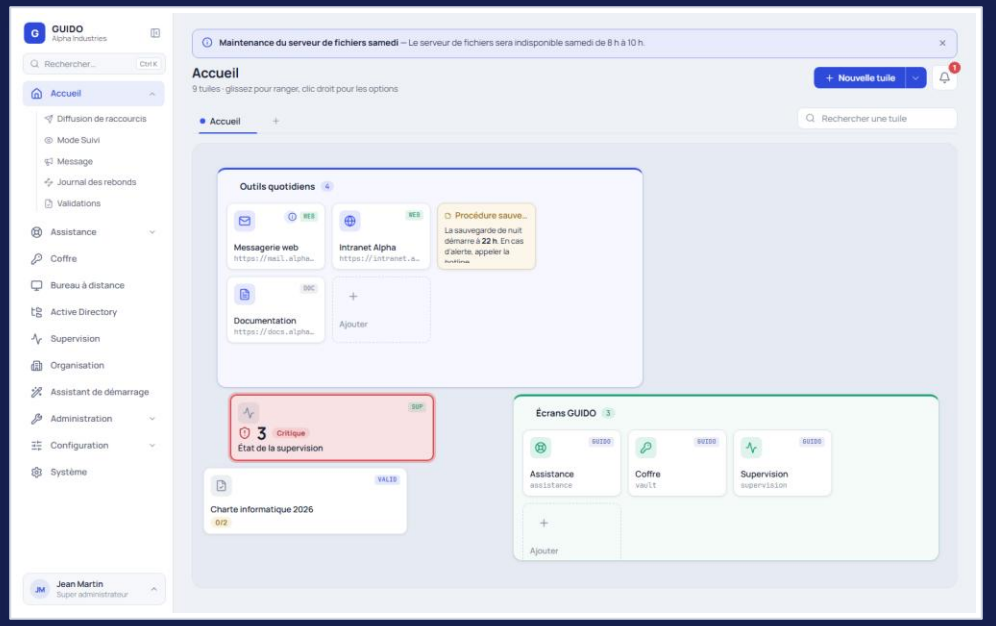
GUIDO

Une seule console, aucun port entrant

Accès, assistance et supervision : l'Accueil des utilisateurs, le coffre, l'annuaire, le bureau à distance, l'assistance et la supervision, avec des droits bornés et une trace de tout.



L'Accueil, données de démonstration

Présentation pour les DSI, chefs de projet et équipes informatiques

POURQUOI GUIDO

Sans GUIDO, avec GUIDO : la différence en un coup d'œil

	Sans GUIDO	Avec GUIDO
Consoles	Une par sujet : annuaire, sessions RDS, tickets, supervision, mots de passe, accès distant.	Une console web ; des modules ouverts à la carte.
Droits	Droits d'administration larges, faute de délégation fine.	Bornés par domaine, OU, groupe, broker, collection ou hôte ; vérifiés par le serveur à chaque appel.
Mots de passe	Fichiers, coffres personnels, envois par messagerie.	Coffre chiffré par entrée ; partage Utiliser, Voir ou Modifier ; chaque affichage et chaque usage tracés.
Sites distants	Ports à ouvrir, accès distant large.	Agents en HTTPS 443 sortant ; rebond limité aux cibles prévues, avec un code MFA.
Outils des équipes	Raccourcis et accès installés poste par poste.	Tuiles diffusées par groupe, mises à jour pour tous d'un coup.
Support	Tickets dans un outil, prise en main dans un autre.	Tickets, prise en main avec consentement et « Lancer et filmer » au même endroit.
Traces	Dispersées, quand elles existent.	Un journal d'audit commun : actions, connexions, rebonds, personnifications.
Coupure réseau	Plus d'accès aux outils.	Mode déconnecté sur le poste : cache chiffré, modifications rejouées au retour.

PÉRIMÈTRE

Un socle commun, des modules à la carte

SOCLE

Accueil et diffusion

Tuiles, onglets, diffusion aux groupes et alias, contenu verrouillable, messages.

SOCLE

Coffre

Identifiants chiffrés par propriétaire, partage à trois niveaux, clé de secours.

SOCLE

Postes et machines

Inventaire, prise en main avec consentement, ajout par groupes et approbation.

