



Architecture Système & Spécifications Globales

Document de référence exhaustif pour les 10 sous-domaines, l'infrastructure duale 2x VM Oracle (1GB sans Docker), l'isolation native Systemd, le pipeline de sauvegarde chiffrée GFS et la gouvernance globale de sécurité.

AUTEUR & DESIGN
Léo Trédille

DOMAINE MAÎTRE
*.t-leo.fr (Cloudflare)

INFRASTRUCTURE
2x VM Oracle (1GB RAM)

STATUT GLOBAL
Production Ready (v4.0)

⚡ SYNTHÈSE D'INGÉNIERIE & DÉCISIONS CLÉS

Élimination de la taxe mémoire Docker (~150 Mo libérés par VM) compensée par un confinement natif Systemd (ProtectSystem=strict, cgroups MemoryMax). Sauvegardes nocturnes atomiques SQLite WAL chiffrées par clé asymétrique age vers Google Drive. Séparation géographique des accès Break-Glass matériels FIDO2 et alerte SSH instantanée.

SECTION 01

Topologie Dual-VM & Caddy

Répartition VM1/VM2, budget mémoire 70% libre, règles WAF Cloudflare.

SECTION 02

Les 10 Modules de l'Écosystème

Spécifications architecturales et maquettes vectorielles détaillées.

Topologie 2x VM Oracle (1GB RAM sans Docker)

VM 1 : Frontends Publics & CADDY 2.8 NATIF

Hébergement statique compilé, temps de réponse < 200ms et distribution Edge.

- **t-leo.fr** : Vitrine principale d'architecture et fabrication numérique (Astro SSG).
- **tools.t-leo.fr** : Base de calculs et mémos d'atelier avec moteur Pagefind sans DB.
- **welcome.t-leo.fr** : Portail d'accueil dynamique pour invités et synchronisation menu.
- **diy.t-leo.fr & world.t-leo.fr** : Rendus 3D WebGL et moteur physique Matter.js.

VM 2 : Données, Contrôle & IoT POCKETBASE + MOSQUITTO

Poste de commande sécurisé, ingestion télémétrique et bases SQLite WAL.

- **admin.t-leo.fr** : Cockpit central protégé par Cloudflare Zero Trust (FIDO2 MFA).
- **home.t-leo.fr** : Broker MQTT Mosquitto avec certificats mTLS stricts et CRL.
- **cook.t-leo.fr** : Base culinaire et moteur de calcul des portions.
- **/var/backups/t-leo/** : Destination des snapshots atomiques SQLite WAL à 04:00 AM.

Budget Mémoire Système Réconcilié (1024 Mo par VM)

70% DE MARGE LIBRE

Composant Système	VM 1 (Frontends)	VM 2 (Admin / Data)	Rôle & Confinement
Linux Kernel + Systemd + SSHD	~240 Mo	~240 Mo	Kernel 6.x durci, ports SSH isolés
Caddy 2.8 Reverse Proxy	~35 Mo	~35 Mo	ProtectSystem=strict, buffers TLS minimales
PocketBase (SQLite WAL)	0 Mo (Non présent)	~25 Mo	StateDirectory=/var/lib/pocketbase
Mosquitto Broker (mTLS + CRL)	0 Mo (Non présent)	~15 Mo	ProtectHome=true, PrivateTmp=true
Marge Libre Utilisable	~749 Mo (73% libre)	~709 Mo (69% libre)	Tampon de sécurité OOM absolu

t-leo.fr — Vitrine d'Architecture & Fabrication Numérique

1. Architecture & Conception t-leo.fr

Vitrine principale hébergée directement sur t-leo.fr, compilée sous Astro SSG pour des temps de réponse < 200ms sans calcul serveur.

- **Moteur Astro SSG** : Génération statique complète servie par Caddy 2.8 natif avec mise en cache Cloudflare Edge.
- **Sync InDesign Dynamique** : Génération de QR codes vectoriels pour les planches de book physique redirigeant vers les pages web interactives.

2. Spécifications Techniques

TIER 1 • ASTRO SSG
• INDESIGN SYNC

Paramètres de déploiement et de sécurité consolidés.

- **Régie Typographique** : Association Space Grotesk, Inter et JetBrains Mono avec palettes d'accent ocre chaud.
- **Performance & Zéro PII** : Aucune dépendance externe invasive, zéro cookie tiers et chargement différé des assets.

