Wazuh Dashboard (OpenSearch Dashboards)** | Interface web | 4 vCPU, 8 Go RAM |
| **Wazuh Agent** | Endpoint sur chaque serveur / poste critique | Linux/Windows/macOS, < 5% CPU |
| **Filebeat** | Forwarder de logs syslog / fichiers tiers | Sur chaque source non-agent |

## X12.3 Cas d'usage de detection JMSI

- File integrity monitoring (FIM) sur fichiers systemes critiques (/etc, registres Windows).
- Detection de connexion SSH multiples echouees (brute force).
- Detection de privilege escalation (sudo, runas).
- Detection d'acces hors heures ouvrees (correlation d'horaire).
- Detection de modification d'agent EDR ou antivirus (tampering).
- Detection de creation de compte admin local non autorise.
- Detection de connexion VPN depuis un pays inhabituel.
- Conformite : verification reguliere (CIS Benchmarks, OWASP).

## X12.4 Installation Wazuh Agent (Linux)

```
# Debian / Ubuntu
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
echo 'deb https://packages.wazuh.com/4.x/apt/ stable main' > /etc/apt/sources.list.d/wazuh.list
apt update && apt install -y wazuh-agent
```

```
# Configuration
# /var/ossec/etc/ossec.conf
sed -i 's|<address>MANAGER_IP</address>|<address>wazuh.jmlab.eu</address>|' \
    /var/ossec/etc/ossec.conf

# Inscription par cle pre-partagee (ou auto-enrollment via authd)
/var/ossec/bin/agent-auth -m wazuh.jmlab.eu -p 1515 -A '$(hostname -f)'

systemctl enable --now wazuh-agent

# Verification
systemctl status wazuh-agent
# Cote manager : /var/ossec/bin/agent_control -l
```

# Complement 13 - Procedures de nuit / weekend (astreinte)

## X13.1 Cas typique 1 - serveur HS dimanche matin

501. [T+0] Appel client : 'le serveur ne demarre plus, on a vu une coupure EDF cette nuit'.
502. [T+5 min] Connexion VPN JMSI > console iLO/iDRAC du serveur.
503. [T+10 min] Diagnostic : POST en boucle, message 'No bootable device'.
504. [T+15 min] Hypothese : controleur RAID en degraded apres microcoupure.
505. [T+20 min] Boot sur iLO console + sortie BIOS controleur RAID.
506. [T+30 min] Reconstruction du virtual drive a partir des disques sains.
507. [T+1h] Boot OS, verification services, communication client.
508. [T+1h30] Compte-rendu detaille, ticket cloture, RAS exceptionnel programme.

## X13.2 Cas typique 2 - mail down samedi soir

509. [T+0] Alerte automatique Zabbix : Mailcow indisponible.
510. [T+2 min] Connexion VPN, etat des conteneurs Docker.
511. [T+5 min] Identification : container postfix-mailcow restart en boucle.
512. [T+10 min] Logs : disque a 100 % (queue saturee suite phishing).
513. [T+15 min] Purge des mails 'spam scoring > 15' : postsuper -d ALL hold.
514. [T+30 min] Espace disque retabli, services redemarres, monitoring vert.
515. [T+1h] Communication client : detection precoce, action JMSI proactive.
516. [T+24h] Analyse avec Rspamd : ajout de regle pour bloquer la campagne future.

## X13.3 Cas typique 3 - ransomware vendredi 19h45

517. [T+0] Alerte Bitdefender + appel client.
518. [T+5 min] Confirmation visuelle : utilisateur a clique sur PJ Outlook.
519. [T+10 min] DECISION : isolation reseau site complet (firewall en deny-all sortant + entrant).
520. [T+15 min] Notification Direction technique JMSI + decideur client.
521. [T+30 min] Direction technique mobilisee, decideur en route sur site.
522. [T+1h] Constat : 12 postes affectes, 1 serveur AD intact (isolation rapide).
523. [T+1h30] Verification integrite sauvegardes Wasabi : OK (immutables, 30 jours).
524. [T+2h] Decision officielle : declenchement PRA - signe par decideur.
525. [T+3h] Plan de reconstruction : restauration veille a partir de Veeam.
526. [T+12h] Premieres VM restaurees en environnement isole, validation integrite.
527. [Lendemain matin] Communication salaries : reprise progressive lundi.
528. [Lundi - J+3] Reprise progressive utilisateur par utilisateur, postes neufs.
529. [J+10] Retex complet, mise a jour PRA, durcissement post-incident.