SOCLE

Organisation

Alias d'équipes, validation de documents, suivi de fichiers, Mode Suivi.

MODULE

Active Directory

Comptes, groupes, mots de passe, droits bornés par domaine, OU ou groupe.

MODULE

Bureau à distance

Sessions de tous les hôtes RDS, par broker et collection ; actions sur les hôtes.

MODULE

Assistance

Tickets, délais, formulaires, base de connaissance, enquêtes, rapports.

MODULE

Supervision

Agents Windows et Linux, sondes, alertes, incidents, rapports, audit AD.

Un module fermé disparaît du menu et de l'assistant de démarrage. Installé chez vous : tous les modules ouverts. Hébergé : selon l'abonnement.

VOS OUTILS ACTUELS

Ce que GUIDO prend en charge, et ce qui reste à vos outils

GUIDO prend en charge

- Le coffre d'équipe et les fichiers de mots de passe.
- L'intranet de liens et les raccourcis posés poste par poste.
- Un outil de tickets avec base de connaissance.
- L'exploitation des sessions de bureau à distance.
- Les messages « à tous » et les accusés de lecture.
- Les traces dispersées : un journal commun.

GUIDO complète

- **Validations :** une trace interne, à côté de vos circuits d'approbation.
- **Annuaire :** une délégation fine, à côté de vos consoles.
- **Accès distant :** un rebond ciblé, à côté de votre VPN.
- **Supervision :** vos serveurs, à côté de la supervision réseau.
- **Prise en main :** avec consentement, depuis le ticket.

Reste à vos outils

- La signature électronique réglementaire et la gestion documentaire.
- Le déploiement de logiciels et de correctifs, les mobiles.
- La gestion des changements et l'inventaire de configuration.
- L'authentification unique de vos autres applications.
- L'astreinte par SMS.

La différence : une console, une délégation de droits et un journal pour tout ce qui est dans les deux premières colonnes.

ARCHITECTURE

Comment GUIDO s'insère dans votre infrastructure



1. **Au bureau.** Le navigateur joint GUIDO en HTTPS (session Windows). L'agent poste ouvre les applications locales sur ticket à usage unique.
2. **À distance.** La même adresse, par Internet. Règles par origine (autoriser, exiger la double authentification, interdire) et code MFA à chaque rebond.
3. **Tunnel sortant.** L'Agent du site ouvre lui-même une connexion 443 vers GUIDO et la garde ouverte ; GUIDO lui passe les demandes par ce tunnel.
4. **Depuis l'intérieur.** L'Agent parle aux serveurs du site : annuaire, sessions RDS, partages, SSH, sites web internes. Les identifiants ne vont jamais au navigateur.
5. **Mesures.** Les agents de supervision envoient leurs mesures en direct, ou par le relais du site (pointillé).

Aucun port entrant sur vos machines : seul le serveur GUIDO reçoit du HTTPS. Un répartiteur ou un pare-feu peut se placer devant.

COMPOSANTS

Ce qui s'installe, où, et comment ça se connecte

Composant	Rôle	Installation	Connexion
Serveur GUIDO	API, interface web, tunnels, tâches de fond, moteur de supervision	Windows Server 64 bits, installateur guidé	HTTPS 443 entrant : le seul point d'entrée
Agent GUIDO (relais de site)	Annuaire (LDAP), sessions RDS, SSH, partages, pages web internes, relais de supervision	Une machine par site ; jeton à usage unique ou installateur de groupe ; Système local, gMSA ou compte du domaine	Tunnel permanent sortant
Agent poste « Guido »	Applications locales avec l'identifiant du coffre, inventaire, prise en main, mode déconnecté	Par utilisateur, sans droits d'administrateur ; déployable par stratégie de groupe	Tunnel sortant ; écoute sur 127.0.0.1 seulement
Agent de supervision	Sondes, file locale, envoi des mesures	Windows ou Linux	Direct, ou par le relais du site
Base de données	Données de la structure	PostgreSQL, 17 recommandée ; option répliquée	Locale ou distante

Publication auto-suffisante : aucun runtime .NET à installer sur les machines cibles.