Matrice d'Exploitation & Routage Caddy

SYSTEMD UNIT

PARAMÈTRE	VALEUR RETENUE	DIRECTIVE D'EXÉCUTION
Hébergement & Cible	VM1 (Oracle Cloud Free Tier)	root /var/www/t-leo.fr/dist
Routage Caddy	HTTPS natif avec HTTP/3 QUIC	encode zstd gzip; file_server
Mise en Cache	Cloudflare Edge Cache 1 an	Cache-Control: public, max-age=31536000, immutable
Budget Mémoire	0 Mo en veille (fichiers statiques)	Caddy buffer ~2 Mo lors des requêtes

admin.t-leo.fr — Cockpit Contrôle & Procédure Break-Glass

1. Architecture & Conception

admin.t-leo.fr

Poste de commande centralisé pour la télémétrie des 2 VMs, les commutateurs de maintenance sélectifs et la gestion des accès.

- **Accès Zero Trust** : Filtrage Cloudflare Access avec authentification matérielle FIDO2 (YubiKey) obligatoire.
- **Toggles de Maintenance** : Désactivation d'un clic d'un sous-domaine avec page d'attente instantanée sans toucher au DNS.

2. Spécifications Techniques

TIER 1 • CONTROL PLANE • FIDO2 MFA

Paramètres de déploiement et de sécurité consolidés.

- **Surveillance Télémétrique** : Monitoring Systemd de l'usage mémoire et CPU avec alertes automatiques en cas de pression.
- **Break-Glass Décentralisé** : Codes de secours chiffrés et clés matérielles stockés dans des coffres géographiquement séparés.

⚙ Matrice d'Exploitation & Routage Caddy

SYSTEMD UNIT

PARAMÈTRE	VALEUR RETENUE	DIRECTIVE D'EXÉCUTION
Hébergement & Cible	VM 2 (Isolation Systemd renforcée)	PocketBase internal binary :8090
Sécurité Ingress	Cloudflare Tunnel + FIDO2 Access	Zero ports ouverts sur Internet public
Confinement Systemd	ProtectSystem=strict, PrivateTmp=true	StateDirectory=/var/lib/pocketbase
Budget Mémoire	PocketBase Admin Engine ~25 Mo	MemoryMax=120M hard cgroup limit

db.t-leo.fr — Studio Design-Build & Visionneuse 3D WebGL

1. Architecture & Conception db.t-leo.fr

Plateforme de direction de chantiers universitaires avec inspection 3D en orbite de structures massives et détails constructifs.

- **Moteur 3D WebGL** : Rendu fluide 60 FPS sous Three.js exécuté intégralement sur le GPU client (0 Mo sur la VM).
- **Ségrégation Confidentielle** : Maquette 3D publique vs plans tamponnés d'ingénieur confinés dans /confidential/ sous Cloudflare Access.

2. Spécifications Techniques

TIER 1 • WebGL 3D • CONFIDENTIAL TIER

Paramètres de déploiement et de sécurité consolidés.

- **Explosion des Couches** : Visualisation dynamique des calepinages de panneaux, quincaillerie et plans d'assemblage.
- **Fiches de Découpe CNC** : Nomenclatures matière (BOM) et listes d'usinage exportables pour atelier de fab.

Matrice d'Exploitation & Routage Caddy

SYSTEMD UNIT

PARAMÈTRE	VALEUR RETENUE	DIRECTIVE D'EXÉCUTION
Hébergement & Cible	VM1 (Assets statiques glTF / Three.js)	root /var/www/db.t-leo.fr
Protection /confidential/	Cloudflare Access (Auth TMU)	Gated to @torontomu.ca and verified architects
Stockage Maquettes 3D	Fichiers compressés Draco/glTF	Distribution Cloudflare R2 / CDN
Budget Mémoire	0 Mo serveur (calcul 100% GPU client)	Empreinte statique Caddy ~15 Mo

group.t-leo.fr — Espace Équipe TMU DAS & Passerelle Notion

1. Architecture & Conception

group.t-leo.fr

Portail de travail collaboratif pour les camarades de promo TMU DAS, 100% sans stockage de données personnelles.

- Notion Edge Proxy** : Cloudflare Worker sans serveur injectant le token secret Notion sans exposition client.
- Tableau Natif Réactif** : Tableau dynamique sans forcer les camarades à installer l'application lourde Notion.

2. Spécifications Techniques

TIER 2 • EDGE
WORKER • NOTION
PROXY

Paramètres de déploiement et de sécurité consolidés.

- Filtrage par Email** : Accès restreint aux adresses universitaires @torontomu.ca pour préserver les notes de projet.
- Super Productivity Sync** : Tâches communes publiques et synchronisation chiffrée vers la file locale de Léo.