# Complement 14 - Specificites secteurs metier

## X14.1 Sante - cabinets medicaux et professions liberales sante

- Conformite RGPD donnees de sante : niveau renforce (sante = donnees sensibles, art. 9 RGPD).
- Hebergement de donnees de sante (HDS) : si hebergement, certification HDS obligatoire (JMSI partenaire OVH HDS).
- Logiciels metier specifiques : Crossway, Doctolib, MediStory, Almapro (compatibilite a verifier).
- Sauvegarde : RPO 1h max, RTO 4h max (continuite des soins).
- Securite physique : armoire sous cle pour serveur cabinet.
- MFA obligatoire pour tout acces dossier patient.
- Sensibilisation specifique : phishing simulant CPAM, pharmacie, etc.

## X14.2 Hotellerie / restauration / camping

- Wi-Fi public conforme + portail captif (cf. chap. 7) - amende 75 000 EUR sans logs.
- Telephonie : SVI multi-langue, file d'attente accueil, mobiles equipiers.
- Vidéosurveillance pour caisses + zones publiques (CNIL, autorisation prefectorale).
- PMS (Property Management System) : Mews, Ohra, Cloudbeds (hebergement infogere si SaaS, integration mail/CRM).
- TPE/Caisse : connectivite Internet + sauvegarde paramets pour cas defaillance.

## X14.3 Industrie / atelier / production

- Reseau OT (Operational Technology) souvent isole IT - segmentation VLAN forte.
- Postes de production : Win 10 LTSC ou IoT Enterprise (longue duree de vie).
- Imprimantes etiquettes : Zebra, Brother, configuration reseau IP fixe.
- ERP : Sage 100, Cegid, Dolibarr personnalise.
- Controle qualite : automate type Beckhoff, Siemens - hors scope JMSI sauf demande.
- Sauvegarde redondee : critique pour la productivité.

## X14.4 Cabinet d'expertise comptable / avocats

- Logiciels metier : Cegid Quadra, ACD, Sage Coala, ACL Robotique.
- Confidentialite ultra-renforcee : MFA partout, postes chiffres, EDR Pro.
- Sauvegarde 7 ans (obligation legale).
- Conformite REQI / Reglements professionnels.
- Souvent : multi-site, mobilite, RDS pour acces nomade.

# X14.5 Mairies et collectivites locales

- Marche public : reponse via plateforme PLACE, dossier de consultation.
- Securite : NIS2 (transposition collectivites > 5000 hab).
- Logiciels metier : Berger-Levrault (etat civil), Ciril, Inetum.
- Site internet : conformite RGAA (accessibilite numerique).
- Telephonie : forfait specifique service public.
- Wi-Fi mairie / espaces : portail captif obligatoire.

# Complement 15 - Cas particuliers et integrations

## X15.1 Migration vers Microsoft 365 (PME existant Exchange)

### X15.1.1 Cas typique : 25 utilisateurs Exchange Server 2016 -> M365

530. Audit prealable : volume boites, public folders, partages calendrier, regles utilisateurs.
531. Choix de la methode : Hybrid (Exchange + M365 coexistance), Cutover (< 150 boites), Staged (de plus en plus rare).
532. Pour 25 utilisateurs : Cutover migration recommandee.
533. Souscription : Microsoft 365 Business Premium (22 EUR/utilisateur/mois) ou Standard (10 EUR).
534. Verification du tenant Microsoft 365 (initial setup CSP).
535. Configuration des domaines (TXT verification, MX a basculer le D-Day).
536. Pre-creation des utilisateurs M365 (script PowerShell).
537. Lancement de la migration cutover (depuis Exchange Admin Center > Recipients > Migration).
538. Bascule des MX (TTL court depuis 24h avant).
539. Reconfigurer les clients Outlook (auto-discover + nouveaux profils).
540. Decommission Exchange : 30 jours apres validation de la migration.