SÉCURITÉ

Sécurité : ce qui est en place, sans effet d'annonce

Authentification

Session Windows pour les postes du domaine. Double authentification (application, courriel, Windows Hello, clé d'accès), réservable aux actions sensibles. Blocage automatique.

Coffre

Chaque identifiant chiffré. Partage à trois niveaux (utiliser, voir, modifier), chaque affichage tracé. Clé de secours.

Transport

HTTP redirigé vers HTTPS. Certificat Let's Encrypt obtenu et renouvelé par GUIDO, ou le vôtre ; alerte avant expiration. Secrets de configuration chiffrés.

Rebond

Depuis l'extérieur, un code MFA à chaque ouverture (preuve à usage unique). Seules les origines prévues sont joignables. Ouvertures et refus journalisés.

Traçabilité

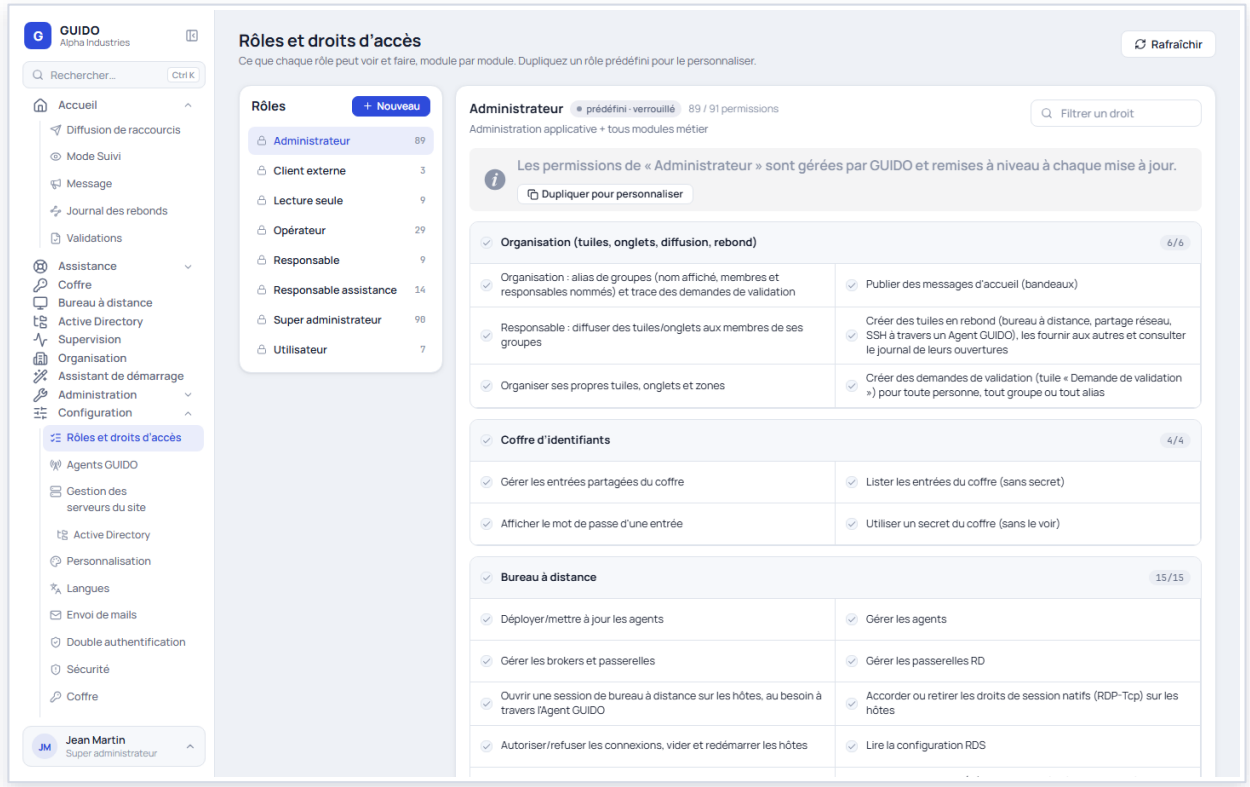
Journal d'audit, connexions, personnifications (30 minutes, sans le coffre), Mode Suivi borné et motivé. Rétention réglable.

Revue

Revue de sécurité interne du code menée en novembre 2026. Aucune certification n'est revendiquée.