Matrice d'Exploitation & Routage Caddy		SYSTEMD UNIT
PARAMÈTRE	VALEUR RETENUE	DIRECTIVE D'EXÉCUTION
Hébergement & Cible	Cloudflare Serverless Workers (Edge)	0 Mo sur les VMs Oracle
Secrets API	NOTION_API_KEY injecté à l'Edge	Variables chiffrées Cloudflare Worker Secrets
Filtrage d'Accès	Cloudflare Access Email OTP	Allowlist @torontomu.ca
Budget Mémoire	0 Mo sur VM1 et VM 2	Exécution serverless < 15ms

tools.t-leo.fr — Boîte à Outils d'Atelier & Formules d'Usinage

1. Architecture & Conception

tools.t-leo.fr

Base de connaissances, formules de fabrication d'atelier et pense-bêtes de développement immédiatement consultables.

- **Recherche Pagefind** : Moteur de recherche côté navigateur sans aucune requête ni latence de base de données.
- **Calculateurs CNC** : Formules de vitesses d'avance (IPM/RPM) selon les essences de bois et l'aluminium.

2. Spécifications Techniques

TIER 2 • WORKSHOP MATH • PAGEFIND

Paramètres de déploiement et de sécurité consolidés.

- **Dosages Résine Époxy** : Calculateur au gramme près selon la température ambiante et le volume de coulée.
- **Snippets en 1 Clic** : Commandes Bash, directives Caddy, Docker et raccourcis Grasshopper prêts à copier.

⚙ Matrice d'Exploitation & Routage Caddy

SYSTEMD UNIT

PARAMÈTRE	VALEUR RETENUE	DIRECTIVE D'EXÉCUTION
Hébergement & Cible	VM1 (Distribution statique Caddy)	root /var/www/tools.t-leo.fr
Moteur d'Indexation	Pagefind WebAssembly (Client)	Index précompilé lors du build Astro
Sécurité & Données	Site 100% statique en lecture seule	Aucun formulaire, aucun traitement dynamique
Budget Mémoire	0 Mo en veille	Distribution directe par Caddy et Cloudflare

welcome.t-leo.fr — Menu Hospitalité & Carte Hebdomadaire

1. Architecture & Conception

welcome.t-leo.fr

Portail d'accueil convivial pour les convives : carte hebdomadaire des repas, cocktails signatures et connexion rapide au Wi-Fi.

- **Carte Hebdomadaire** : Affichage automatisé des plats cuisinés, cocktails signatures et suggestions de vins.
- **Wi-Fi Flash QR** : QR code de connexion instantanée pour réseau invité sécurisé sans dictée de mot de passe.

2. Spécifications Techniques

TIER 2 • HOSPITALITY • WI-FI QR

Paramètres de déploiement et de sécurité consolidés.

- **Filtre Allergènes & Végan** : Synchronisé directement avec la base culinaire cook.t-leo.fr pour adapter les portions.
- **Design Chaleureux** : Interface hospitalière optimisée pour smartphone avec mode sombre/clair harmonisé.

Matrice d'Exploitation & Routage Caddy

SYSTEMD UNIT

PARAMÈTRE	VALEUR RETENUE	DIRECTIVE D'EXÉCUTION
Hébergement & Cible	VM1 (Frontend réactif Caddy)	root /var/www/welcome.t-leo.fr
Synchronisation Données	PocketBase API (Lecture seule)	Endpoint /api/collections/weekly_menu
Protection Wi-Fi	Credentials invités isolés sur VLAN séparé	WPA3 / WPA2 Guest Network
Budget Mémoire	< 5 Mo lors des requêtes	Mise en cache edge des menus

home.t-leo.fr — Domotique d'Atelier & Localisation Spatiale

1. Architecture & Conception

home.t-
leo.fr

Supervision domotique d'atelier par microcontrôleurs ESP32 et base de localisation spatiale photographique du matériel.

- **Mosquitto mTLS Durci** : Chiffrement mutuel X.509 et révocation granulaire par liste CRL rechargée à chaud sans coupure.
- **Télémétrie Plantes & Climat** : Humidité du sol, température d'atelier et asservissement de l'arrosage automatique.

2. Spécifications Techniques

TIER 3 • HOMELAB IOT
• MOSQUITTO MTLS

Paramètres de déploiement et de sécurité consolidés.

- **Où sont mes affaires ?** : Inventaire spatial photographique associant chaque outil à une étiquette de casier physique.
- **Ségrégation ACL Stricte** : Les capteurs publient uniquement sur telemetry/* et ne peuvent pas agir sur les actionneurs.