## X15.2 Office 365 / Google Workspace co-existence

Quelques clients hybrides : ENT en Google Workspace + utilisateurs M365 (cas frequent ecoles privees/associations).

- Federation possible via Azure AD B2B + sync.
- Calendrier partage : utiliser des invitations standard (iCal).
- Stockage : prefers OneDrive vs Drive selon utilisateur principal.
- Eviter la duplication : un seul outil officiel par fonction.

## X15.3 Integration Bitwarden + AD (SSO)

Bitwarden Enterprise permet le SSO via SAML 2.0 ou OIDC. Pour les clients Microsoft 365 :

```
# Configuration SAML Bitwarden + Microsoft Entra ID

# Cote Entra ID :
# Identity > Enterprise applications > New application > Bitwarden (gallery)
# Configurer SSO :
#   - Identifier (Entity ID) : https://sso.bitwarden.com/saml2
#   - Reply URL : https://sso.bitwarden.com/saml2/<ORGANIZATION_ID>/Acs
#   - Logout URL : https://sso.bitwarden.com/saml2/<ORGANIZATION_ID>/Slo

# Recuperer le metadata XML SAML (cote Entra)
# Coller dans Bitwarden : Settings > Single Sign-On > IdP entity ID + cert

# Activer pour l'organisation (Bitwarden) :
```

```
# Settings > Policies > Single sign-on authentication = Enabled

# Tester avec un compte de test pilote avant deploiement complet
```

## X15.4 Mise en place Microsoft Defender for Business

Alternative a Bitdefender pour les clients deja Microsoft 365 Business Premium (Defender for Business inclus).

- Activation : Microsoft 365 Defender > Configuration > Defender for Business.
- Onboarding : script PowerShell genere par Microsoft Defender, deploye via TacticalRMM.
- Politiques : Next-generation protection, ASR rules, Web content filtering.
- Integration ATP : EDR avec timeline, alertes consolidees.
- Choix entre Bitdefender (multi-OS, console JMSI) et Defender (integre M365) : selon contrat client.

# Complement 16 - Performances et tuning

## X16.1 Tuning serveur Windows

- Disable unused services (Print Spooler hors print server, Fax, etc.).
- Power Plan : 'High Performance' sur serveur (par defaut Balanced lent).
- Verifier : NTFS allocation unit size, MBR vs GPT, alignment.
- Page file : 1.5x RAM si < 16 Go, 16 Go fixe au-dela.
- Indexation Windows : desactiver sur volumes data servers.
- Antivirus exclusions : DB Exchange, SQL, Veeam, fichiers VHD/VHDX, fichiers virtualisation, repertoires AD.

## X16.2 Tuning Linux

```
# /etc/sysctl.d/99-jmsi-tuning.conf

# Reseau
net.core.somaxconn = 4096
net.core.netdev_max_backlog = 5000
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.tcp_fin_timeout = 15
net.ipv4.tcp_keepalive_time = 300
net.ipv4.tcp_keepalive_intvl = 30
net.ipv4.tcp_keepalive_probes = 3

# Memoire
vm.swappiness = 10
vm.dirty_background_ratio = 5
vm.dirty_ratio = 10

# Securite
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.rp_filter = 1

# Application
sysctl -p /etc/sysctl.d/99-jmsi-tuning.conf

# Limites systeme
# /etc/security/limits.d/99-jmsi.conf
# *  soft  nofile  65536
# *  hard  nofile  131072
# *  soft  nproc   32768
# *  hard  nproc   65536
```