Chacun ses droits, bornés à son périmètre

- **Rôles prédéfinis modifiables** et matrice de droits par module ; « Comparer à l'origine » et « Réinitialiser ».
- **Profils de délégation :** des actions limitées à un domaine, une OU, un groupe, un broker, une collection ou un hôte, accordées à des groupes AD.
- **Responsables d'équipe :** diffusion, comptes et sessions de leur équipe, dans leur seul périmètre.
- **Le serveur contrôle chaque appel,** même si un bouton est affiché. Ce qu'on ne peut pas voir n'existe pas, y compris dans les compteurs.
- **Comptes externes :** un prestataire suit ses demandes, rien d'autre.
- **Compte de service géré (gMSA) :** GUIDO interroge l'annuaire sans stocker de mot de passe ; assistant de création intégré.



Rôles et droits d'accès, données de démonstration

ENVIRONNEMENTS WINDOWS

Annuaire, sessions et postes, sans donner les clés du domaine

Active Directory

- Un ou plusieurs domaines depuis le navigateur.
- Retrouver un compte, réinitialiser, déverrouiller, désactiver, fixer une expiration.
- Créer ou copier un utilisateur, gérer les membres d'un groupe.
- Actions journalisées, sans jamais écrire de mot de passe.

Bureau à distance

- Les sessions de tous les hôtes RDS, par broker et collection.
- Message, déconnexion, fermeture, prise de main, processus.
- Refuser les connexions sur un hôte, le vider, le redémarrer.
- Droits bornés par broker, collection ou hôte.

Postes et machines

- Inventaire : modèle, série, processeur, mémoire, disques, réseau.
- Prise en main : demander, informer ou silencieux, selon la politique ; historique.
- Ajout par groupes, pré-enregistrement et approbation.

GUIDO interroge annuaires et hôtes avec un compte d'interrogation (compte de service géré possible), puis borne chaque opérateur à ses délégations ; le serveur contrôle chaque appel.

Navigateur ou agent poste, dehors ou hors ligne

Tuile	Navigateur seul	Avec l'agent poste
Bureau à distance	Dans la page, via l'Agent GUIDO	mstsc avec l'identifiant du coffre
Partage réseau	Explorateur de fichiers dans la page	Explorateur Windows sur le partage
Terminal SSH	Terminal dans la page	Terminal local, ou dans la page
Inventaire, prise en main	Non	Oui

La page détecte l'agent toute seule et se replie sur le navigateur seul s'il est absent.

Rebond

Tuiles en rebond créées par les seuls auteurs habilités. Bureau à distance, partage, SSH ou page web interne à travers l'Agent du site ; mode navigateur (origine dédiée) ou poste. Code MFA à chaque ouverture depuis l'extérieur, option même en interne.

Mode déconnecté

L'agent poste sert une copie vérifiée de l'interface et un cache chiffré (AES-256-GCM, clé DPAPI ou TPM). Modifications mises en file et rejouées au retour ; conflits présentés à l'utilisateur. L'Agent du site garde sa configuration et une file chiffrée.

ACCÈS À DISTANCE

Le rebond : un code MFA à chaque ouverture

1

Ouvrir la tuile

Depuis l'Accueil, chez soi ou en déplacement.

2

GUIDO lit l'origine

Adresse réelle de la connexion ; réseaux internes et répartiteurs de confiance réglables.

3

Code MFA exigé

Preuve à usage unique, 2 minutes, liée à cette seule ouverture.

4

L'Agent ouvre

L'Agent du site atteint : bureau à distance, partage, SSH, site web interne, hôte RDS.

5

Tout est tracé

Ouvertures, refus, fermetures ; aucun code ni secret au journal.

Seulement ce qui est prévu

Pas un accès au réseau entier : seules les cibles des tuiles sont joignables. Pour le web, les origines autorisées de la tuile et les ports réglés par Agent (80, 443, 8080, 8443 par défaut) ; adresses locales refusées par défaut.

Qui peut

Créer une tuile en rebond : droit dédié. L'ouvrir dans le navigateur ou par l'agent poste : droits distincts, par utilisateur ou groupe. Une copie diffusée ne s'ouvre plus si son auteur perd l'habilitation.