⚙ Matrice d'Exploitation & Routage Caddy

SYSTEMD UNIT

PARAMÈTRE	VALEUR RETENUE	DIRECTIVE D'EXÉCUTION
Hébergement & Cible	VM 2 (Broker Mosquitto durci)	Port 8883 (mTLS uniquement, port 1883 fermé)
Certificats X.509	Autorité racine CA locale hors-ligne	Certificats clients signés individuellement
Confinement Systemd	ProtectSystem=strict, PrivateTmp=true	StateDirectory=/var/lib/mosquitto
Budget Mémoire	Mosquitto Broker ~15 Mo	Empreinte mémoire ultra-faible

diy.t-leo.fr — Gestion Atelier, Matières & Tutos de Fab

1. Architecture & Conception

diy.t-leo.fr

Gestion des stocks de matières premières, suivi des chutes (offcuts bin) et éditeur de documentation par blocs visuels.

- **Registre de Matières** : Suivi précis des panneaux de bois massif, profilés d'aluminium et bobines de filament 3D.
- **Éditeur Blocs WYSIWYG** : Rédaction modulaire visuelle intégrée à l'admin (style Gutenberg) pour tutoriels de fab.

2. Spécifications Techniques

TIER 3 • MAKERSPACE • BLOCK CMS

Paramètres de déploiement et de sécurité consolidés.

- **Calculateur de Coût BOM** : Calcul instantané du prix de revient matière et calepinage des découpes de panneaux.
- **Gestion des Chutes** : Répertoire photographique des chutes de matière réutilisables pour petits projets.

⚙️ Matrice d'Exploitation & Routage Caddy

SYSTEMD UNIT

PARAMÈTRE	VALEUR RETENUE	DIRECTIVE D'EXÉCUTION
Hébergement & Cible	VM1 (Interface) & VM2 (Données)	PocketBase collection: makerspace_inventory
Authentification	Admin FIDO2 pour modification / Public lecture	Accès en écriture restreint
Stockage Médias	Photos des chutes et tutoriels en WebP	Stockage local sur VM 2 chiffré GFS
Budget Mémoire	Partagé avec PocketBase (~25 Mo)	Zéro instance superflue

world.t-leo.fr — Nexus Écosystème & Moteur de Fusion

1. Architecture & Conception

world.t-leo.fr

Graphe relationnel nodal inspiré d'Infinite Craft pour explorer de manière organique les connexions entre savoir-faire et projets.

- **Moteur Physique Canvas** : Bulles interactives flottantes gérées en temps réel sous Matter.js / Three.js avec 0 calcul serveur.
- **Fusion de Compétences** : L'association de bulles (ex: 'Ébénisterie' + 'IoT') révèle les projets hybrides réalisés.

2. Spécifications Techniques

TIER 3 • CANVAS
2D/3D • INFINITE
CRAFT

Paramètres de déploiement et de sécurité consolidés.

- **Portail Spatial Direct** : Navigation organique permettant de se propulser instantanément vers n'importe quel sous-domaine.
- **Fluidité 60 FPS** : Optimisation Canvas 2D accéléré par le GPU client pour un usage tactile sur iPad et mobile.

Matrice d'Exploitation & Routage Caddy

SYSTEMD UNIT

PARAMÈTRE	VALEUR RETENUE	DIRECTIVE D'EXÉCUTION
Hébergement & Cible	VM1 (Frontend Canvas statique)	root /var/www/world.t-leo.fr
Moteur Graphique	Matter.js 2D Physics + WebGL Canvas	Exécution 100% navigateur client
Graphe de Relations	Fichier JSON statique pré-compilé	nodes.json distribué via CDN Edge
Budget Mémoire	0 Mo sur les serveurs backend	Rendu autonome côté client

cook.t-leo.fr — Plateforme Culinaire & Recettes Scalables

1. Architecture & Conception

cook.t-leo.fr

Base gastronomique avec calcul des portions au gramme près, détection de minuteries et passerelle directe vers welcome.t-leo.fr.

- **Portions Dynamiques** : Calcul automatique des quantités d'ingrédients selon le nombre d'invités sans erreur de dosage.
- **Minuteurs Intelligents** : Détection automatique Regex des temps de cuisson (#timer:15m) avec alertes sonores Web Audio.

2. Spécifications Techniques

TIER 2 • CULINARY ENGINE • PRISMA

Paramètres de déploiement et de sécurité consolidés.

- **Mode Chef Plein Écran** : Maintien de l'écran allumé (Screen WakeLock API) pour cuisiner sans interruption.
- **Intégration Welcome** : Alimente directement le portail d'accueil des invités pour la carte du week-end.