## X16.3 Tuning MariaDB (cas applicatif)

```
# /etc/mysql/mariadb.conf.d/99-jmsi-tuning.cnf
# Pour serveur dedie 8 Go RAM
```

```
[mysqld]
# Buffer Pool (50-70 % RAM pour serveur dedie)
innodb_buffer_pool_size = 4G
innodb_buffer_pool_instances = 4
innodb_log_file_size = 512M
innodb_log_buffer_size = 16M
innodb_flush_log_at_trx_commit = 2   # 1 = ACID strict (paye), 2 = securite + perf, 0 = perf
max
innodb_flush_method = O_DIRECT
innodb_io_capacity = 2000          # SSD
innodb_io_capacity_max = 4000

# Tables temporaires
tmp_table_size = 256M
max_heap_table_size = 256M

# Connexions
max_connections = 200
thread_cache_size = 50
table_open_cache = 4000

# Slow query log (audit perf)
slow_query_log = 1
slow_query_log_file = /var/log/mysql/slow.log
long_query_time = 2

# Binary log (replication / backup point-in-time)
log_bin = /var/log/mysql/mysql-bin
binlog_format = ROW
expire_logs_days = 7

# Application puis redemarrage
systemctl restart mariadb

# Verification
mysql -e "SHOW VARIABLES LIKE 'innodb_buffer_pool_size';"
mysql -e "SHOW STATUS LIKE 'Threads_connected';"
```

## X16.4 Tuning Apache / Nginx

```
# Nginx - /etc/nginx/nginx.conf
# Pour serveur 4 vCPU, 8 Go RAM

worker_processes auto;        # ou nb vCPU
worker_rlimit_nofile 65535;

events {
    worker_connections 4096;
    use epoll;
    multi_accept on;
}

http {
    sendfile on;
    tcp_nopush on;
    tcp_nodelay on;
    keepalive_timeout 30;
    keepalive_requests 100;
```

```
    # Compression
    gzip on;
    gzip_comp_level 5;
    gzip_min_length 256;
    gzip_types text/plain text/css application/json application/javascript application/xml;

    # Buffers
    client_body_buffer_size 16K;
    client_header_buffer_size 1k;
    client_max_body_size 64M;
    large_client_header_buffers 4 16k;

    # Cache file descriptors
    open_file_cache max=10000 inactive=30s;
    open_file_cache_valid 60s;
    open_file_cache_min_uses 2;
    open_file_cache_errors on;

    # Securite
    server_tokens off;
    add_header X-Frame-Options SAMEORIGIN always;
    add_header X-Content-Type-Options nosniff always;
    add_header X-XSS-Protection '1; mode=block' always;
    add_header Strict-Transport-Security 'max-age=31536000; includeSubDomains' always;
    add_header Referrer-Policy 'strict-origin-when-cross-origin' always;

    # SSL
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers 'ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:...';
    ssl_prefer_server_ciphers on;
    ssl_session_cache shared:SSL:10m;
    ssl_session_timeout 10m;
    ssl_stapling on;
    ssl_stapling_verify on;
}
```

# Complement 17 - Documentation client (modeles)

## X17.1 Documentation utilisateur 'Cle USB de demarrage' (modele)

Le technicien JMSI livre a chaque collaborateur une fiche pratique 'Cle USB de demarrage'. Modele JMSI standardise, a personnaliser au logo client.

- Page 1 : Identifiants - login / mot de passe / serveur mail / VPN / Wi-Fi.
- Page 2 : Comment ouvrir un ticket JMSI (3 methodes : portail, mail, telephone).
- Page 3 : Comment verrouiller son poste (Windows + L), eteindre, redemarrer.
- Page 4 : Comment se connecter en VPN, en RDP, a la messagerie sur mobile.
- Page 5 : Comment reconnaitre un mail de phishing (5 signes).
- Page 6 : Que faire en cas de doute - cas concrets.

## X17.2 Charte informatique - modele JMSI a faire valider client

- Section 1 : Objet de la charte - protection des actifs informatiques.
- Section 2 : Champ d'application - tous les utilisateurs du SI client.
- Section 3 : Regles d'usage - utilisation loyale, professionnelle, respectueuse.
- Section 4 : Mots de passe - 12 chars min, complexite, non-divulgation.
- Section 5 : Mail - usage professionnel, pas de transfert de donnees personnelles, pas d'usage commercial personnel.
- Section 6 : Internet - usage non professionnel raisonnable et tolere, sites interdits.
- Section 7 : Bring Your Own Device - politique stricte ou interdite selon client.
- Section 8 : Sortie d'effectif - retour materiel, suppression comptes, signature charte de discretion.
- Section 9 : Sanctions - rappel, avertissement, sanction disciplinaire.
- Section 10 : Signature obligatoire avant remise du materiel.