Quand ça se ferme

Durée maximale et inactivité réglables, fin de la session GUIDO, déconnexion de l'Agent. Option : un code même depuis le réseau interne.

DOUBLE AUTHENTIFICATION

La double authentification là où elle compte

À la connexion

- **Règles par origine :** adresse, plage, « publique » ou « privée » ; autoriser, exiger la double authentification ou interdire.
- La première règle qui correspond gagne ; liste blanche possible, avec un garde-fou contre l'enfermement.
- Une origine interdite coupe les sessions ouvertes à leur prochain renouvellement.

Aux actions sensibles

- **Au choix :** bureau à distance, Active Directory, diffusion de raccourcis, prise en main, révéler un identifiant du coffre.
- Dès la consultation, ou seulement pour les actions.
- Pour tous, ou des utilisateurs et groupes choisis ; validité réglable (15 minutes par défaut).

À chaque rebond

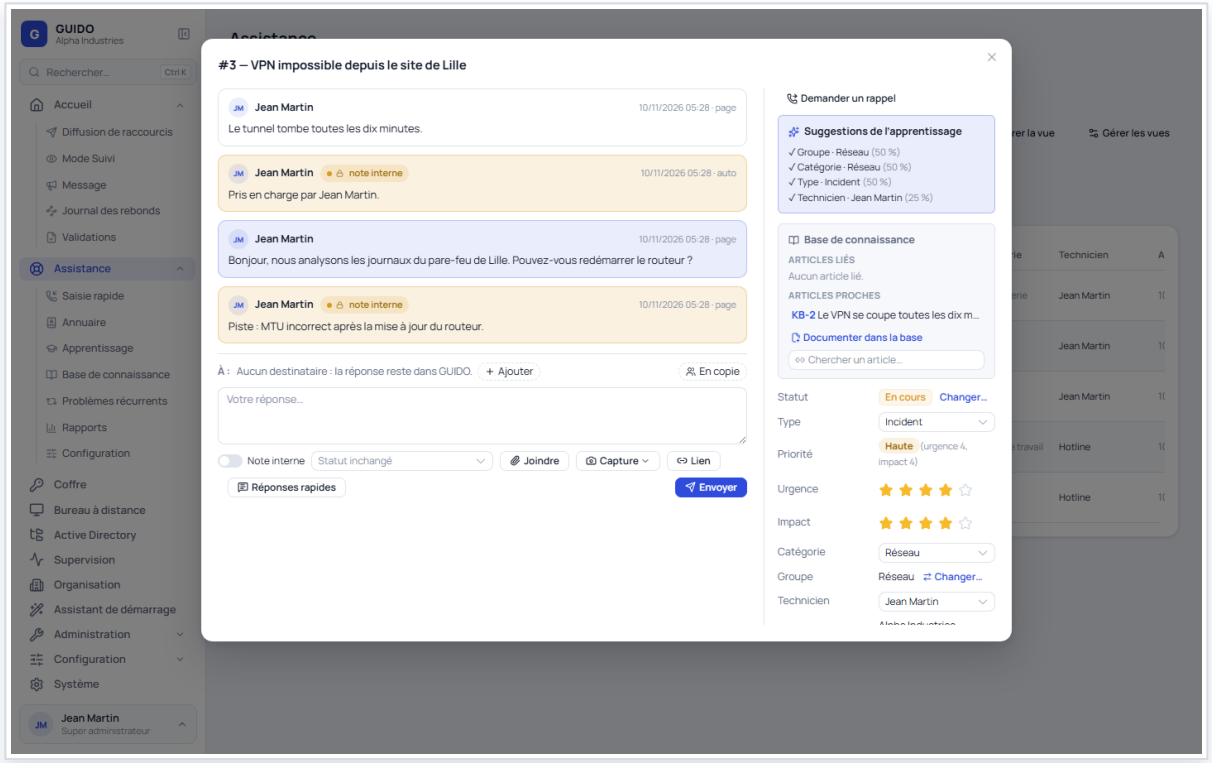
- Depuis l'extérieur : un code MFA par ouverture, jamais celui de la connexion.
- Option : le même contrôle depuis le réseau interne.
- Sans méthode enregistrée, l'utilisateur est envoyé vers l'enregistrement : aucun passe-droit.