⚙ Matrice d'Exploitation & Routage Caddy

SYSTEMD UNIT

PARAMÈTRE	VALEUR RETENUE	DIRECTIVE D'EXÉCUTION
Hébergement & Cible	VM 2 (PocketBase / SQLite WAL)	Endpoint /api/collections/recipes
Calculs Ingrédients	Exécution client-side réactive	Zéro latence lors du changement de portion
Synchronisation Menu	Liaison directe avec welcome.t-leo.fr	Mise à jour en 1 clic depuis l'admin
Budget Mémoire	Partagé avec PocketBase (~25 Mo)	Faible consommation mémoire

Pipeline de Sauvegarde GFS & Sécurité Chiffrée

📦 Pipeline Sauvegarde GFS SQLITE WAL (04:00 AM) + AGE

Protocole nocturne non-bloquant de rétention chiffrée vers Google Drive.

- **Snapshot Atomique** : Exécution cron de `VACUUM INTO '/var/backups/t-leo/db_snapshot.db'` (isolé hors des répertoires /tmp systemd).
- **Chiffrement Asymétrique** : Chiffrement immédiat du flux par l'outil `age` avec la clé publique présente sur la VM.
- **Séquestration Clé Privée** : La clé privée de déchiffrement réside exclusivement sur machine locale sécurisée hors du cloud.
- **Rotation GFS Google Drive** : Rétention stricte de 7 sauvegardes journalières, 4 hebdomadaires et 3 mensuelles via `rc1one`.

🛡️ Gouvernance des Accès & Sécurité

ZERO TRUST
+ FIDO2

Périmètre périphérique Cloudflare et procédures d'urgence hors-ligne.

- **Cloudflare Zero Trust** : Authentification MFA matérielle FIDO2 (YubiKey) obligatoire pour accéder à `admin.t-leo.fr`.
- **Procédure Break-Glass** : Clé matérielle de secours et codes de déverrouillage imprimés stockés dans deux coffres séparés.
- **Durcissement SSH Ed25519** : Accès console sous clé matérielle ; toute connexion déclenche une alerte Slack/Email instantanée.
- **Révocation CRL Mosquitto** : Bannissement à chaud d'un ESP32 compromis sans interrompre le réseau de capteurs actifs.

🔄 Cycle de Rétention GFS & Scripts Cron Système

RCLONE & CRON

Période	Fréquence d'Exécution	Destination & Rétention	Chiffrement
Journalière	Tous les soirs à 04:00 AM	Google Drive /t-leo-backups/daily/ (7 jours)	<code>age -r age1leo...</code>
Hebdomadaire	Dimanche à 04:15 AM	Google Drive /t-leo-backups/weekly/ (4 semaines)	<code>age -r age1leo...</code>
Mensuelle	1er du mois à 04:30 AM	Google Drive /t-leo-backups/monthly/ (3 mois)	<code>age -r age1leo...</code>
Test Restauration	Trimestriel automatisé	Vérification intégrité du hash SHA256 & déchiffrement	Validation sans impact

Matrice Complète des 10 Sous-Domains

🌐 Matrice de Synthèse & Déploiement

v4.0 CONSOLIDÉE

Module / Domaine	Tier	Hébergement	Sécurité & Ingress	Base de Données
t-leo.fr	Tier 1	VM1 · Astro Static SSG	Cloudflare Edge Public	Fichiers Statiques / Markdown
admin.t-leo.fr	Tier 1	VM 2 · PocketBase Admin	Zero Trust (FIDO2 Hardware)	SQLite WAL Natif
db.t-leo.fr	Tier 1	VM1 · Three.js 3D Viewer	Public + /confidential/ Gated	glTF / Draco + Cloudflare R2
group.t-leo.fr	Tier 2	Cloudflare Serverless Worker	Email OTP (@torontomu.ca)	Notion API Broker
tools.t-leo.fr	Tier 2	VM1 · Astro / Pagefind WASM	Cloudflare Edge Public	Index Client-Side Pagefind
welcome.t-leo.fr	Tier 2	VM1 · HTML5 Dynamic Menu	Public / Jeton Temporaire	PocketBase API (Lecture seule)
home.t-leo.fr	Tier 3	VM 2 · Mosquitto Broker	mTLS X.509 + CRL Hot Reload	SQLite WAL Telemetry
diy.t-leo.fr	Tier 3	VM1 (UI) & VM 2 (Données)	Admin FIDO2 / Public Lecture	PocketBase SQLite WAL
world.t-leo.fr	Tier 3	VM1 · Matter.js Physics	Cloudflare Edge Public	Graphe JSON Statique
cook.t-leo.fr	Tier 2	VM 2 · PocketBase Culinaire	Public / Recettes Familiales	SQLite WAL Recipes