# Complement 18 - References techniques et veille

## X18.1 Sites de veille a consulter quotidiennement

- https://cert.ssi.gouv.fr/ - alertes ANSSI / CERT-FR.
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog - CISA KEV.
- https://nvd.nist.gov/ - National Vulnerability Database.
- https://msrc.microsoft.com/update-guide/ - Microsoft Security Updates.
- https://www.lemagit.fr/ - actualite IT FR.
- https://forum.synology.com/ - communaute Synology.
- https://forum.opnsense.org/ - communaute OPNsense.
- https://reddit.com/r/sysadmin - veille internationale.
- https://reddit.com/r/msp - veille MSP.

## X18.2 Certifications et formations a viser

| Certification | Editeur | Niveau | Pertinence JMSI |
|---|---|---|---|
| **CompTIA Network+** | CompTIA | Junior | Base reseau, recommandee a l'embauche |
| **Microsoft 365 Fundamentals (MS-900)** | Microsoft | Junior | Pour tout technicien M365 |
| **Azure Fundamentals (AZ-900)** | Microsoft | Junior | Pour deploiement cloud |
| **Microsoft 365 Modern Desktop (MD-100/101)** | Microsoft | Senior | Specialiste poste de travail |
| **Microsoft 365 Security (SC-200/300)** | Microsoft | Senior | Specialiste securite cloud |
| **Bitdefender GravityZone (BCSP)** | Bitdefender | Standard | Obligatoire pour deployer EDR |
| **Veeam VMCE** | Veeam | Senior | Specialiste sauvegarde |
| **Synology Certified Professional** | Synology | Standard | NAS expert |
| **Stormshield Network Engineer (SNCE)** | Stormshield | Senior | Pare-feu qualifie ANSSI |
| **3CX Advanced Certification** | 3CX | Standard | Telephonie deploiement |

| | | | |
|---|---|---|---|
| **RNCP Administrateur Systemes et Reseaux** | France Compet. | Senior | Equivalent BTS+ pour RH |
| **ANSSI Hygiene Informatique** | ANSSI | Tous | Recommandee pour tout technicien |

## X18.3 Outils a connaitre (pas tous deployes JMSI mais a savoir)

| Outil | Categorie | Notes JMSI |
|---|---|---|
| **Wireshark** | Analyse reseau | Indispensable pour technicien itinerant |
| **Nmap / Zenmap** | Scan reseau | Audit, decouverte, pre-vente |
| **Process Explorer / Process Monitor** | Sysinternals | Diagnostic Windows avance |
| **Autoruns** | Sysinternals | Detection persistance malware |
| **FRST (Farbar Recovery Scan Tool)** | Diagnostic Windows | Suspicion infection |
| **Glasswire** | Monitoring reseau Windows | Diagnostic detaille flux |
| **Etherpad / CryptPad** | Collaboration | Note partagee chiffree |
| **BleachBit** | Nettoyage | Avant remise materiel |
| **Recuva / TestDisk / PhotoRec** | Recuperation donnees | Niveau 1 recuperation |
| **HWInfo / CPU-Z / GPU-Z** | Inventaire hardware | Specs detaillees |
| **CrystalDiskInfo / CrystalDiskMark** | Sante / perf disque | SMART + benchmark |
| **MemTest86** | Test memoire | Suspicion RAM defectueuse |
| **Belarc Advisor** | Inventaire | Audit poste rapide |
| **Lansweeper** | Inventaire reseau | Alternative GLPI commerciale |
| **Termius / MobaXterm** | Client SSH | Plus convivial que PuTTY |

# Fin du document

Ce livre blanc technique est l'outil de reference des techniciens JMSI. Il evolue avec votre retour d'experience : signalez toute correction, complement ou nouveau mode operatoire a la Direction technique pour integration dans la prochaine edition.

**JM Sud Informatique**

04 48 26 00 66 - contact@jmlab.eu - b2b.jmlab.eu

*Edition 2026 - version 1.0*