MÉTHODES **Application d'authentification** **Code par courriel (10 minutes)** **Windows Hello ou clé d'accès**

Sessions : jeton de 60 minutes, renouvelé jusqu'à 8 heures ; fermeture après inactivité réglable. Tout refus est au journal d'audit.

ASSISTANCE

Un outil de tickets complet, branché sur le reste



Fiche d'un ticket, données de démonstration

- **Toutes les entrées :** page GUIDO, mail entrant, fiche d'un poste, saisie rapide d'un appel, API, import.
- **Le contexte déjà là :** demandeur reconnu, poste et session RDS relevés, contrat et délais calculés.
- **Attribution :** règles que l'on peut tester, et apprentissage qui ne propose que ce qu'il a vu.
- **Délais :** calendriers, alertes avant échéance, escalades, attente avec motif public et interne.
- Regroupement, incident principal, problèmes récurrents.
- Formulaires versionnés, réponses rapides, modèles de mails, base de connaissance, enquêtes, rapports.
- **Réglages en couches :** structure, entité, service, logiciel, groupe, personne ; la plus précise l'emporte.
- **Import :** GLPI, CSV, Excel, mails ; API à clé.

Savoir ce qui ne va pas avant les utilisateurs

- **Agents Windows et Linux,** en direct ou par le relais du site, sans port ouvert sur la machine.
- **Mesures :** processeur, mémoire, disques, services, certificats, réseau, fichiers, bases (Oracle, PostgreSQL, MySQL/MariaDB), sondes par script.
- **Modèles par rôle :** fichiers, impression, RDS, DNS, DHCP, Hyper-V, IIS, SQL Server, Veeam.
- **Pas de faux « OK » :** « sans données » et « inconnu » avec leur motif.
- **Pas d'alerte inutile :** confirmation, marge de retour, maintenances, horaires ; les alertes qui persistent deviennent un incident, donc un ticket.
- **Active Directory :** réplication, DNS, SYSVOL, horloge, FSMO ; audit de sécurité par gravité, sans score.
- Graphiques de 1 heure à 1 an, rapports de disponibilité (Excel, CSV, envoi planifié).

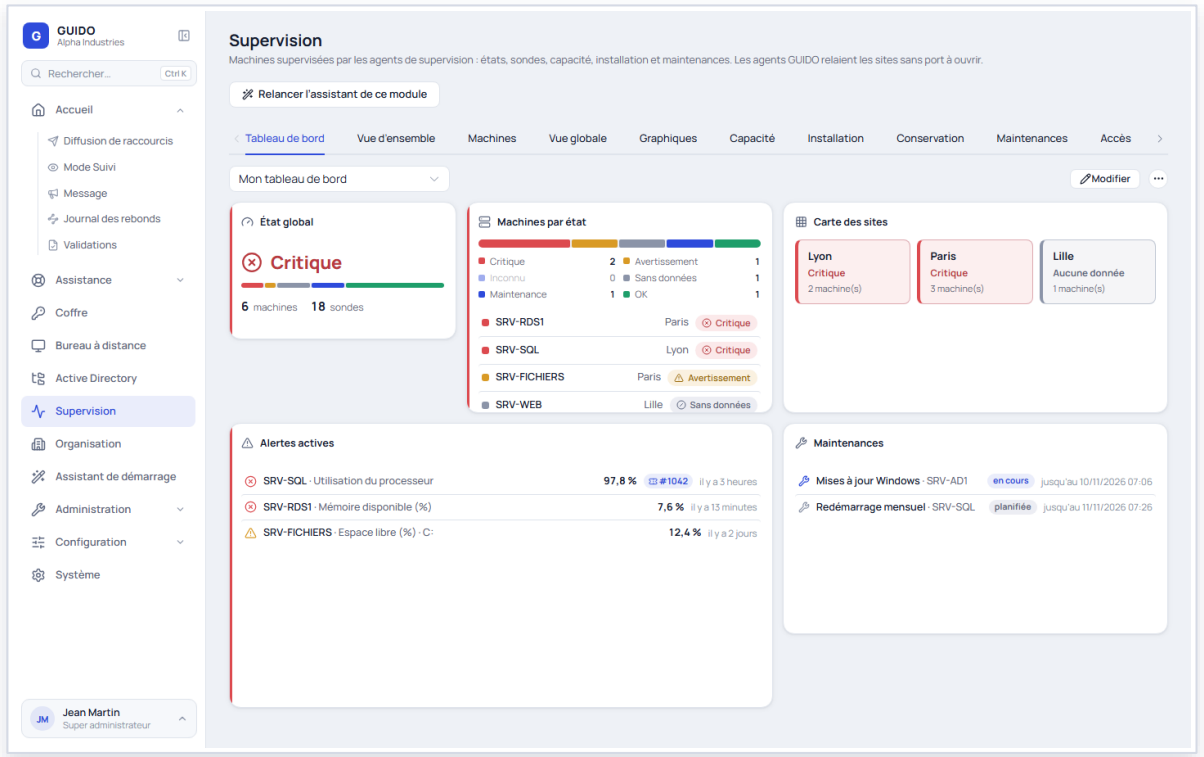


Tableau de bord de la supervision, données de démonstration

DÉPLOIEMENT

Chez vous ou hébergé, le même produit

Installé chez vous

- Serveur Windows de votre réseau et sa base PostgreSQL.
- Installateur guidé : base, structure, premier administrateur, nom DNS, certificat, compte du service.
- Tous les modules ouverts.

Espace hébergé

- Un environnement isolé : service, dossier, secrets, base et rôle PostgreSQL propres.
- Votre nom de domaine et votre certificat.
- Deux instances actives (de 1 à 3) ; mises à jour sans coupure.

Zéro coupure

Une mise à jour démarre une instance neuve avant d'arrêter l'ancienne ; nœuds et portails multiples.

Base répliquée

Deux serveurs PostgreSQL et un arbitre : bascule automatique, restauration à un instant donné. Scripts pour Debian 13.

Sauvegarde

Écran de sauvegardes, ligne de commande, console de restauration ; marche à suivre pour l'installation dédiée.

Prérequis : serveur Windows 64 bits · PostgreSQL (17 recommandée) · Edge ou Chrome récent · HTTPS 443 sortant depuis les agents.

MISE EN PLACE

Un parcours type, guidé par GUIDO lui-même

1

Installer le serveur

Installateur guidé ; en hébergé, l'espace est fourni.

2

Suivre l'assistant de démarrage

Un chapitre par module ouvert ; l'état de chaque étape est vérifié par le serveur.

3

Enrôler les Agents des sites

Jeton à usage unique ou installateur de groupe.

4

Déclarer annuaire et serveurs

Compte de service géré, avec l'assistant de création.

5

Équiper les postes et les équipes

Agent poste par stratégie de groupe ; tuiles diffusées aux groupes.

6

Ouvrir les autres modules

Assistance : groupes, délais, modèles. Supervision : agents.

L'assistant n'est jamais imposé : on suit un chapitre, on s'arrête, on reprend ; plusieurs administrateurs partagent le même avancement.

EXPLOITATION

Au quotidien, et ce qui a été réellement essayé

Au quotidien

- Journal d'audit, historique des connexions, journal des rebonds ; durées de conservation réglables.
- Sauvegarde et restauration outillées.
- Mises à jour des agents depuis la console.
- Interface et messages en français et en anglais.
- Votre nom, vos couleurs, votre logo, votre icône sur les applications.

Essayé en conditions réelles

- Laboratoire Windows Server 2025 : serveur GUIDO, nœuds du portail, hôte RDS, contrôleur de domaine.
- Poste Windows 11 Pro.
- Grappe PostgreSQL de trois machines Debian 13.
- Interface avec Edge et Chrome.
- Le reste est indiqué « annoncé » ou « non validé » dans la matrice de compatibilité.

Évaluons GUIDO sur votre infrastructure

Une démonstration sur vos cas, puis un espace d'essai hébergé, tous modules ouverts, pendant 15, 30 ou 45 jours.

Demandez une démonstration

[À COMPLÉTER : site web]

[À COMPLÉTER : téléphone]

[À COMPLÉTER : courriel]

Installé chez vous ou hébergé · Prix sur devis

Aucun port entrant

Des droits bornés, tout est tracé

Une console au lieu de six

Chez vous ou hébergé